WithSecure Elements delavnica

Marko Kašić

A1 Slovenija, d.d.

WITH secure

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

Formerly
F-Secure Business

F-Secure Business je zdaj WithSecure

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

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

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

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

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

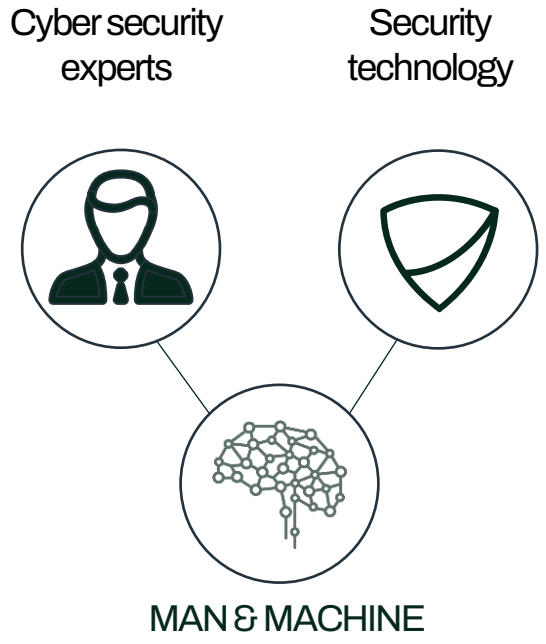
WITH secure

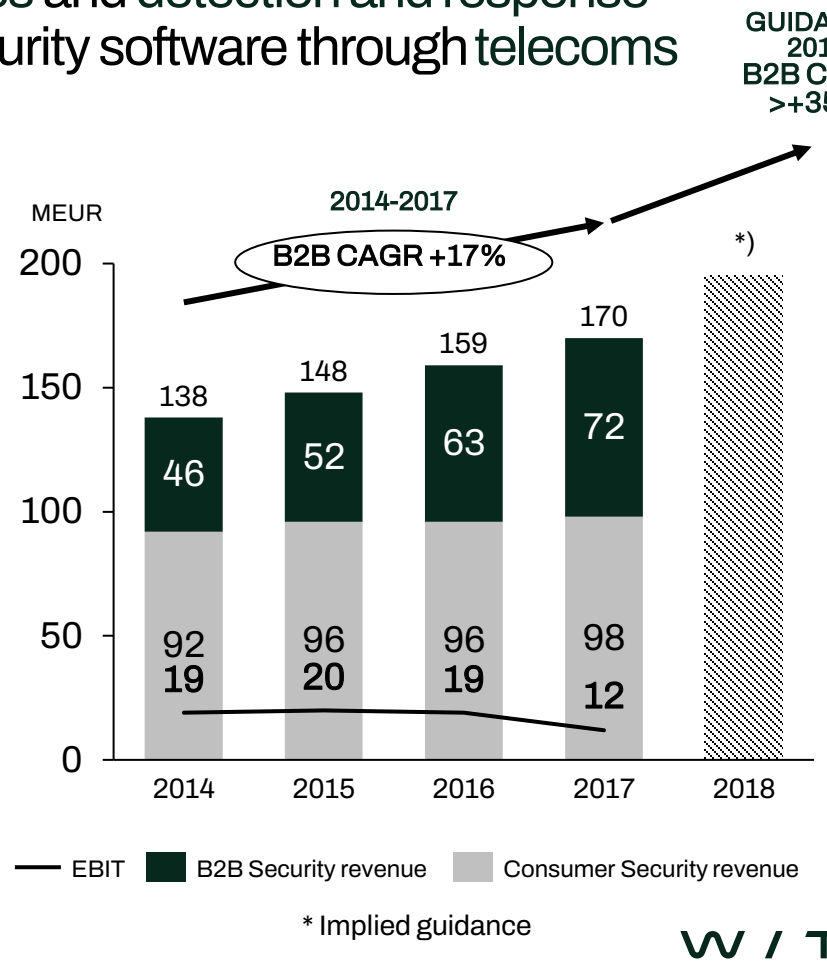
WithSecure – a front runner in cyber security

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.

Key figures

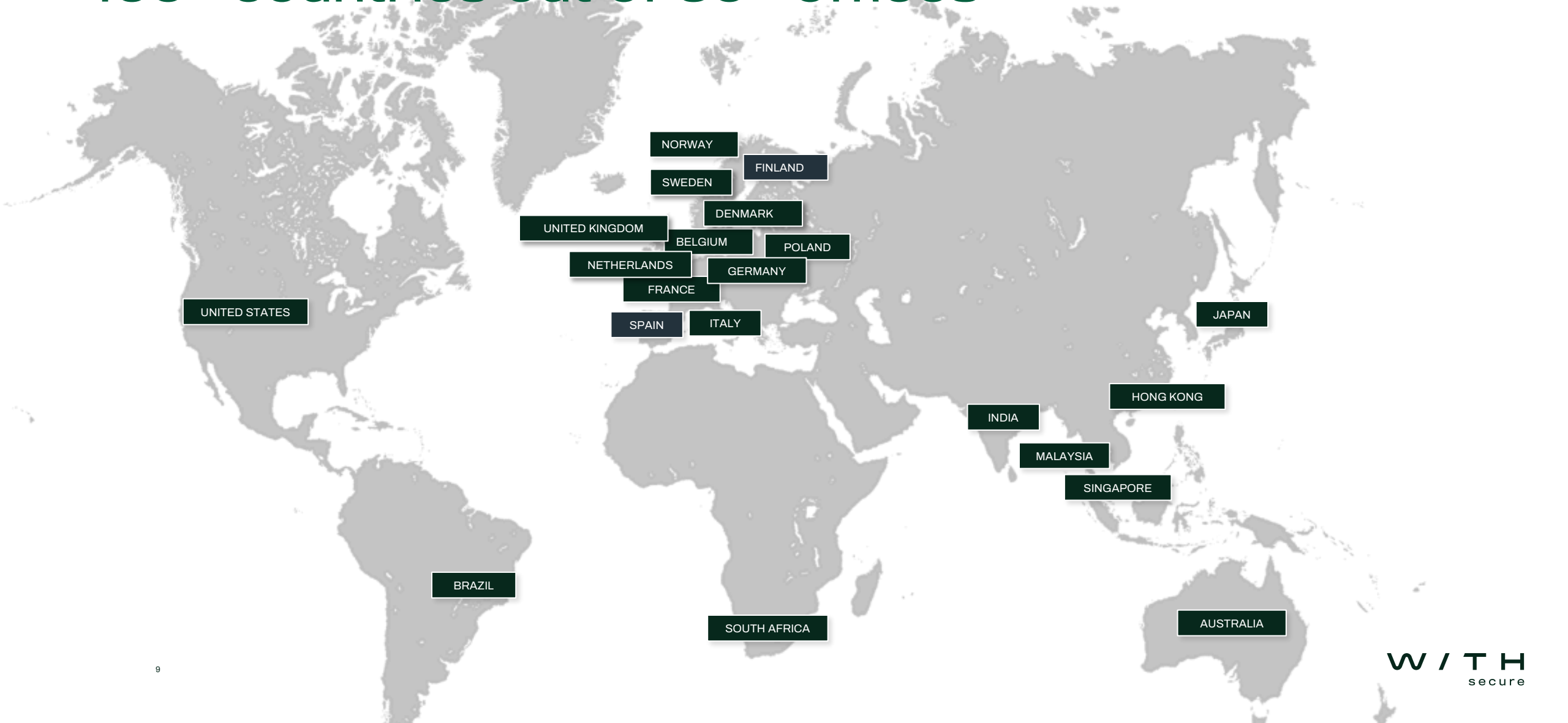
170 MEUR revenue	18 MEUR Adjusted EBITDA
1600 employees	25 locations





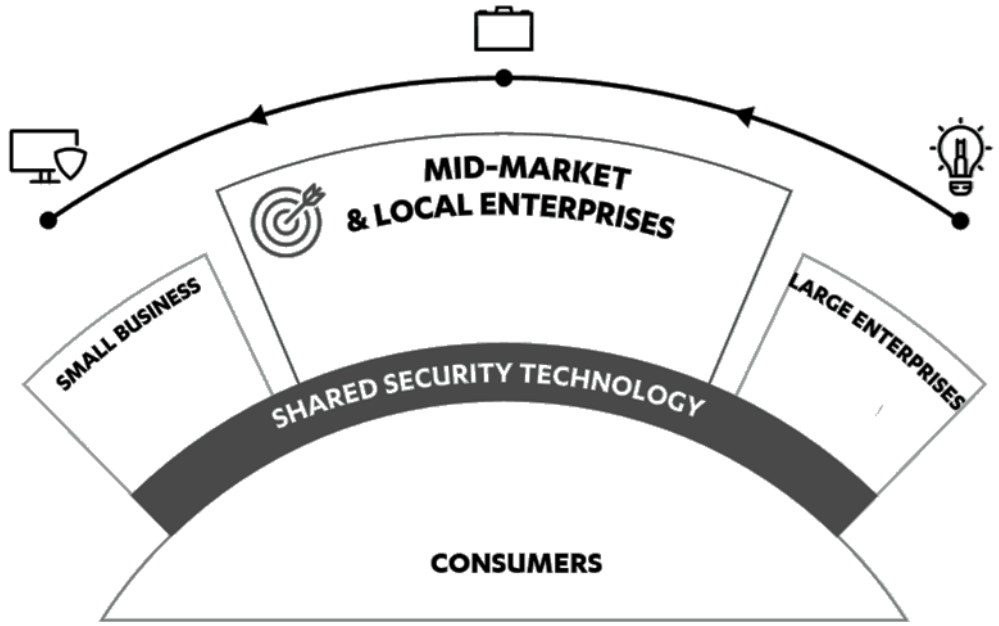
* Implied guidance

Protecting businesses in 100+ countries out of 30+ offices



WITH secure

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

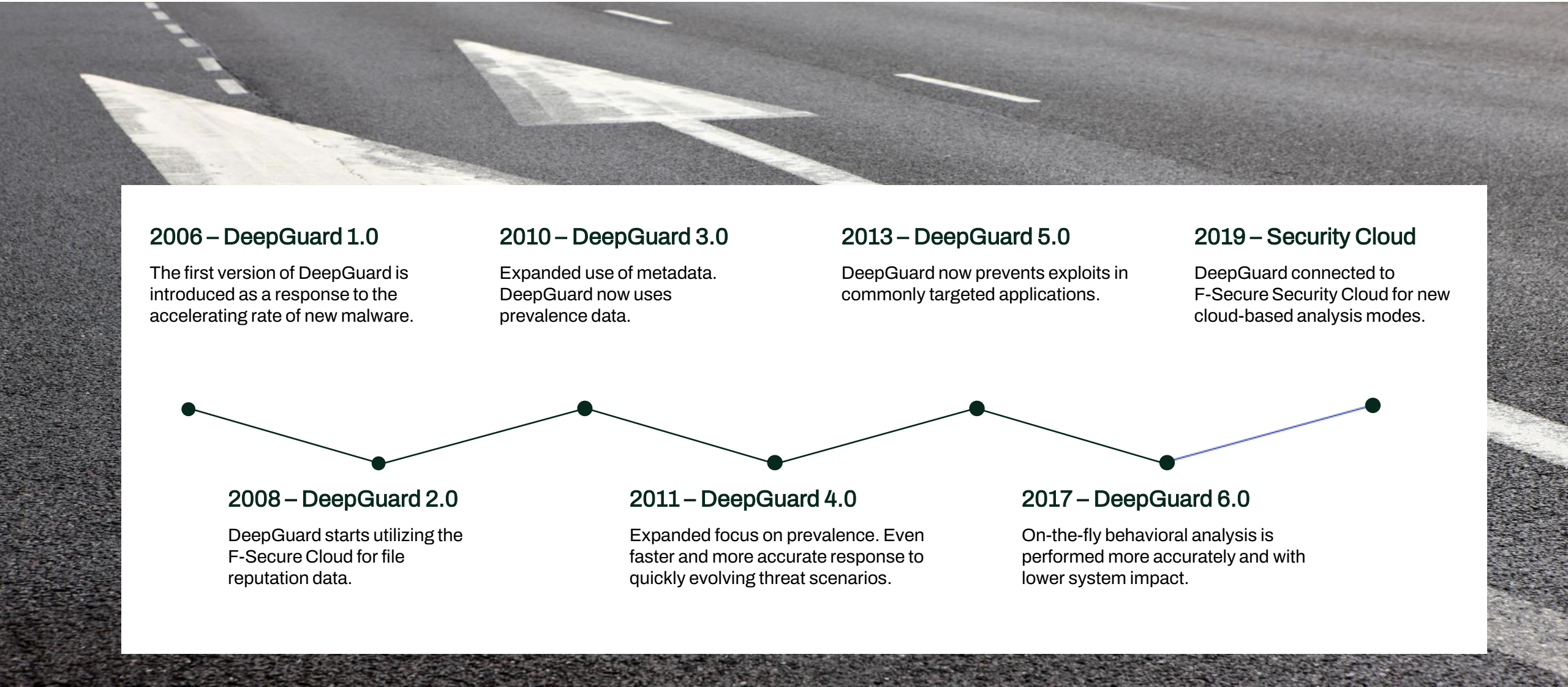
OPERATORS
200+ globally

Tens of millions
of consumers

We sell our solutions through
a global network of channel partners

WITH secure

“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.

2008 – DeepGuard 2.0

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

2010 – DeepGuard 3.0

Expanded use of metadata. DeepGuard now uses prevalence data.

2011 – DeepGuard 4.0

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

2013 – DeepGuard 5.0

DeepGuard now prevents exploits in commonly targeted applications.

2017 – DeepGuard 6.0

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

2019 – Security Cloud

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

WithSecure EPP agents

Elements EPP and Business Suite agents/clients

WITH secure

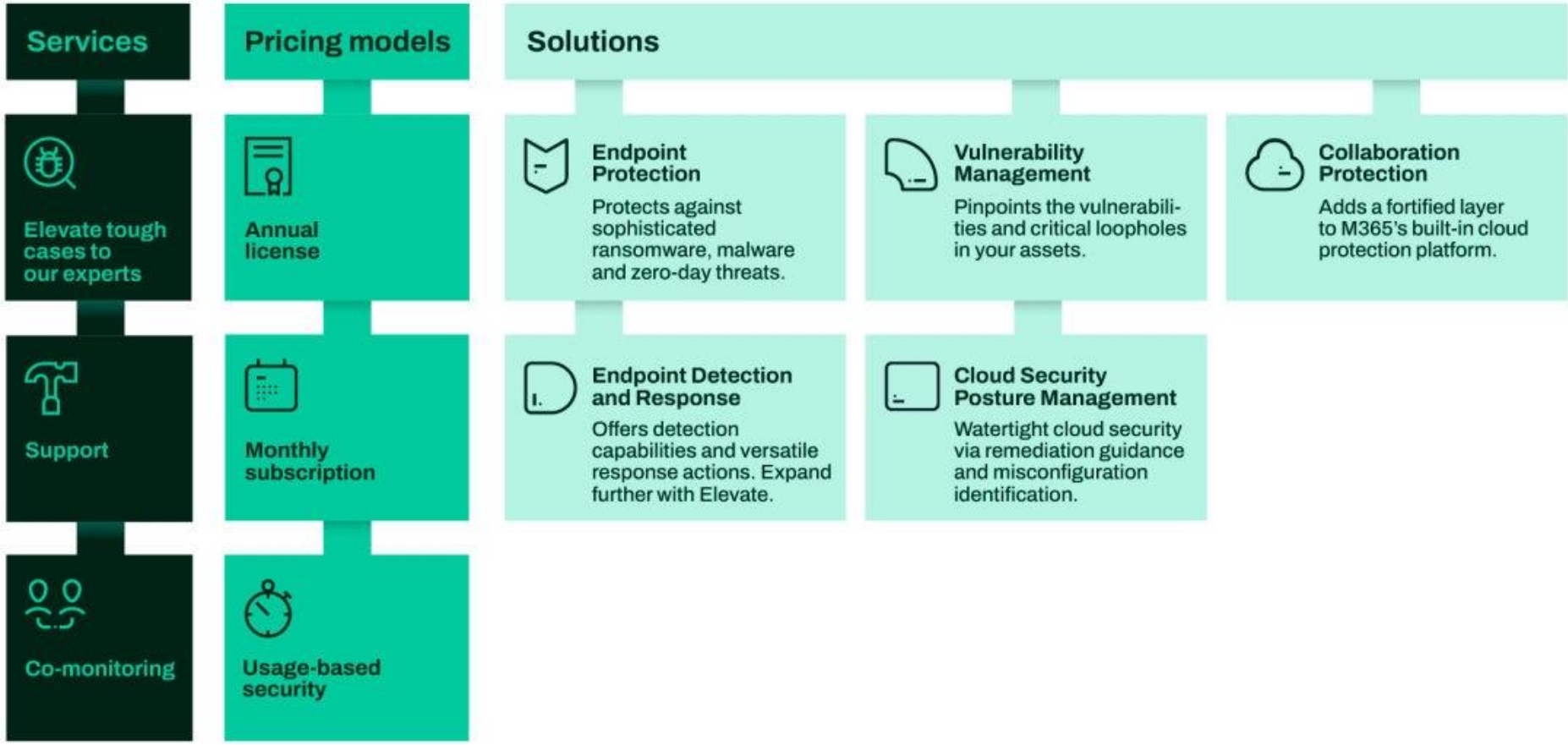
WithSecure EPP

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.



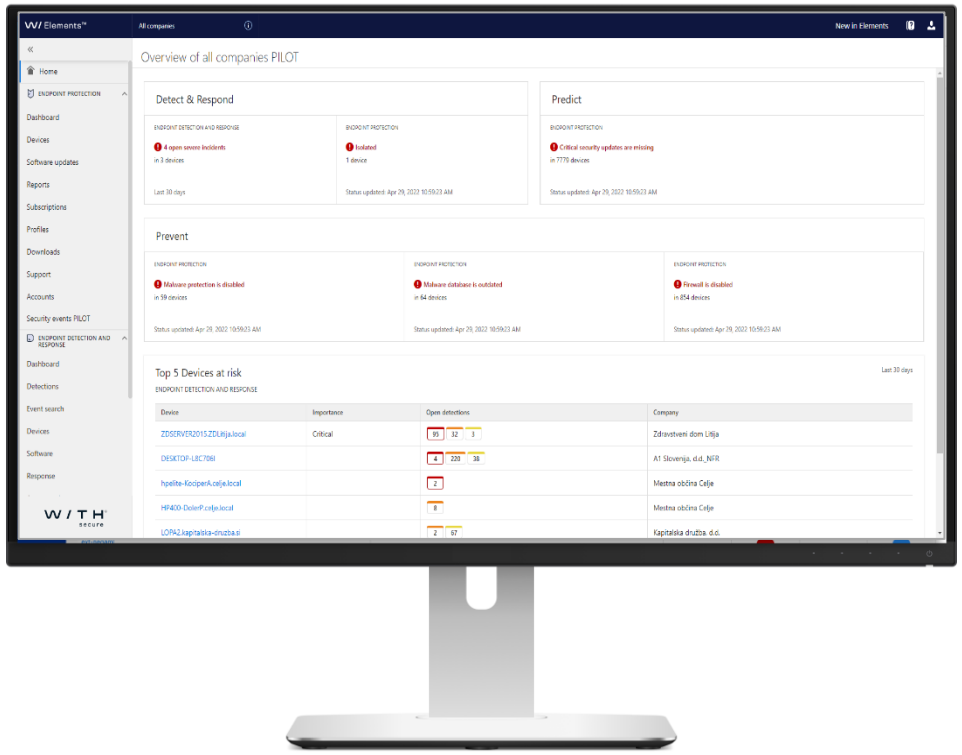
WITH secure

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

W / T H secure

Elements EPP clients

Windows PCs and MACs

- Elements EPP for Computers
  - Windows
  - Mac

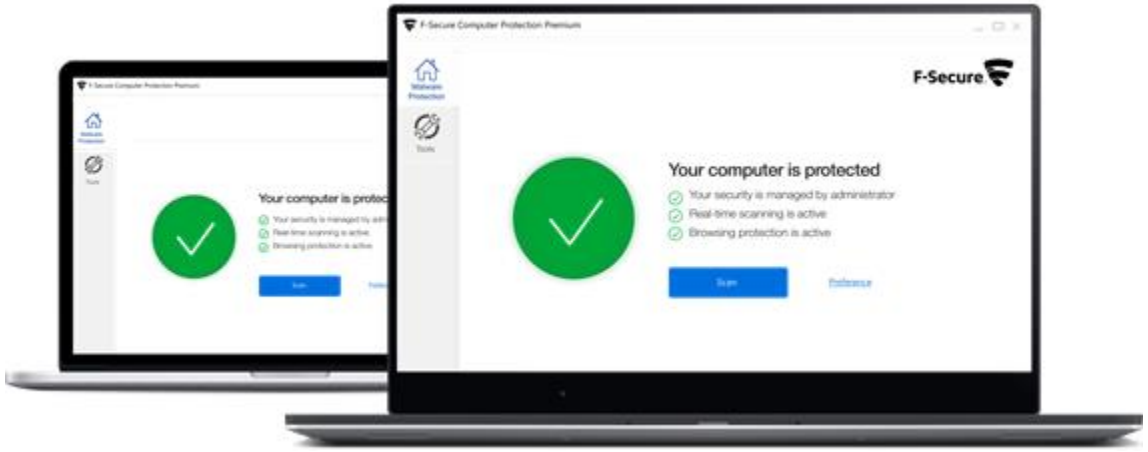
Mobile Devices

- 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

DEEPGUARD

APPLICATION CONTROL*

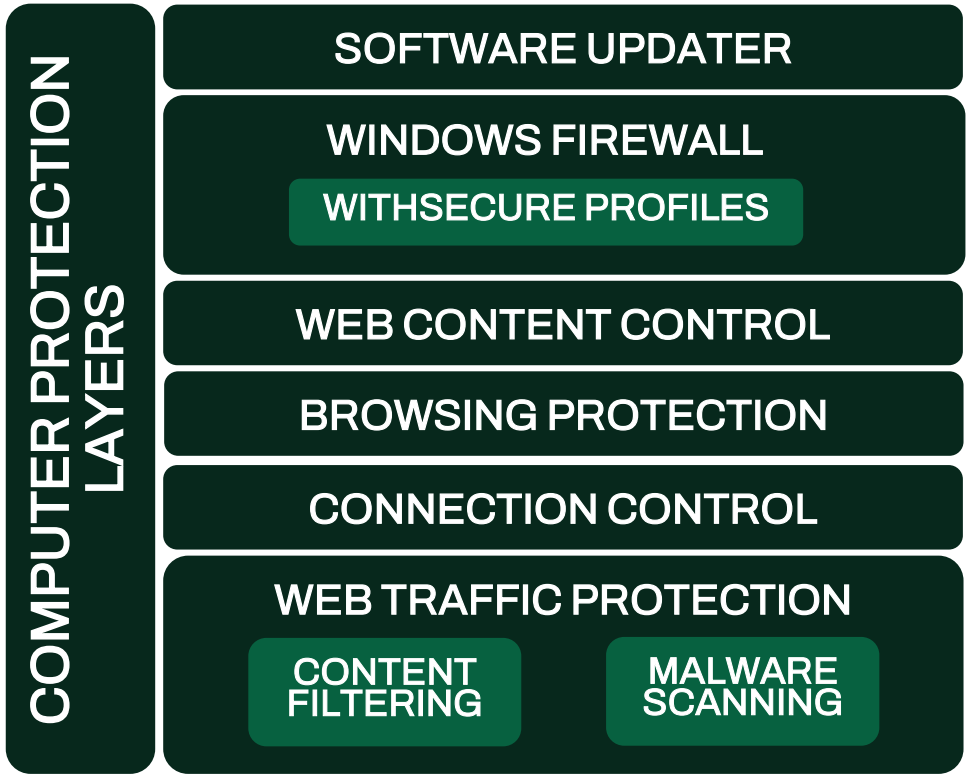
DATAGUARD*

* = PREMIUM FEATURE

WITH secure

Elements EPP for Computers – PC

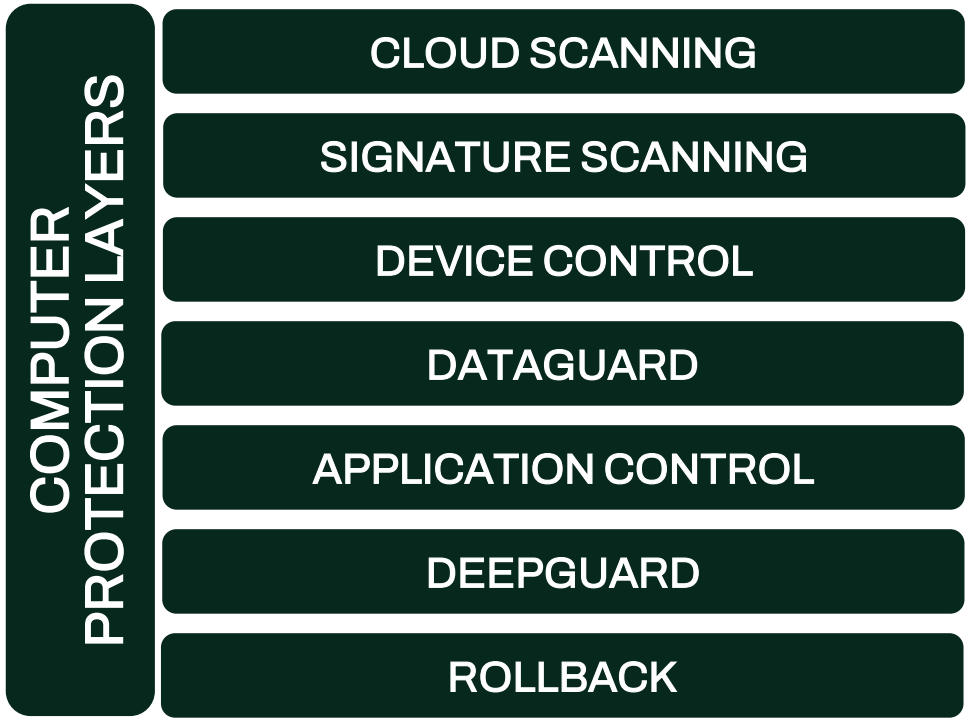
- Software Updater reduces threats by keeping OS and 3rd party software up to date
- Windows Firewall with WithSecure profiles monitors and controls network traffic based on set rules
- Web Content Control restricts sites based on their category
- Browsing Protection blocks malicious URLs based on reputation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



WITH secure

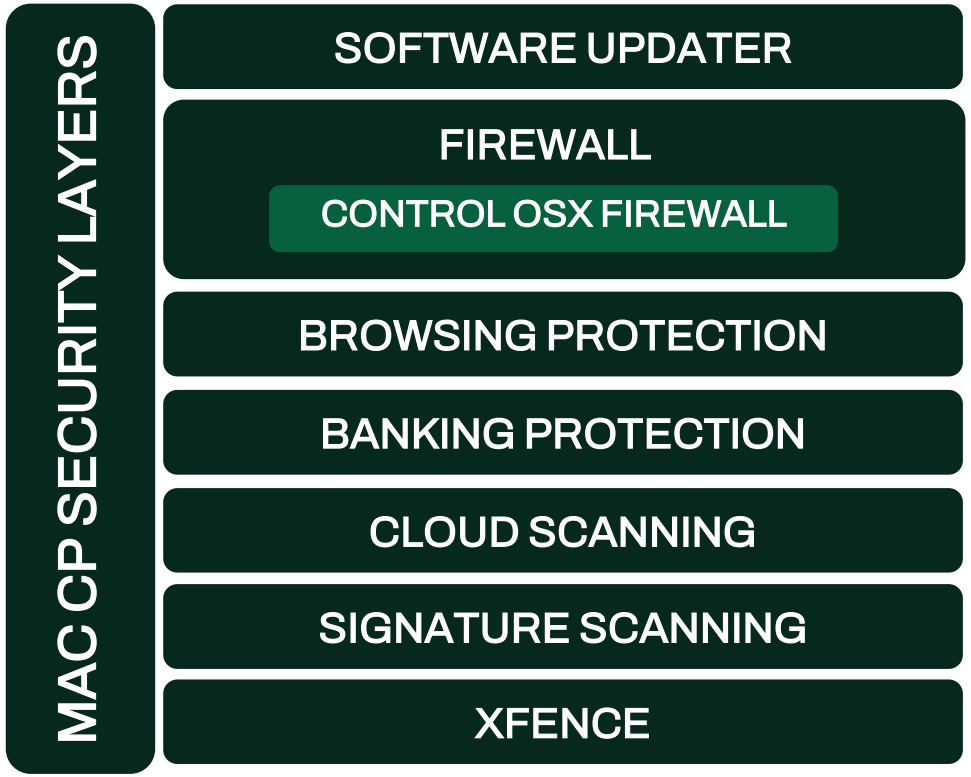
Elements EPP for Computers – PC

- 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

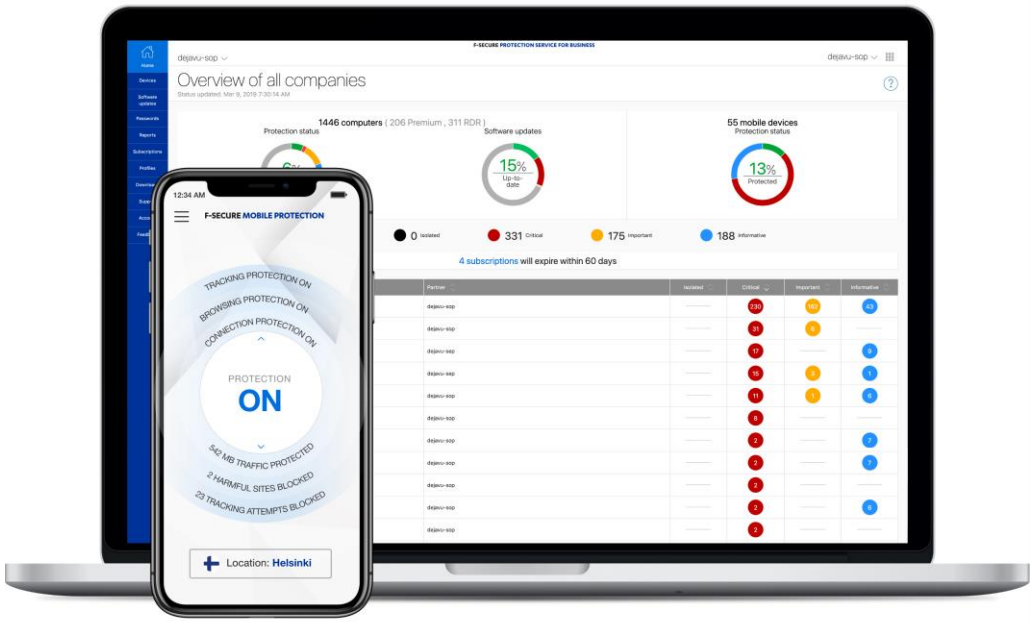
APPLICATION CONTROL*

DATAGUARD*

* = PREMIUM FEATURE

WITH secure

Elements for Mobile



MOBILE VPN

SECURITY CLOUD

APPLICATION PROTECTION

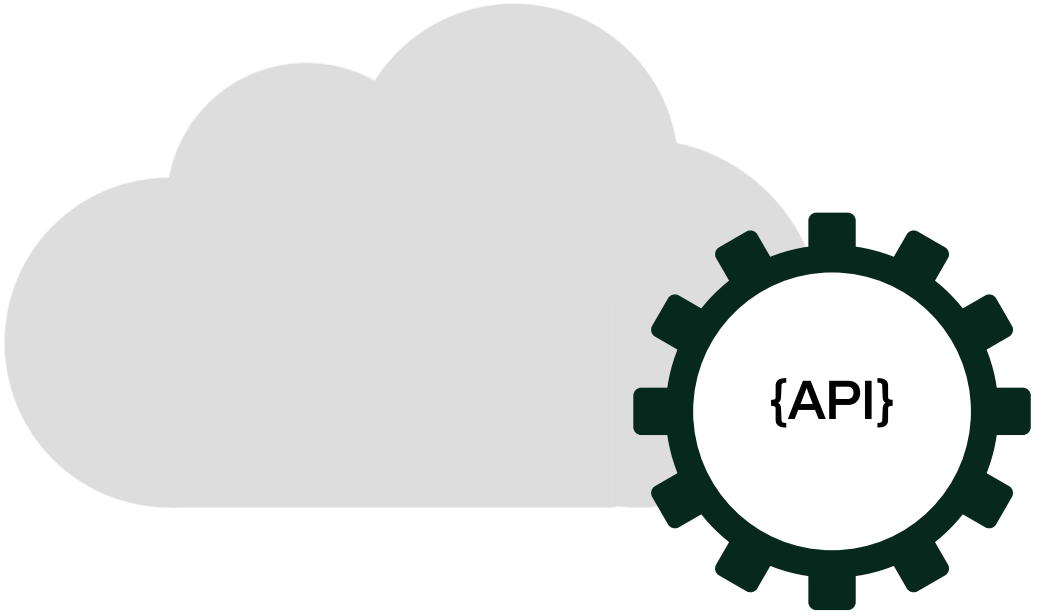
BROWSING PROTECTION

TRACKING PROTECTION

MDM SUPPORT

WITH secure

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

WITH secure

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

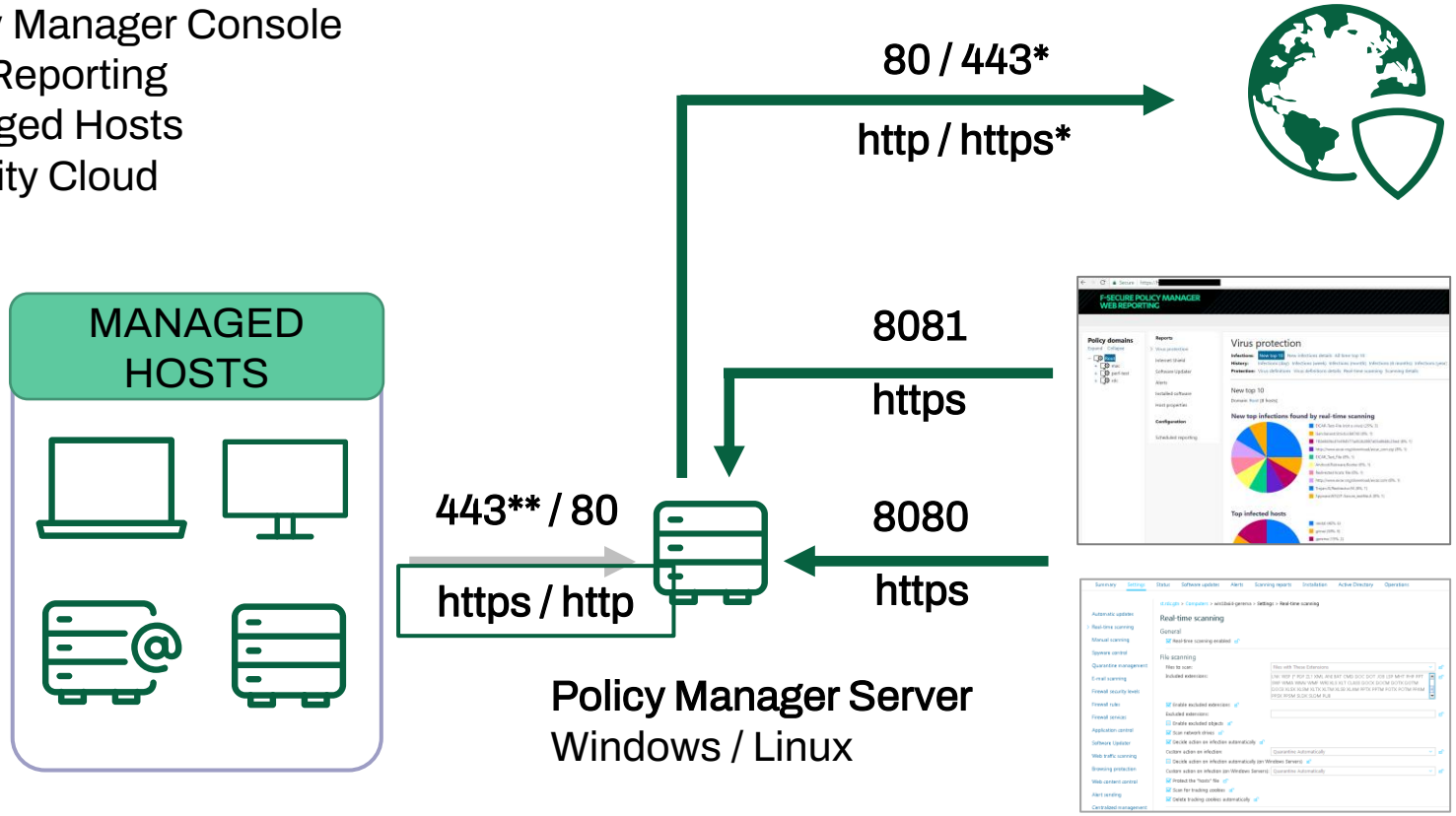
WITH secure

WithSecure Business Suite

Communication paths:

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

Security Cloud URL-ji se spremenijo na v16

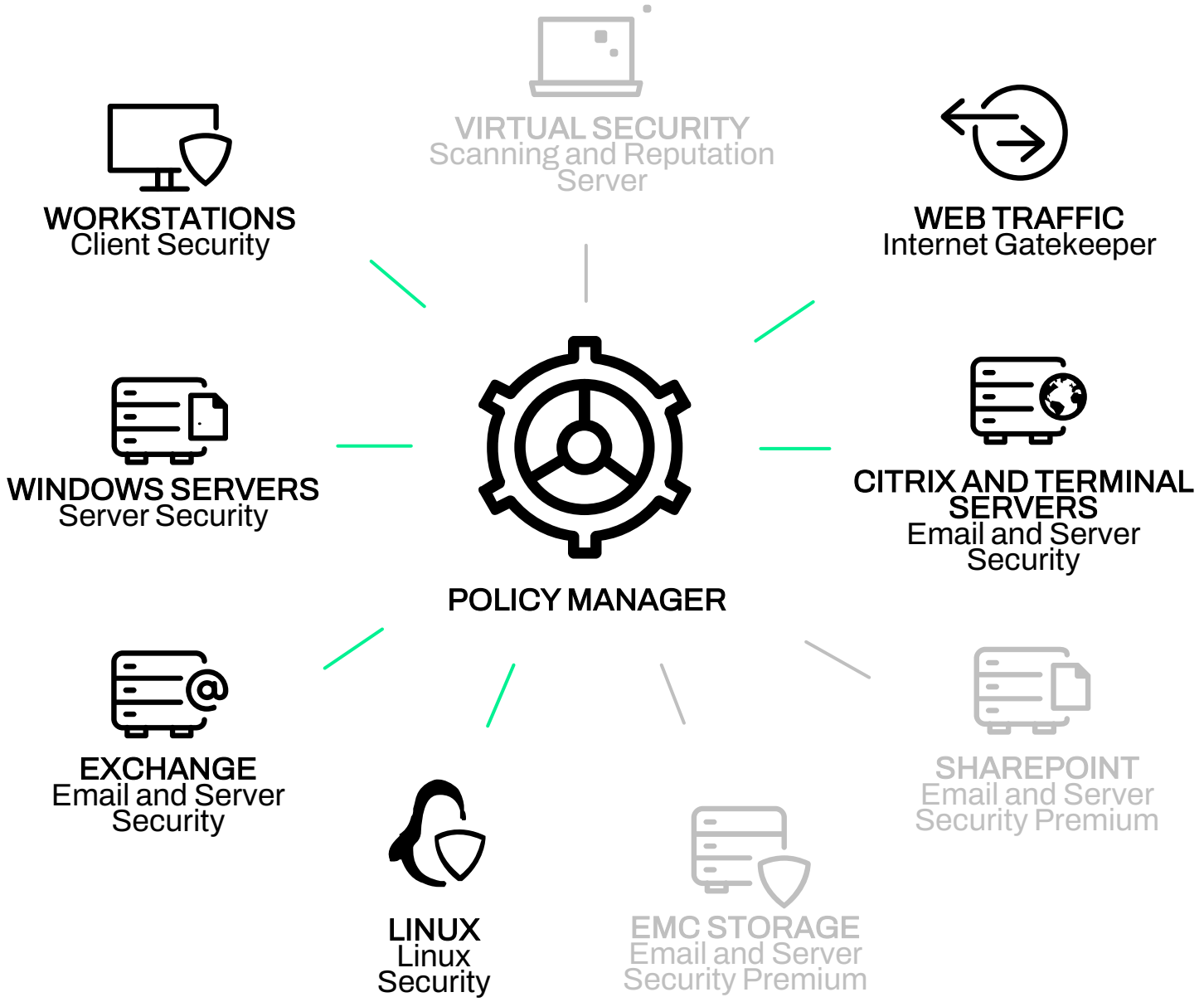


WithSecure Security Cloud
fsdbupdate.f-secure.com
orsp.f-secure.com
corp-reg.f-secure.com*

WithSecure Policy Manager Web Reporting

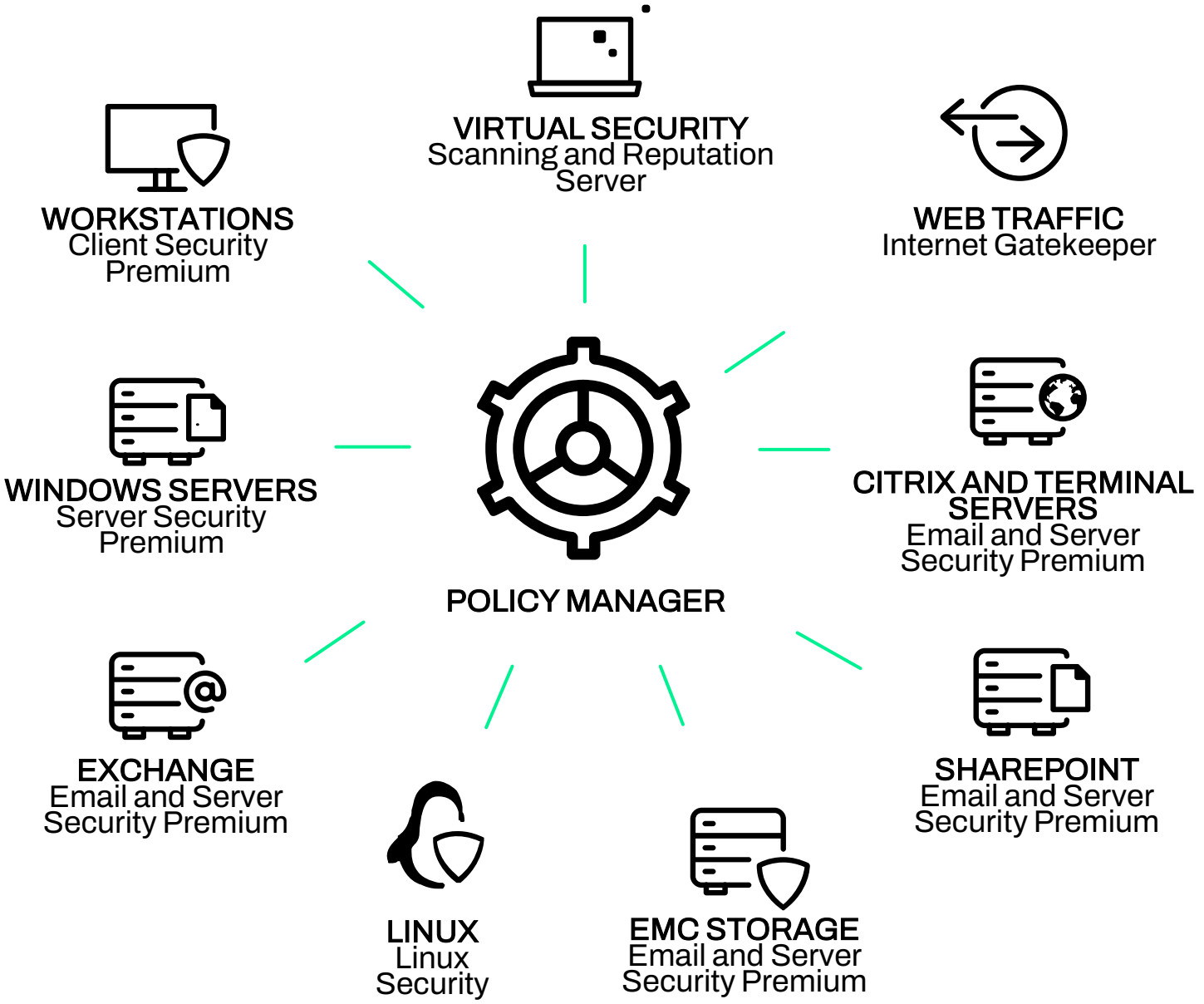
WithSecure Policy Manager Console

Business Suite Standard



WITH secure

Business Suite Premium



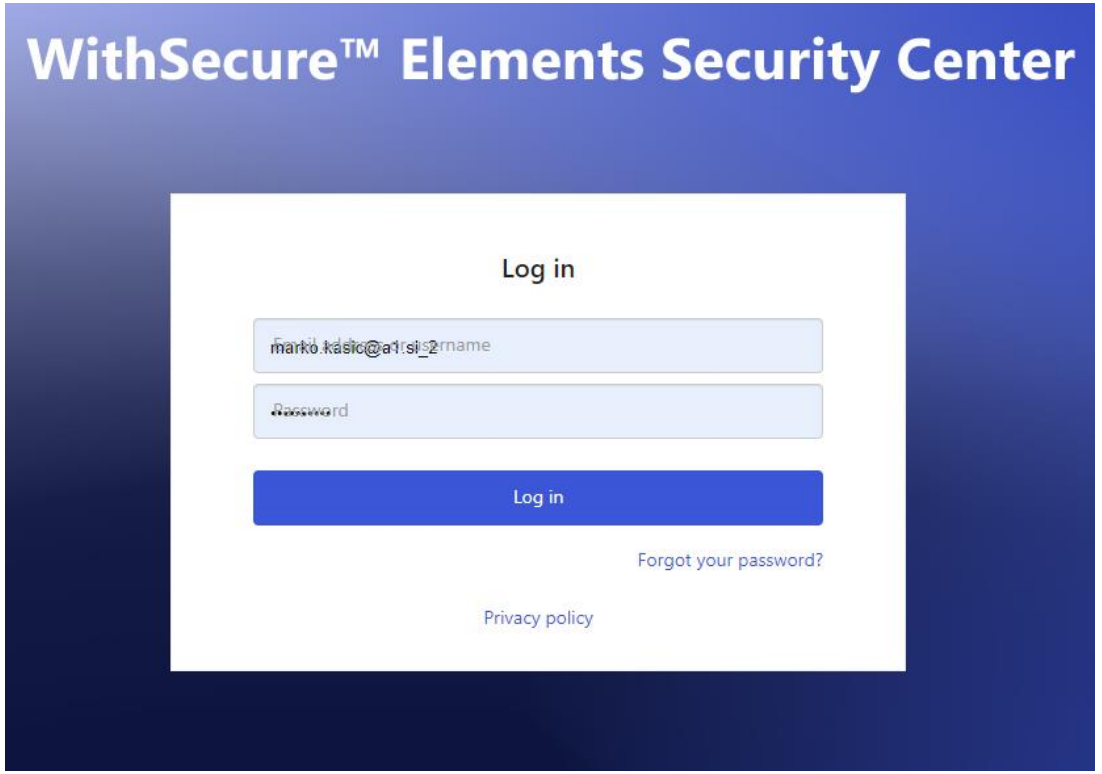
WITH secure

Elements Security Center Usage

WITH secure

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



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

WITH secure

Prijava v ESC training portal

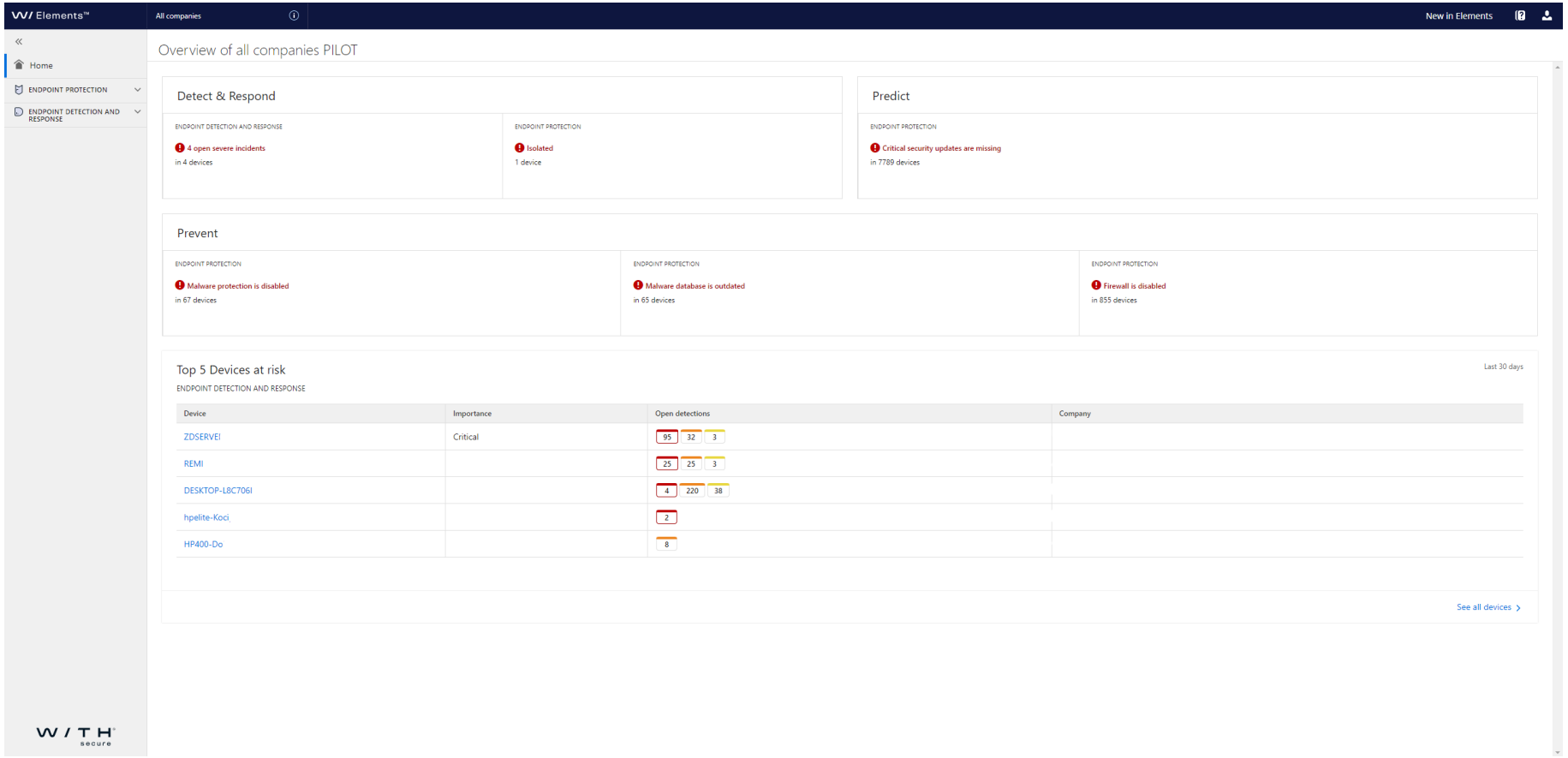
1. Prijava skozi login okno
2. Zamenjava začasnega gesla
3. Preveritev dodeljenih licenc

WITH secure

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.



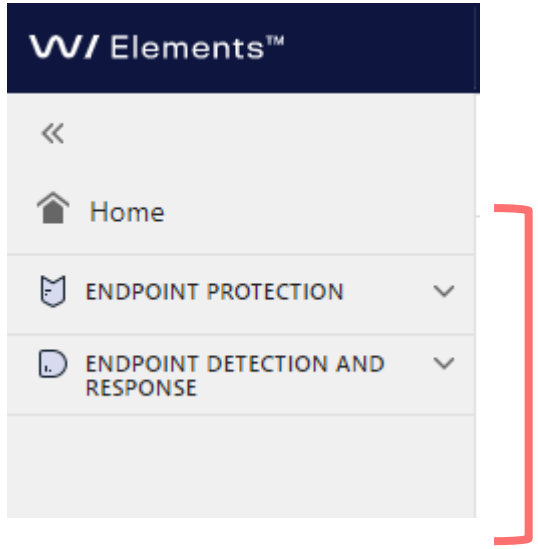
The Action Bar

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.

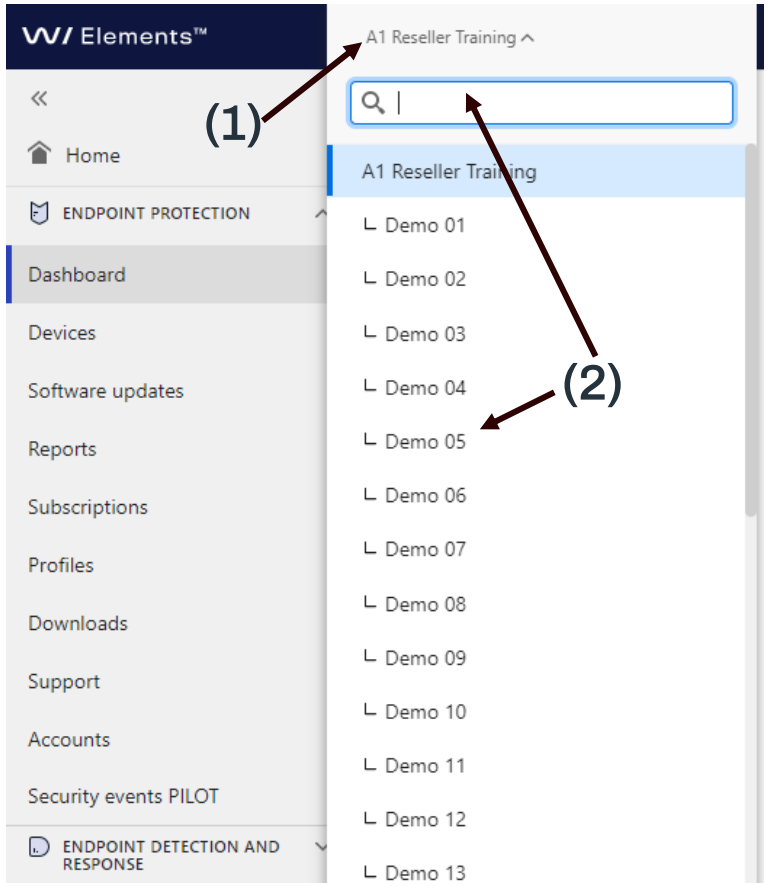


Note: *This menu will only display the Elements solutions your account is subscribed to.*

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:

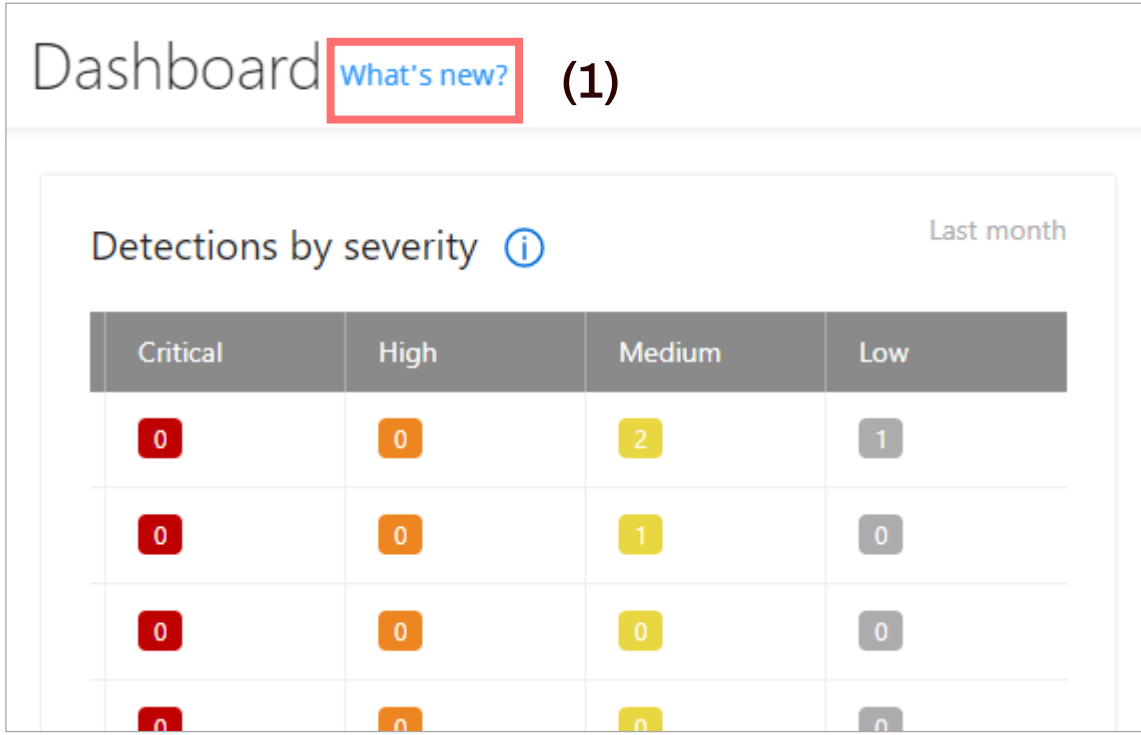
1. Click on the Scope selector (1) on the left side of the Action bar at the top of the screen.
2. Click on the name of the company you want to administer (2) from the dropdown that opens. Or type the name into the Search field.
3. By selecting a company, you have switched to the Organization view.
4. 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?

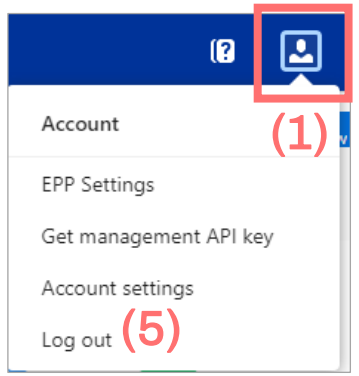
- When you visit any of the Elements Product pages, a pop-up may launch to explain new portal features that have been added. This pop-up will only play once. To view it again later, simply click the "What's new?" (1) link at the top of the Dashboard page.*

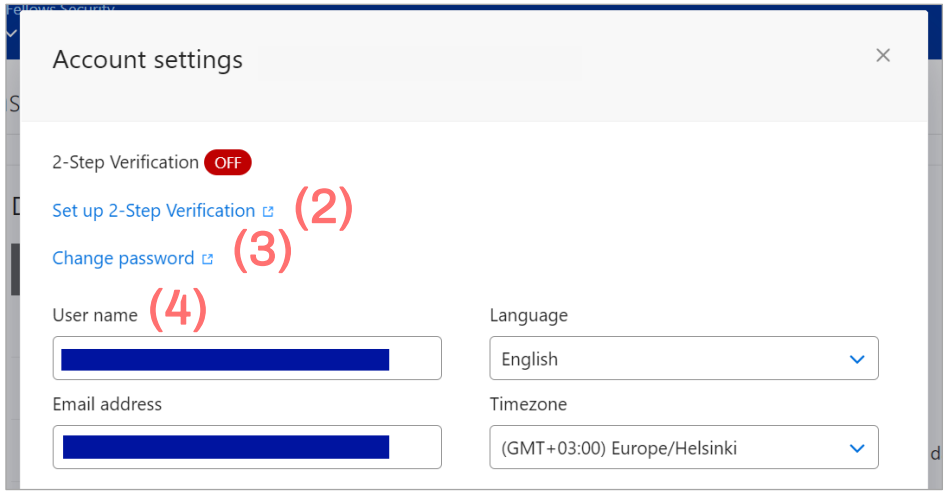
- "What's new?" is a part of interactive guidance, meaning you must enable 3rd party cookies in your browser or add https://elements.withsecure.com/ to your browser's exceptions for it to work.

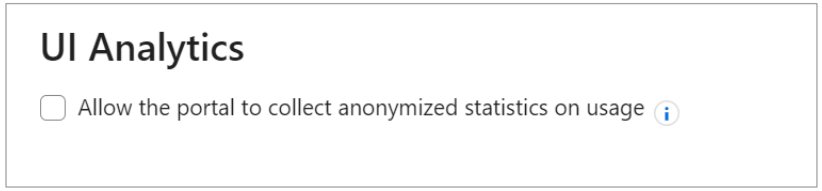


The Account Settings

- 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).



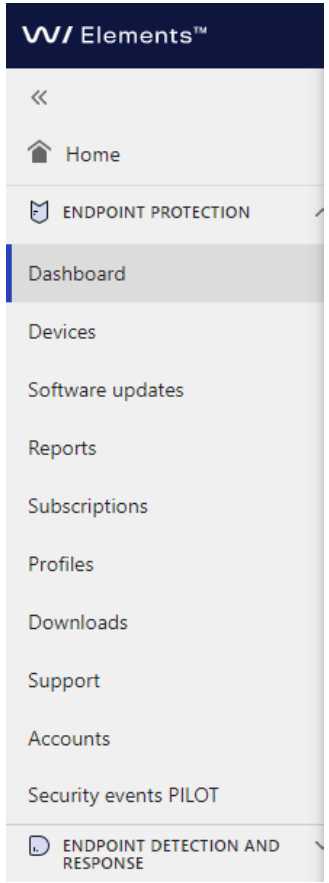




WITH secure

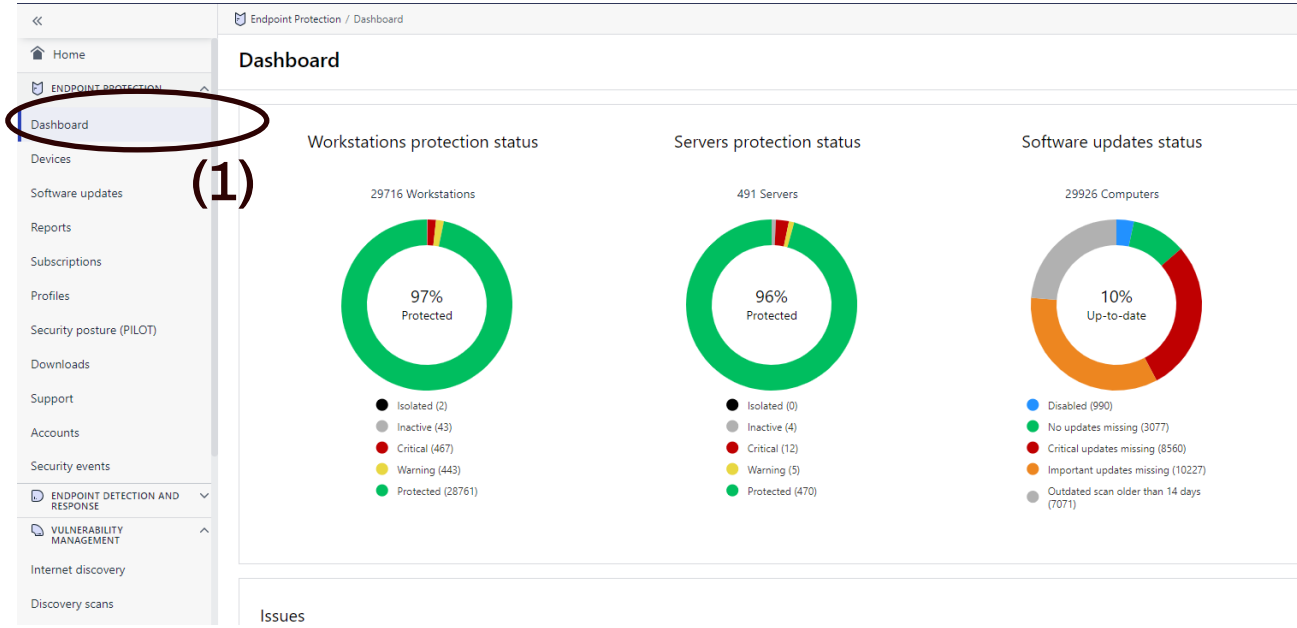
ESC Navigation

- 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

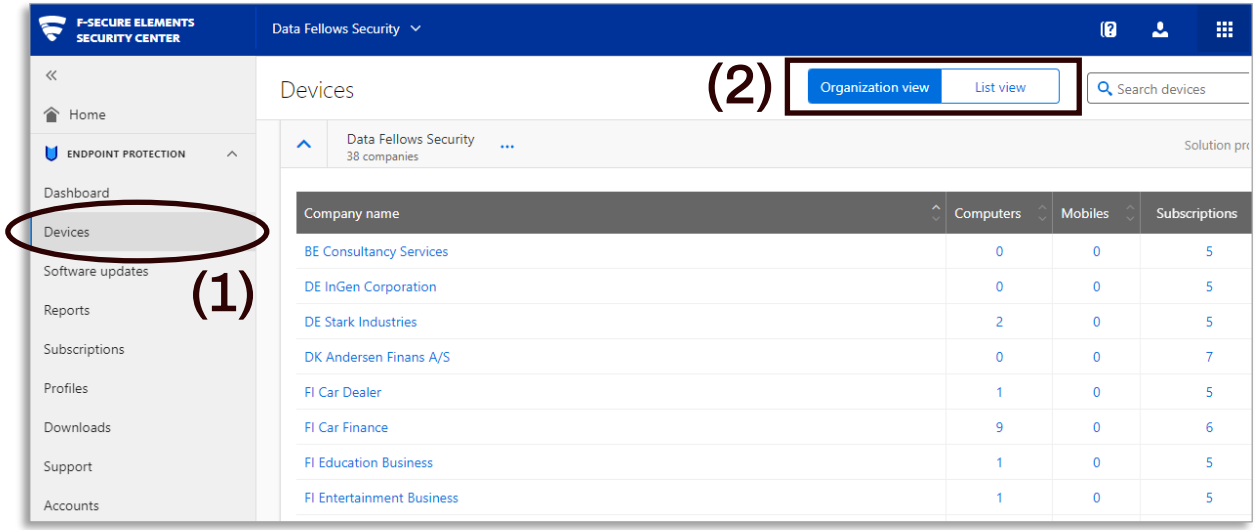
- Check Issues displayed on the dashboard on Solution Provider (SoP), Service Partner (SeP) or Company level.
- These are prioritized by severity and give the option to access more detail on device level for each issue.

Issues

Item type	Severity	Affected devices
Devices at risk due to missing Windows patch Check all necessary Windows updates are installed Check 1311 devices 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.	Critical	1311
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	Critical	8560
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	Critical	8255
Dangerous exclusions Review and manage exclusions in profile. Ensure no dangerous exclusions are included. Check 287 devices	Critical	287
Malware Definitions Outdated Send full status update to device. Boot device. Check 212 devices	Critical	212
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	Critical	138
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	Critical	127
License Expired Update the subscription. Boot the affected devices. Check 41 devices	Critical	41
Devices with Severe EDR Incidents open Resolve the incidents on the devices. Check 12 devices	Critical	12

Devices
SOP / SEO Level

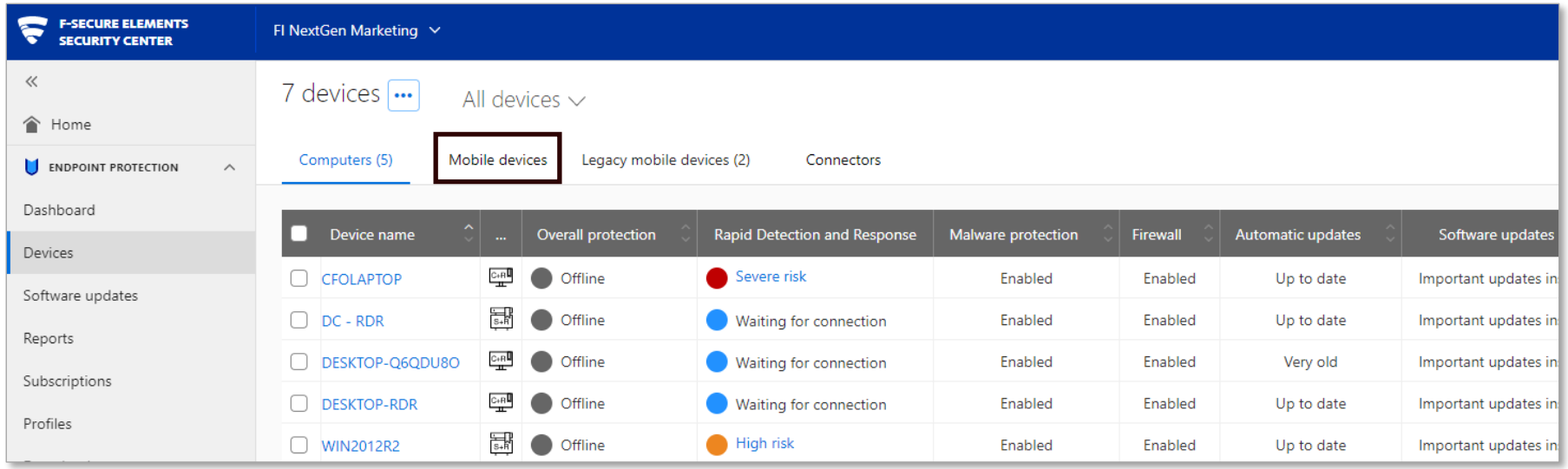
- Click Devices on the navigation pane (1) to view all devices linked to your account.
- At the Solution Provider (SoP) or Service Partner (SeP) level, devices are grouped by company.
  - Click a company name to access the devices of that company.
  - From there, you can click to view specific devices 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.



WITH secure

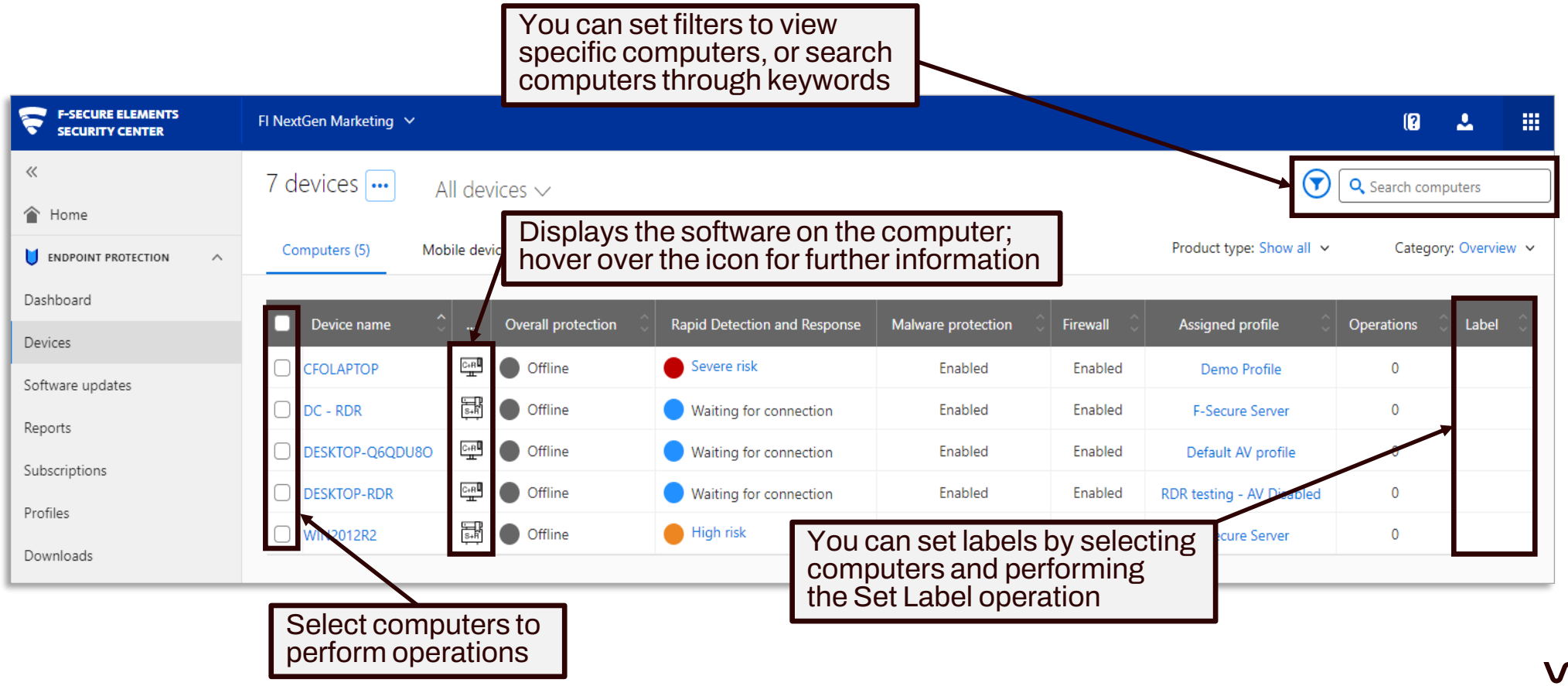
Devices
Company Level

- 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.

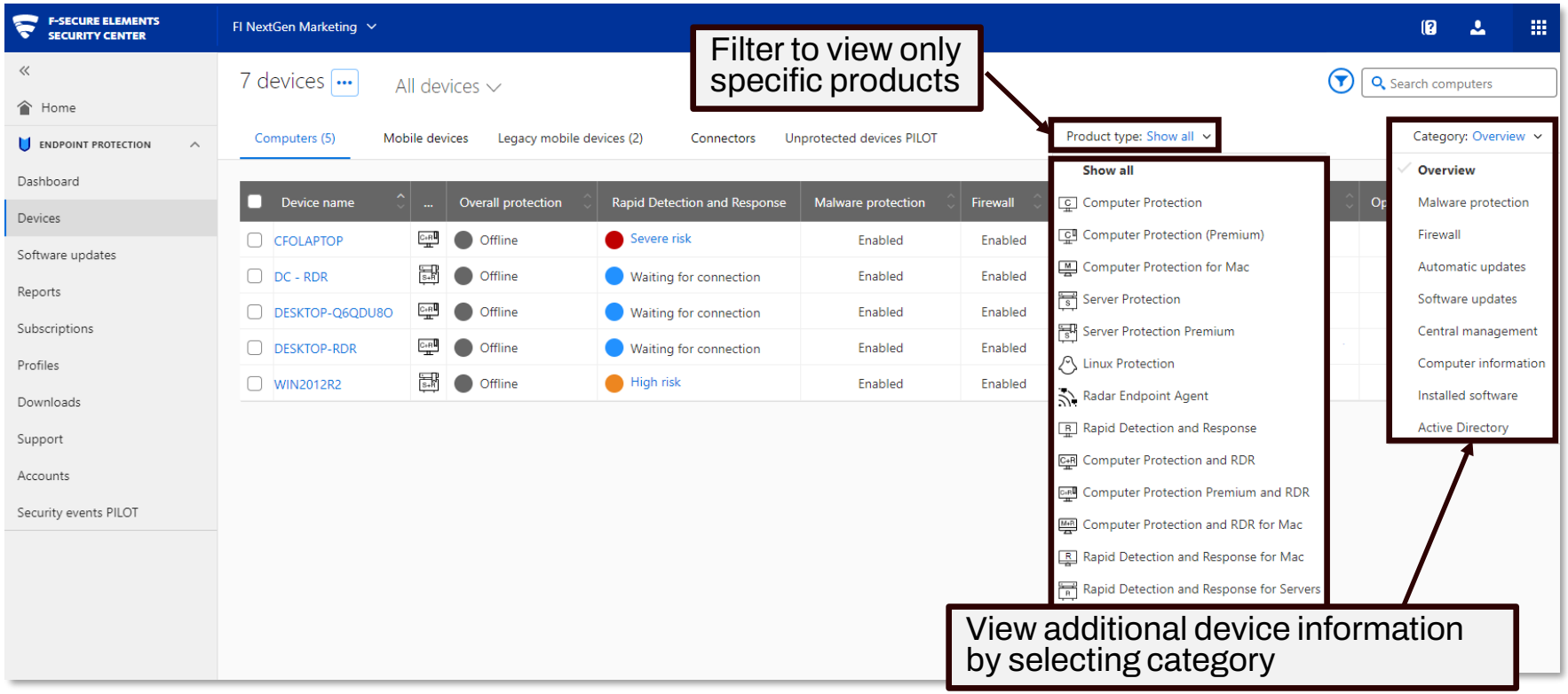


WITH secure

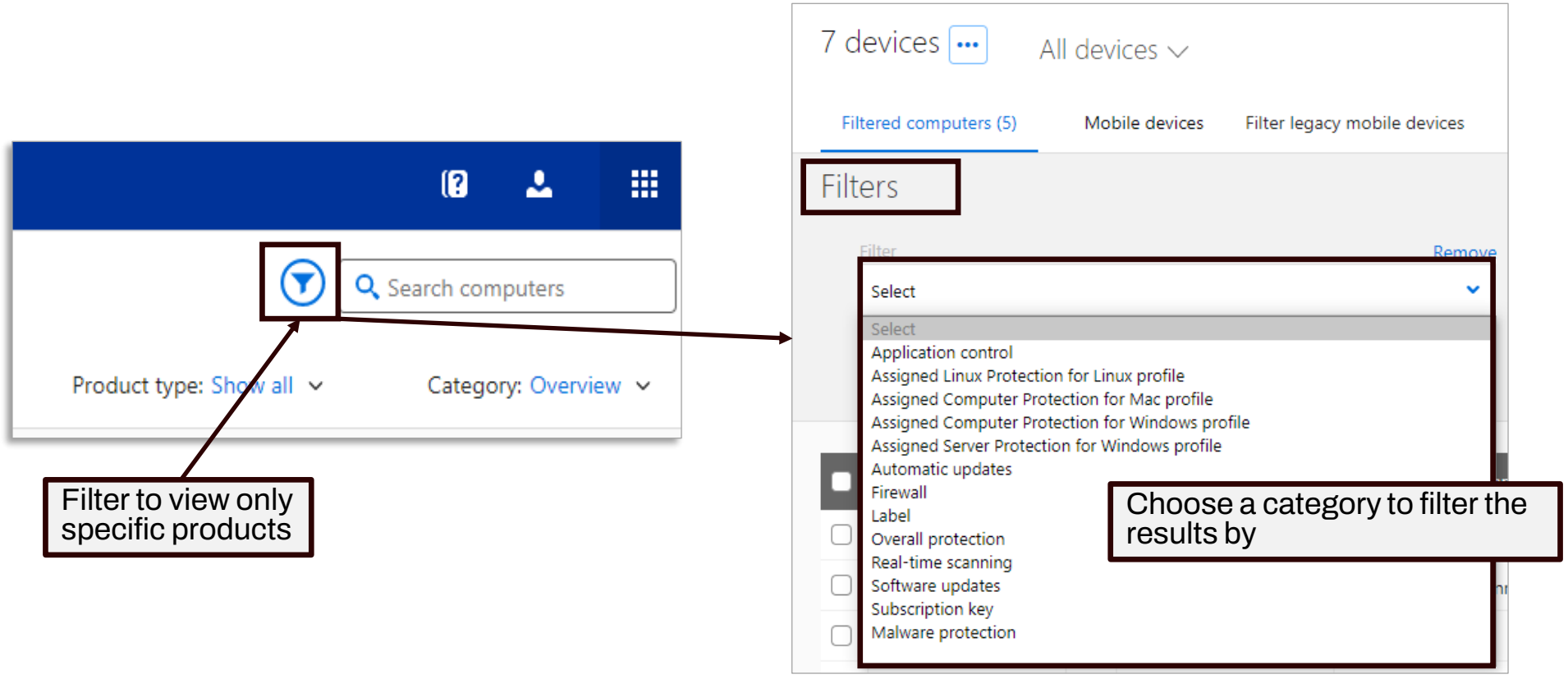
Devices
Features And Operations



Devices
Filtering Devices



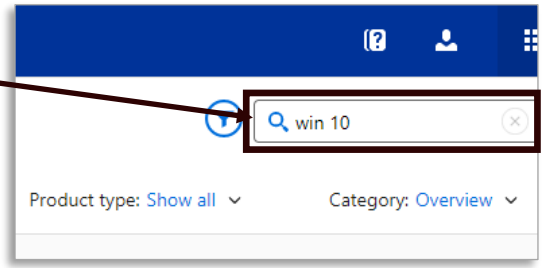
Devices
Filtering Devices

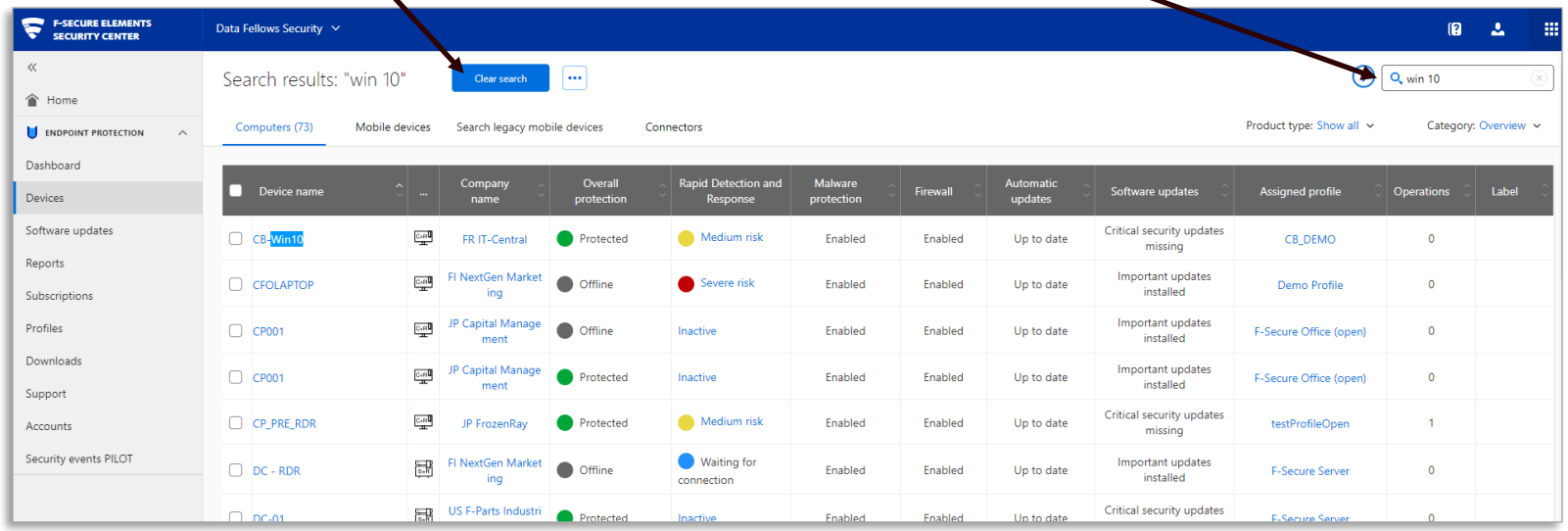


WITH secure

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.



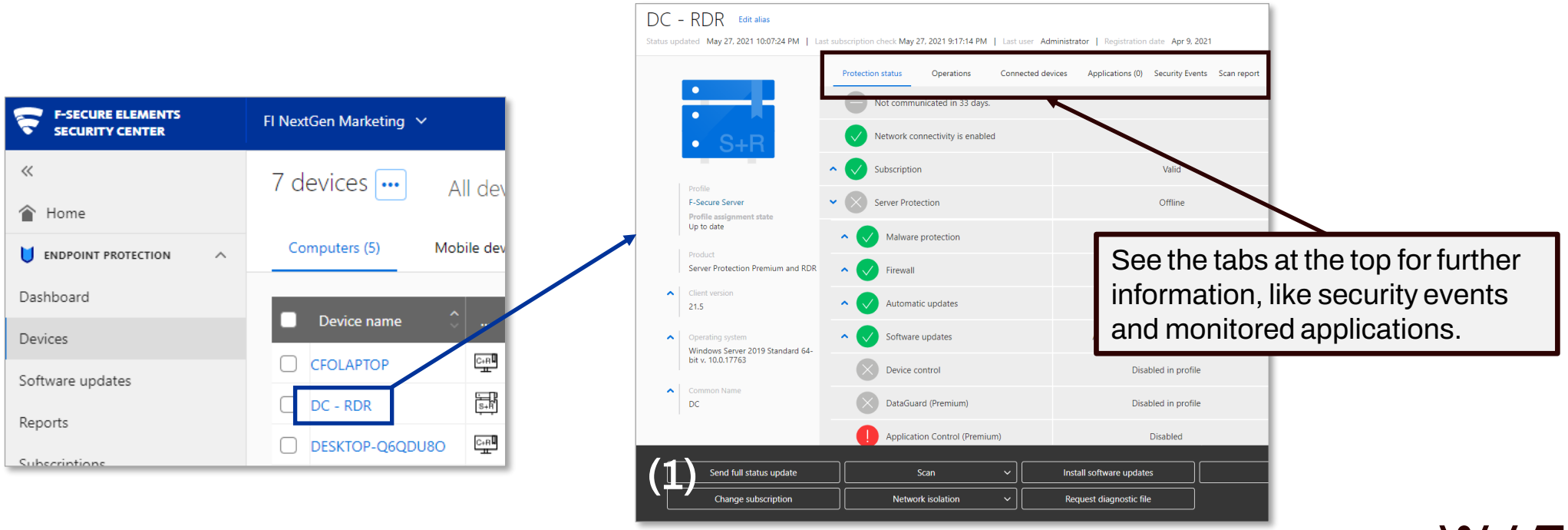


WITH secure

Device View

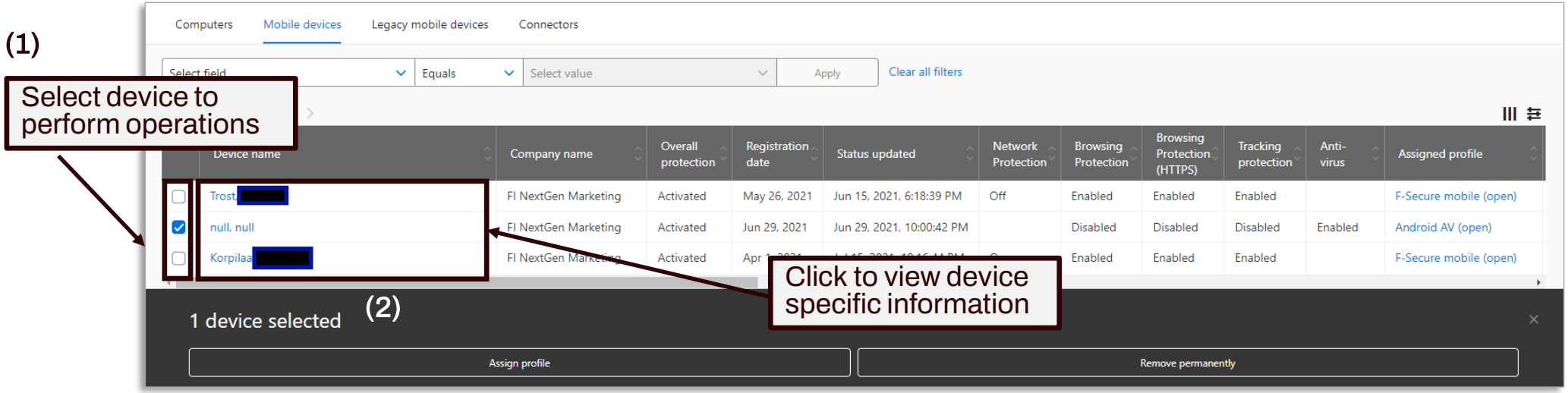
If you click on the name of a specific device (e.g., DC – RDR below), you will be taken to the device view, which provides more in-depth information about that device.

- 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.



Devices
Mobile Devices

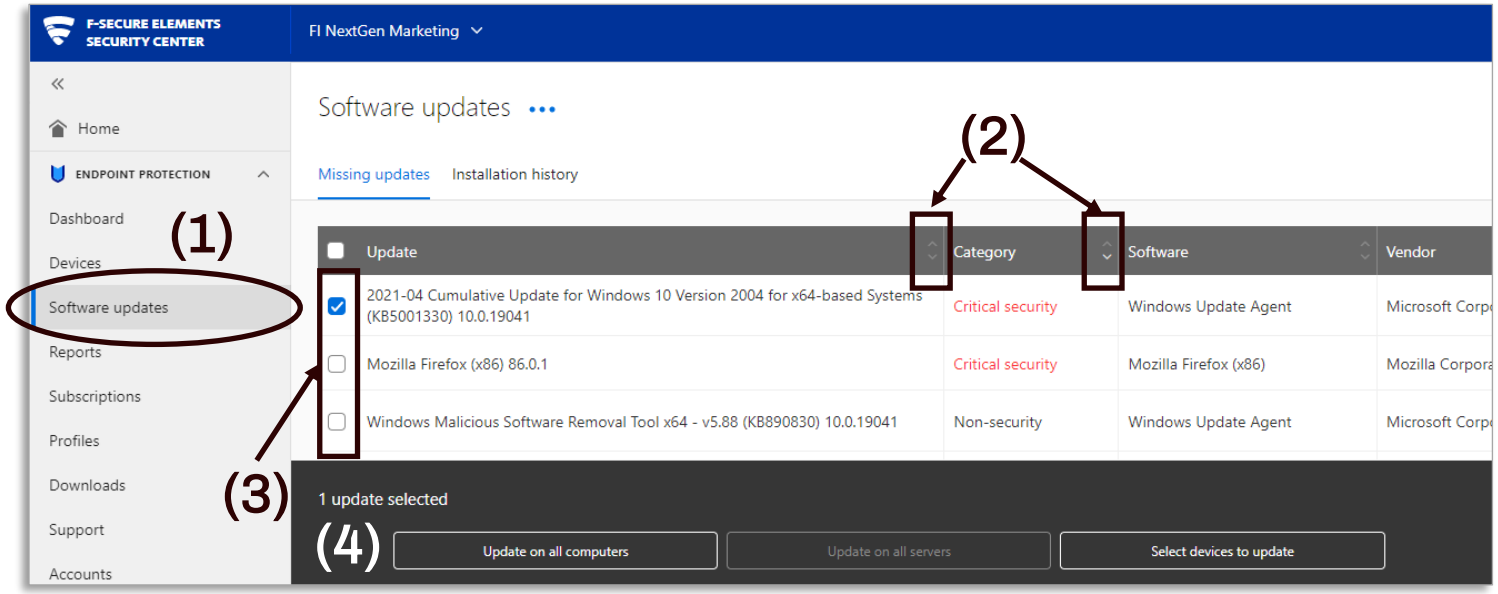
- The Mobile Devices tab under the Devices page lists all mobile devices on the system. This includes all devices protected by Elements Mobile Protection. Older devices can be found in a separate tab, Legacy Mobile Devices.
- You can view device specific information by clicking on the Device name.
- 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.



WITH secure

Software Updater

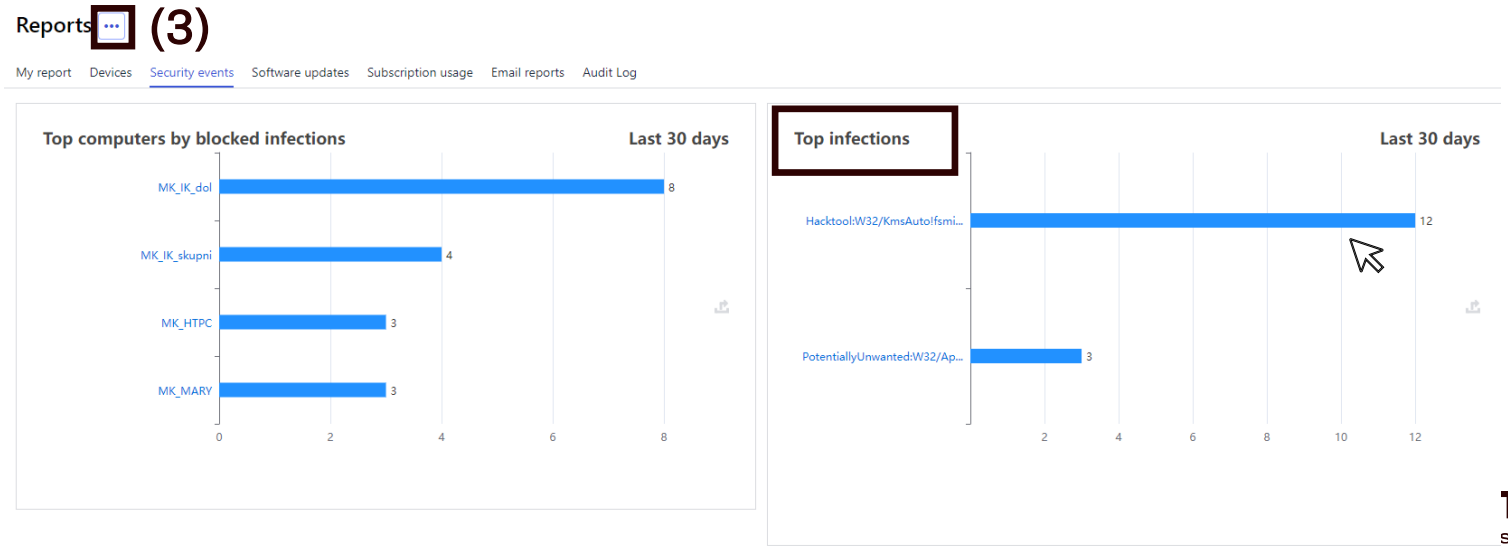
- Click Software Updates (1) on the navigation pane.
- Updates are, by default, categorized by criticality. If you want to see the them categorized another way, simply click the up/down arrows next to the various categories (2) to change the sorting display.
- Choose the updates you want to make (3) 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.



Reports

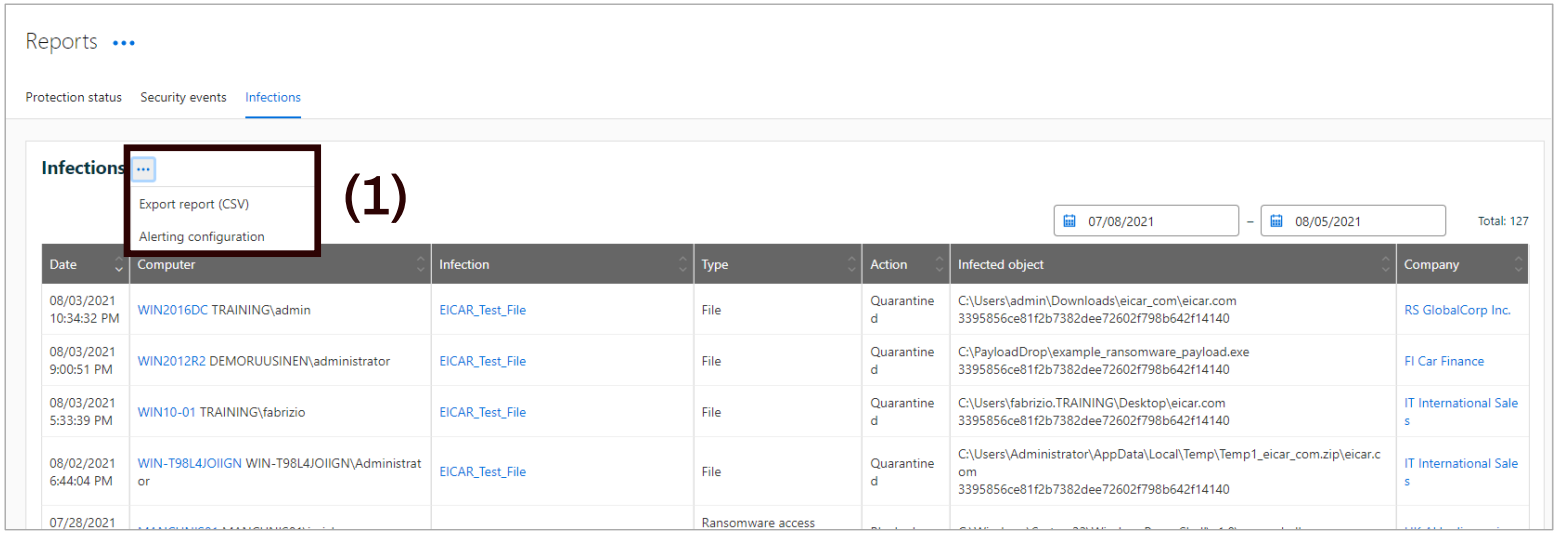
- The Reports tab on the Navigation pane (1) allows you to access protection status and infection information.
  - Much of this data is visualized in different ways to clarify and provide context.

- 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.

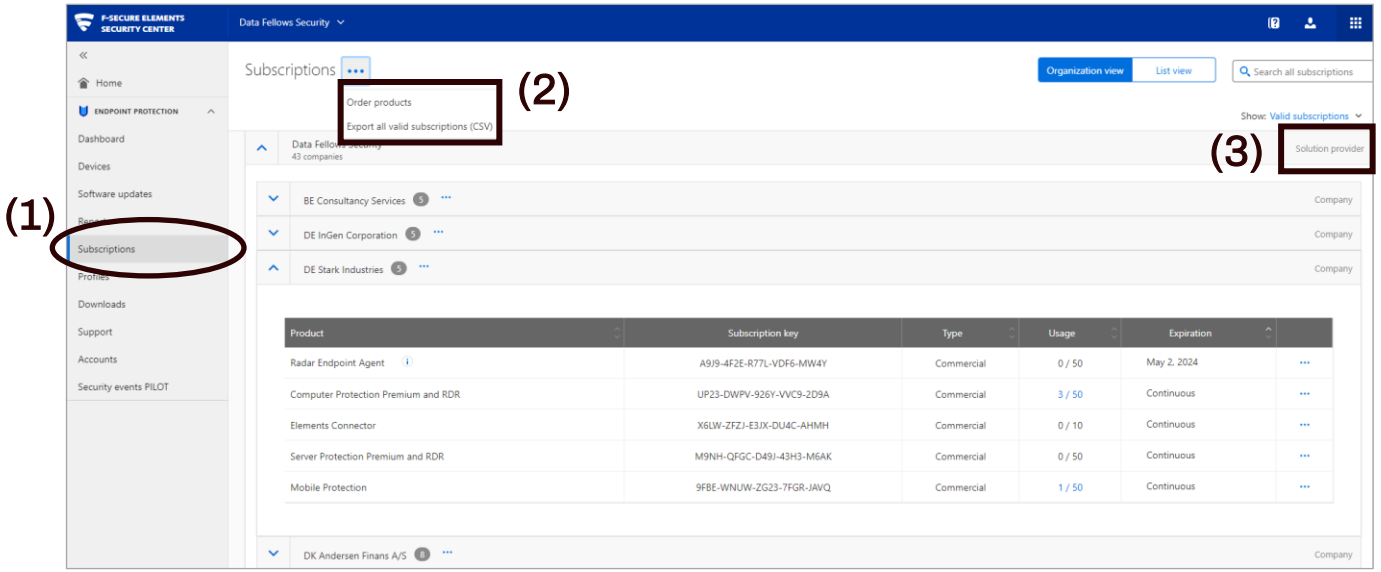


WITH secure

Subscriptions

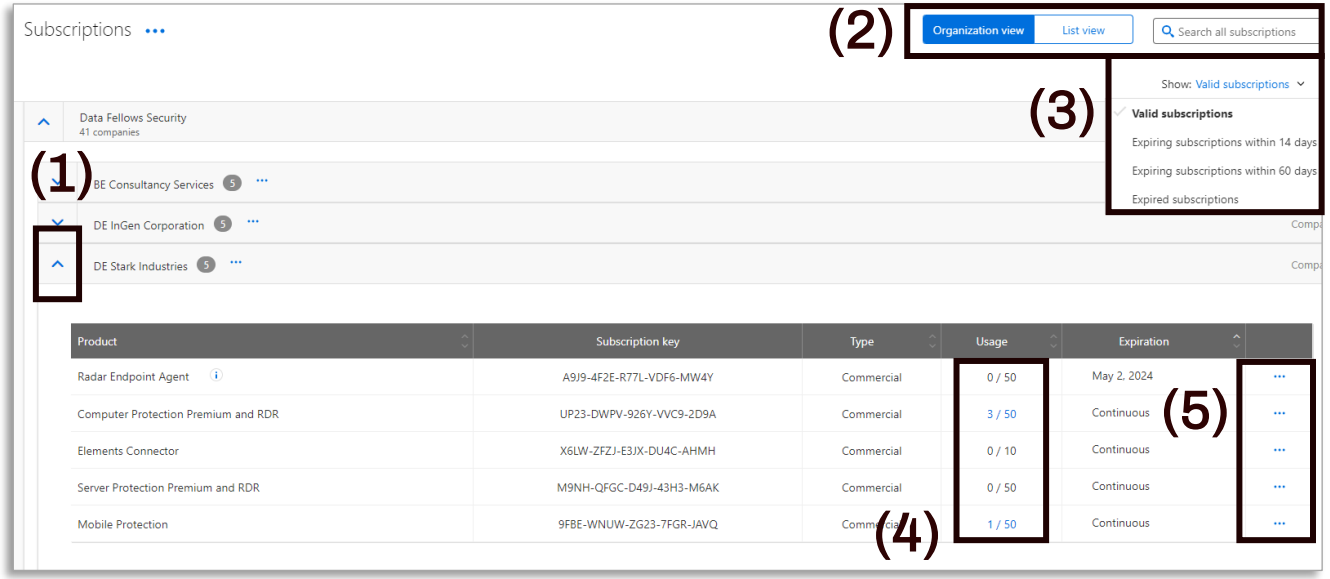
- On the Subscriptions page (1):
  - Order new subscriptions
  - You can view your current, expiring, or expired subscriptions
  - Change subscription plans

- 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.



Subscriptions Continued

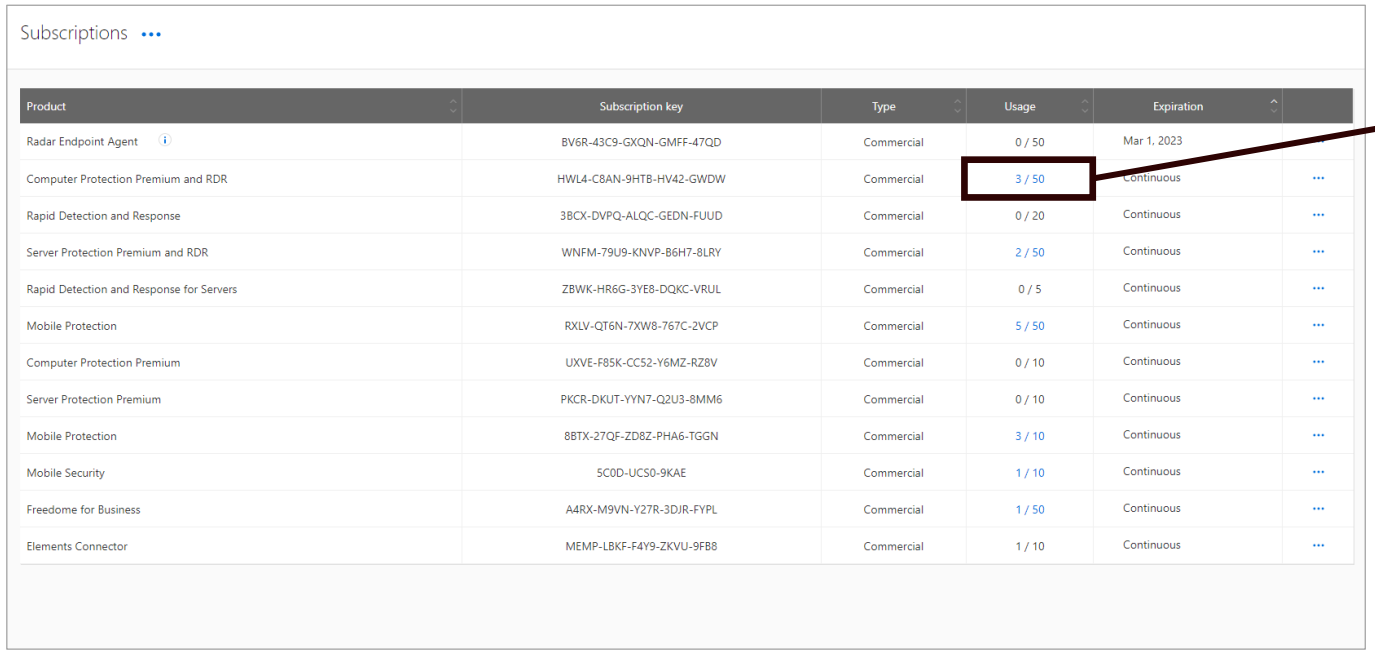
- View a company's subscriptions by clicking the blue arrow next to the company's name (1).
  - This opens a table with more information, as shown here. If you are on the company level, you will see this table from the start.
  - Search your subscriptions using the search bar at the top or switch to 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).

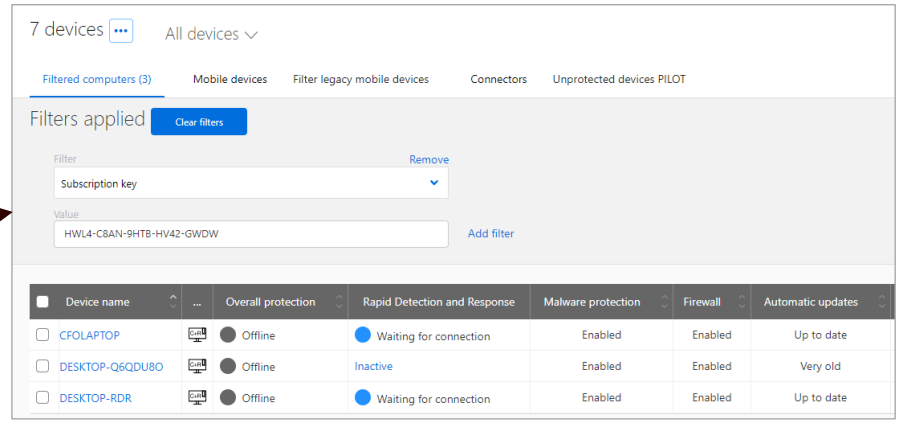


Note: *For information on the devices, click the blue number in the usage column (4). This will take you to the devices view, as covered earlier in this module.*

WITH secure

Subscriptions Organization Level

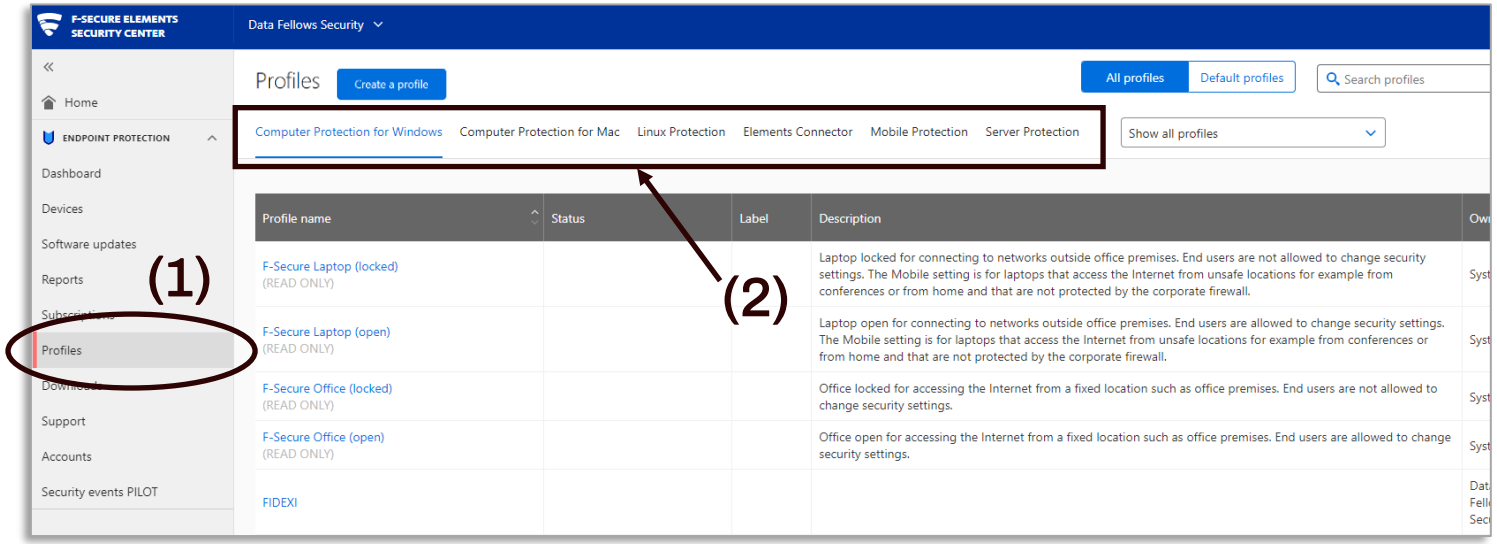




WITH secure

Profiles

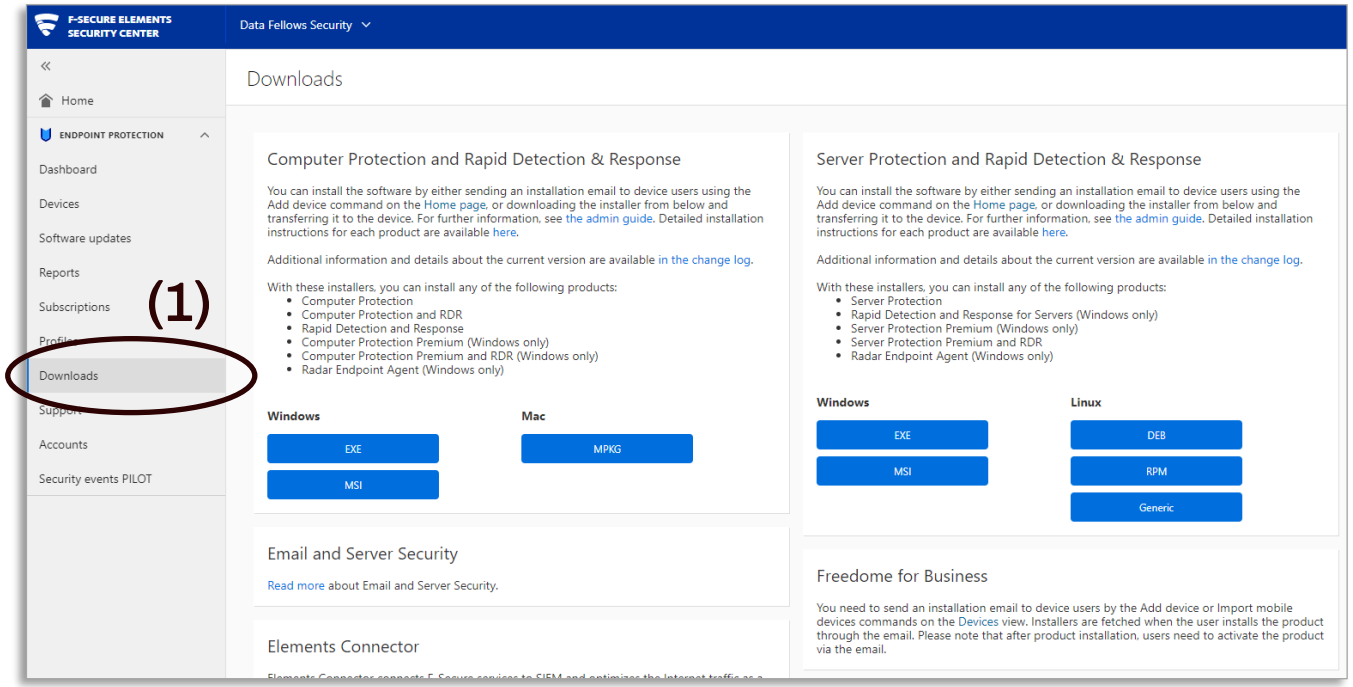
- Click Profiles on the navigation pane (1).
- You can select the Computer Protection for Windows, Computer Protection for Mac, Linux Protection, Mobile Protection, and Server Protection tabs under the page title (2) to view the profiles governing the different devices in your environment.
    - See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



WITH secure

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.

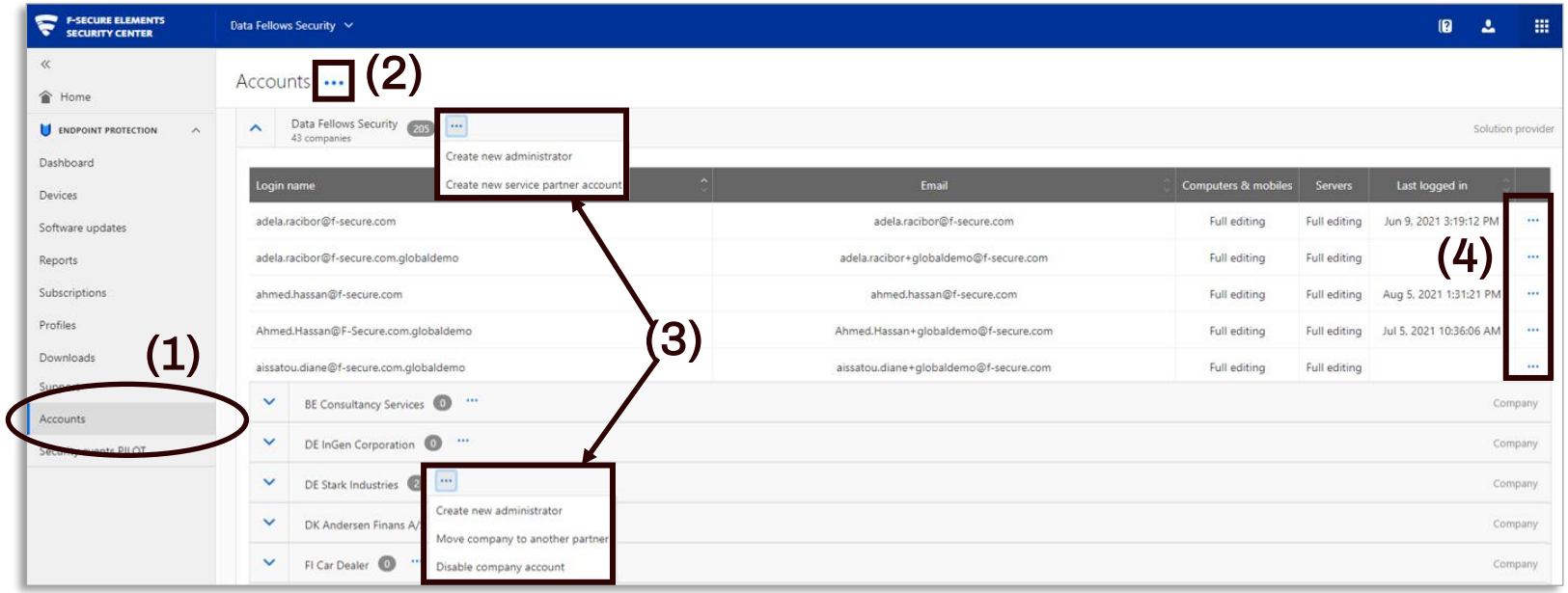


WITH secure

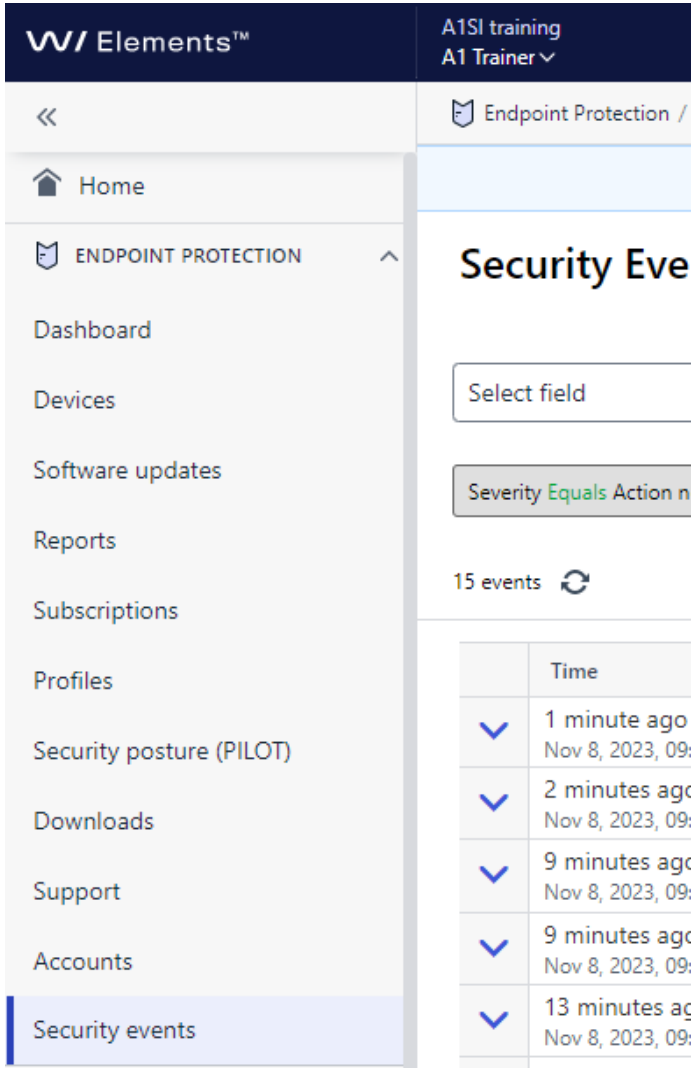
User Accounts

- 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).

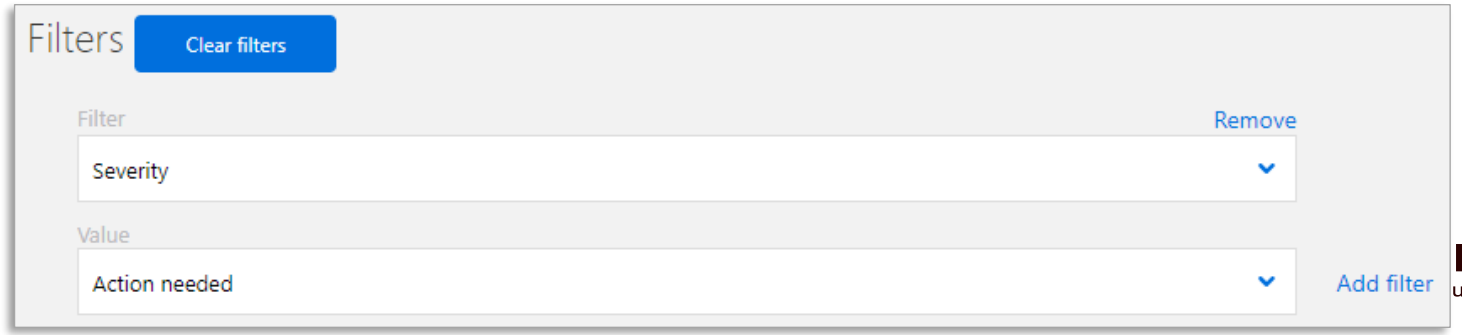
- You can create as many administrator accounts as you need. It is also possible to create read-only accounts.
- To edit or delete a user account, click the (...) menu in the same row as the account details (4).



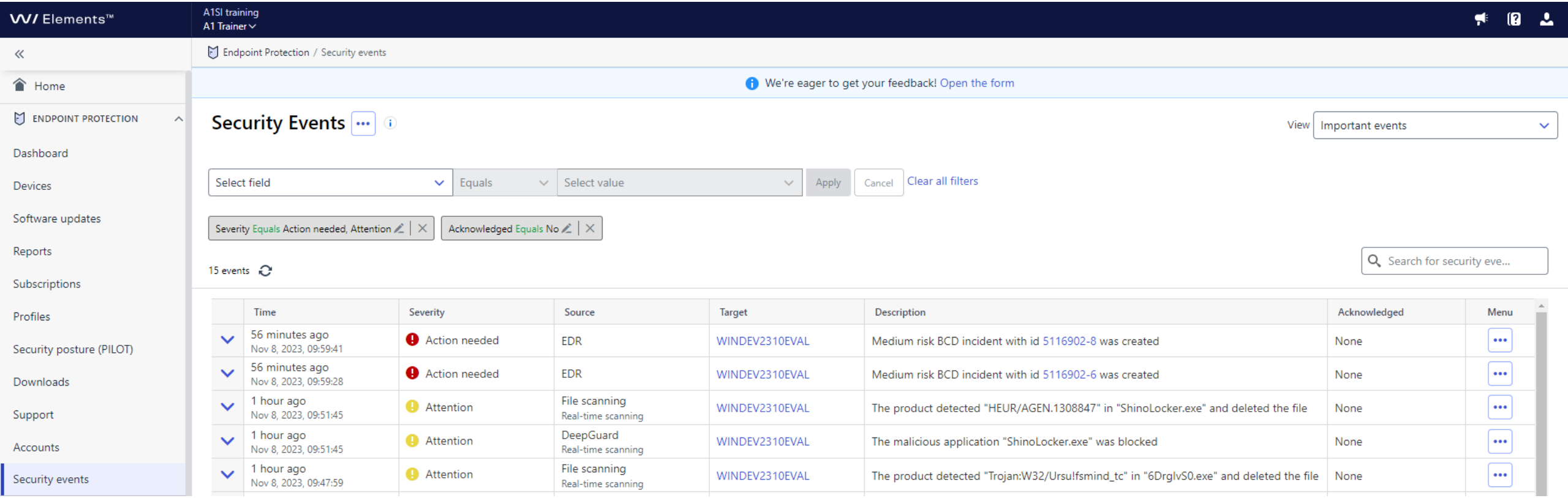
Security Events



- 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:

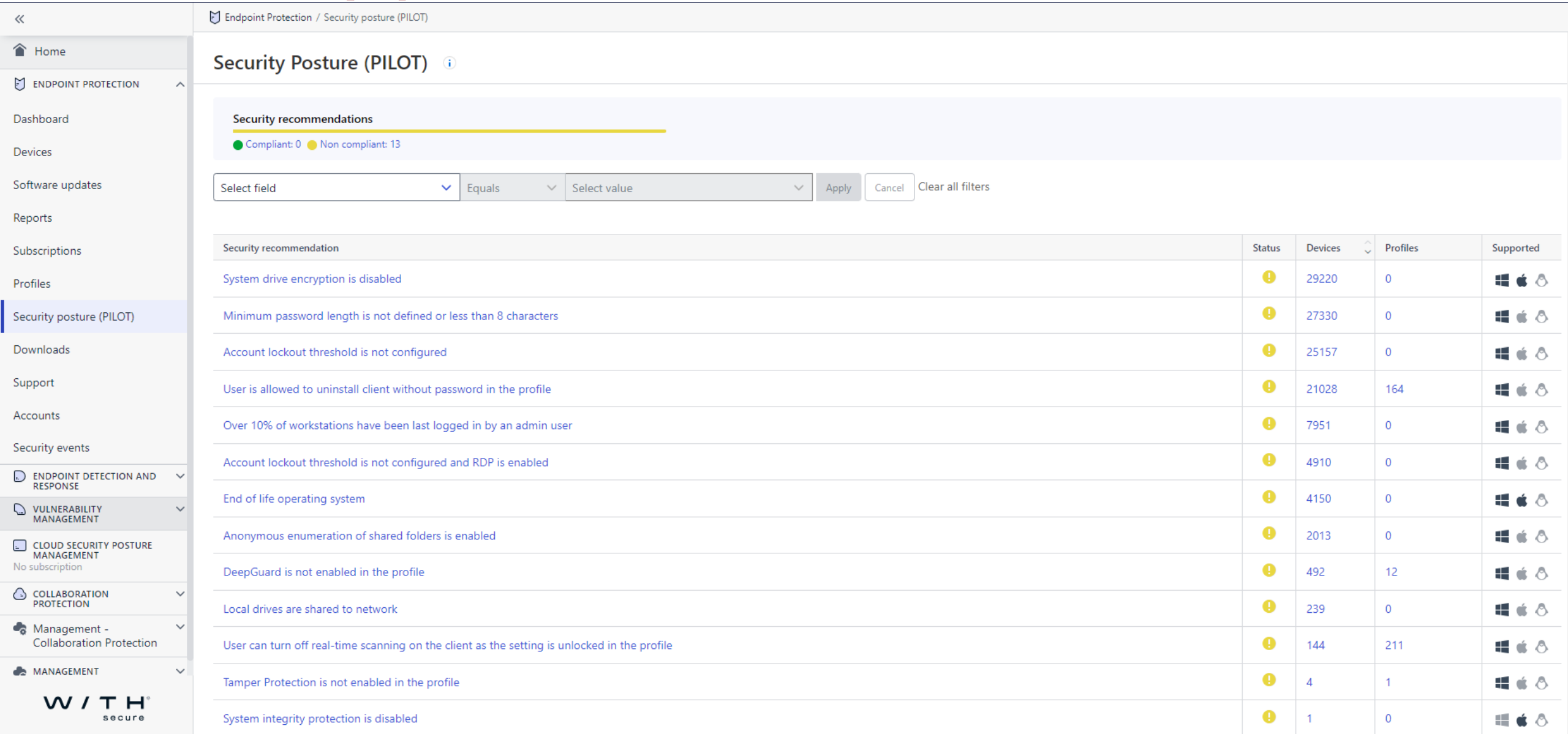


Security Events



WITH secure

Security posture (PILOT)



Agent Deployment

Elements EPP Agent

W/TH secure

Deployment Methods

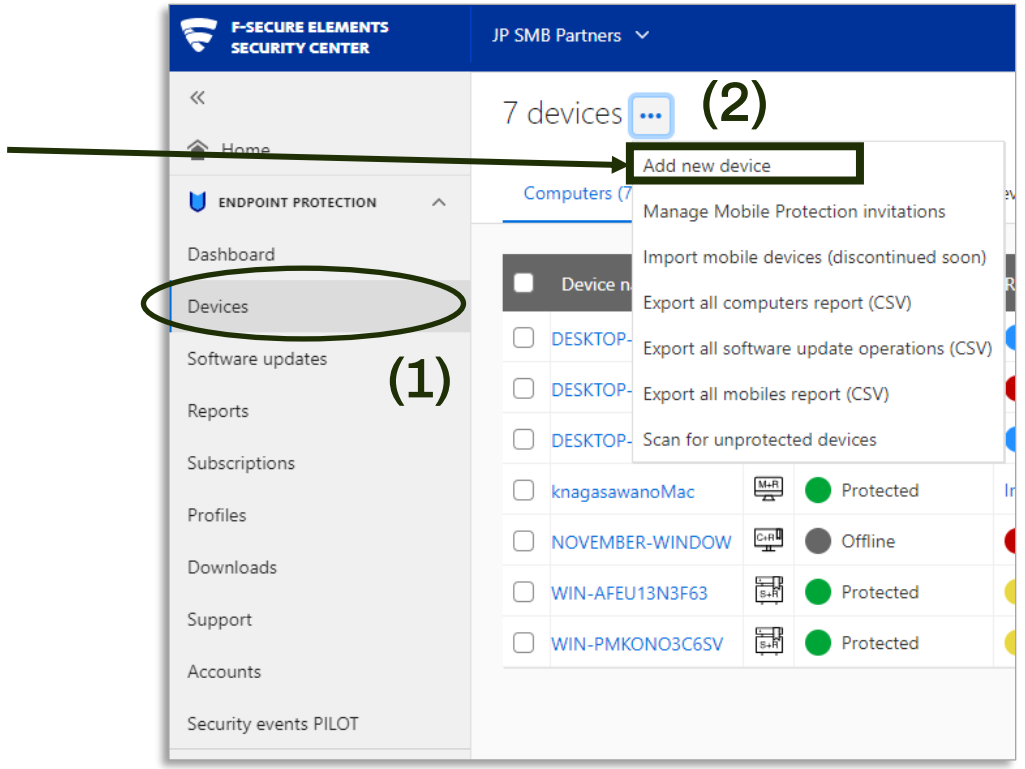
There are various methods for deploying Elements Endpoint Protection software. They are:

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

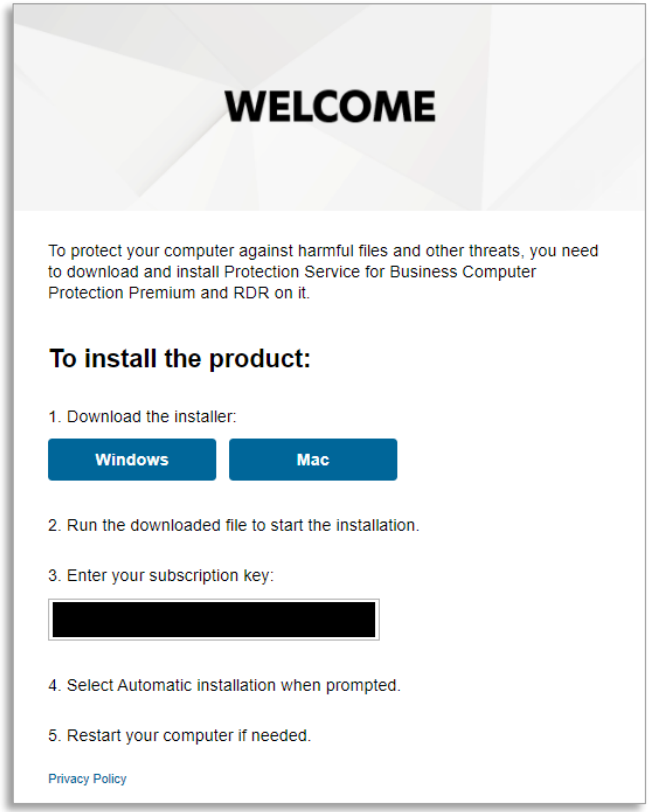
1. In the ESC Portal, on the company level, select Devices on the navigation pane.
2. Click ••• next to the page title and select Add new device.
3. Select the required subscription from the list and click Next.
4. Type in the email address of the recipient. If there are multiple addresses, either use 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.



WITH secure

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.

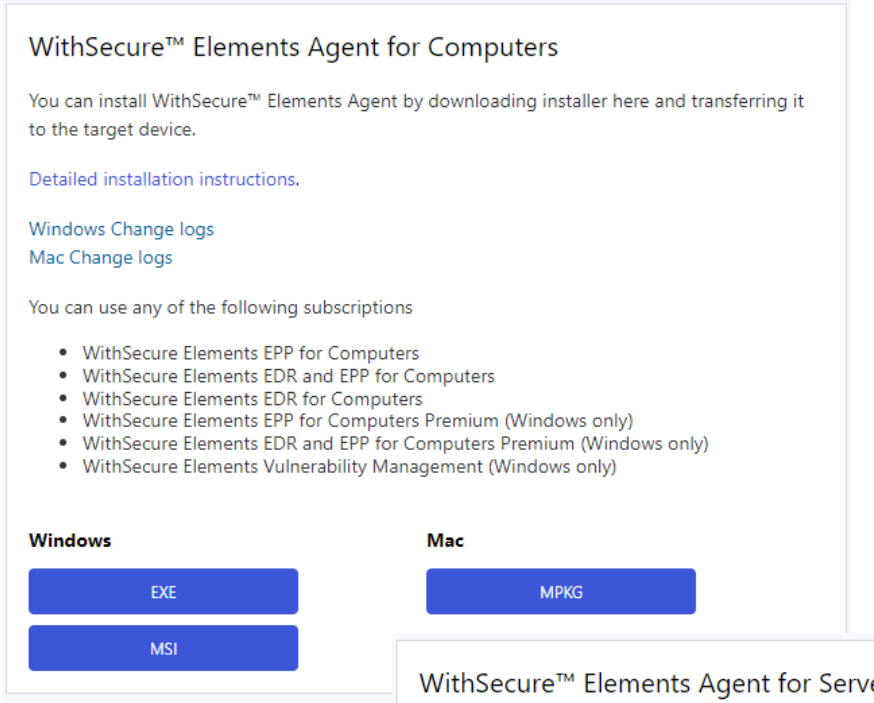


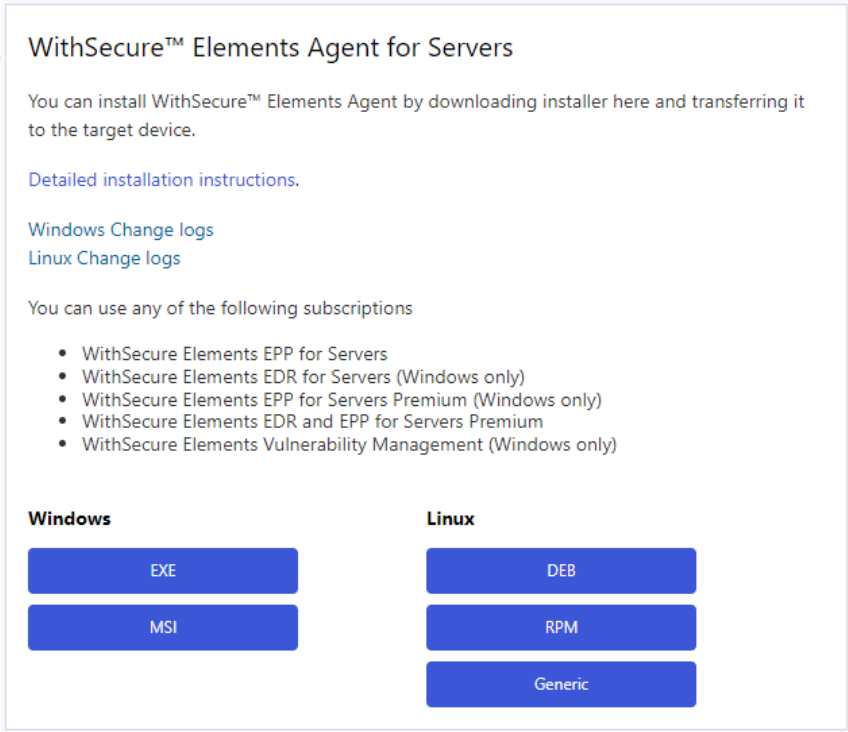
WITH secure

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.



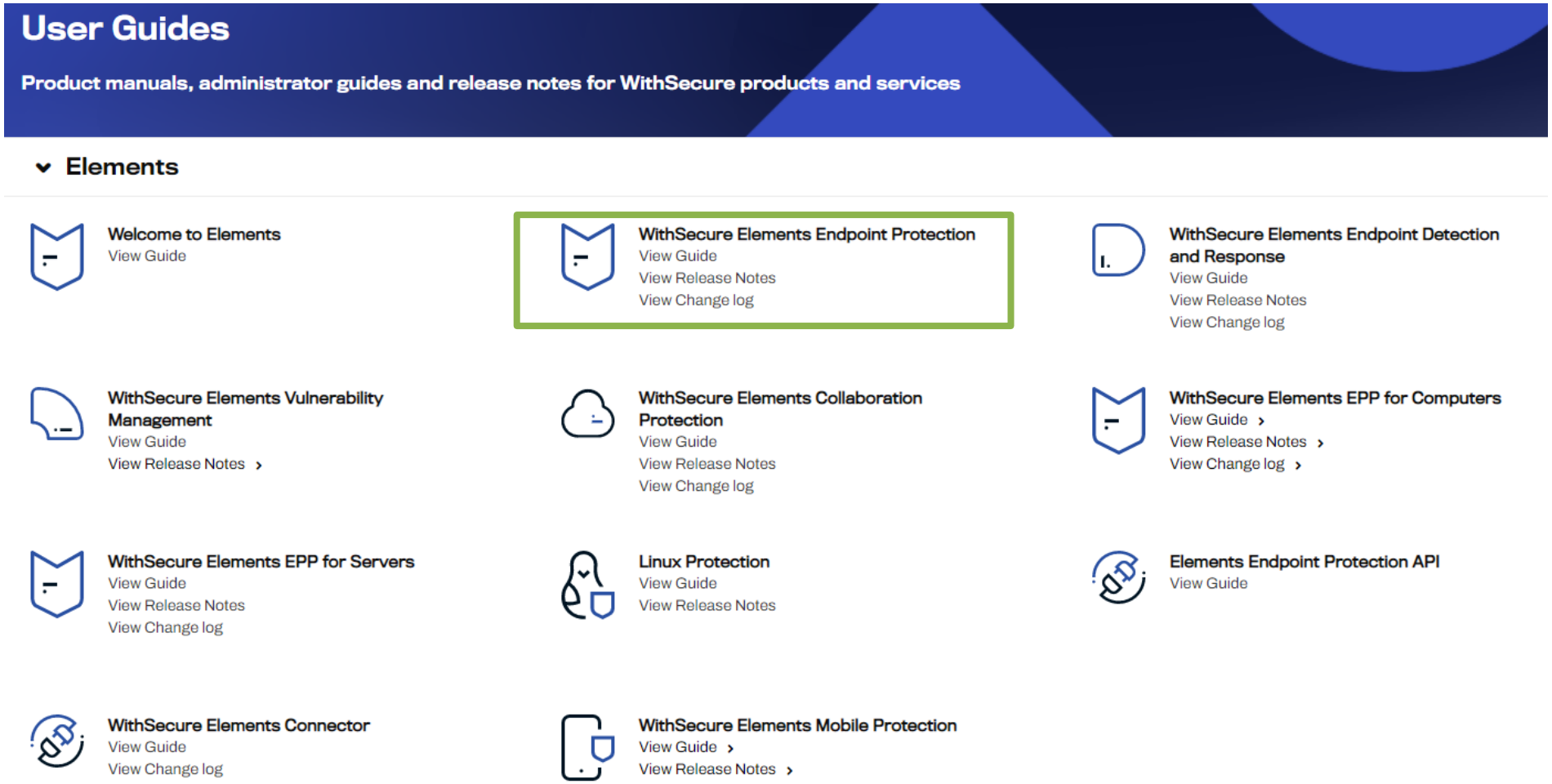


Local Installation
EPP For Computers

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/



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.

WITH secure

Deploying Elements Protection For Mobile

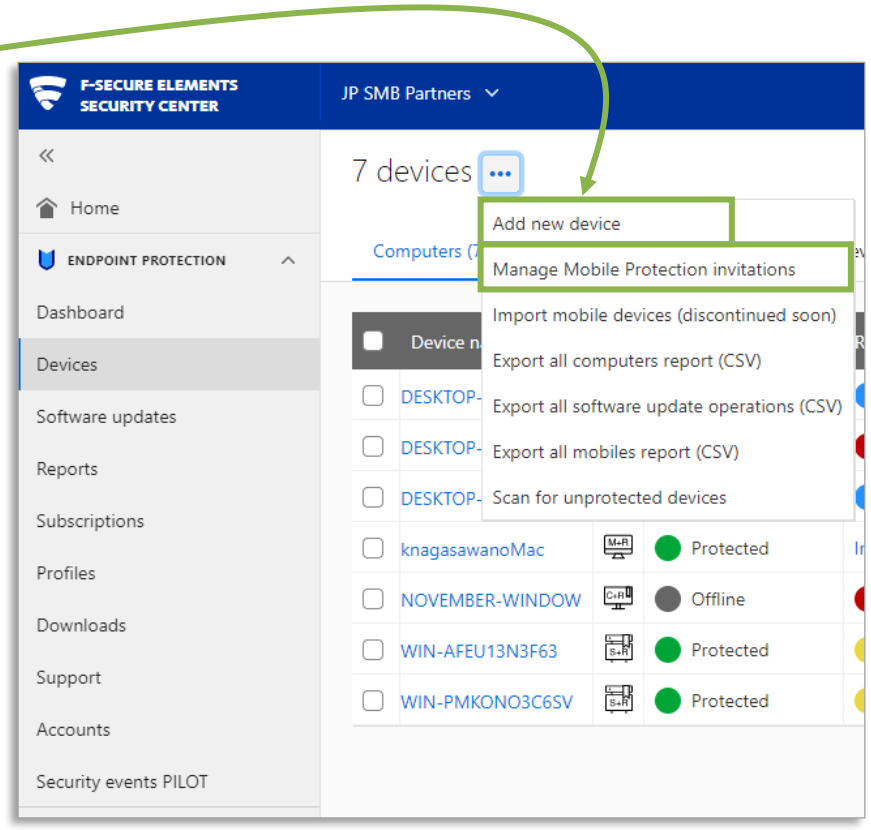
There are two main methods for deploying WithSecure Elements Protection for Mobile:

- 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.



WITH secure

Namestitev Elements Agenta

Elements EPP+EDR for Computers Premium

WITH secure

Namestitev Elements Agenta

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

WITH secure

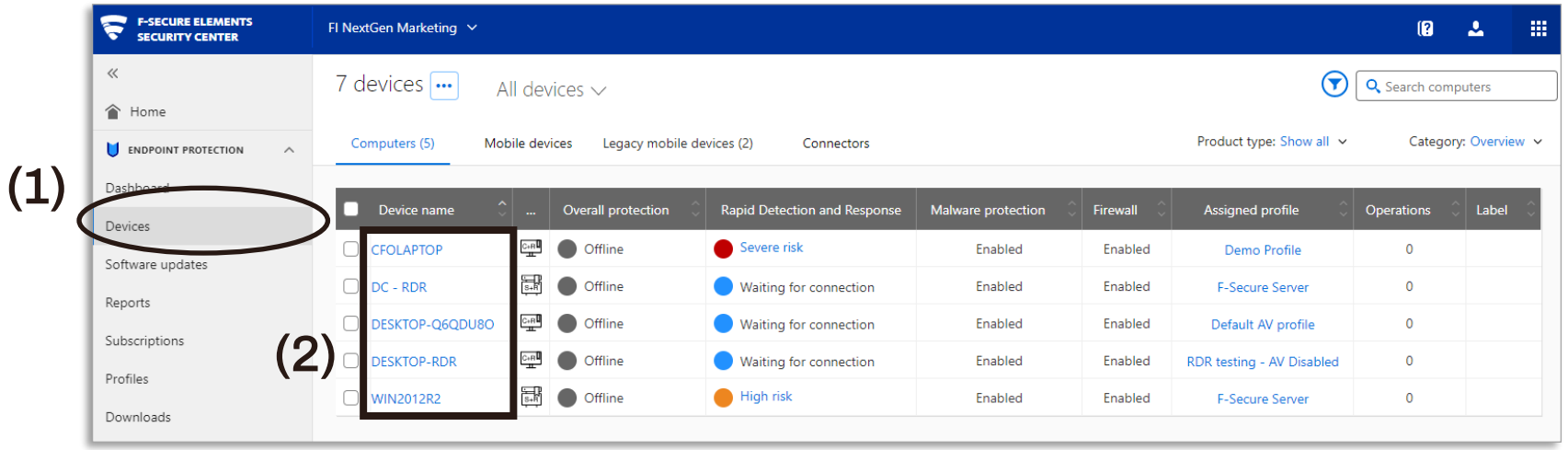
Device operations

Elements ESC portal

WITH secure

Devices
Computer

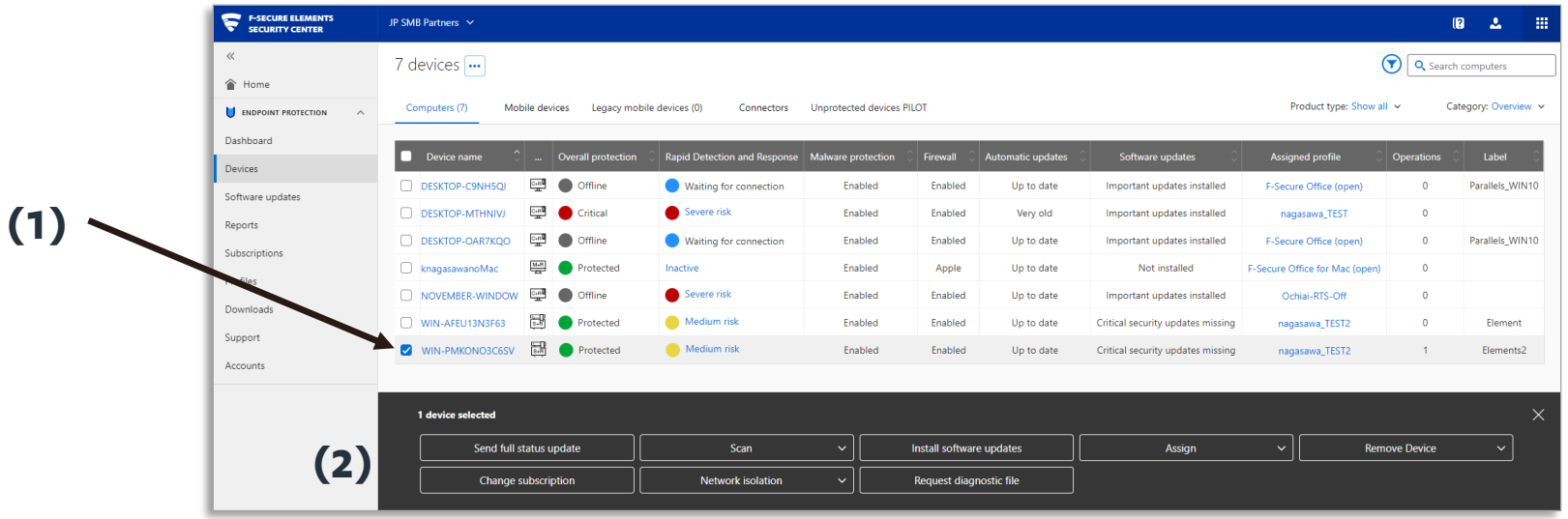
- Select the Devices tab (1) from the navigation pane. Note that we are at the company level.
- Click on the name of a computer (2) to view device specific information.
- From here, you can also perform a variety of operations, which we'll demonstrate how to do next.



WITH secure

Devices
Computer Operations

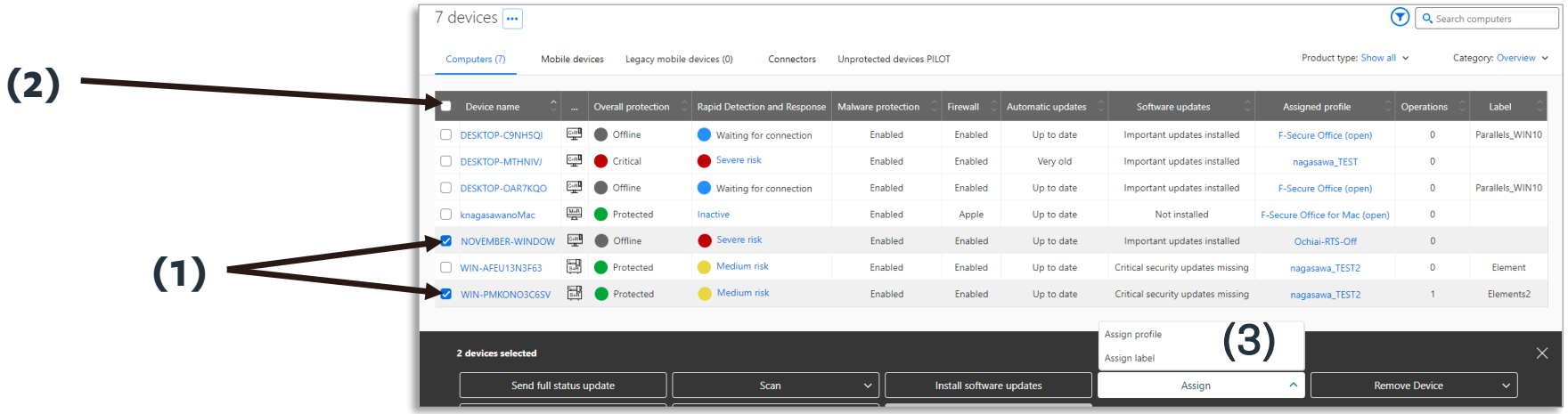
1. To perform operations, start by selecting one or more device checkboxes (1). This will cause the gray Operations pane to appear at the bottom of the screen.
2. Continue by selecting the operation (2) you want to perform, such as installing updates or assigning a profile.



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.

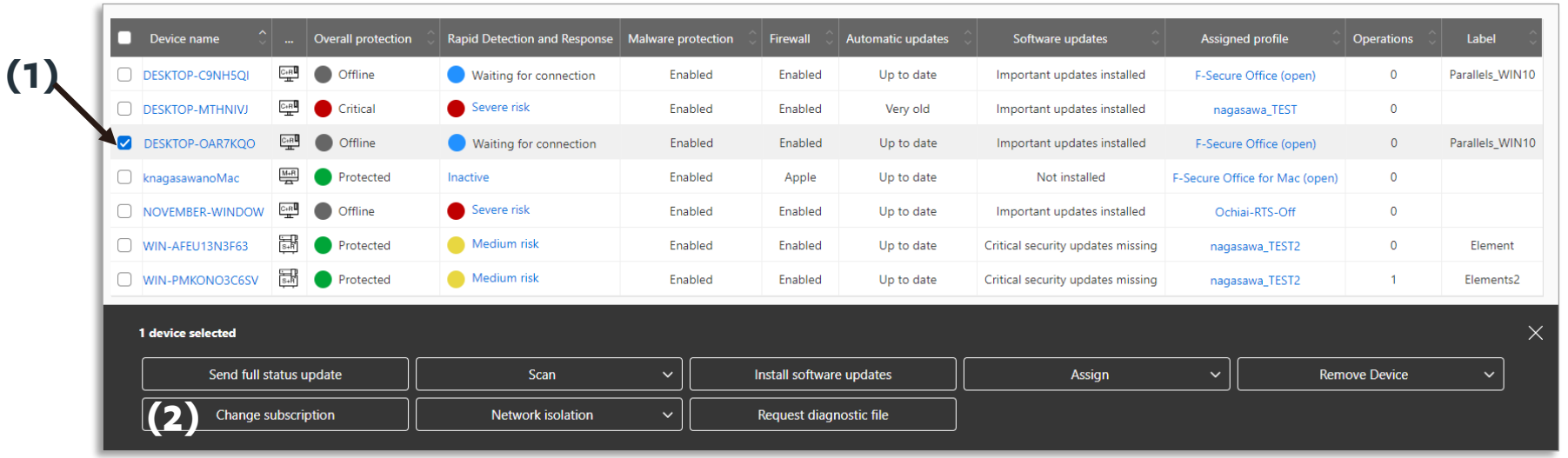


WITH secure

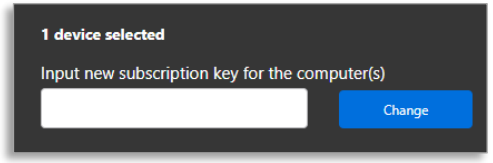
Operations
Changing Subscriptions

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.



(3)



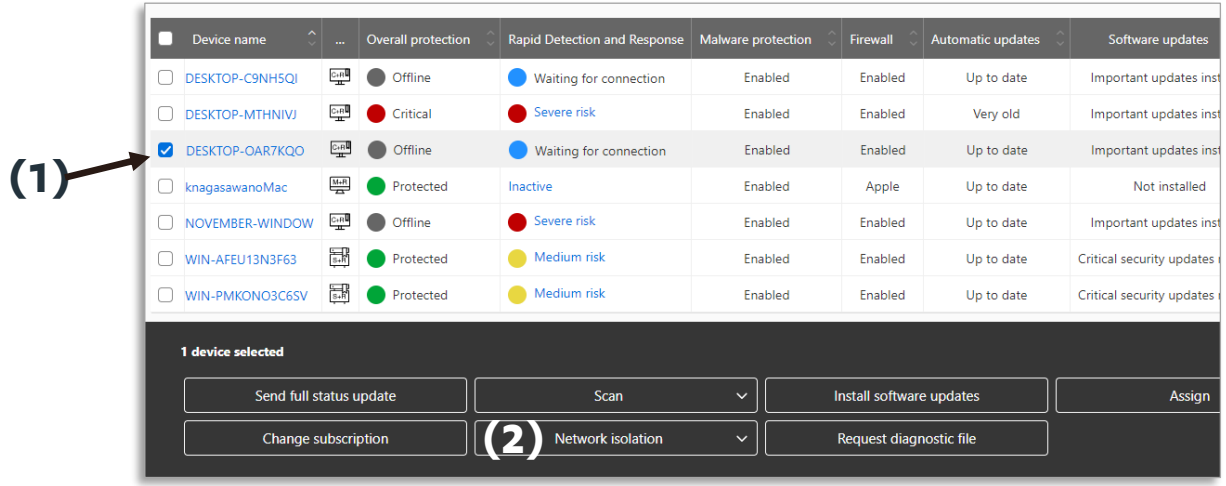
WITH secure

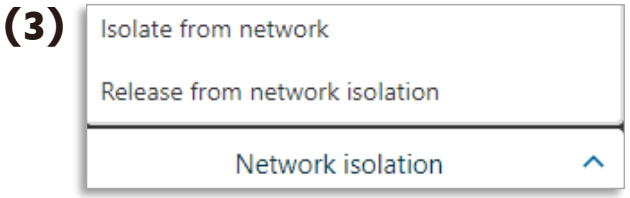
Operations
Network Isolation

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.

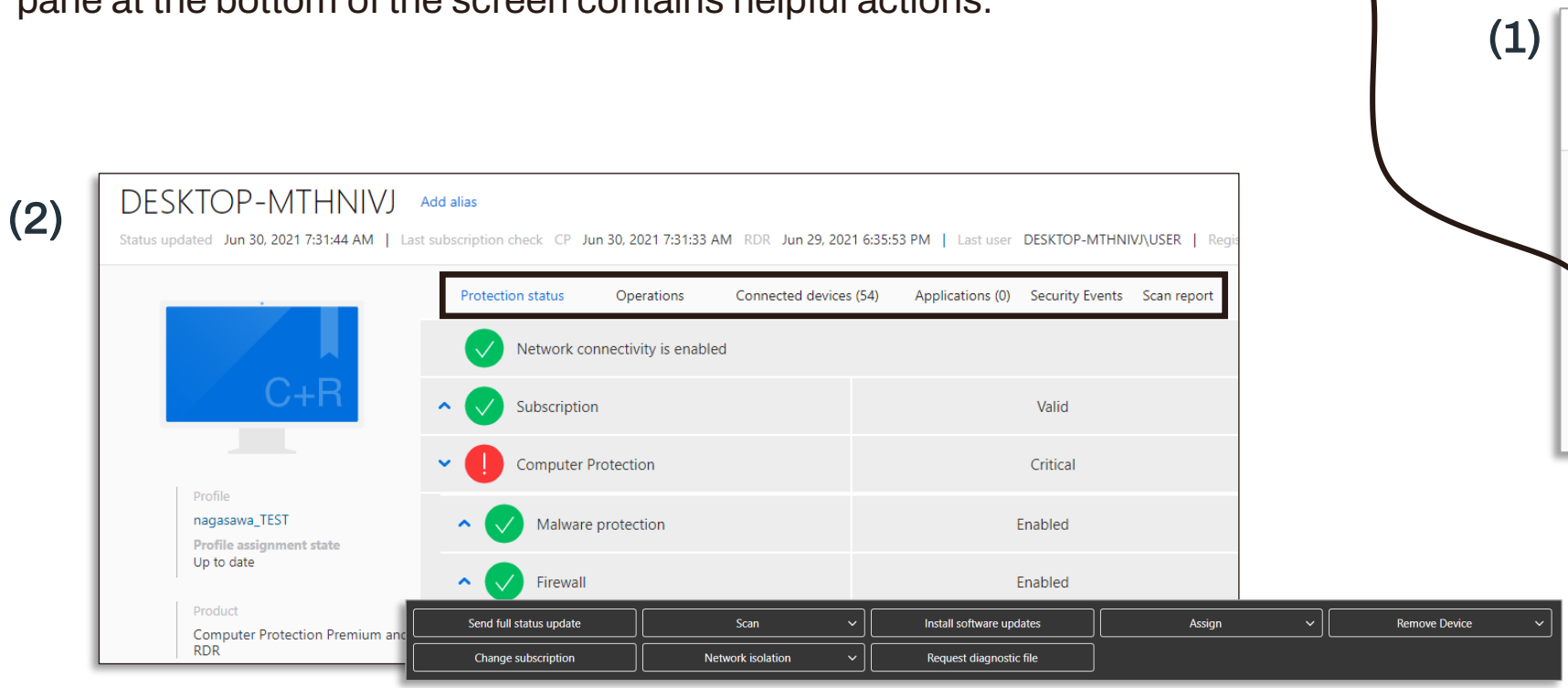


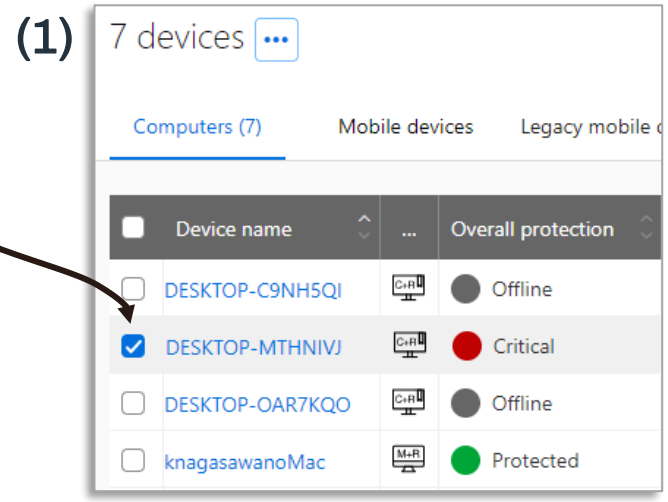


WITH secure

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.

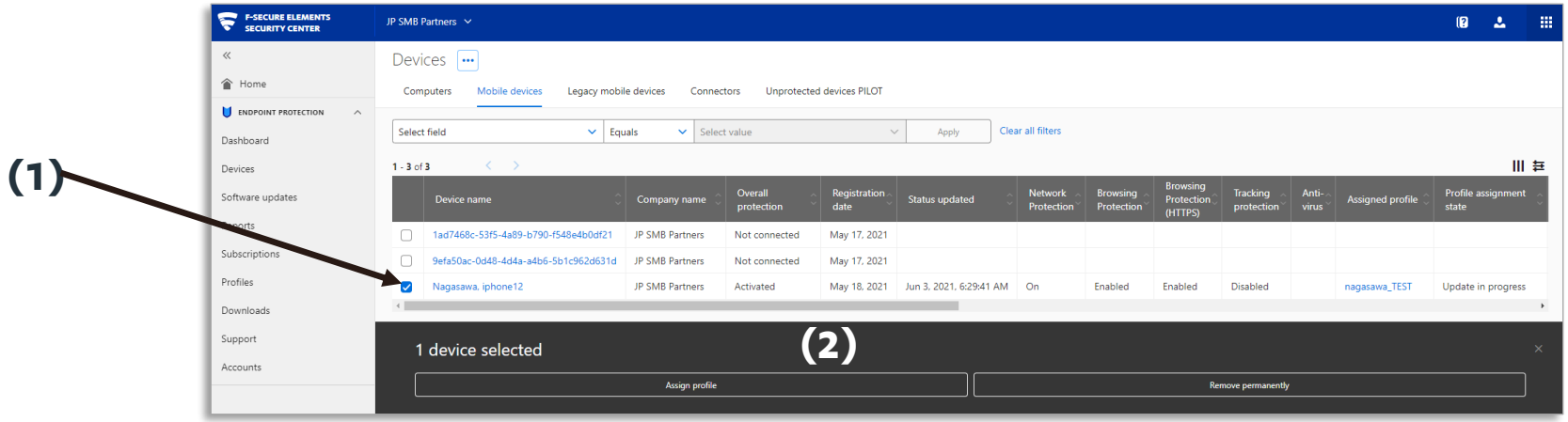




WITH secure

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.



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

WITH secure

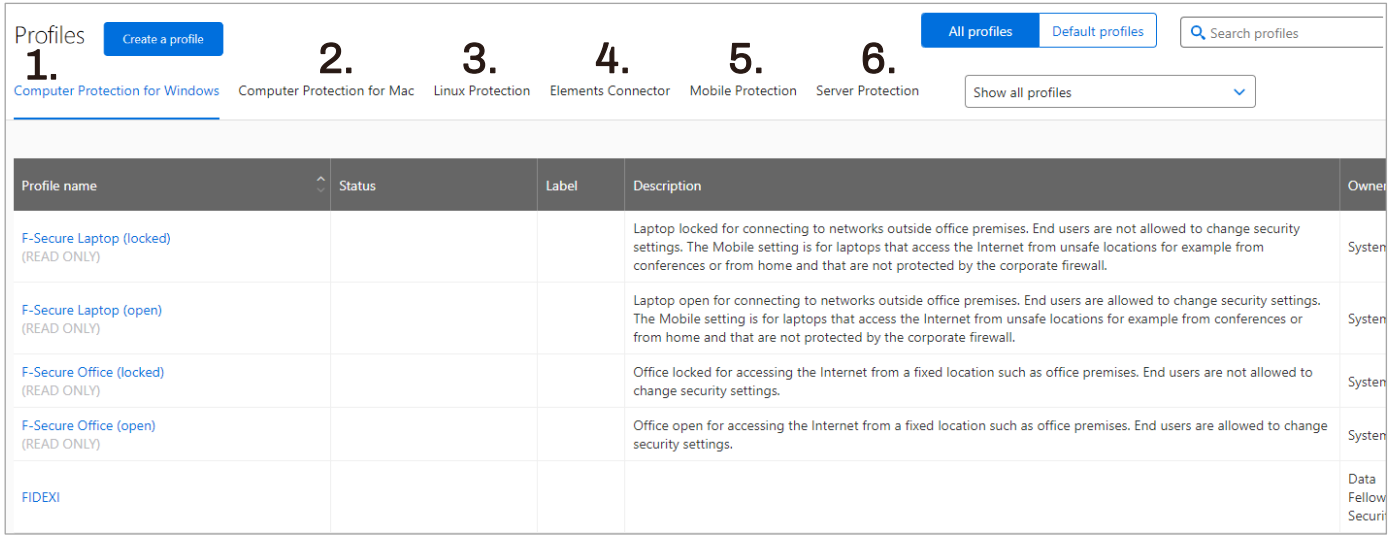
Profile editor

Elements ESC portal

WITH secure

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).

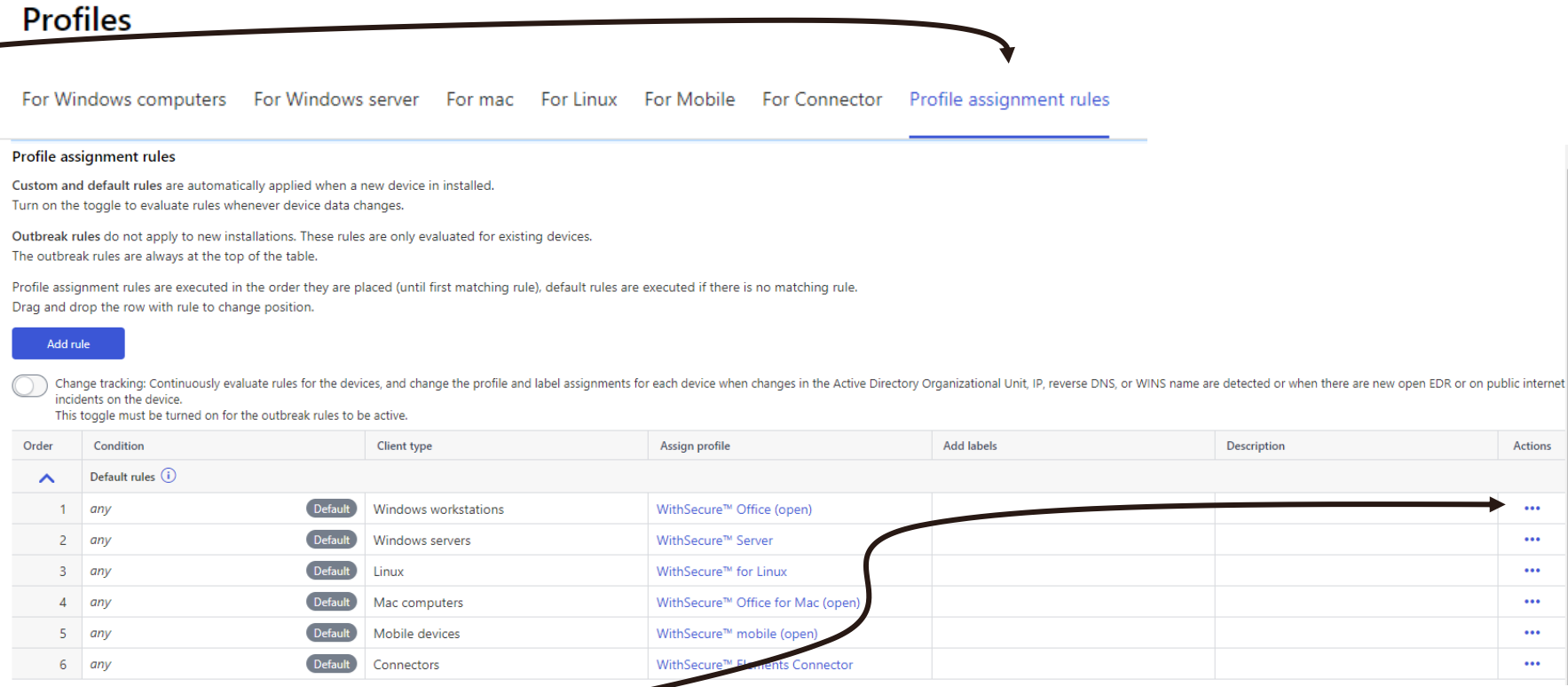


WITH secure

Default Profile

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

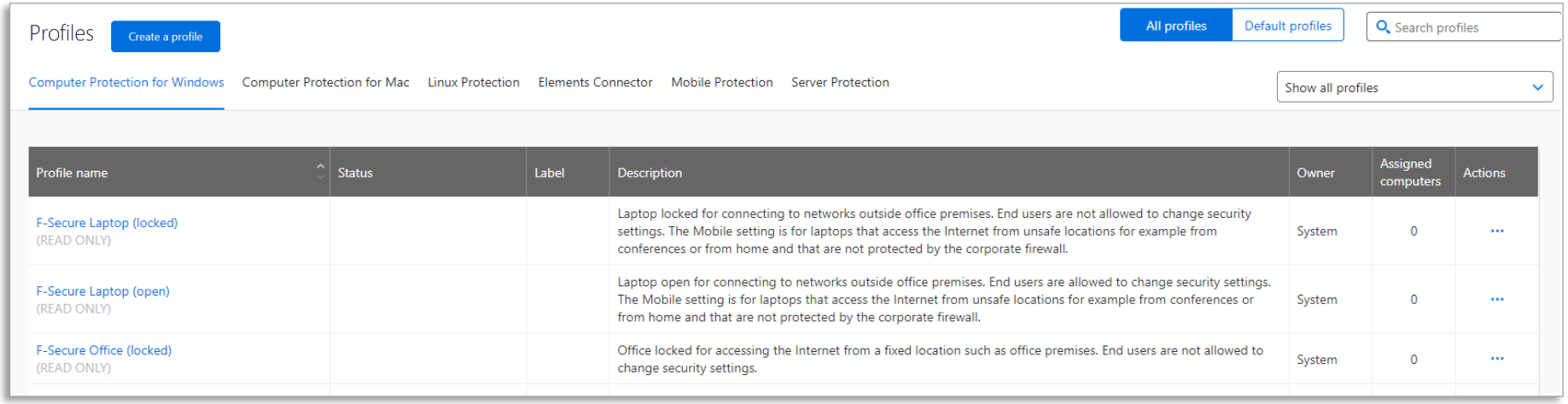
- You can set the default profiles by selecting Profile assignment rules from the top of the Profiles page.



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

Managing Profiles

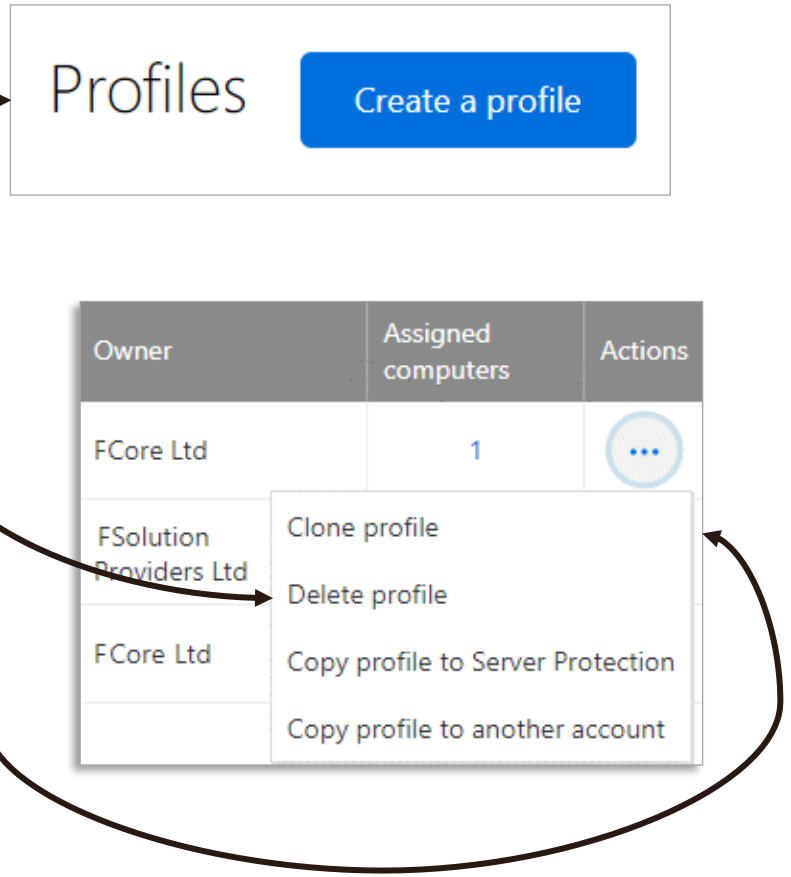
- Back under the general Profiles view, choose from the Computer Protection for Windows, Computer Protection for Mac, Linux Protection, Elements Connector, Mobile Protection, or Server Protection tabs, found below the page title.
- **Note**: There is no inheritance in Computer or Server Protection profiles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



WITH secure

Creating, Editing, Cloning, And Deleting Profiles

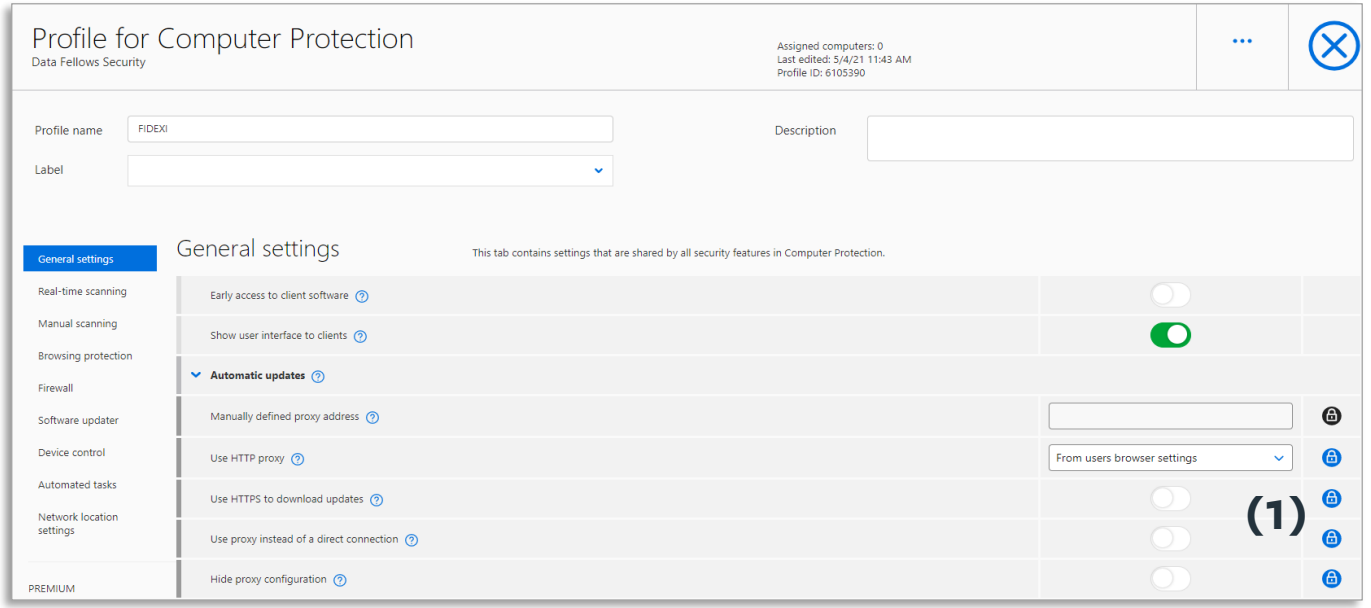
- To create a new profile, click the Create a profile button next to the page title.
- To delete a profile, click the ••• next to it, then select Delete profile.
- To edit a profile, click on its name in the profiles list.
  - You cannot edit or delete profiles marked as READ-ONLY.
    You can clone 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.



WITH secure

Editing Profile Settings

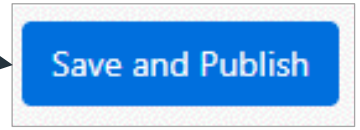
- In the profile editing window, you can change security settings for the EPP clients.
- Click the lock icon (1) to allow or prevent any user changes to the setting from local user interface: 
- If user changes are allowed, the users can freely change the setting regardless of how it is used in the profile.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



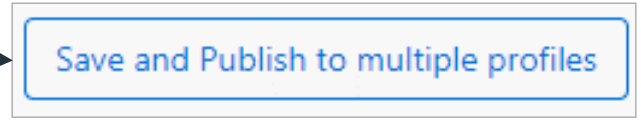
WITH secure

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.

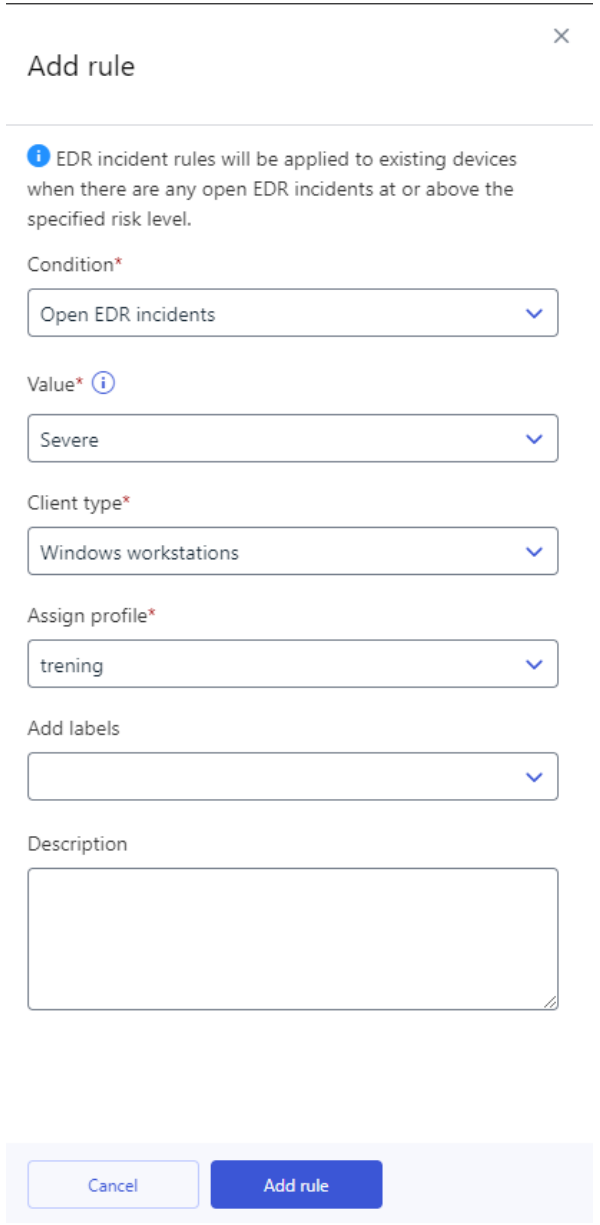


- ...or click X on the top right corner to cancel any changes.

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.

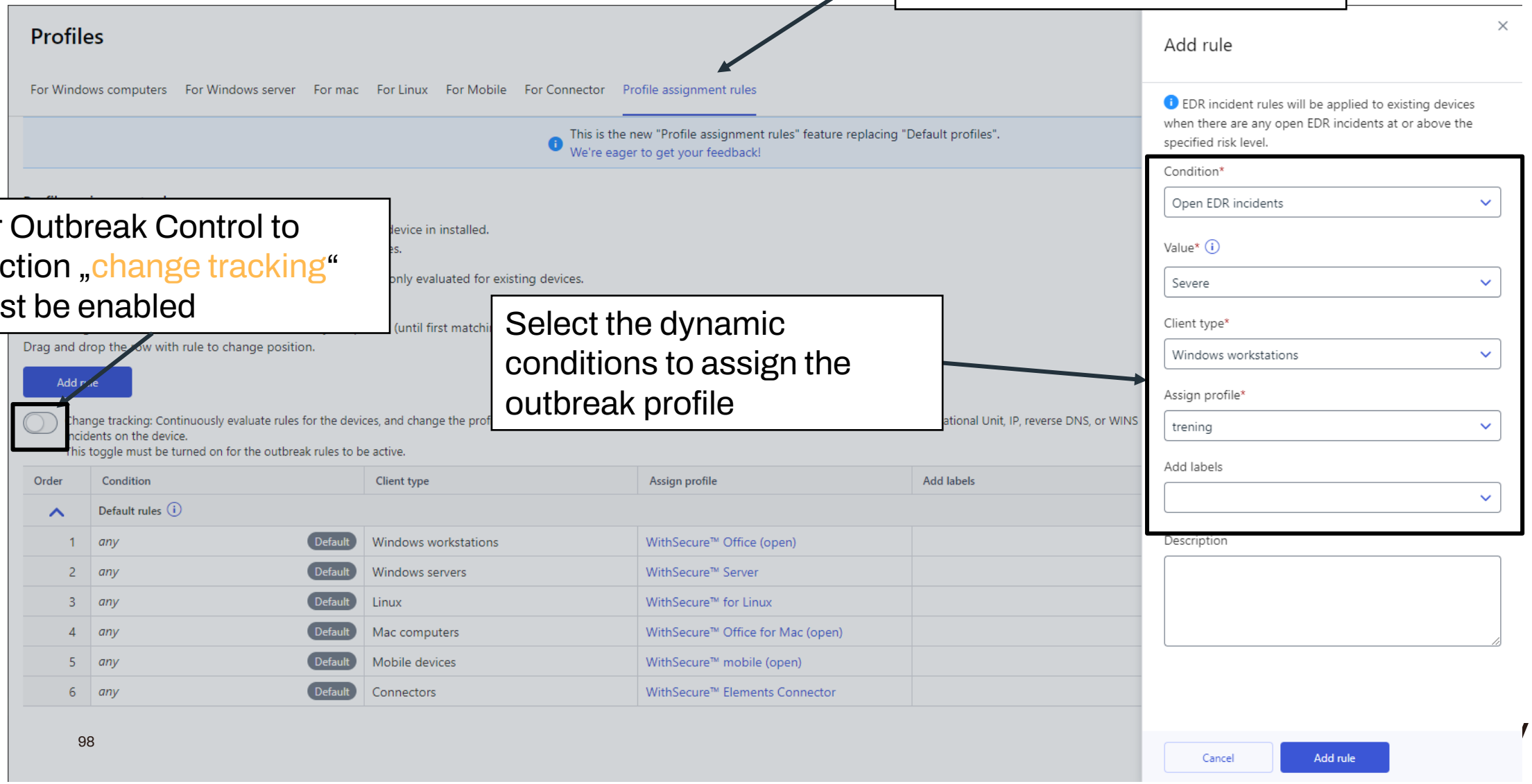


Outbreak Control

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



Operacije in profili

Elements EPP+EDR for Computers Premium

WITH secure

Operacije in profili

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

Profile settings

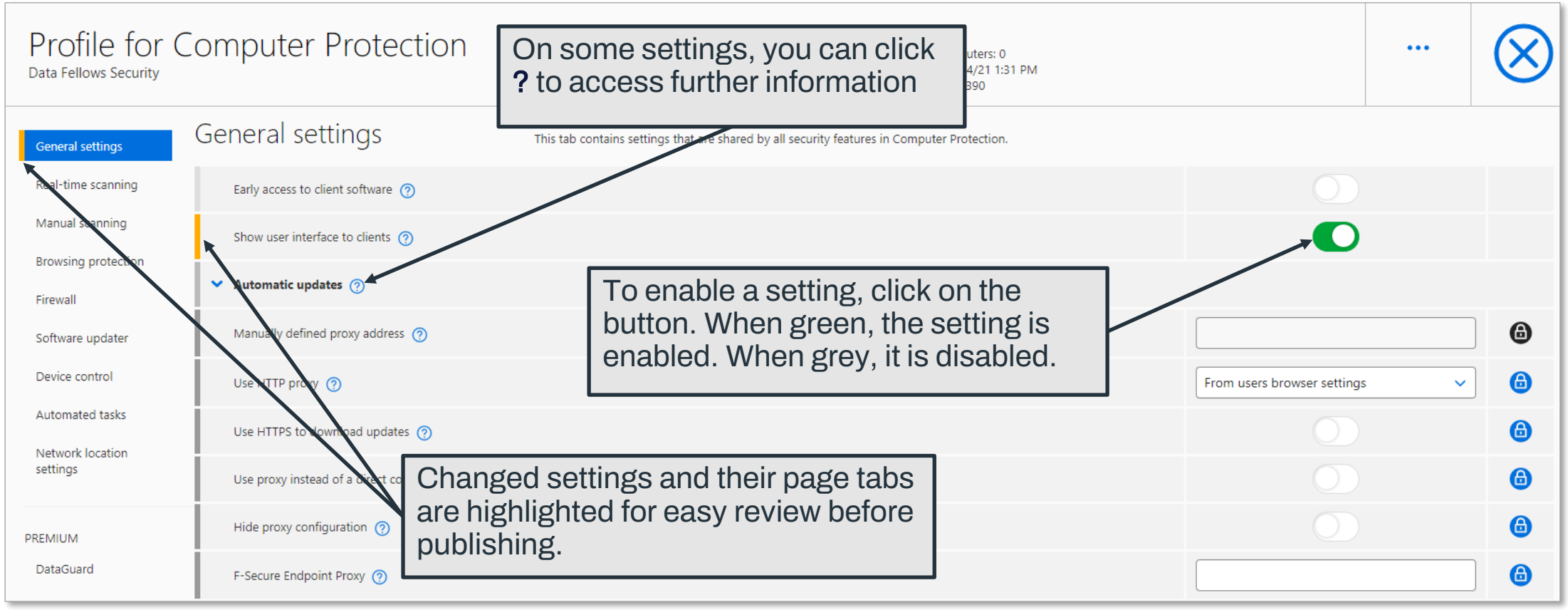
Elements ESC portal

WITH secure

Elements EPP Profiles

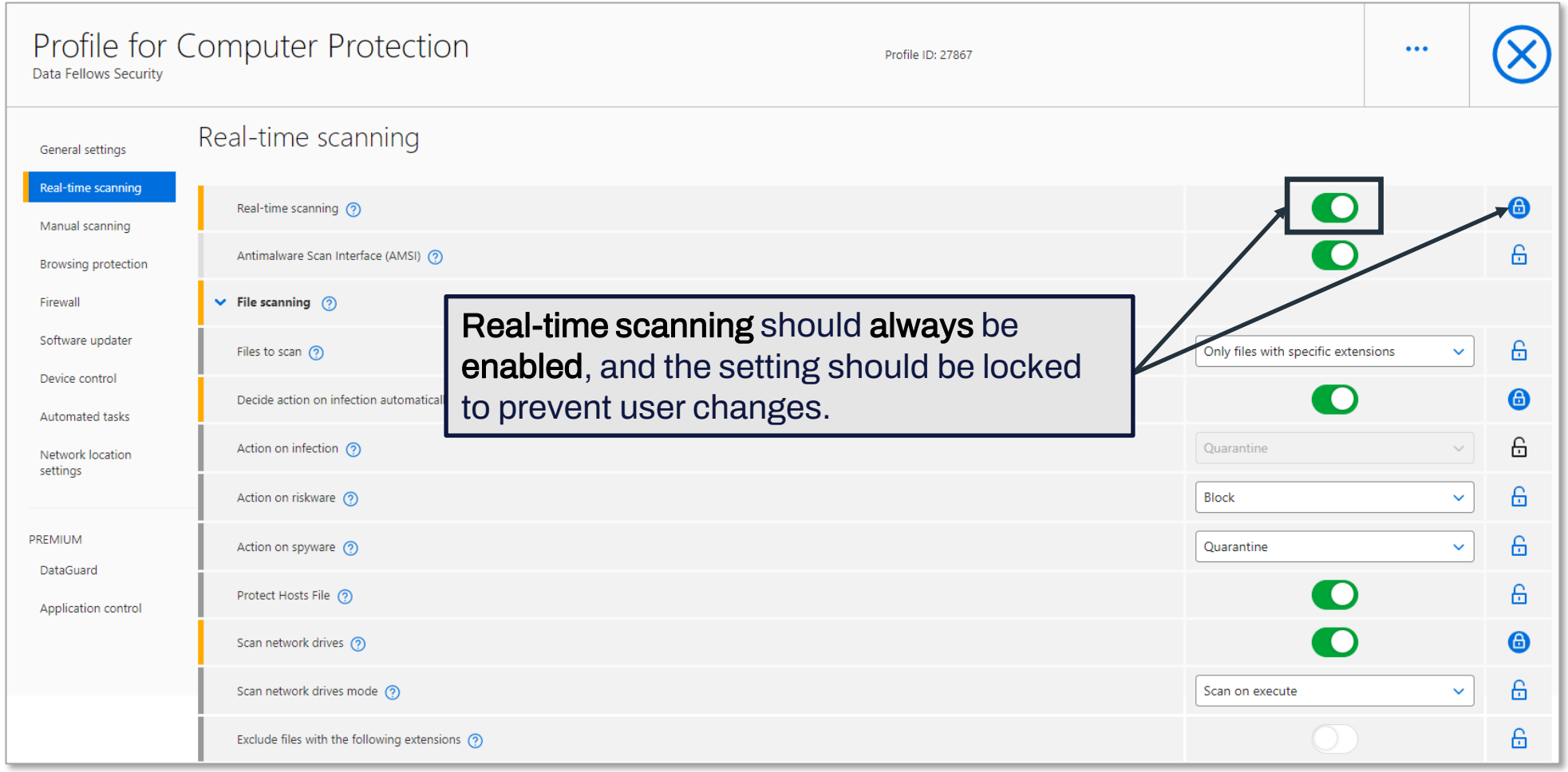
Windows Computers and Servers

General Settings



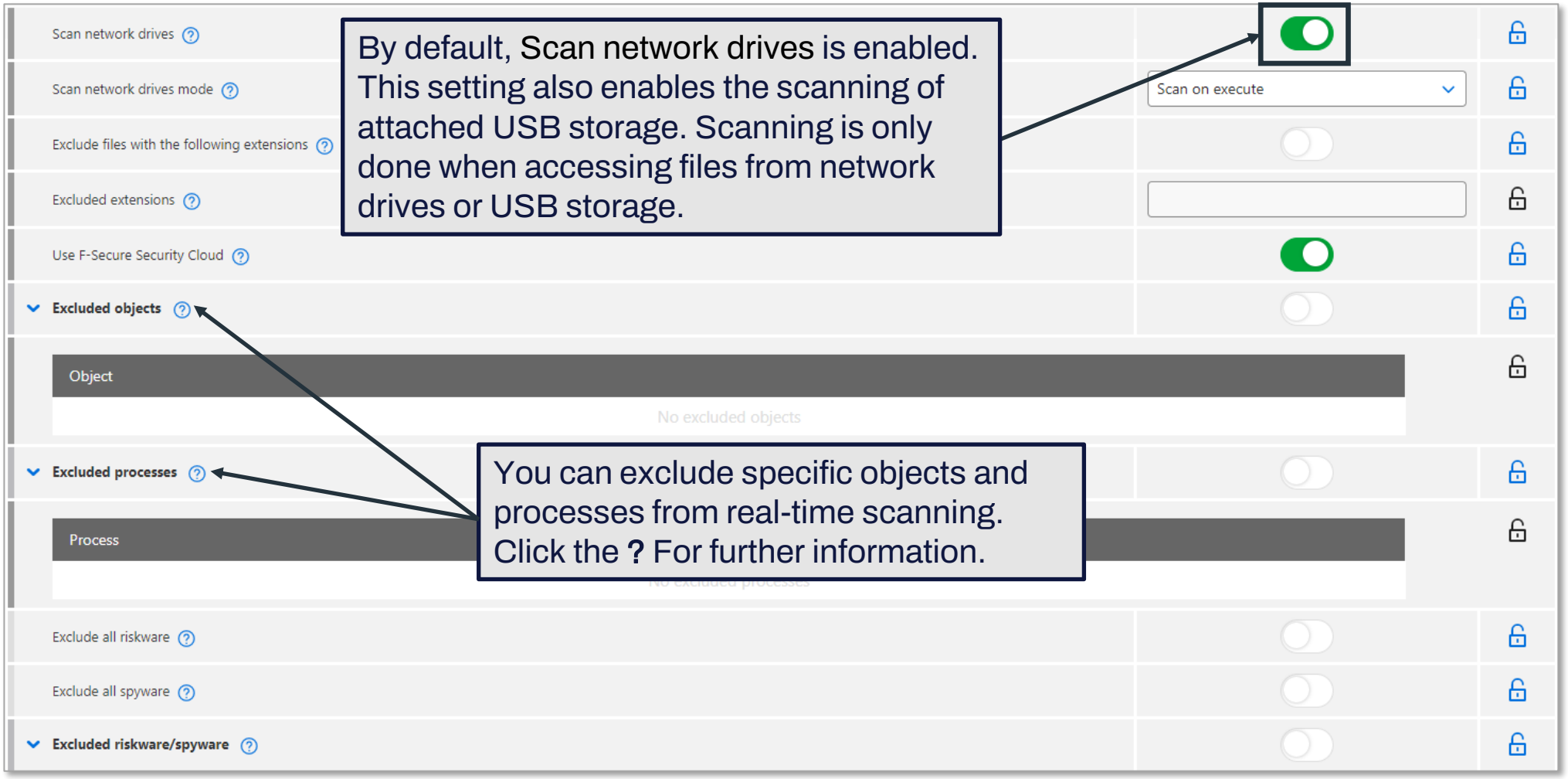
WITH secure

Real-time Scanning



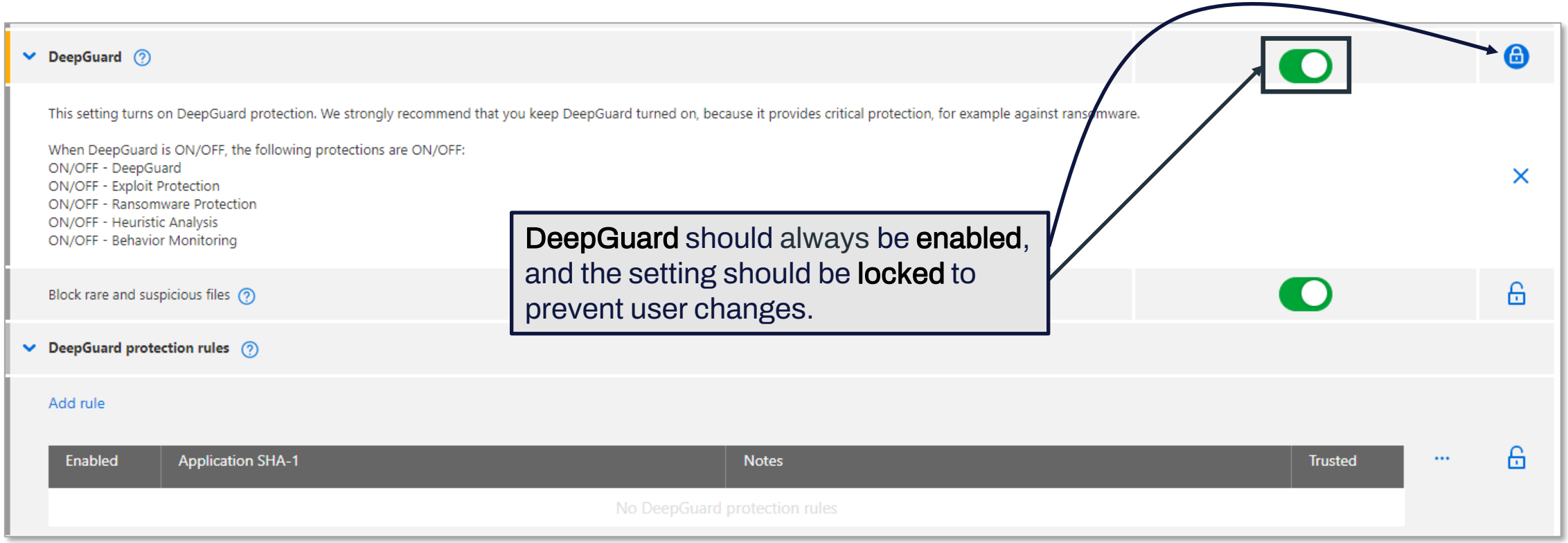
WITH secure

Real-time Scanning Continued



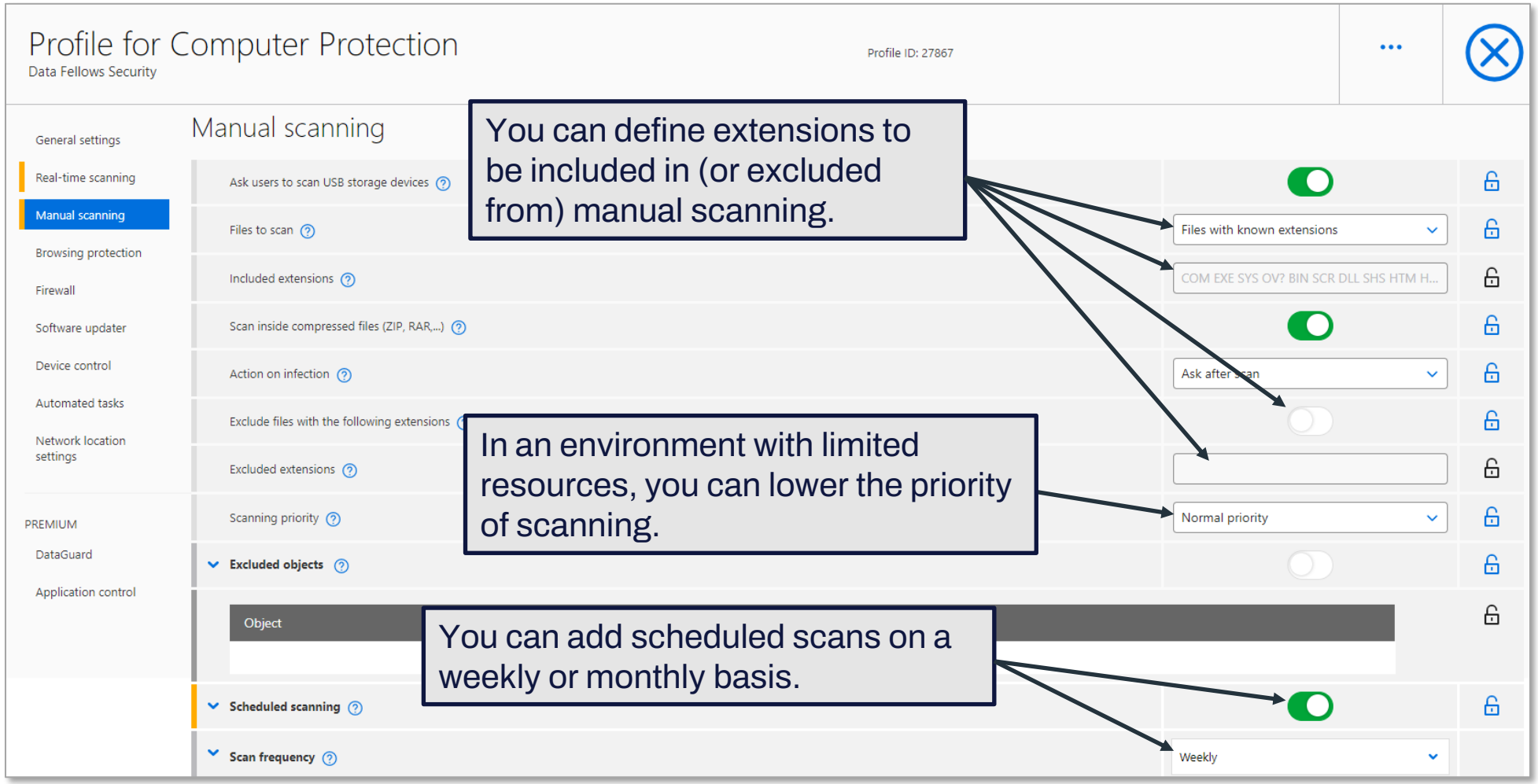
WITH secure

Real-time Scanning: Deepguard

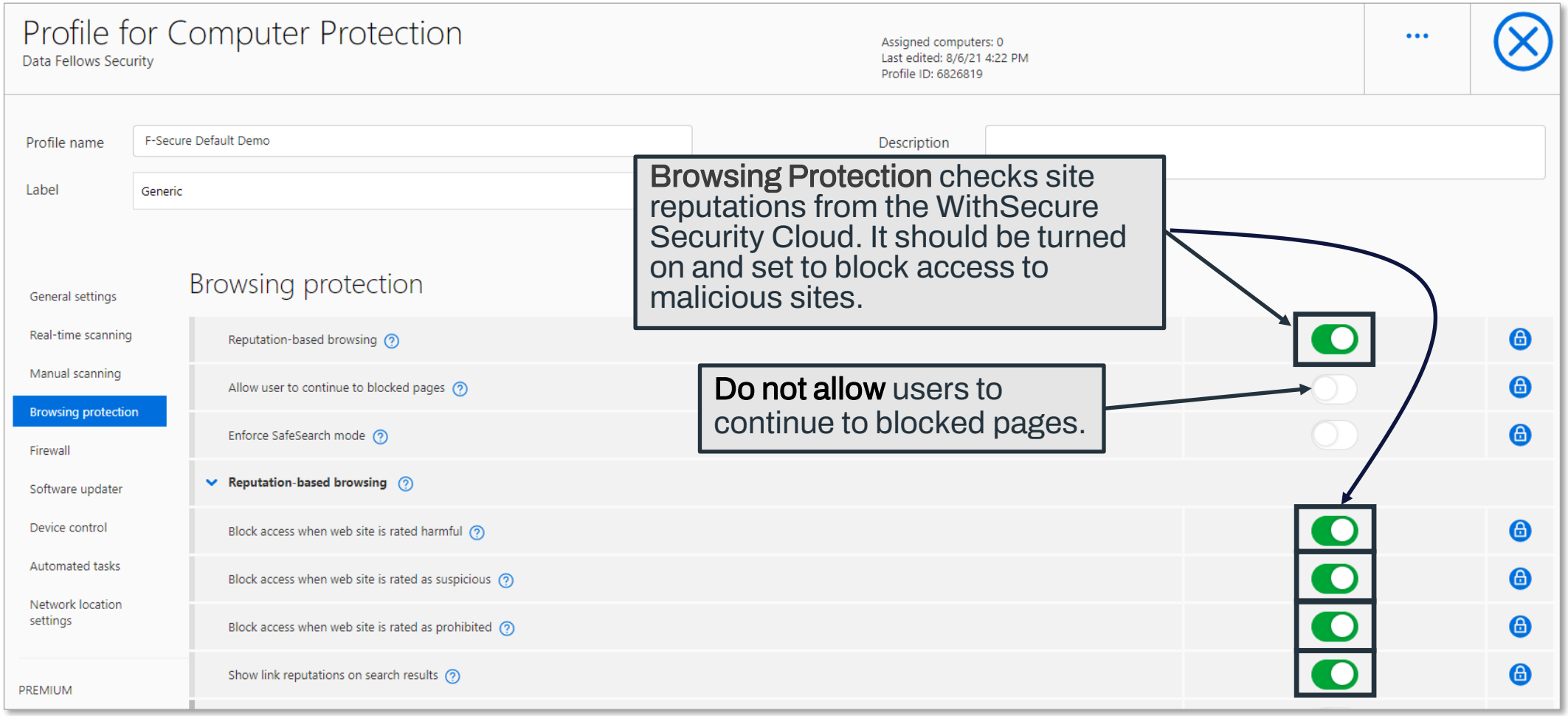


WITH secure

Manual Scanning

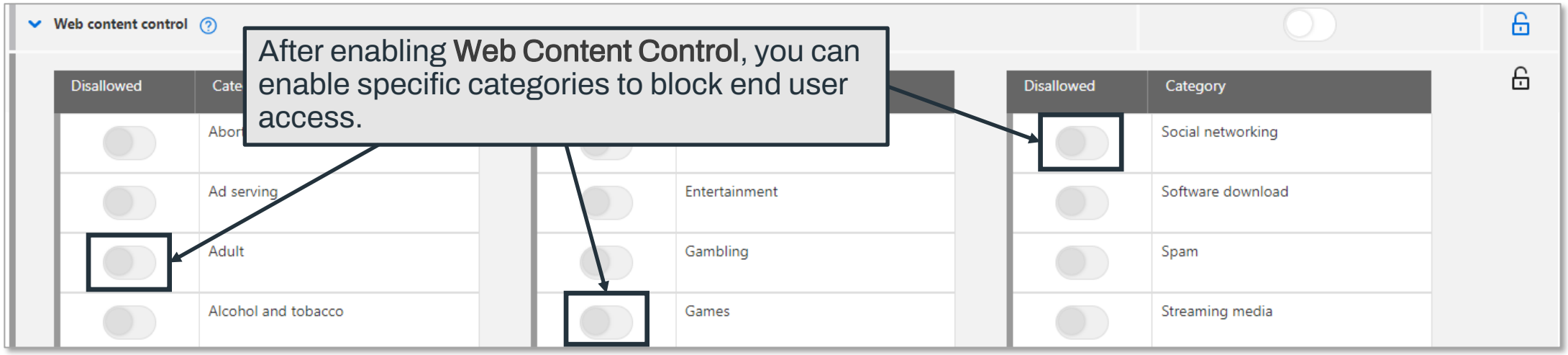


Browsing Protection



Browsing Protection: Web Content Control

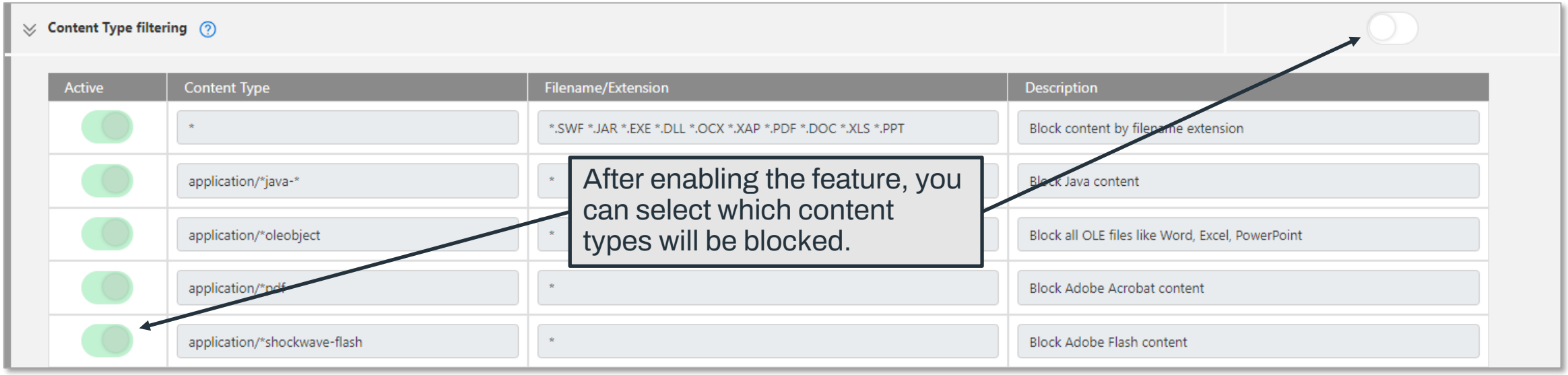
- Web Content Control, located in the Browsing Protection tab, allows administrators to block end users from entering sites. Choose what to restrict from 28 different categories (*such as adult, drugs, or spam*).
- Web Content Control is disabled by default.



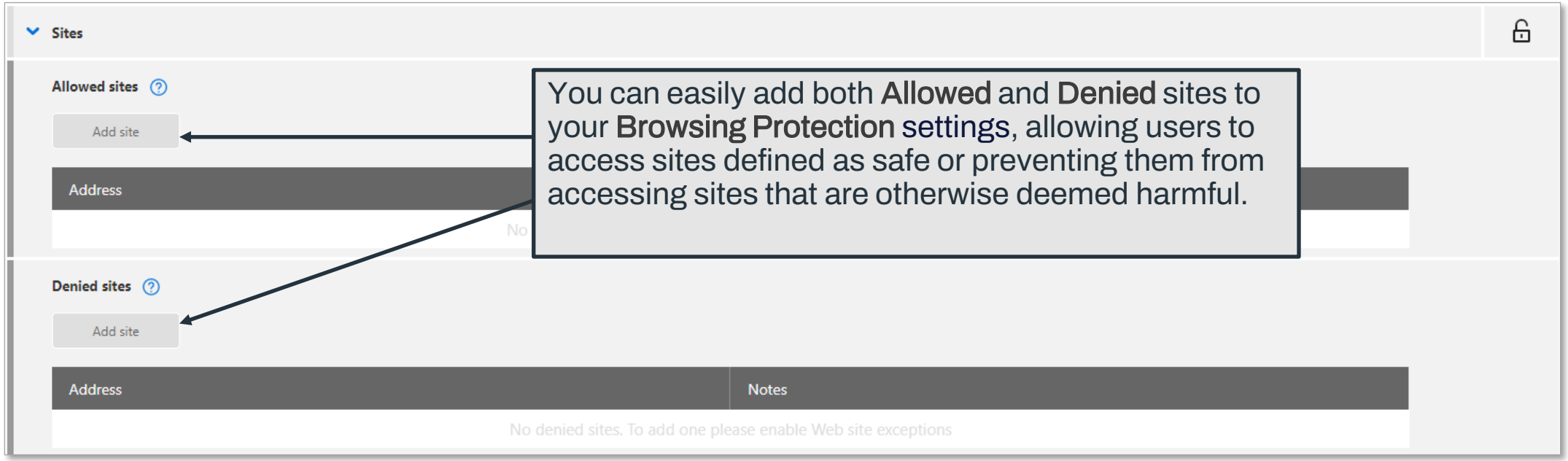
WITH secure

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.



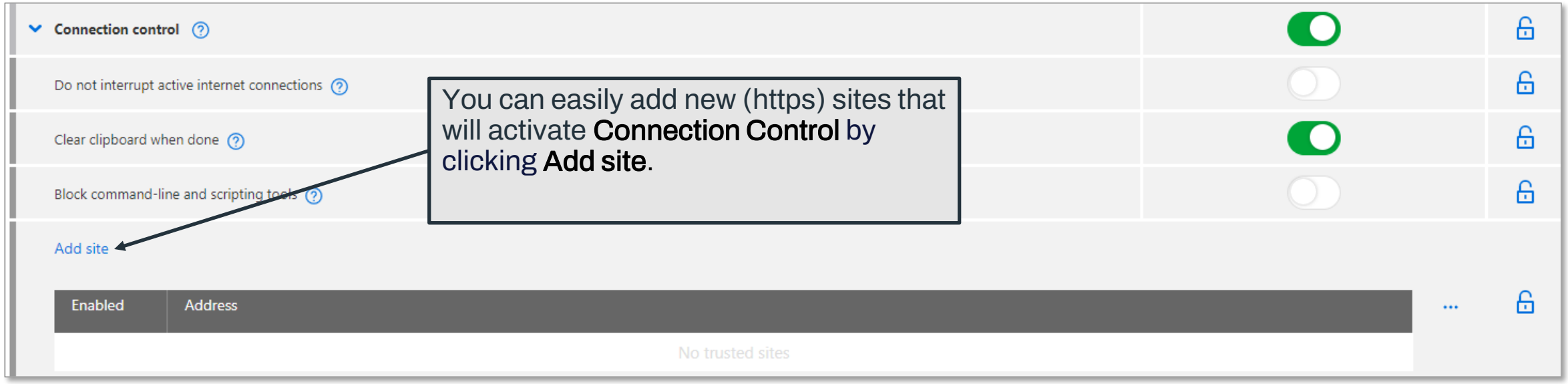
Browsing Protection:
Trusted / Blocked Sites



WITH secure

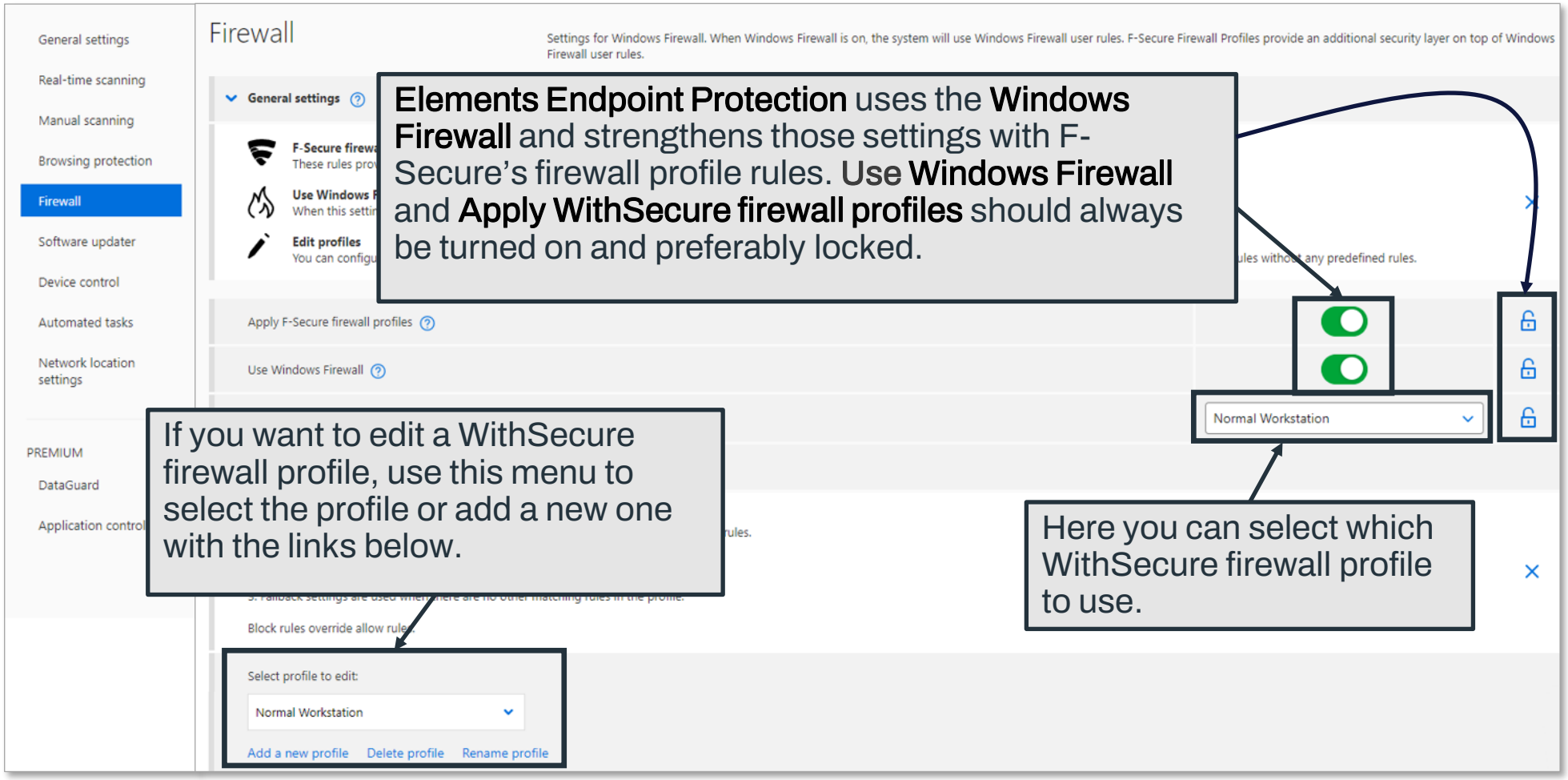
Browsing Protection: Connection Control

- 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.

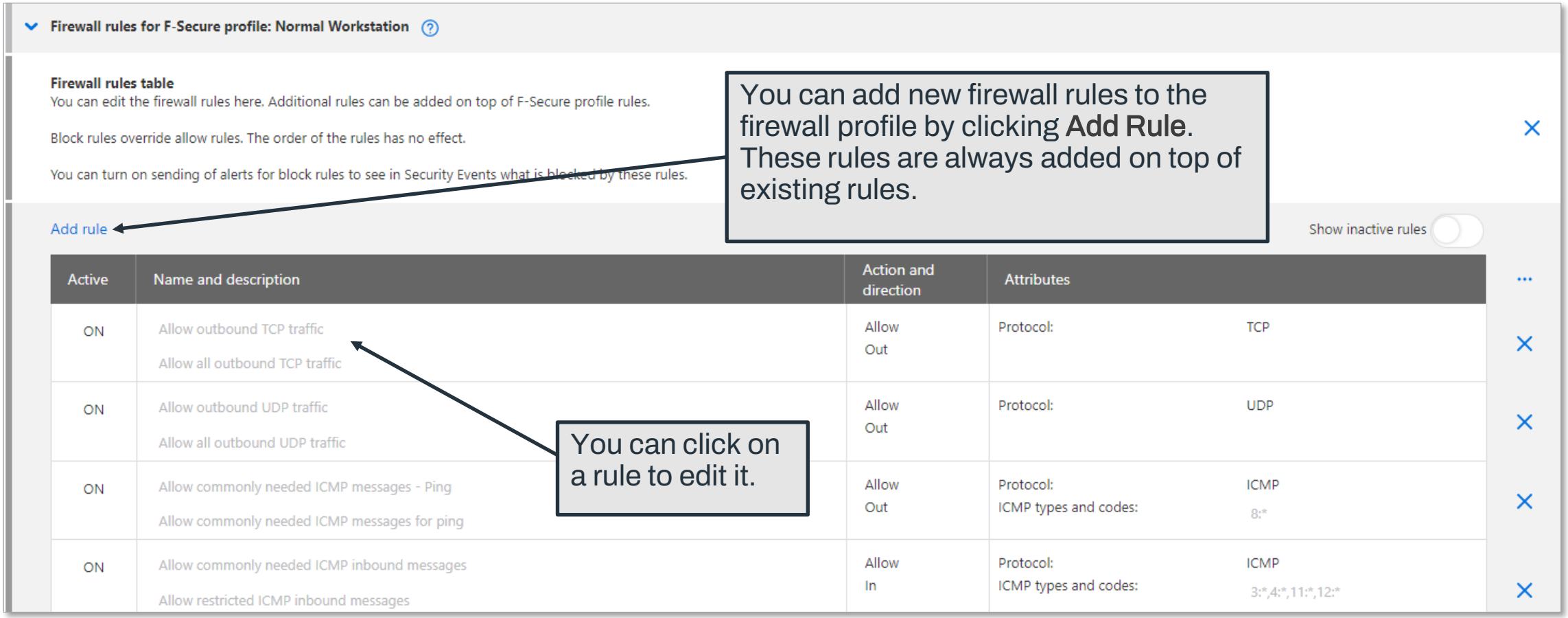


WITH secure

Firewall


General settings
Real-time scanning
Manual scanning
Browsing protection
Firewall
Software updater
Device control
Automated tasks
Network location settings
PREMIUM
DataGuard
Application control
Firewall
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.
General settings
Edit profiles
Apply F-Secure firewall profiles
Use Windows Firewall
Normal Workstation
Block rules override allow rules
Select profile to edit:
Normal Workstation
Add a new profile
Delete profile
Rename profile
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.

Firewall Rules

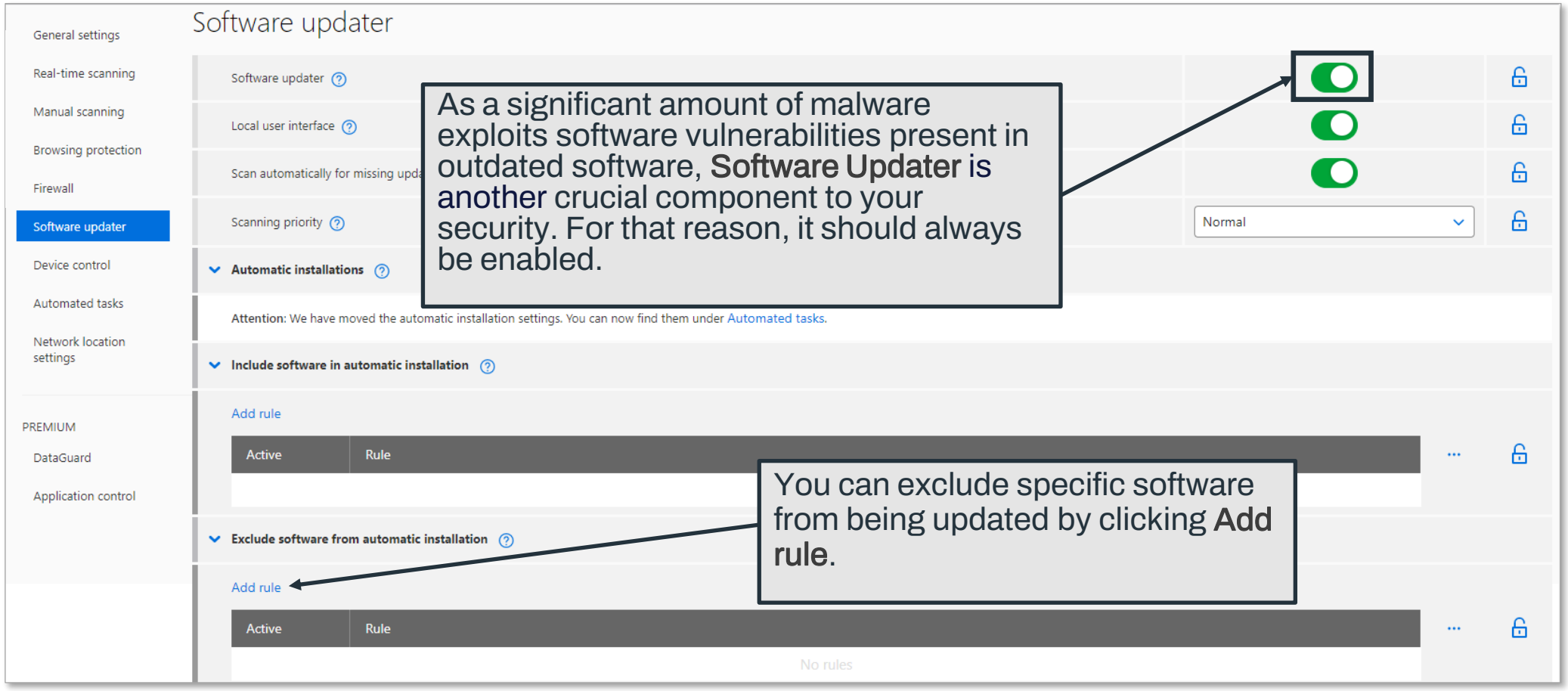


WITH secure

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.

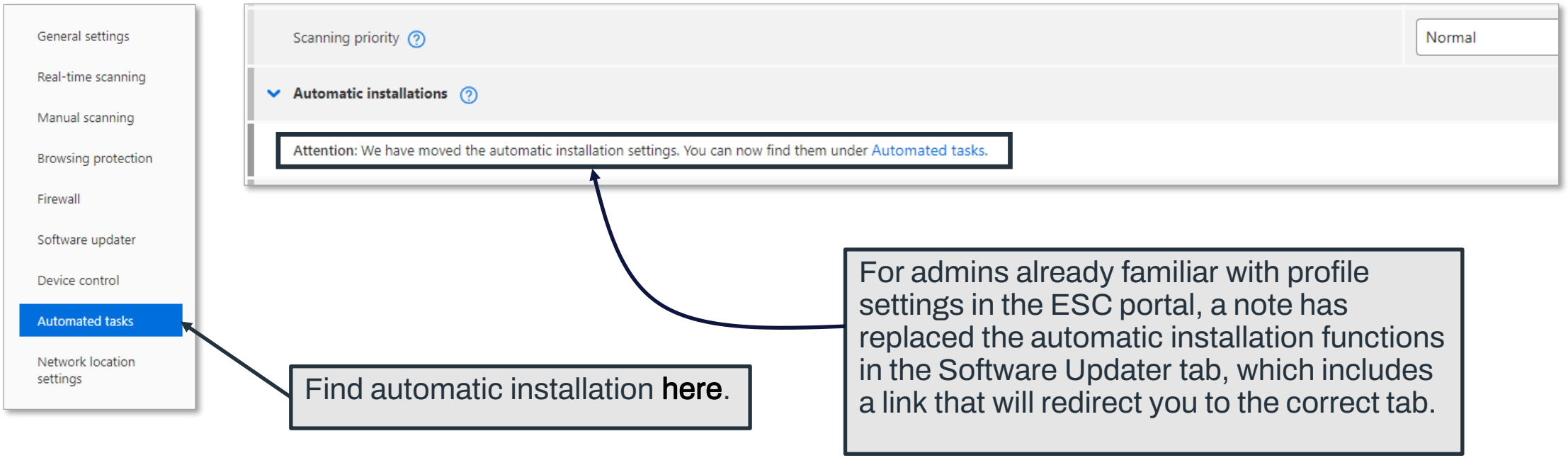
Software Updater



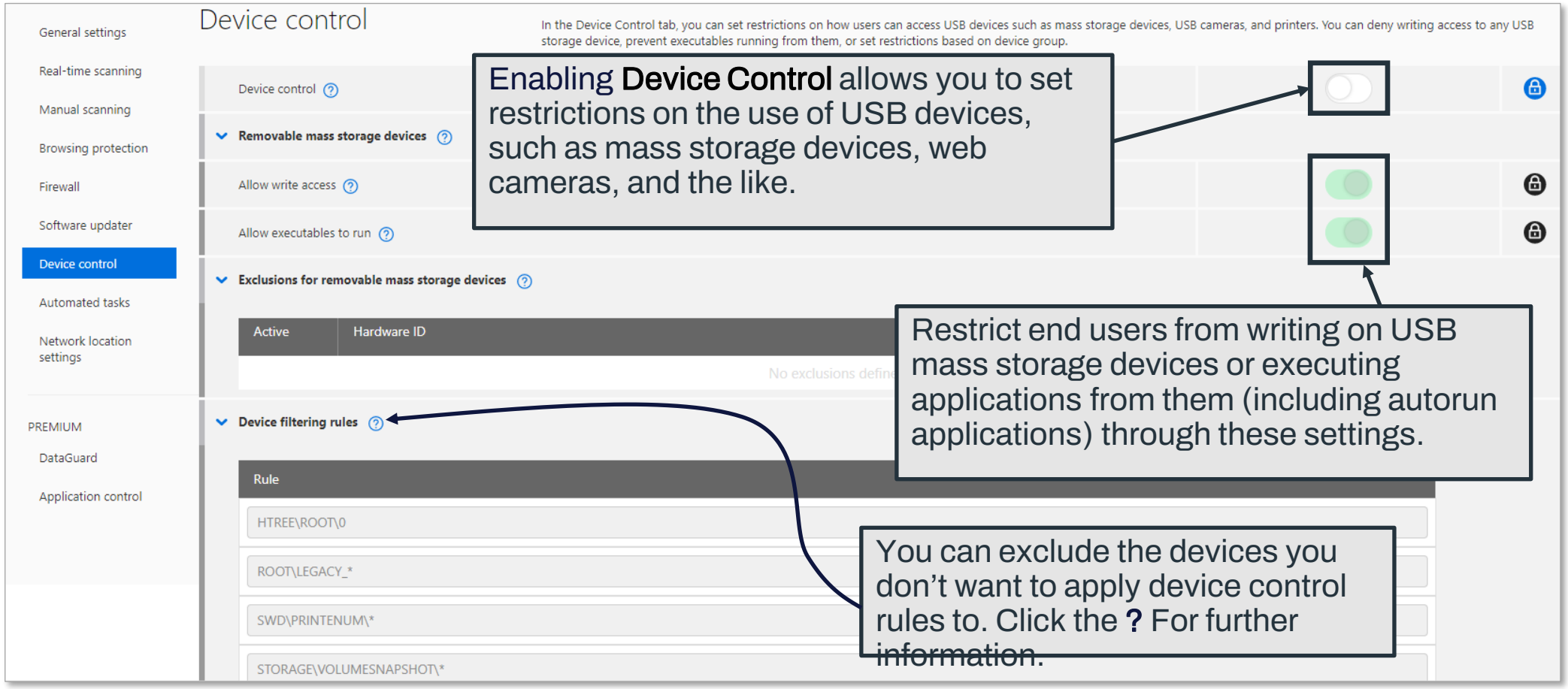
WITH secure

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.

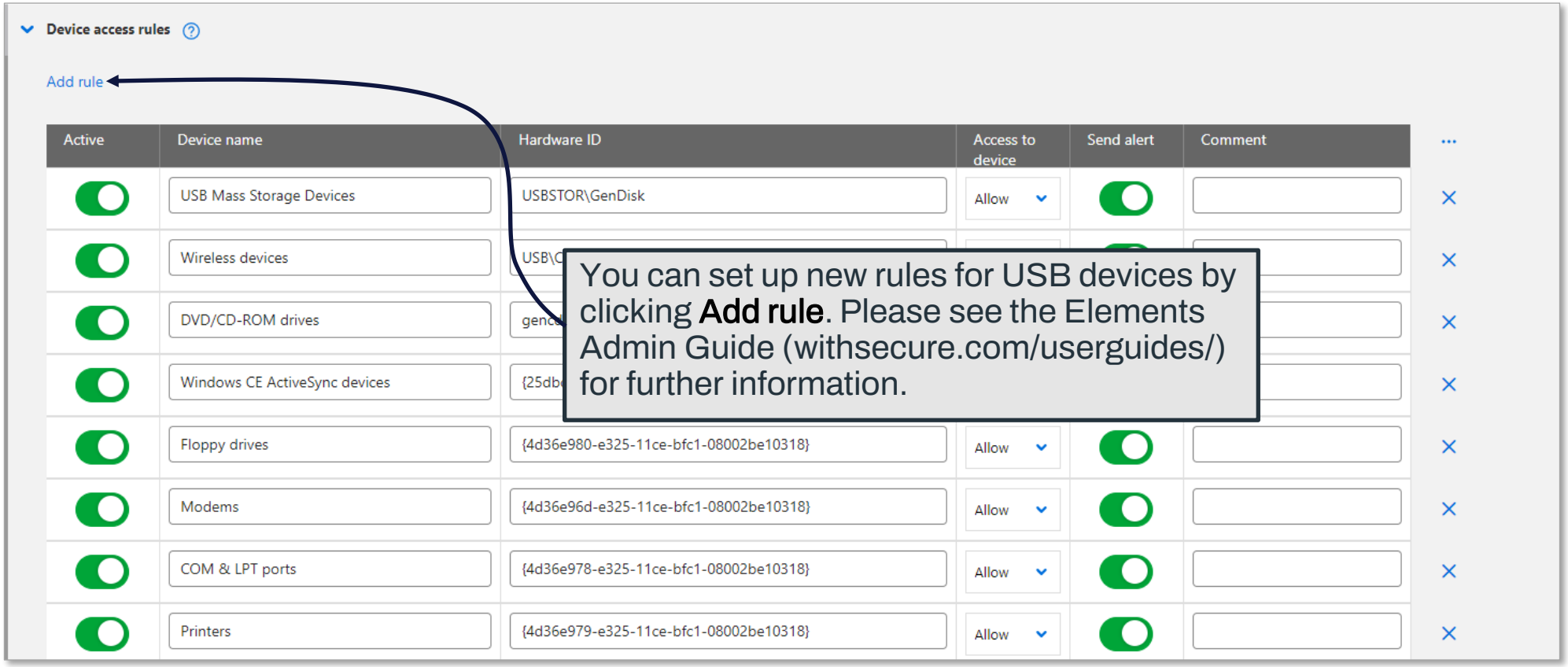


Device Control



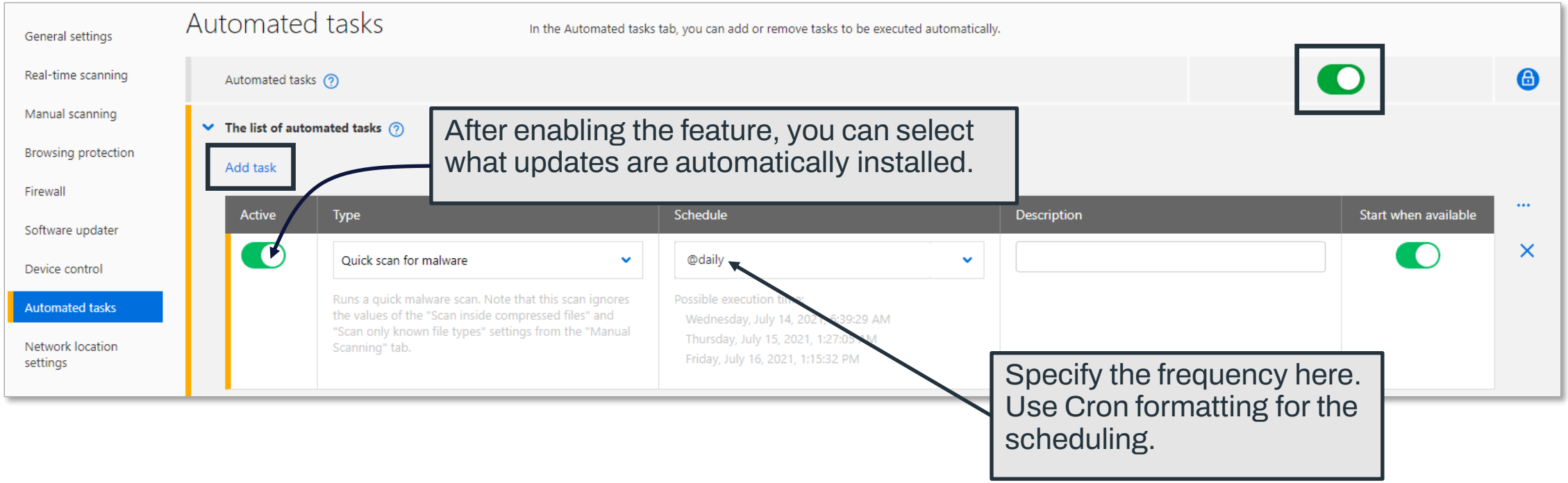
WITH secure

Device Control
Access Rules



Automated Tasks

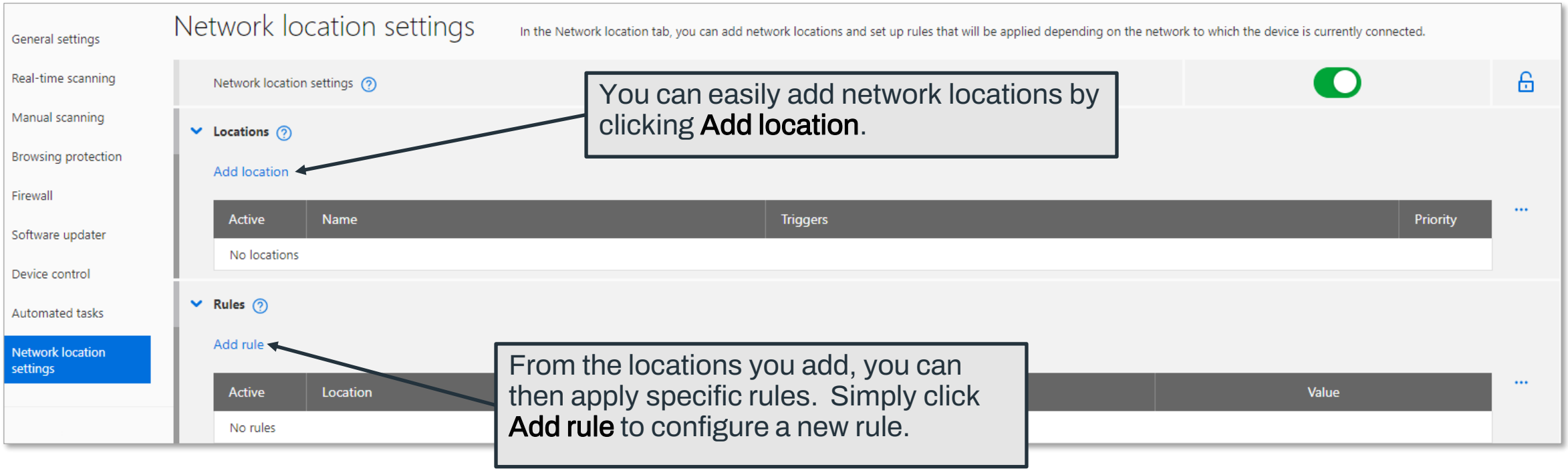
- Once you enable Automated tasks, Add task becomes visible. Click it to add a new automated task to the list. Activate or deactivate your tasks as needed.



WITH secure

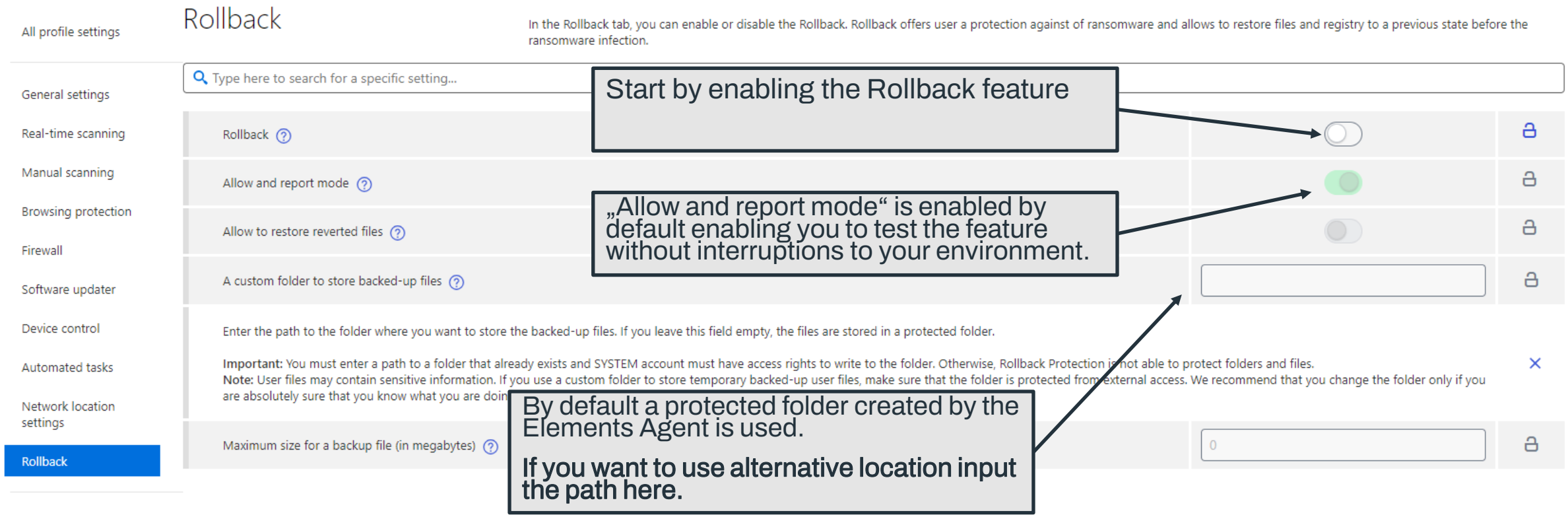
Network Location

- 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.

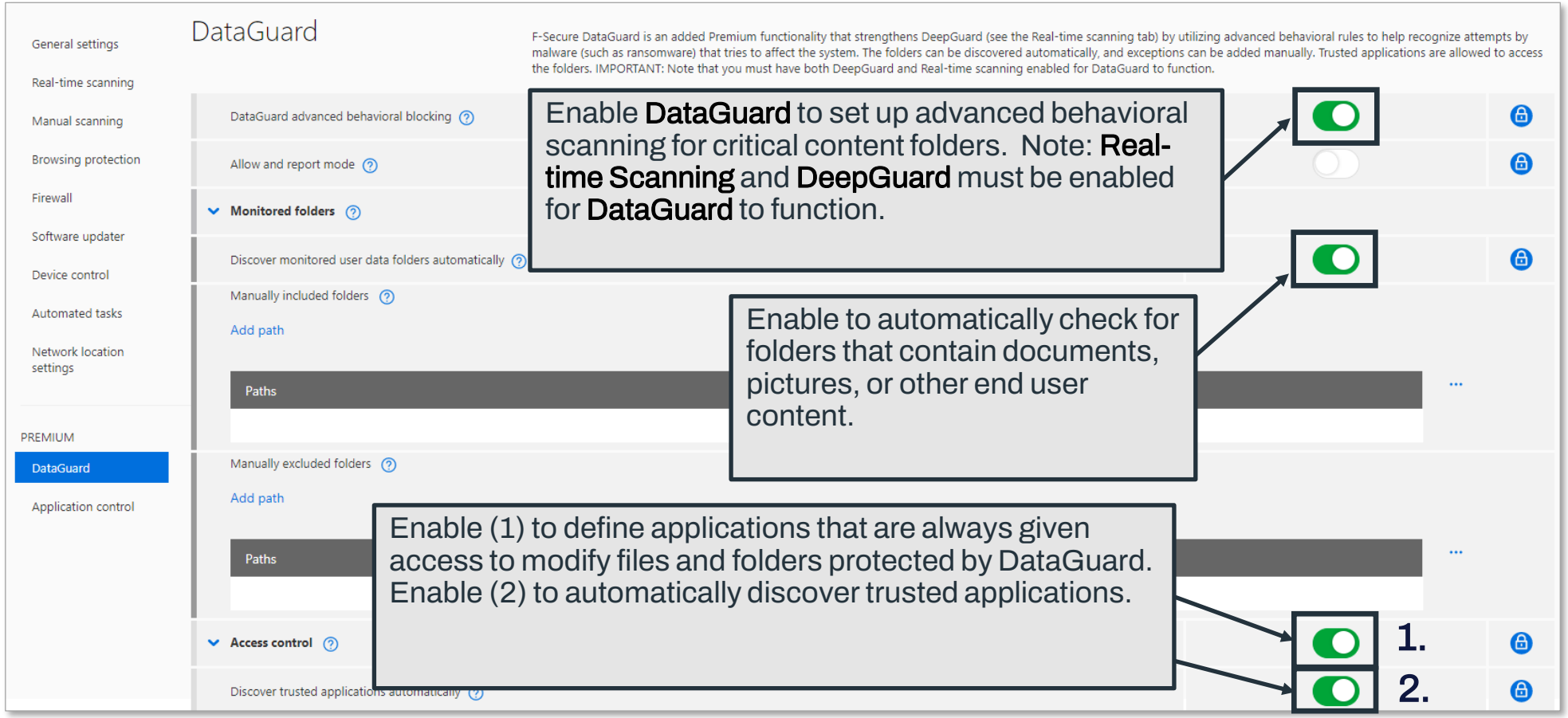


Rollback

- 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.



Dataguard
Premium Feature



WITH secure

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\

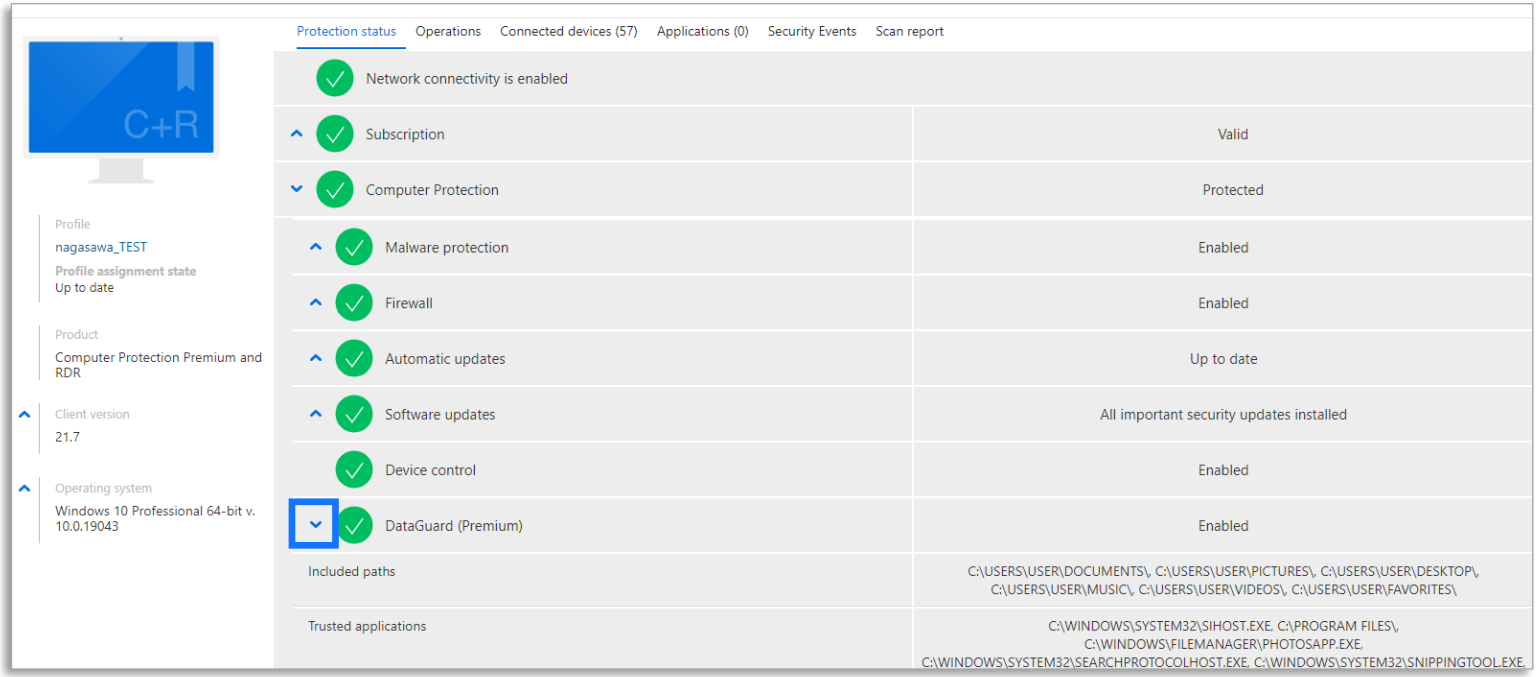
Automatically Trusted Applications

- 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\SYSWOW64\MSPAINT.EXE, C:\WINDOWS\SYSWOW64\NOTEPAD.EXE, C:\WINDOWS\SYSTEM32\WFS.EXE, C:\WINDOWS\SYSWOW64\SEARCHPROTOCOLHOST.EXE, C:\WINDOWS\SYSWOW64\WRITE.EXE, C:\WINDOWS\SYSWOW64\PICKERHOST.EXE, C:\WINDOWS\NOTEPAD.EXE, C:\WINDOWS\SYSTEM32\MSPAINT.EXE, C:\WINDOWS\SYSWOW64\MSTSC.EXE, C:\WINDOWS\FILEMANAGER\PHOTOSAPP.EXE, C:\WINDOWS\WRITE.EXE, C:\WINDOWS\SPLWOW64.EXE, C:\PROGRAM FILES\, C:\WINDOWS\SYSWOW64\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

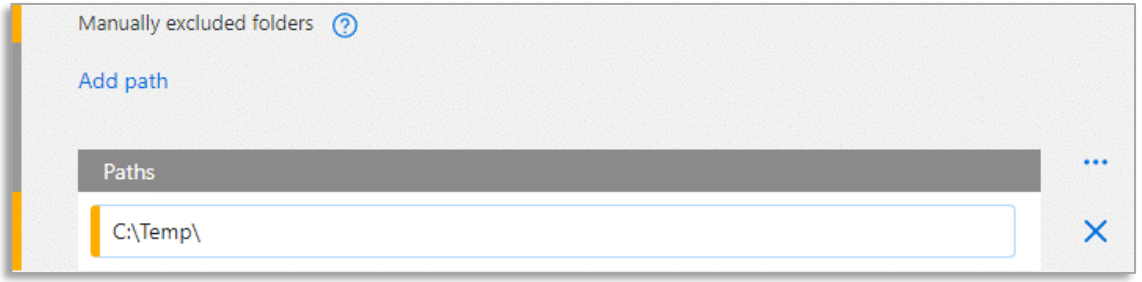
Checking Protected Folders And Applications

- 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.



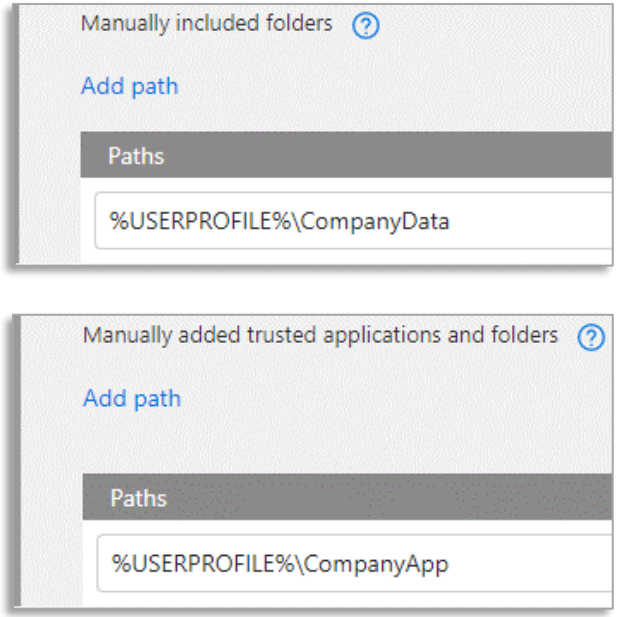
Including And Excluding Folders Manually

- 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

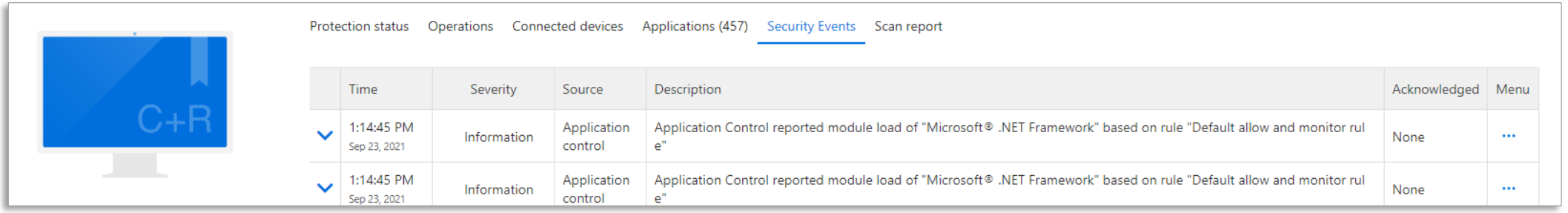
- Manually included and excluded folders and subfolders can be set based on Windows environmental variables.*
- The most common ones for DataGuard would likely be %USERPROFILE% (typically C:\Users\{username}).
- These can be used to define target path-based conditions, for example,
  to specify the user's 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.



WITH secure

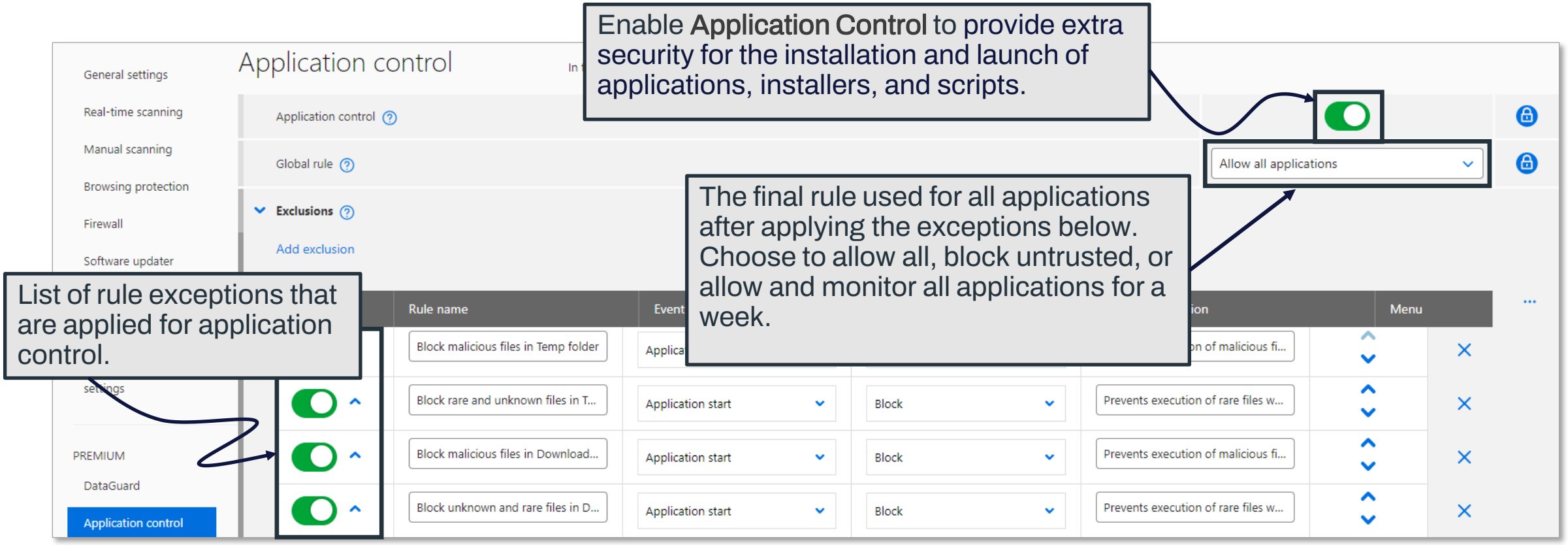
Blocked Modifications

- 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.



WITH secure

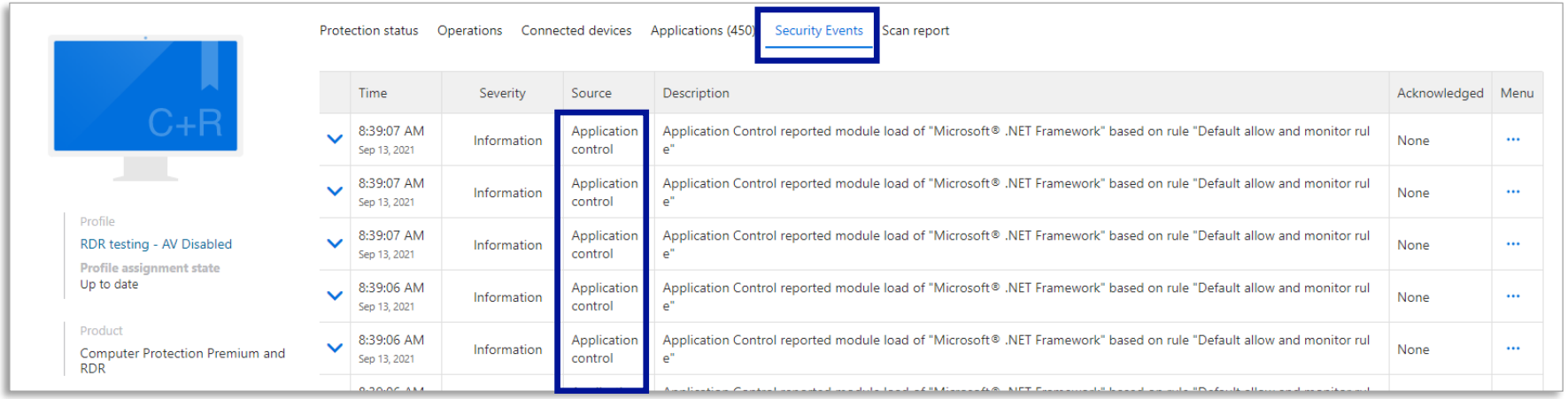
Application Control
Premium Feature



WITH secure

Blocking Applications

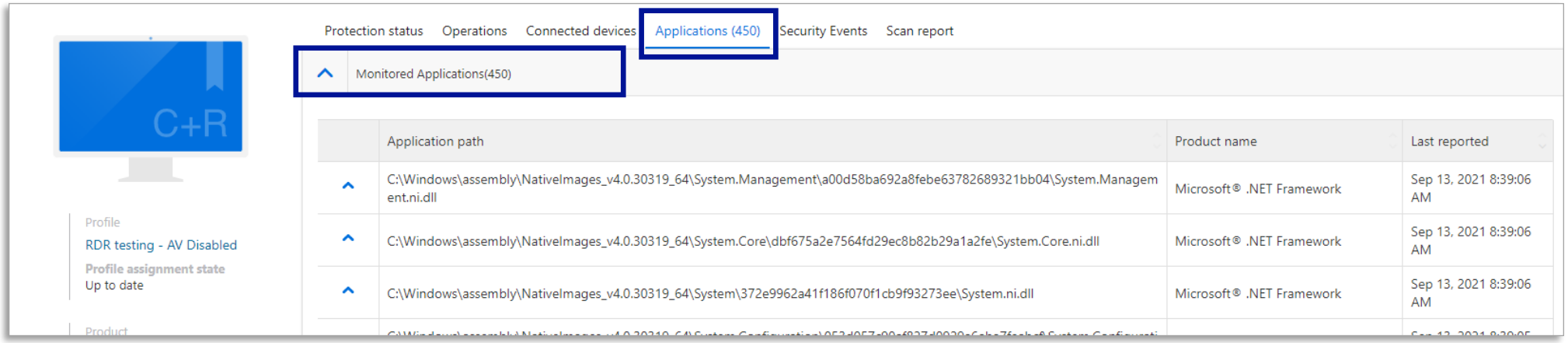
- The main use case for Application Control is to block applications from being used, using DLL files, and/or saving information on a device.
- If you have enabled block rules, the notifications for blocked application or blocked file access show on the device details page (Devices -> *click on a specific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



WITH secure

Block or Monitor?

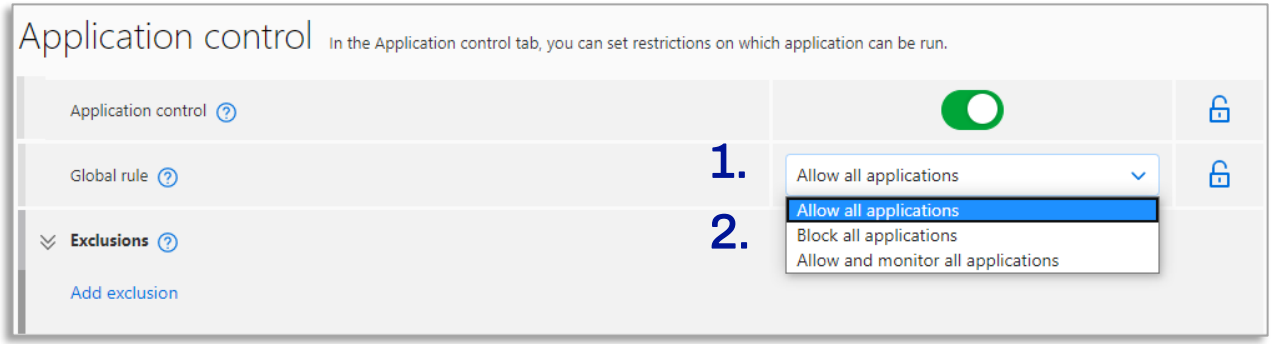
- At times, outright blocking an application is unnecessary, or you may wish to know more about it before taking action. So, Application Control can be set to temporarily monitor program and file access by selecting Allow and monitor all applications.
- When using a Monitor rule, notifications are shown 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.



WITH secure

Setting Up Rules: Global

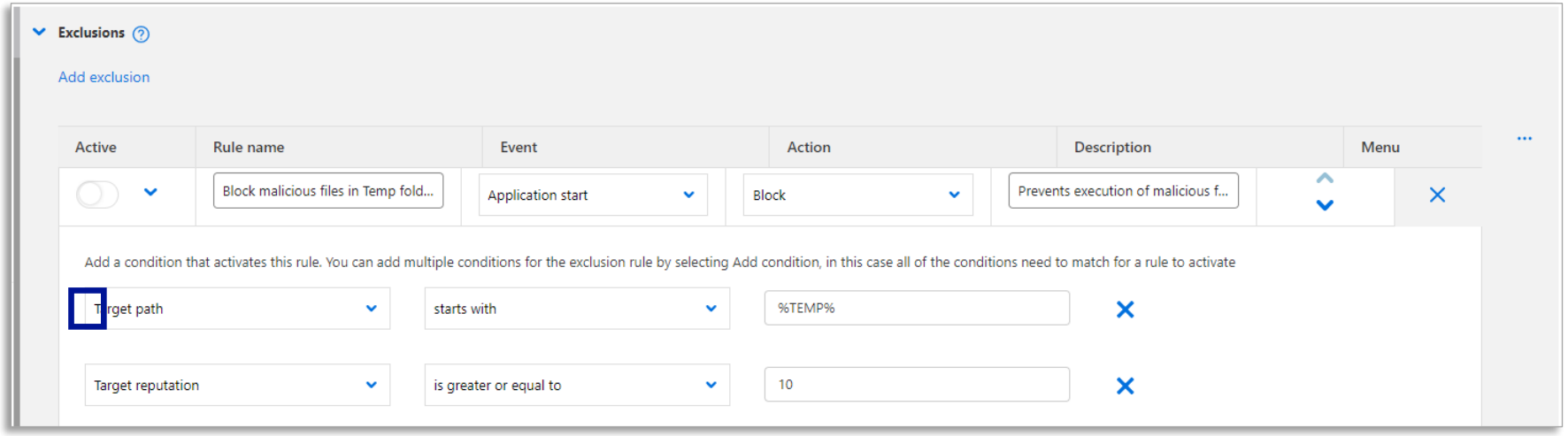
- In profile settings, select Application Control.
- Turn Application Control on (1). It is turned off by default.
- The Global Rule (2) defines how Application Control handles all applications except the exclusions, which will be discussed next. In typical environments, Allow all applications is the 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.



WITH secure

Setting Up Rules: Exclusions

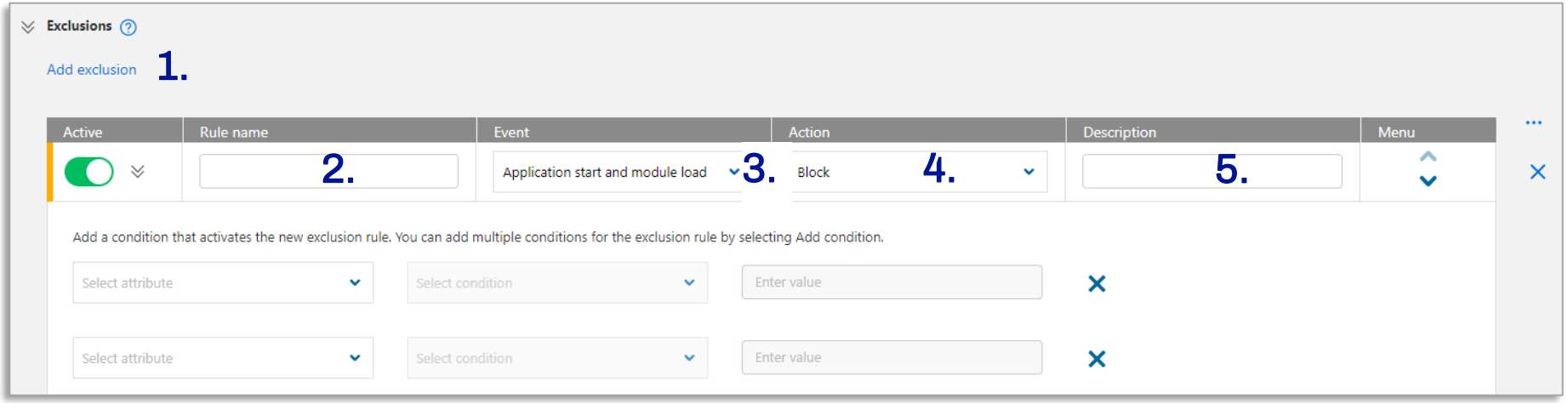
- You can set up exclusions to block or monitor the access to specific programs, programs that run in specific locations, and/or files accessed by different programs.
- The Profile editor has standard rules set up. You can enable these rules, edit them, and view them (by clicking the downward pointing 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*



WITH secure

Setting Up Rules: Exclusions #2

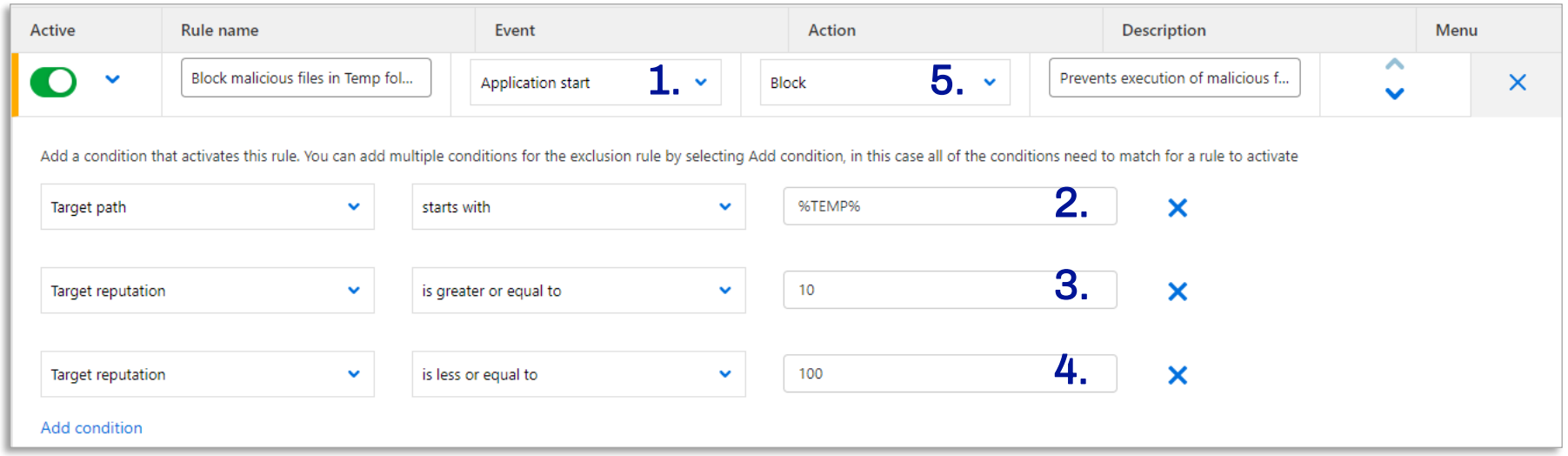
- You can add new exclusions by clicking Add exclusion (1) above the exclusions list.
- Give the rule a name (2) and description (5).
- From the dropdown, specify the event which invokes the rule (3).
- Set the action that will be done when the rule is invoked (4).
- **Note:** The order of exclusions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



WITH secure

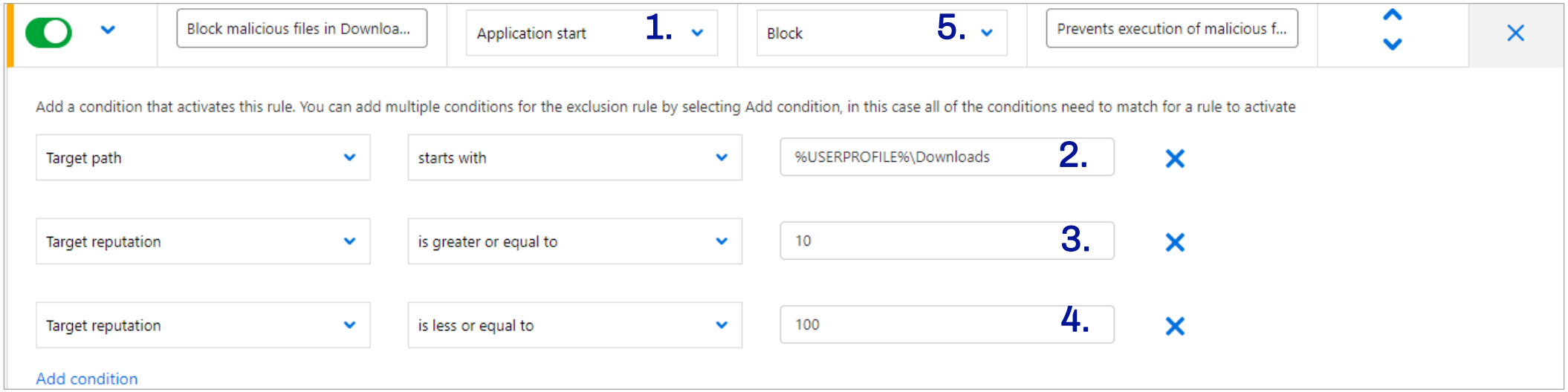
Setting Up Rules: Exclusions #3

- 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.



Setting Up Rules: Exclusions #4

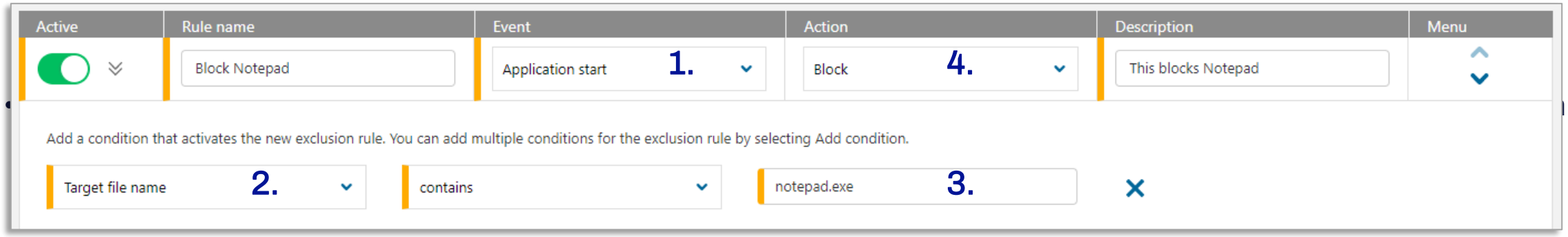
- Another helpful example is the pre-existing rule that blocks users from triggering malicious files in the Downloads folder.
- This rule also consists of three “AND” conditions. They specify that the Application start (1) in the Target path %USERPROFILE%\Downloads and subdirectories (2) with a reputation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



WITH secure

Setting Up Rules: Exclusions #5

- Blocking specific programs from being launched can be done though 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).



WITH secure

Events and Actions

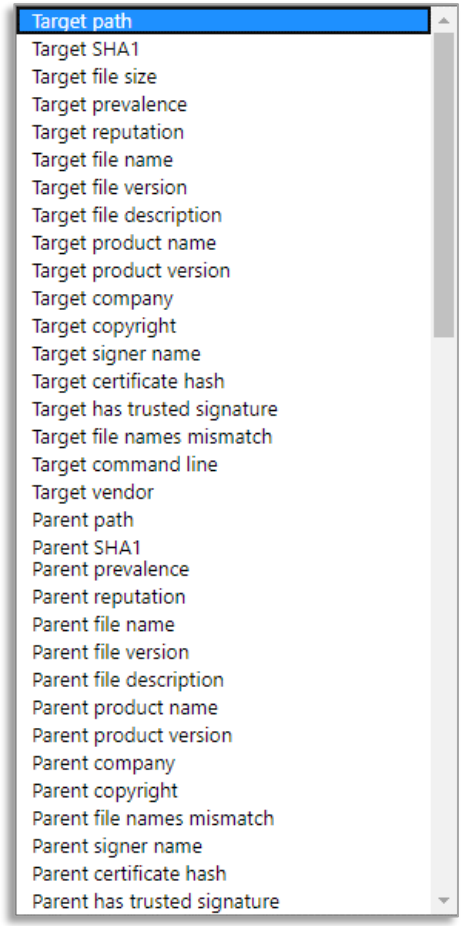
- When selecting the event that invokes the rule, you have the following options:
  - Application start (i.e., when a specific application tries to start or an application in a specific folder is started)
  - Module load (i.e., when a program tries to access to e.g. a DLL file)
  - Installer start (i.e., 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:



WITH secure

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

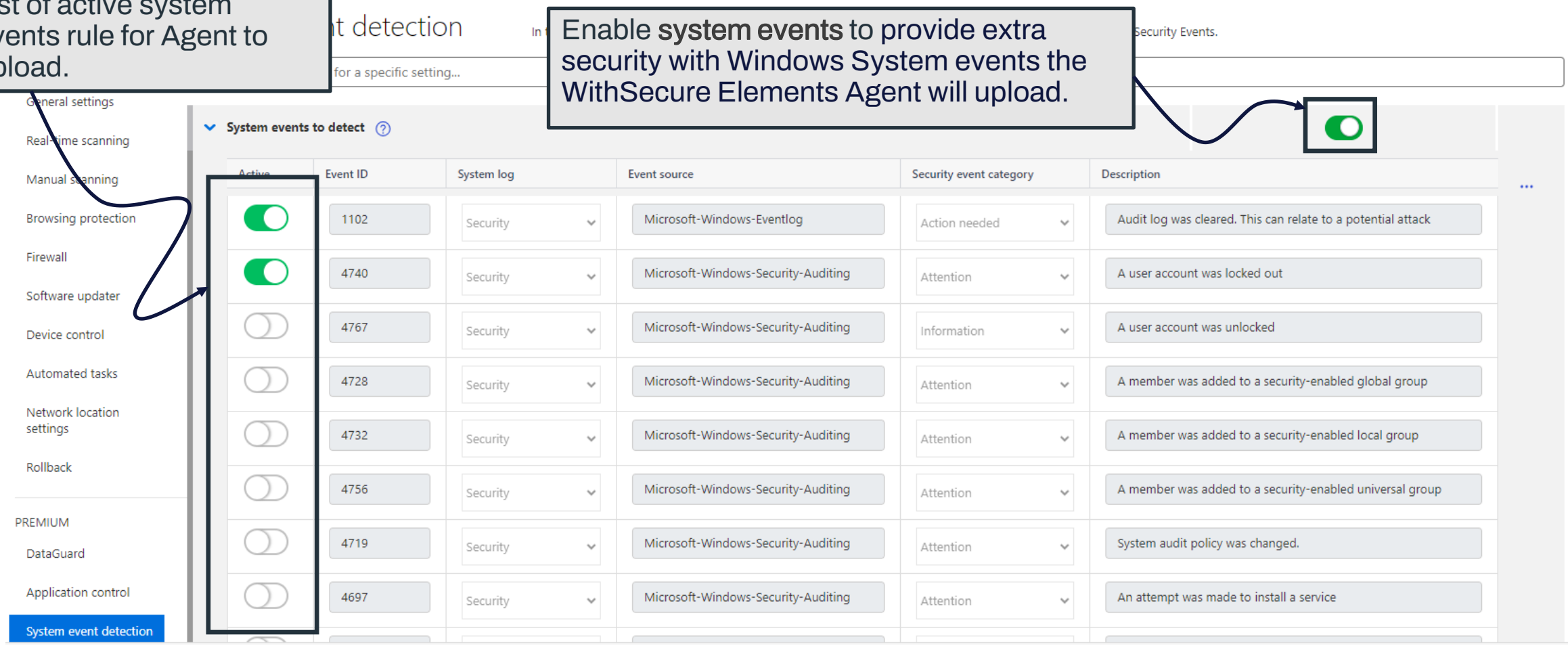
- When you set file Prevalence based rules, the following chart determines the class:

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.



Elements EPP Profiles

Computer Protection for Mac

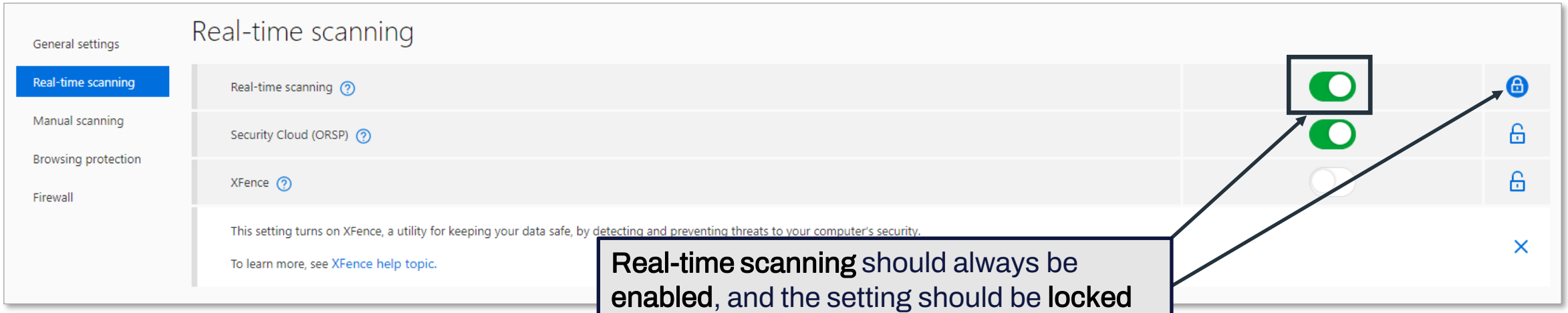
General Settings

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.

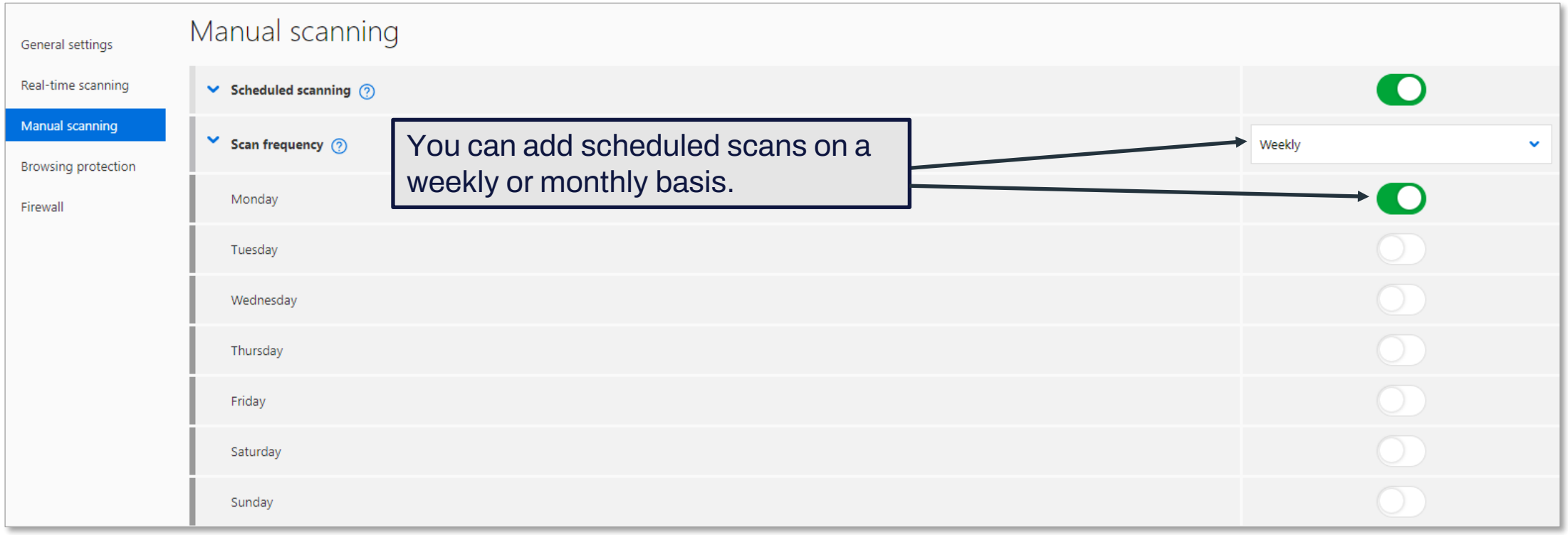
Real-time Scanning



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

WITH secure

Manual Scanning

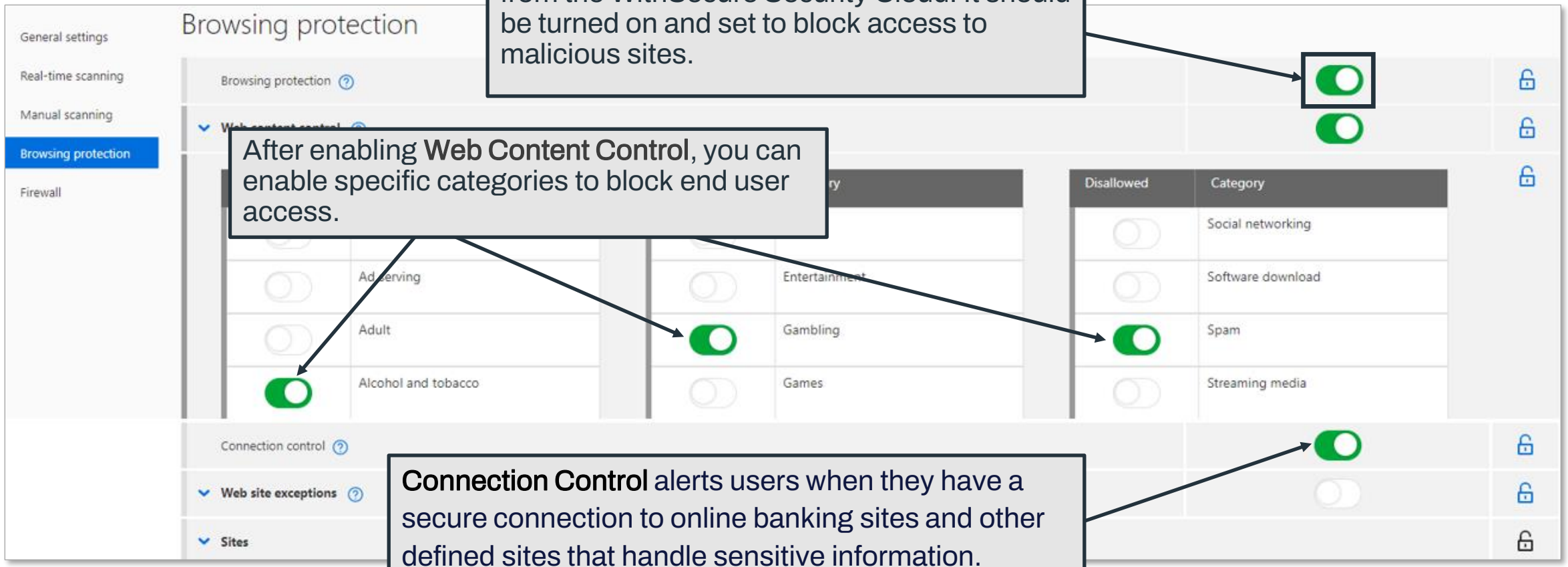


WITH secure

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.

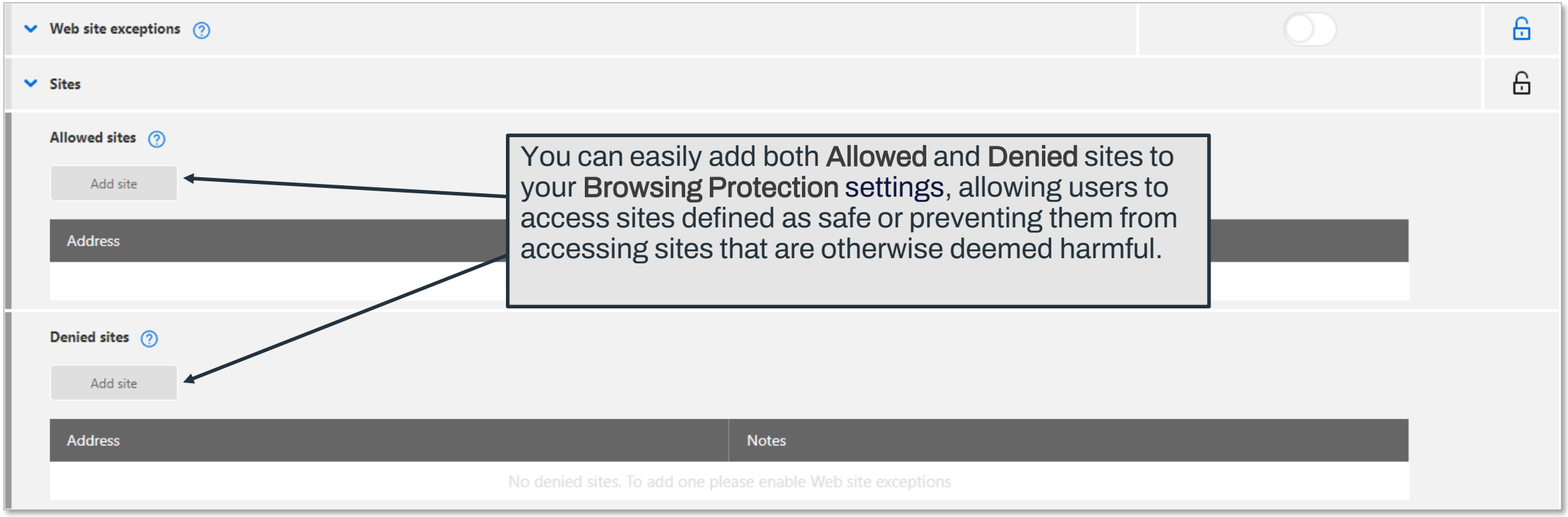
After enabling **Web Content Control**, you can enable specific categories to block end user access.



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

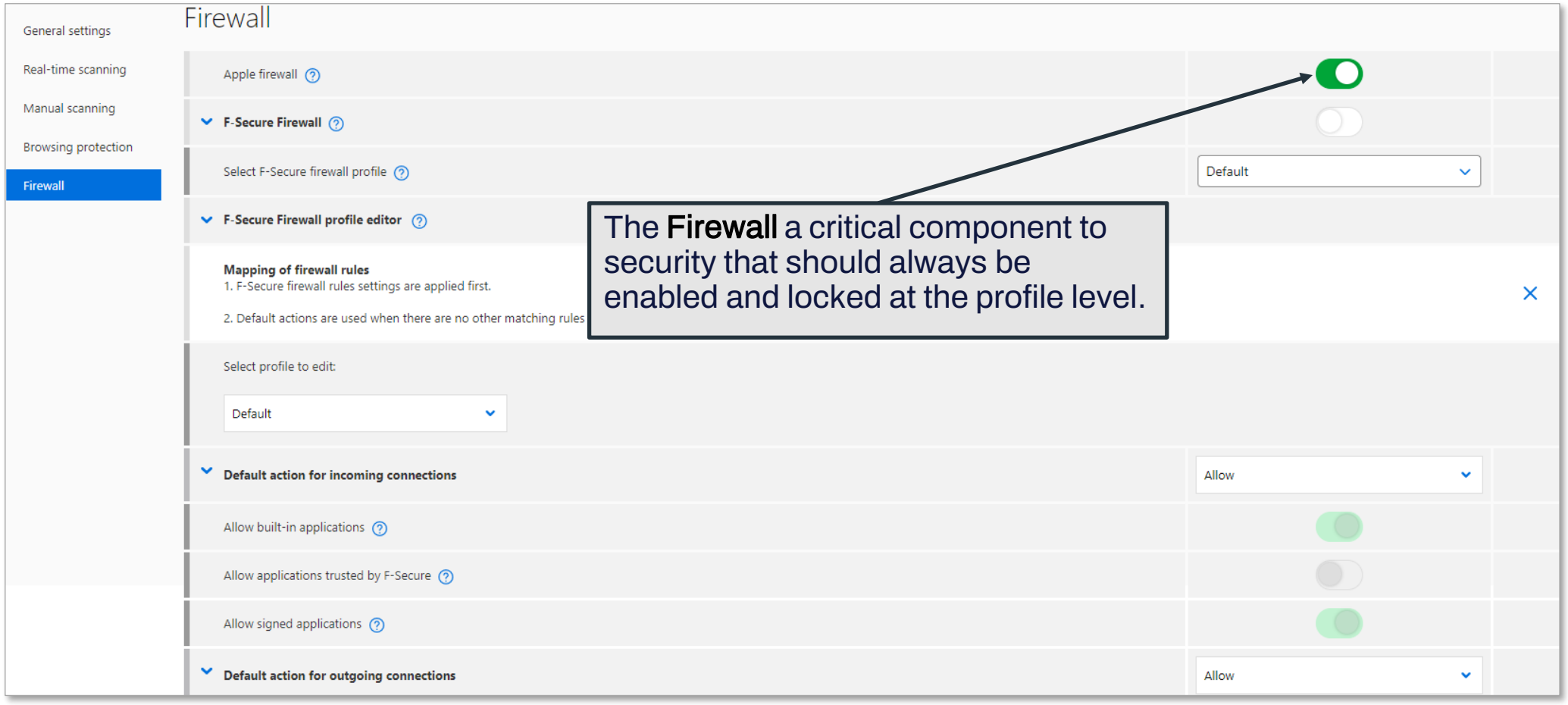
WITH secure

Browsing Protection:
Trusted / Blocked Sites



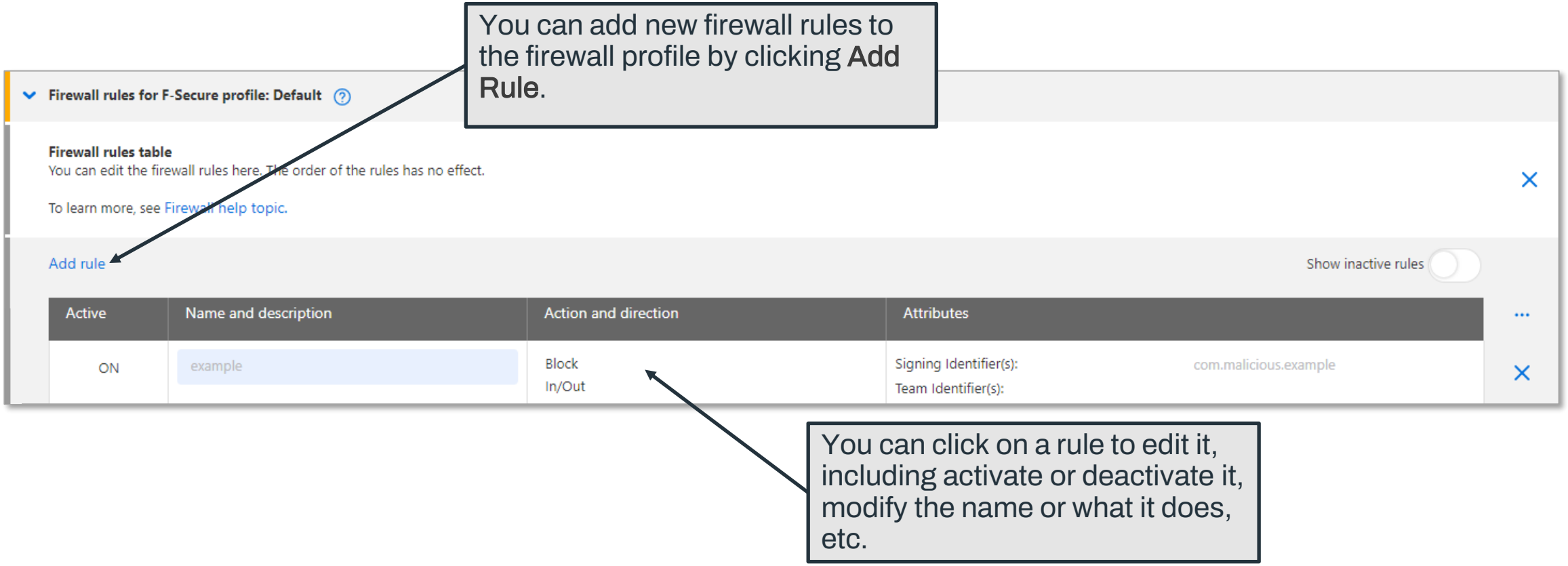
WITH secure

Firewall


General settings
Real-time scanning
Manual scanning
Browsing protection
Firewall
Firewall
Apple firewall
F-Secure Firewall
Select F-Secure firewall profile
Default
F-Secure Firewall profile editor
Mapping of firewall rules
1. F-Secure firewall rules settings are applied first.
2. Default actions are used when there are no other matching rules
Select profile to edit:
Default
Default action for incoming connections
Allow
Allow built-in applications
Allow applications trusted by F-Secure
Allow signed applications
Default action for outgoing connections
Allow
The Firewall a critical component to security that should always be enabled and locked at the profile level.

Firewall Rules

As specified under the Firewall rules table, the order of rules does not have any effect.



WITH secure

Nastavitve for Windows Computers profila

Elements EPP+EDR for Computers Premium

WITH secure

Nastavitve for Windows Computers profila

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

WITH secure

Migracija v Elements EPP

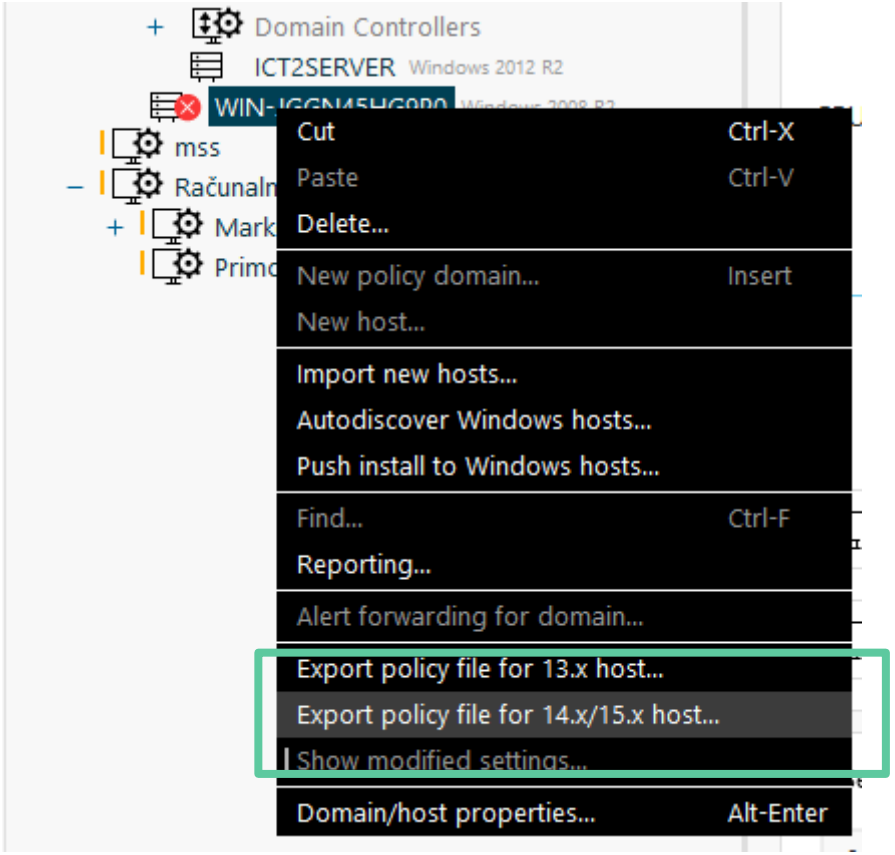
Client Security in Server Security oz. Business Suite

WITH secure

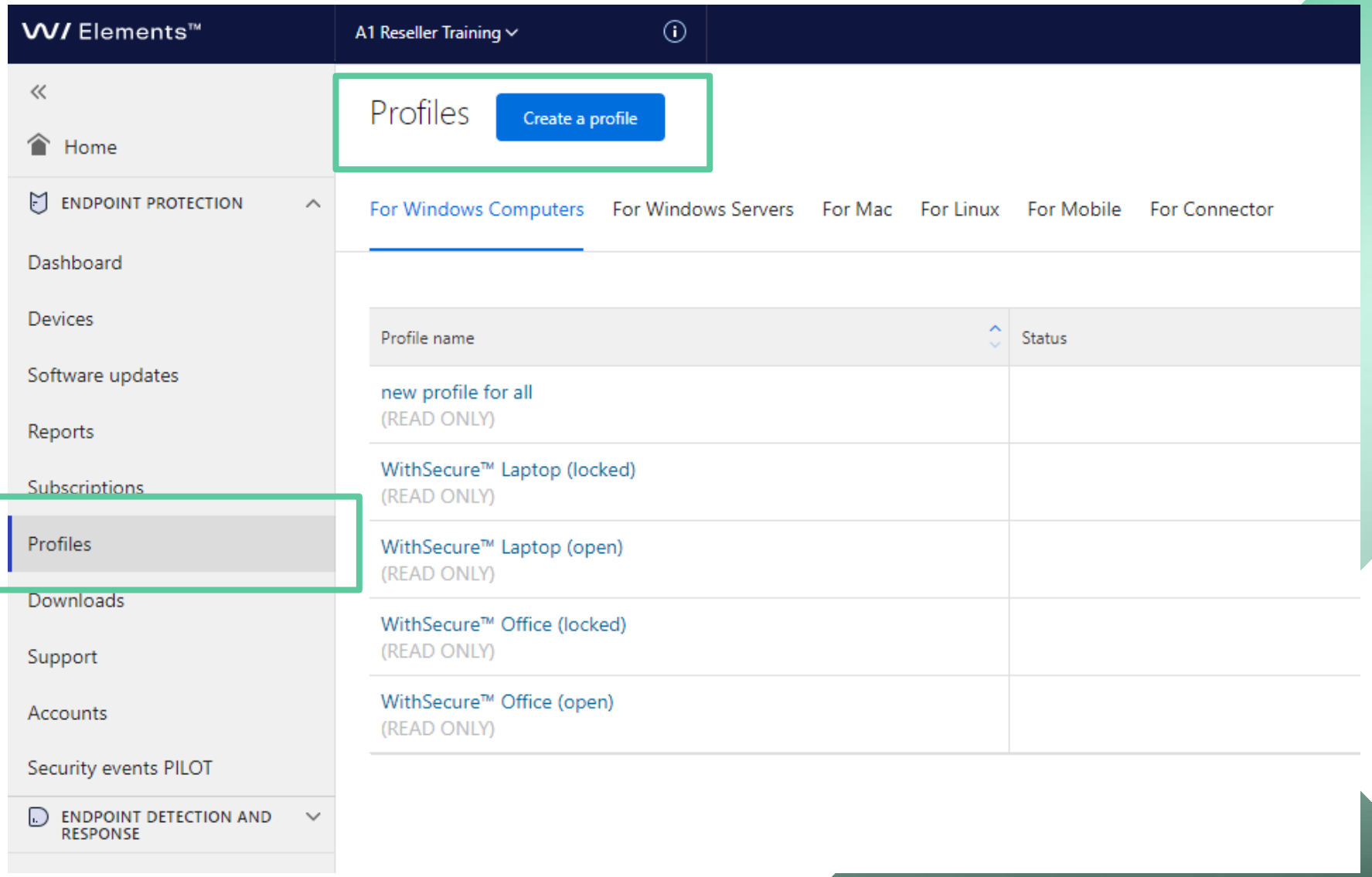
Postopek migracije

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

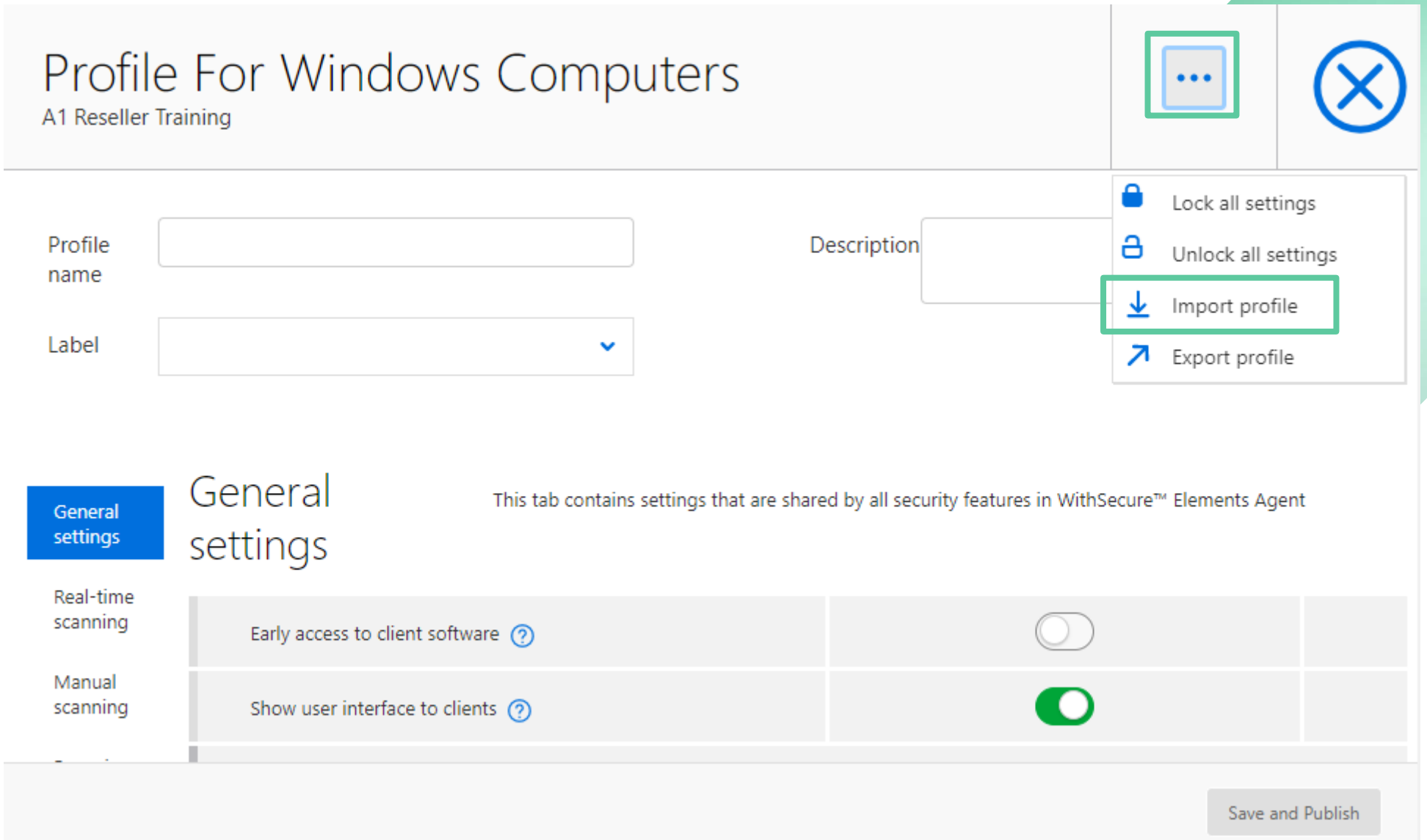
1. Izvoz nastavitev



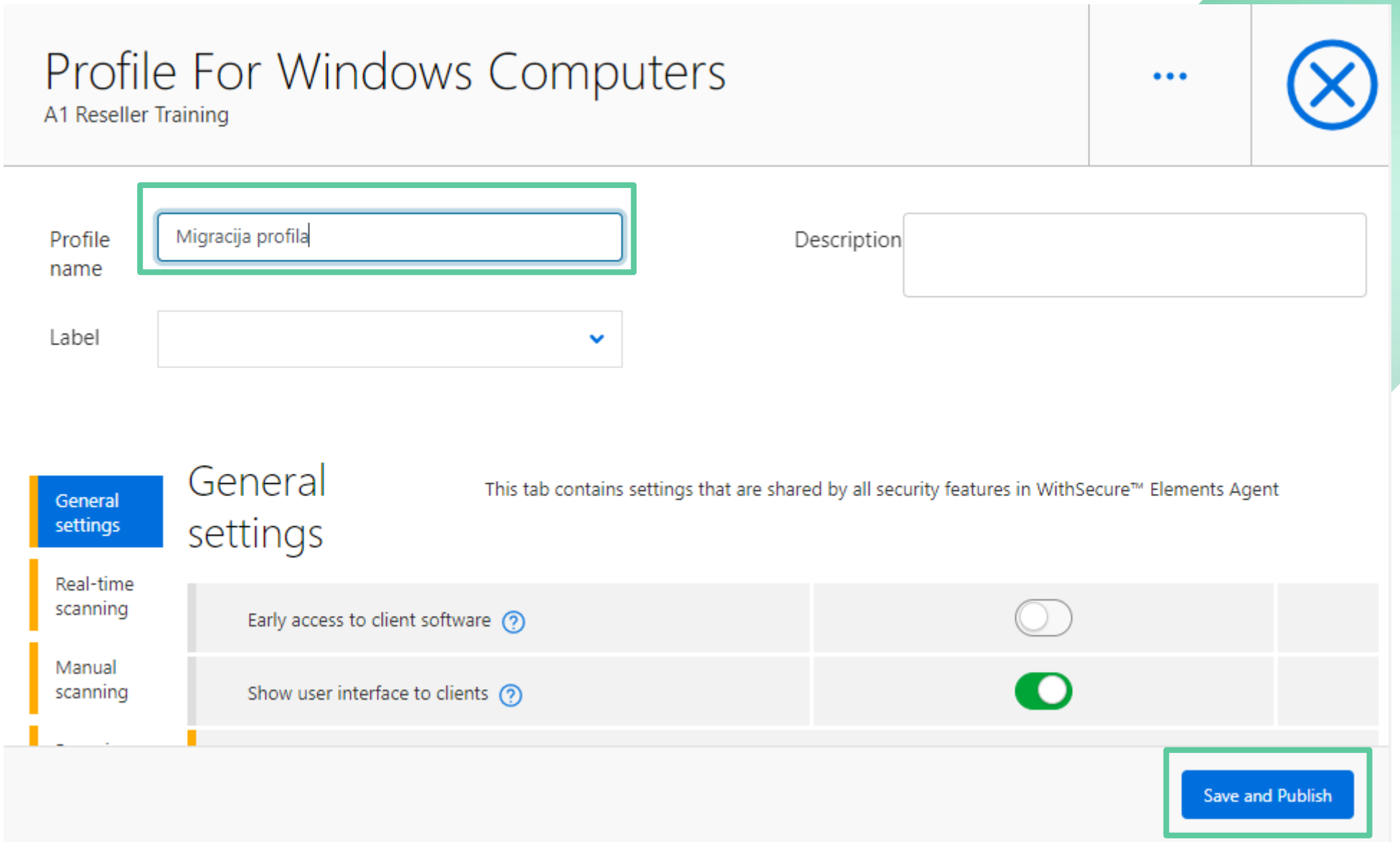
2. Uvoz nastavitev



2. Uvoz nastavitev



2. Uvoz nastavitev



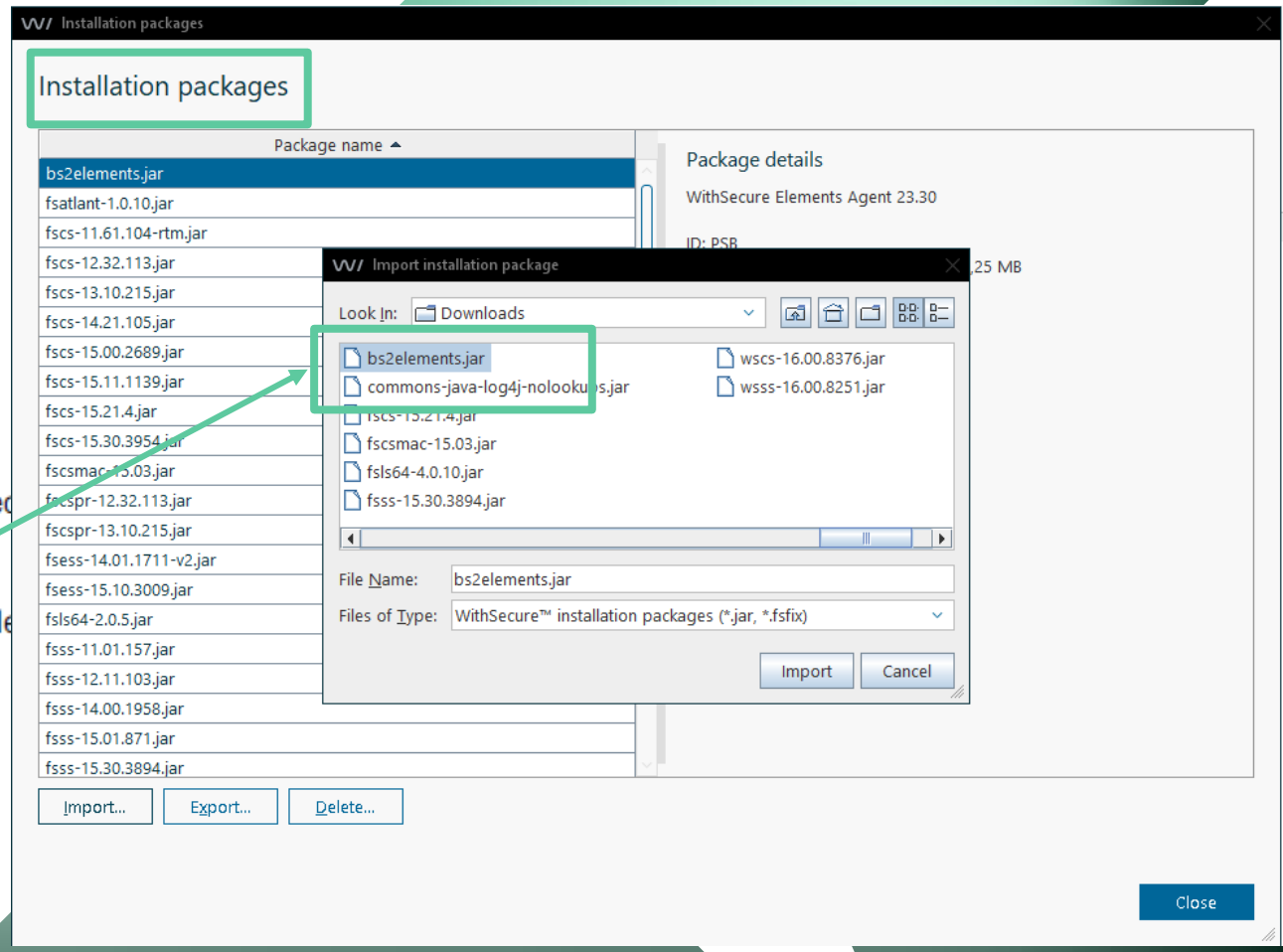
3. Uvoz JAR paketa
https://help.withsecure.com

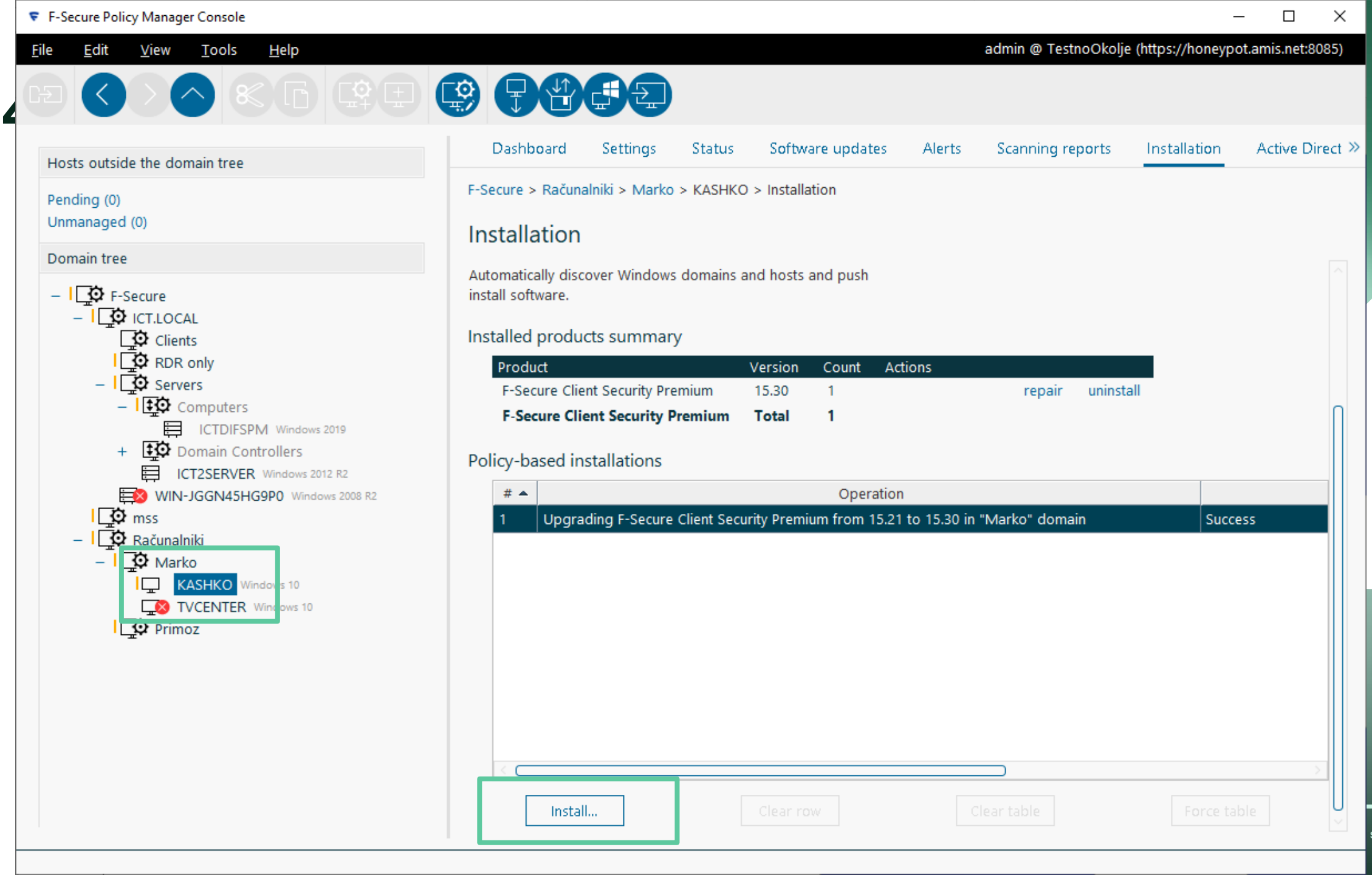
- https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/en/task_92573A8D65A94616915AC3266DB89CE7-psb-portal-latest-en

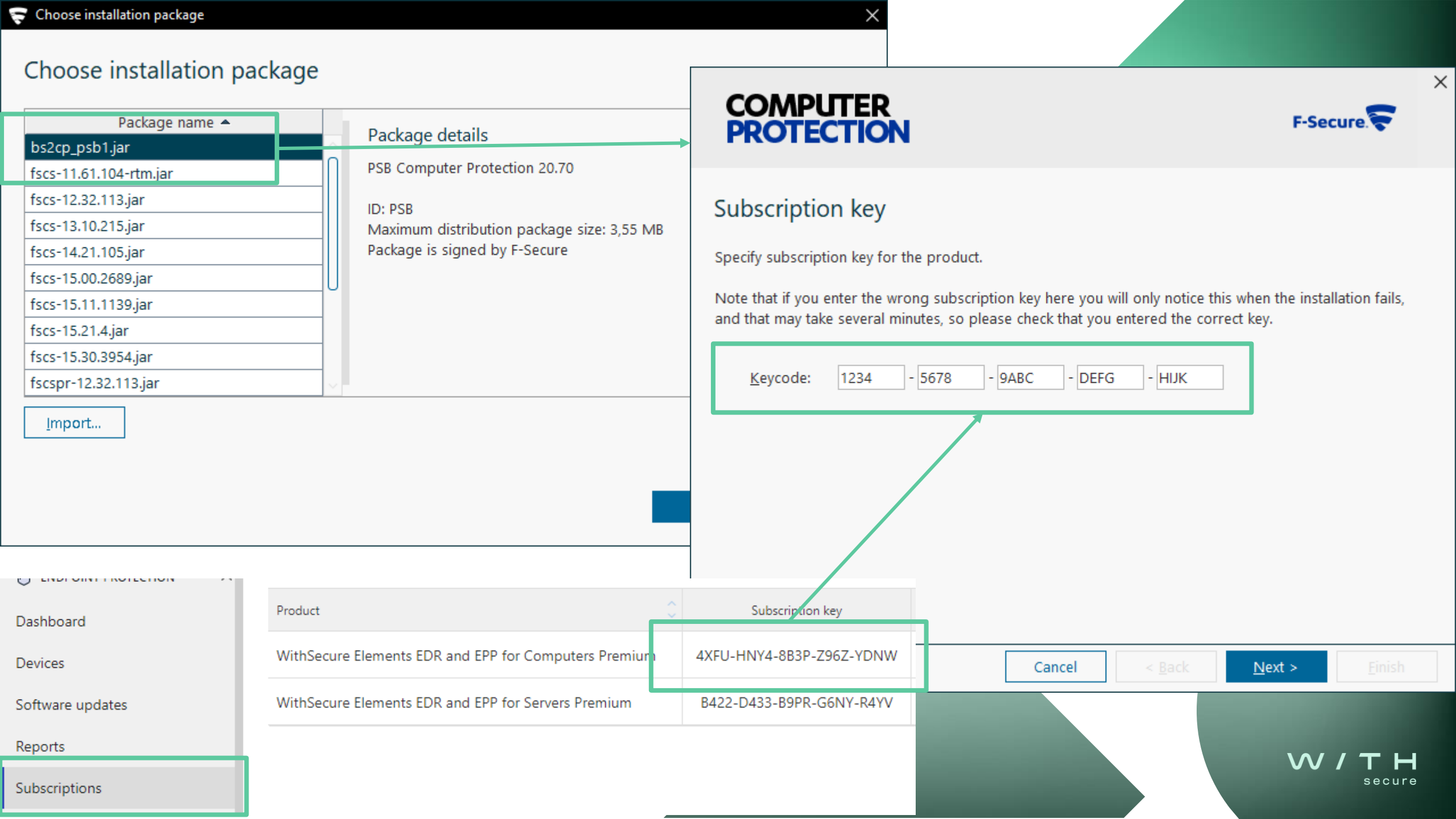
Migrating computers

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

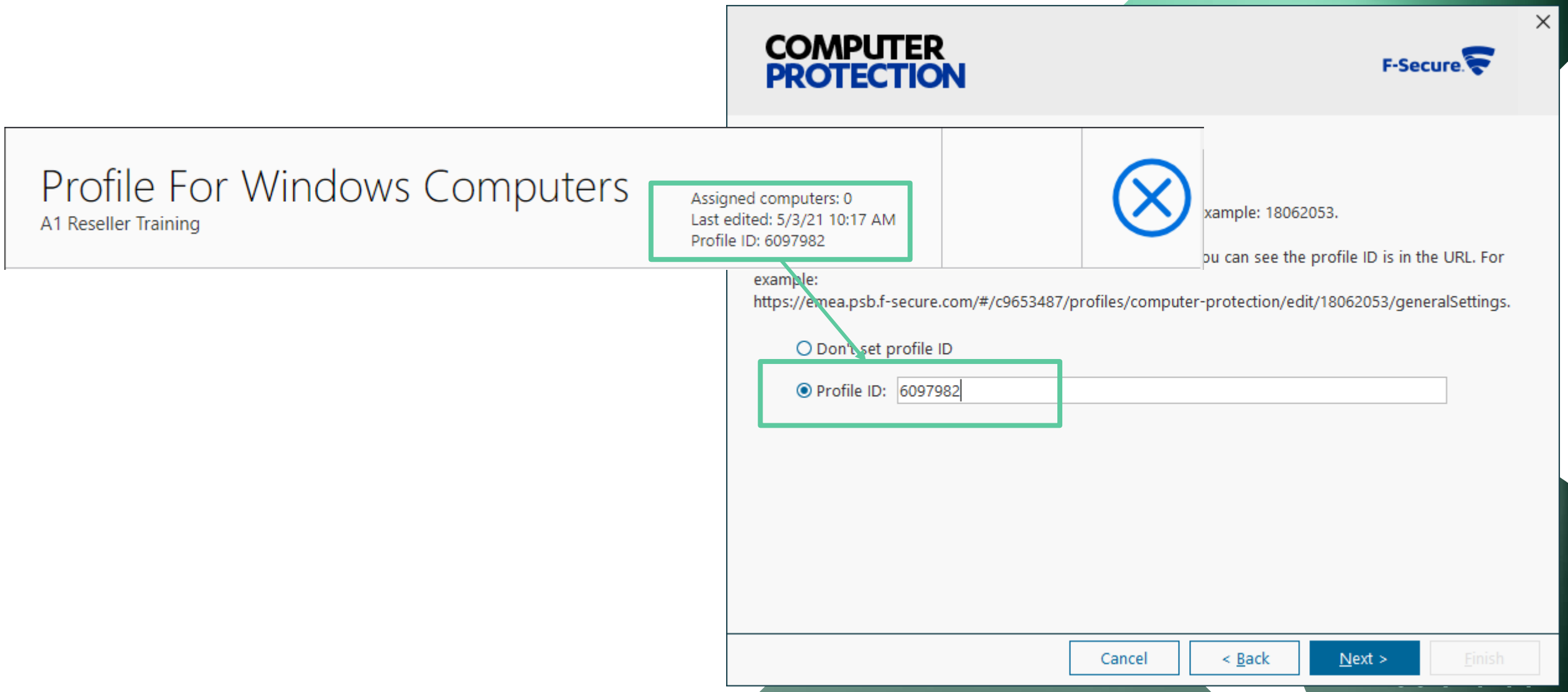
To apply the `.jar` file and migrate, you need a Policy Manager console and the `.jar` file
https://download.withsecure.com/PSB/bs2cp/bs2elements.jar.




F-Secure Policy Manager Console
File Edit View Tools Help
admin @ TestnoOkolje (https://honeypot.amis.net:8085)
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

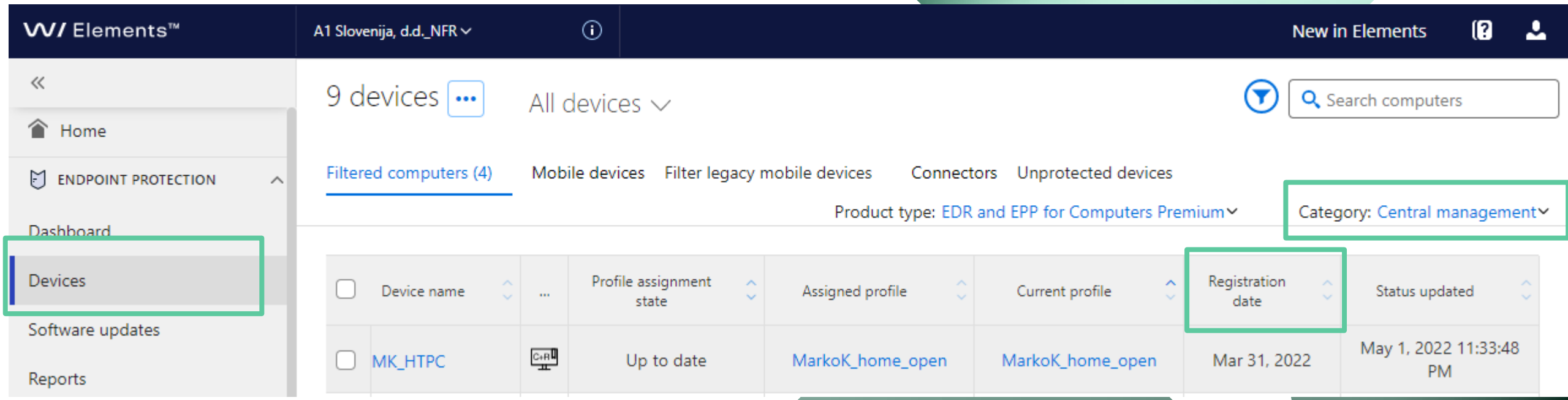

Choose installation package
Choose installation package
Package name
bs2cp_psb1.jar
fscs-11.61.104-rtm.jar
fscs-12.32.113.jar
fscs-13.10.215.jar
fscs-14.21.105.jar
fscs-15.00.2689.jar
fscs-15.11.1139.jar
fscs-15.21.4.jar
fscs-15.30.3954.jar
fscspr-12.32.113.jar
Package details
PSB Computer Protection 20.70
ID: PSB
Maximum distribution package size: 3,55 MB
Package is signed by F-Secure
Import...
COMPUTER PROTECTION
F-Secure
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: 1234 - 5678 - 9ABC - DEFG - HIJK
Cancel
< Back
Next >
Finish
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
W/TH secure

4. Namestitev

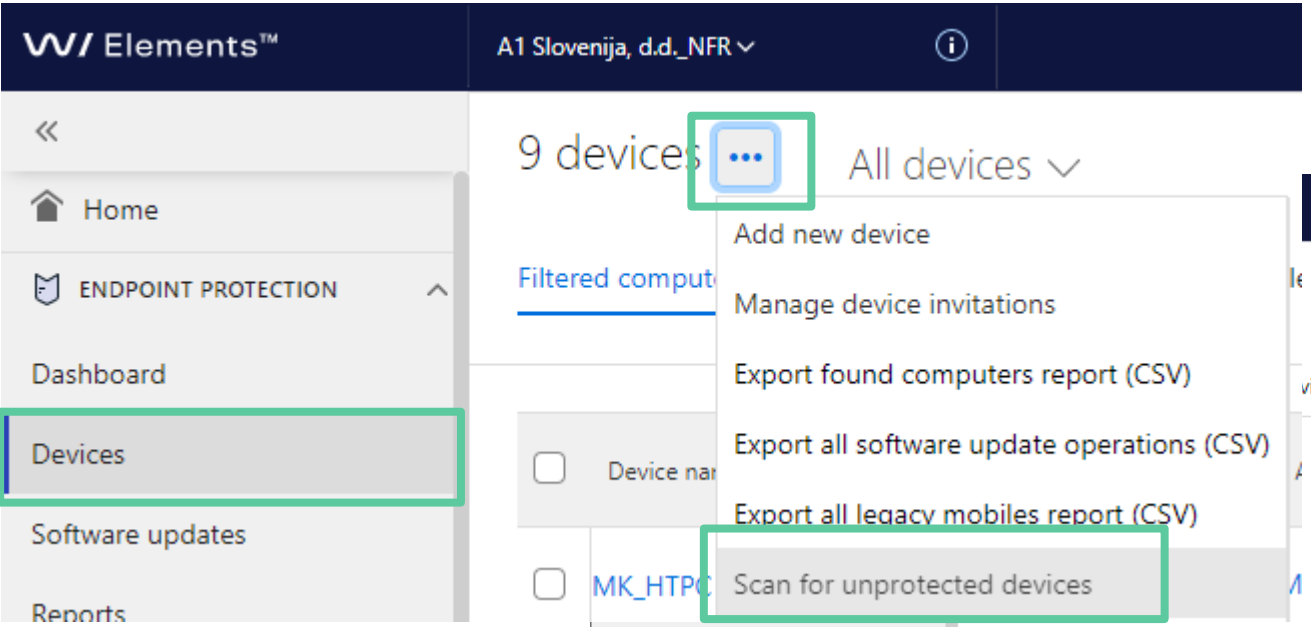


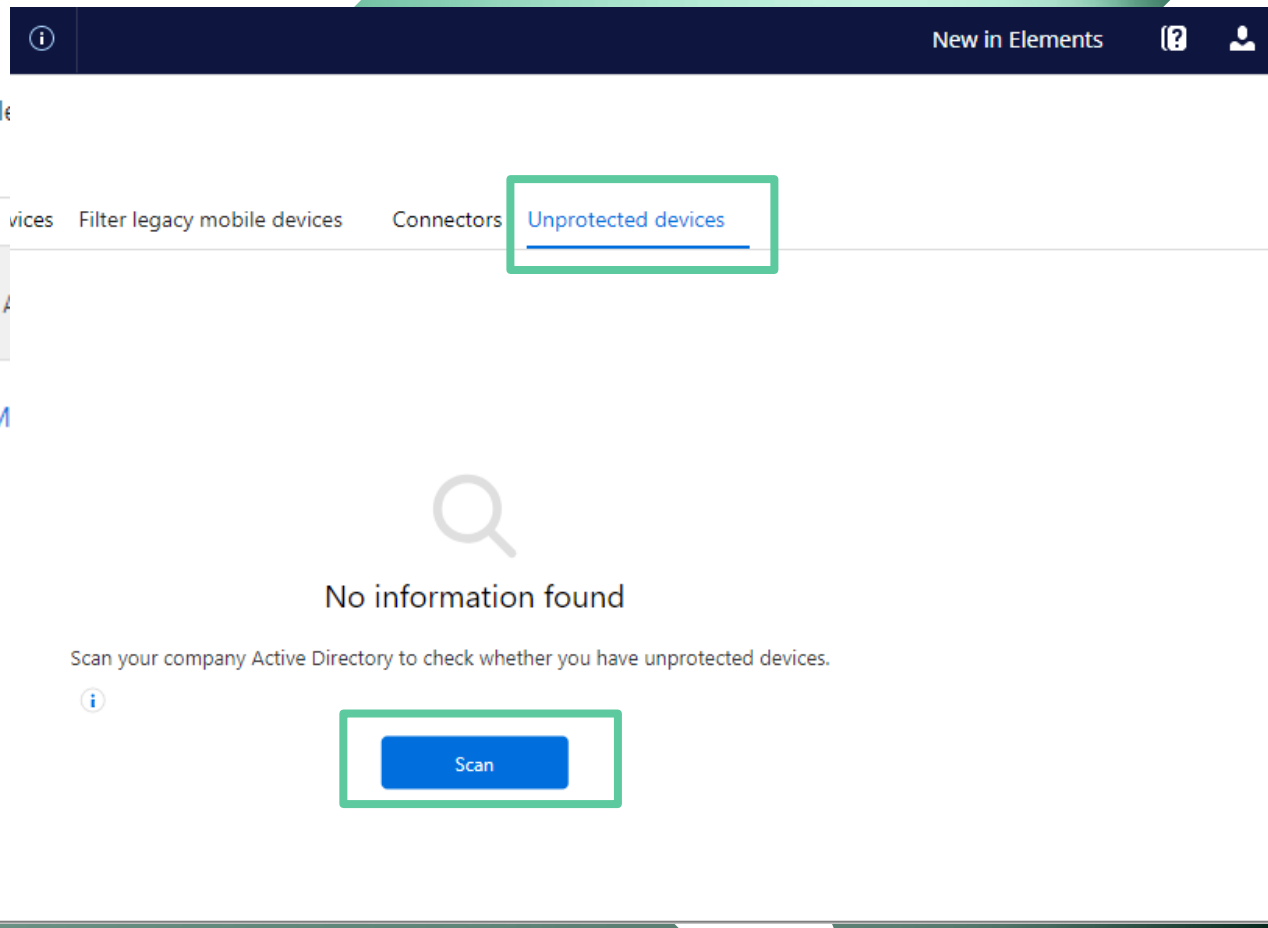
5. Nova naprava v ESC

- Razvrstitev naprav po datumu registracije



AD Discovery





Devices

Computers (0) | Mobile devices | Legacy mobile devices (0) | Connectors | Unprotected devices

Unprotected devices

Last scan: a few seconds ago Success

Scan

Active Directory nodes status (2 nodes)

Node	Status	Device used for scan operation
loca	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
inv404 .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-B42F-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=Computer ola,DC=local	00553194-9D46-C321EA26D4B2

Tips & Tricks

WITH secure

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

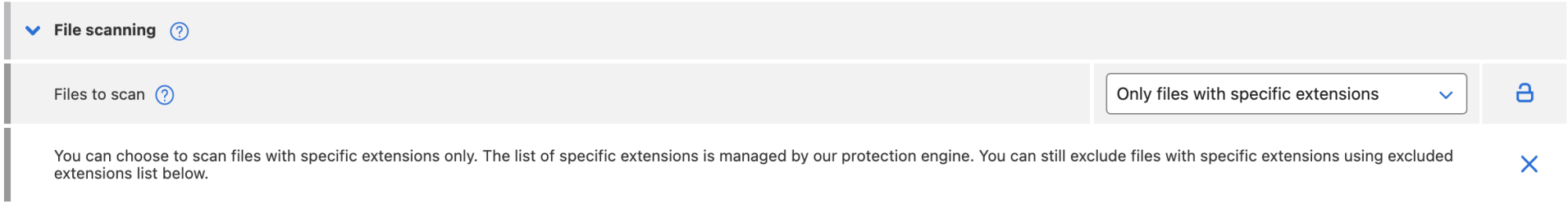
WITH secure

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



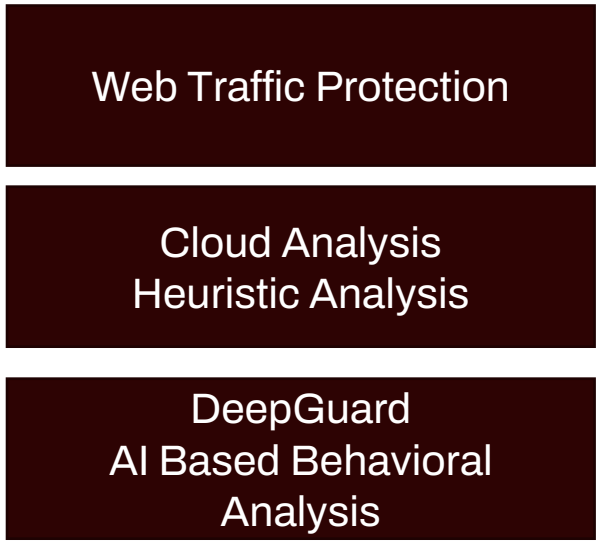
2. All analysed files are stored to a local WithSecure Hive and if a file's TTL is still valid, no need to rescan the file

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

WITH secure

Security Layers In File Analysis

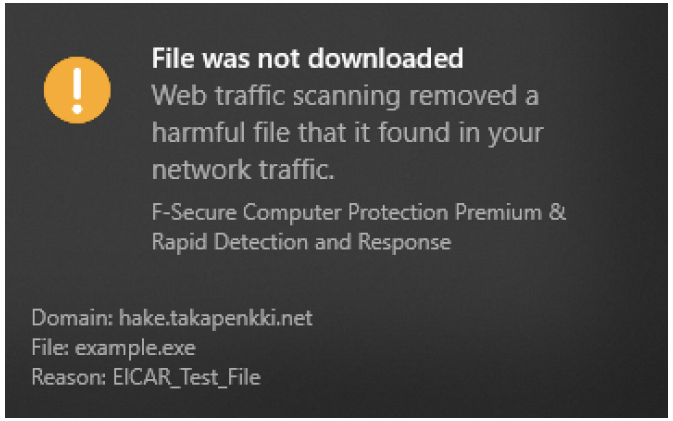


Real-time scanning -> Web traffic scanning

Real-time scanning -> File scanning

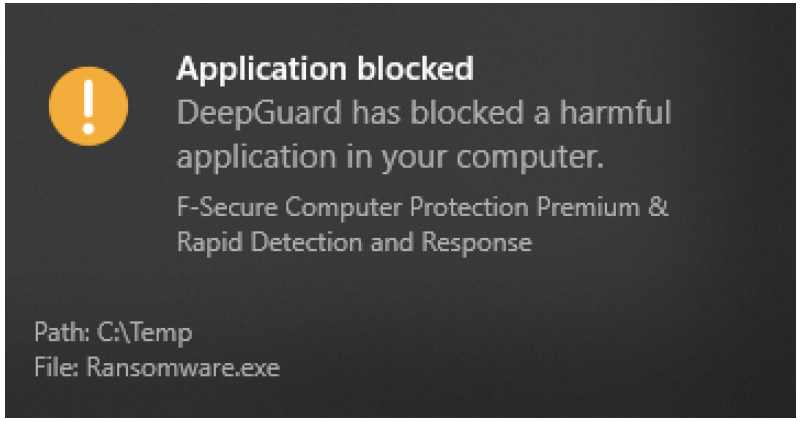
Real-time scanning -> DeepGuard

Security Layers In File Analysis



Web Traffic Protection

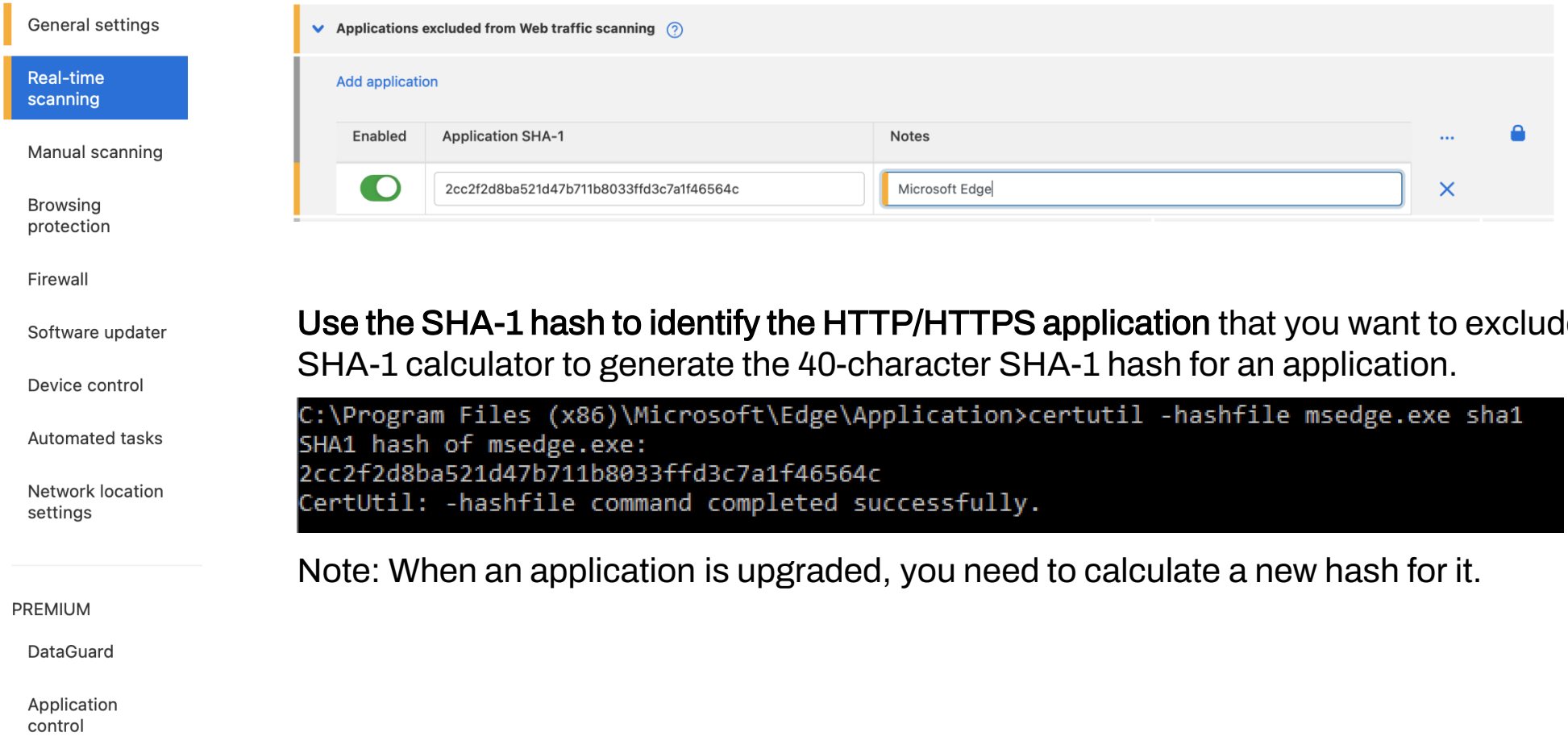
Cloud Analysis
Heuristic Analysis



DeepGuard
AI Based Behavioral Analysis

WITH secure

Web Traffic Scanning Exclusions

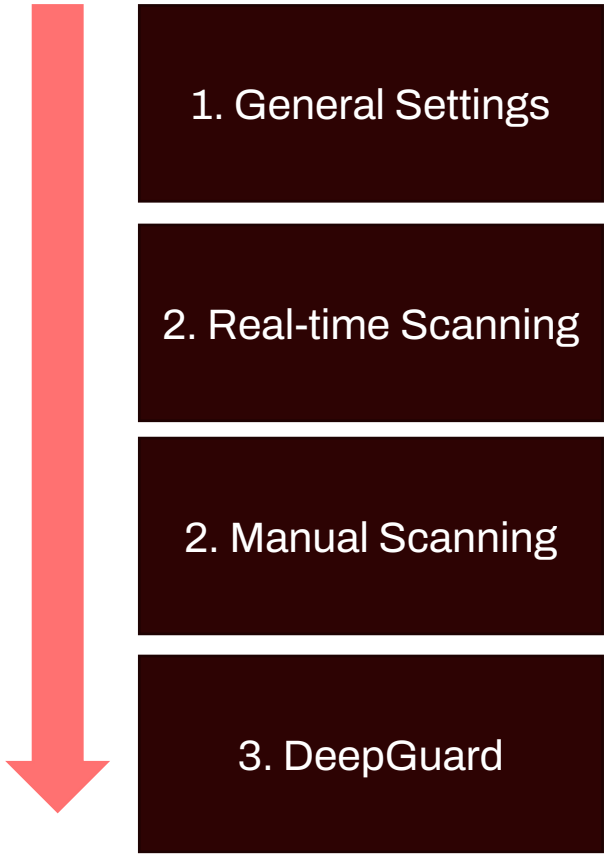


Use the SHA-1 hash to identify the HTTP/HTTPS application that you want to exclude. Use an SHA-1 calculator to generate the 40-character SHA-1 hash for an application.

```
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



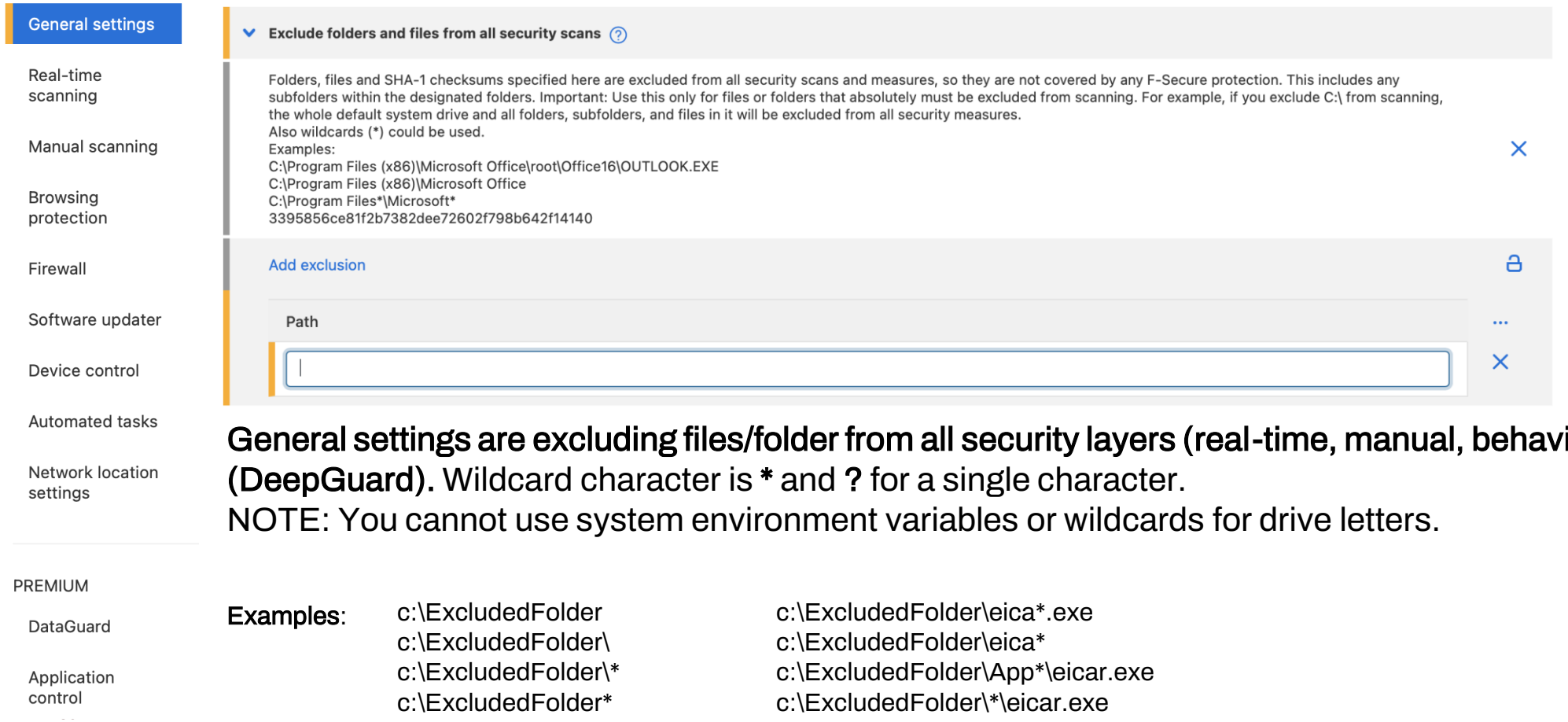
Global exclusions

Module specific exclusion for real-time scanning

Module specific exclusion for manual scanning

Module specific exclusion for behavioral protection

File Analysis – General Settings Exclusions



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.

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

W / T H secure

Wildcard Examples

Exclusion	Description

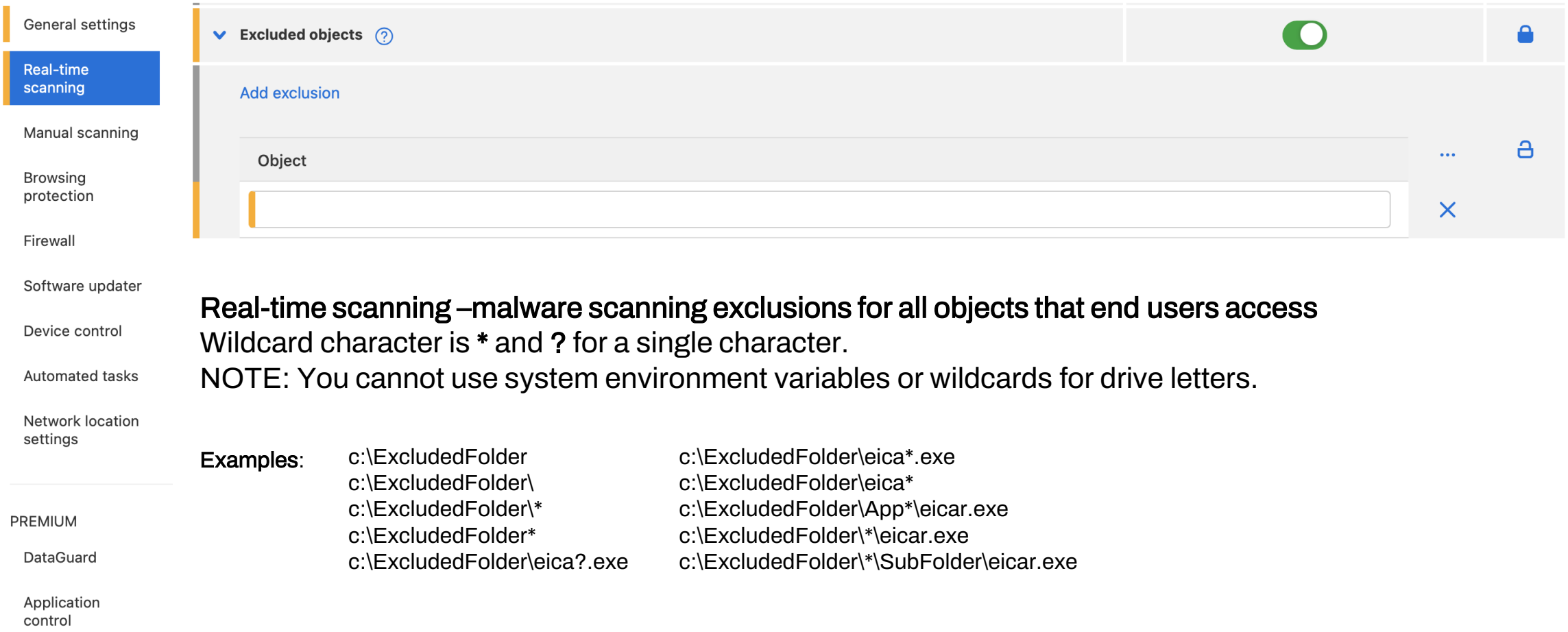
`c:\ExcludedFolder`
`c:\ExcludedFolder\`
`c:\ExcludedFolder\*`
	All files and subfolders are excluded
	Examples:
	`C:\ExcludedFolder\temp\`
	`C:\ExcludedFolder\app\app.exe`

`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\eica1.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\Appications\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



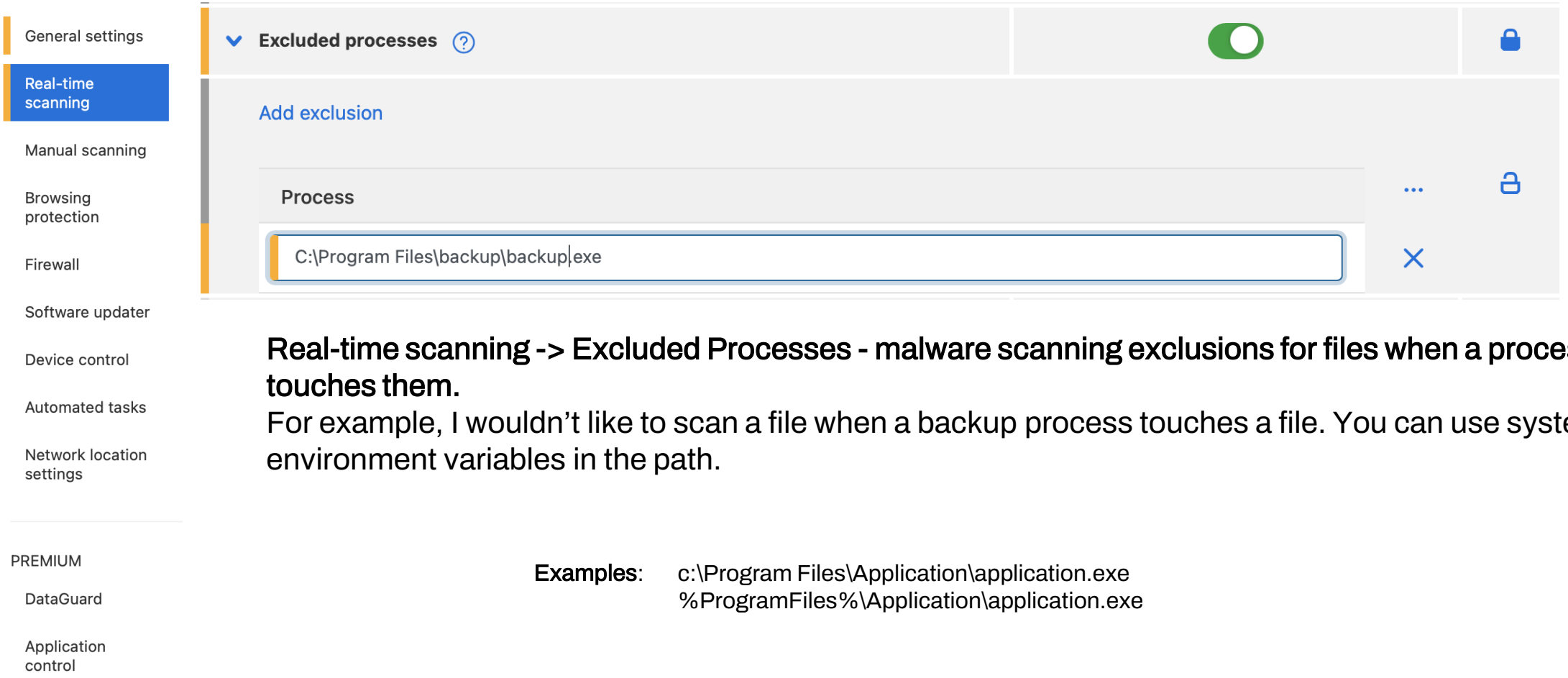
Real-time scanning –malware scanning exclusions for all objects that end users access
Wildcard character is * and ? for a single character.
NOTE: You cannot use system environment variables or wildcards for drive letters.

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

WITH secure

File Analysis – Process Scanning Exclusions

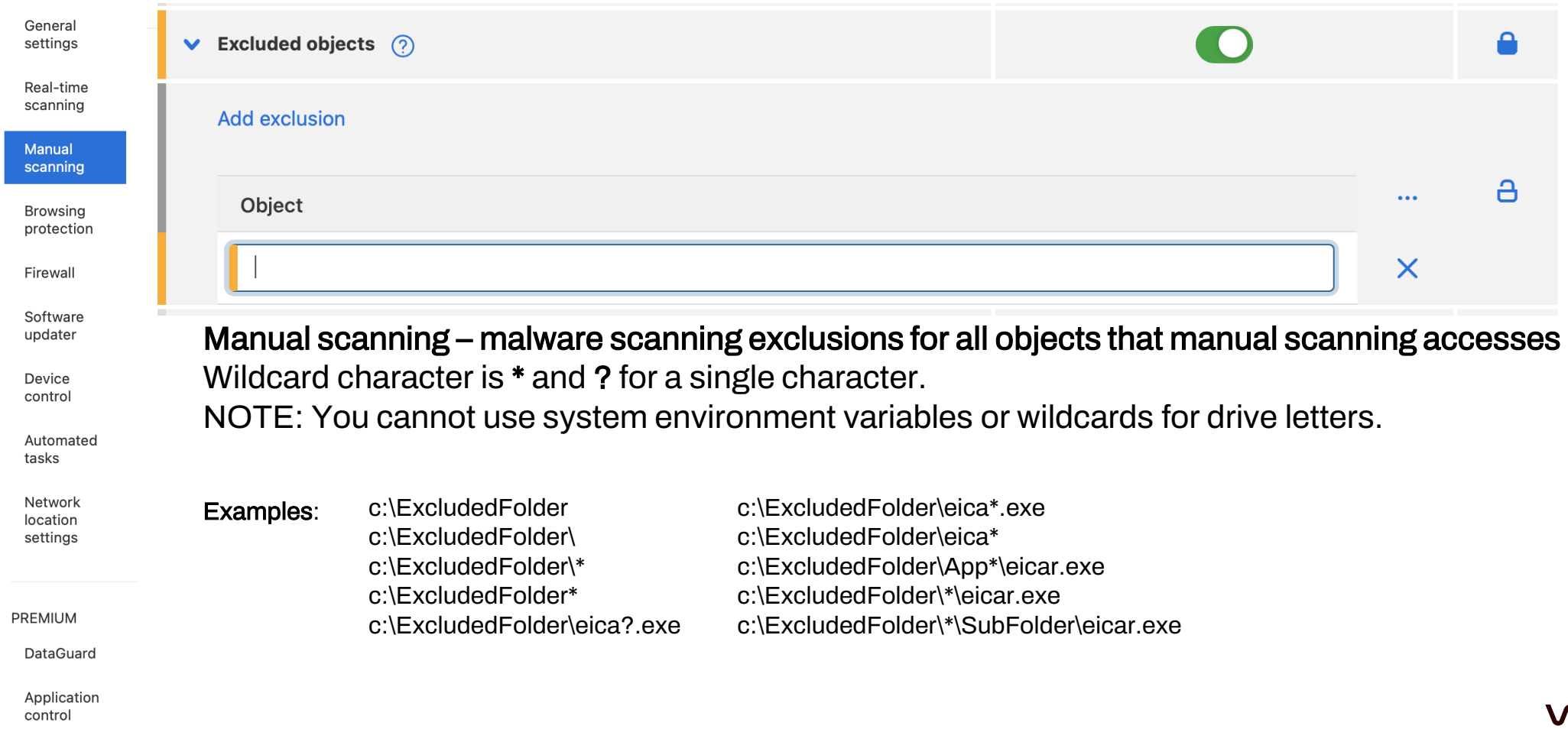


Real-time scanning -> Excluded Processes - malware scanning exclusions for files when a processes touches them.
For example, I wouldn't like to scan a file when a backup process touches a file. You can use system environment variables in the path.

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

WITH secure

File Analysis – Manual Scanning Exclusions

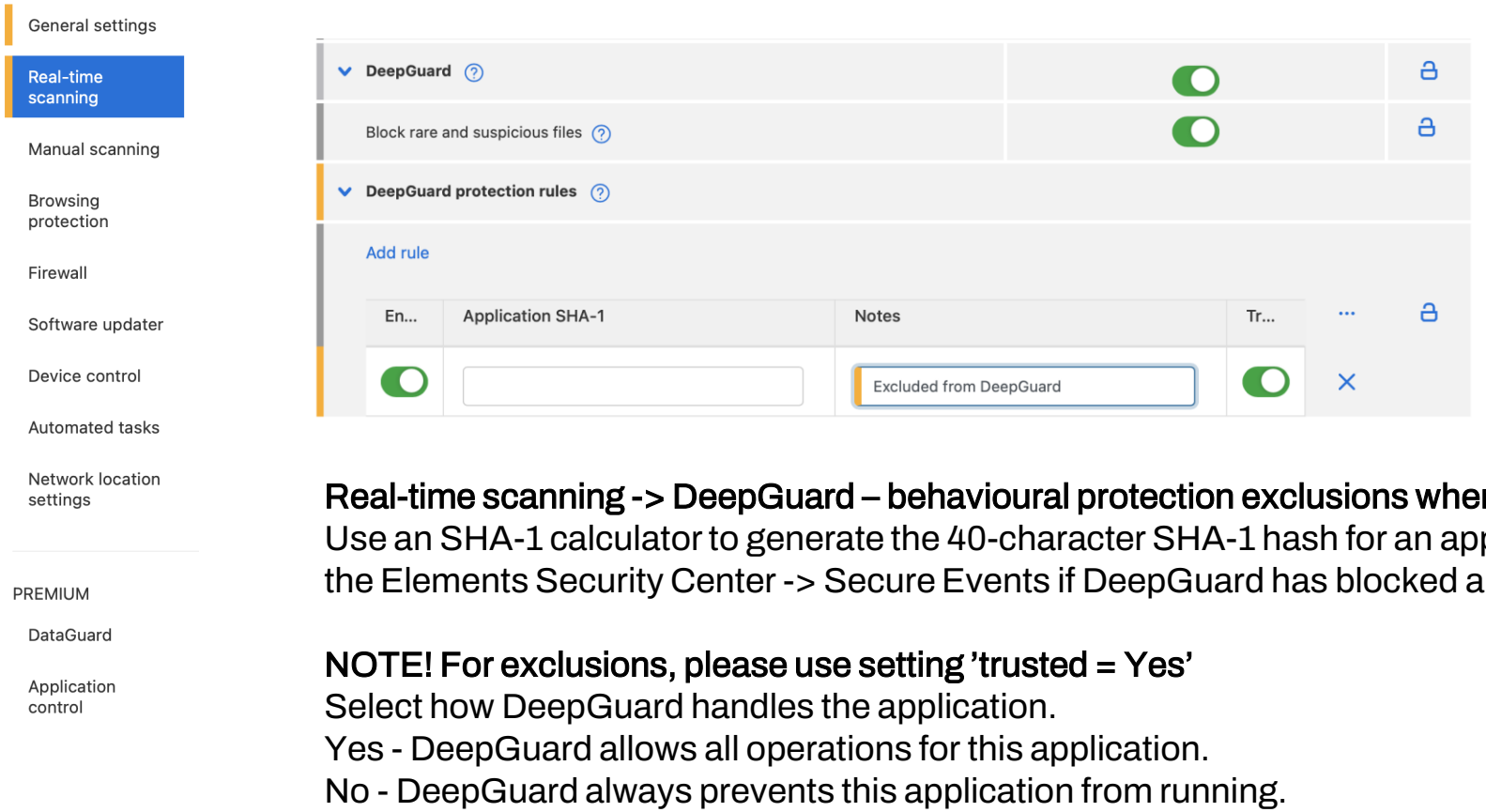


Manual scanning – malware scanning exclusions for all objects that manual scanning accesses
Wildcard character is * and ? for a single character.
NOTE: You cannot use system environment variables or wildcards for drive letters.

Examples:

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

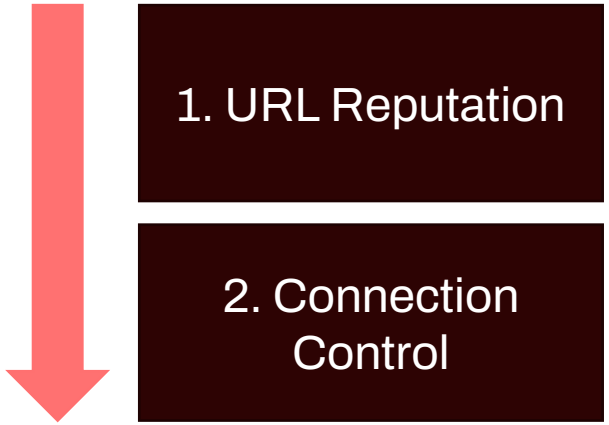
File Analysis – Deepguard Exclusions



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.

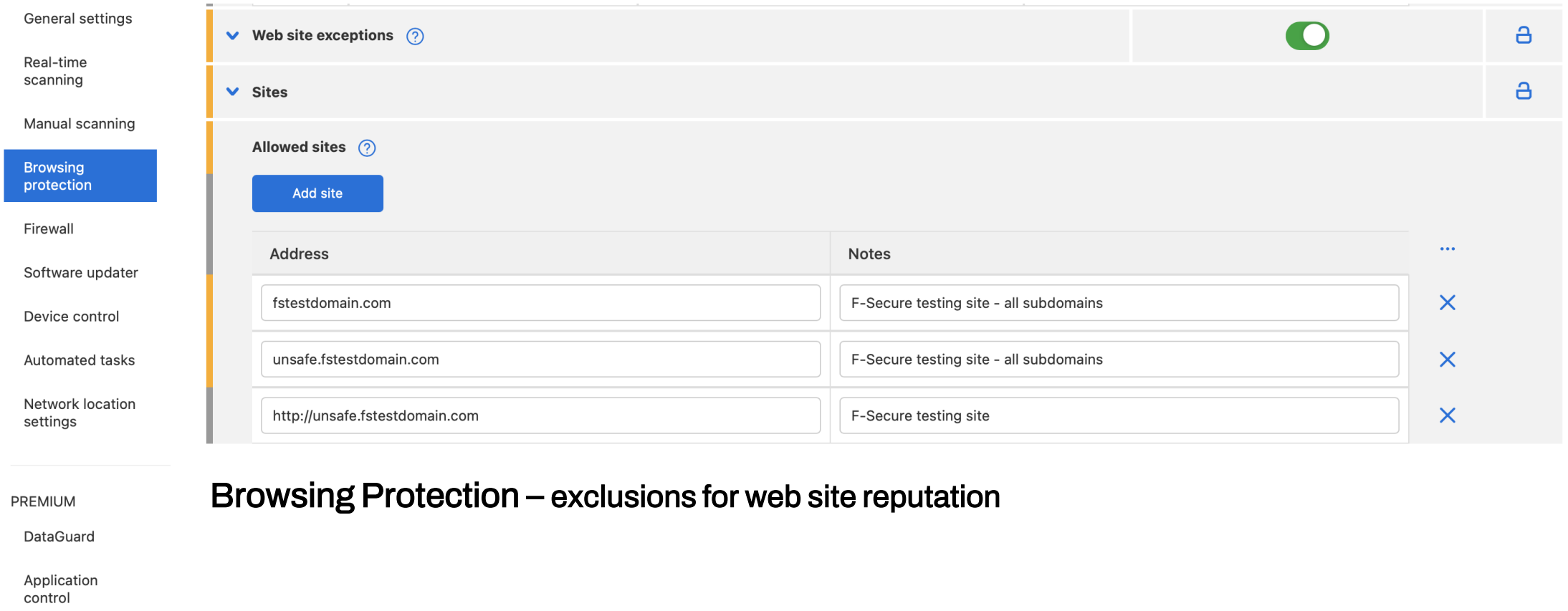
URL Analysis Precedence In Exclusions



All HTTP and HTTPS sites

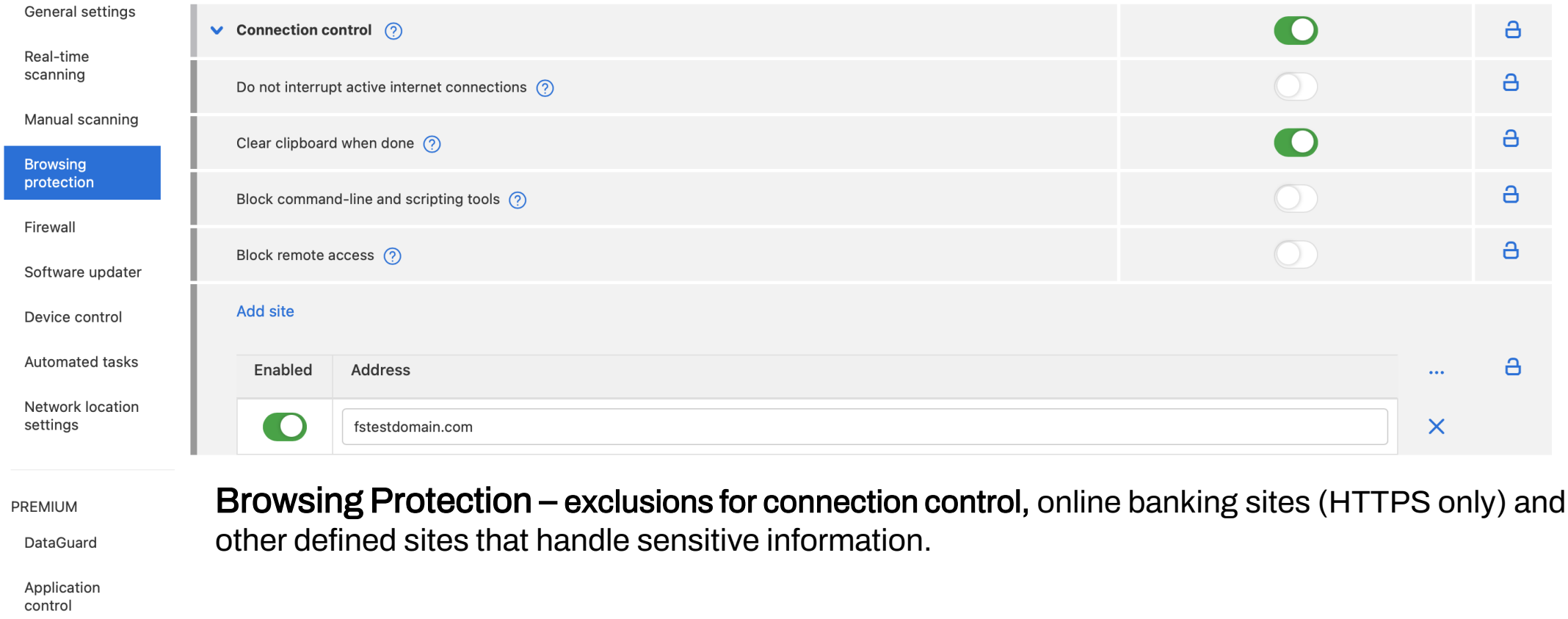
Secure connection to online banking sites (HTTPS only) and other defined sites that handle sensitive information

URL Analysis – Web Site Reputation Exclusions



Browsing Protection – exclusions for web site reputation

URL Analysis – Web Site Reputation Exclusions



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

FSDIAG

Support tool

WITH secure

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

WITH secure

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

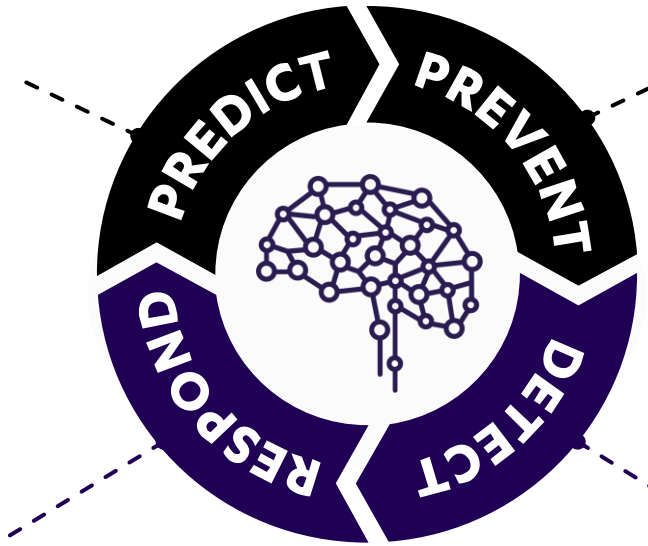
Endpoint Protection remains the foundation for securing your environment

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

WITH secure

Preventing vs. Detecting

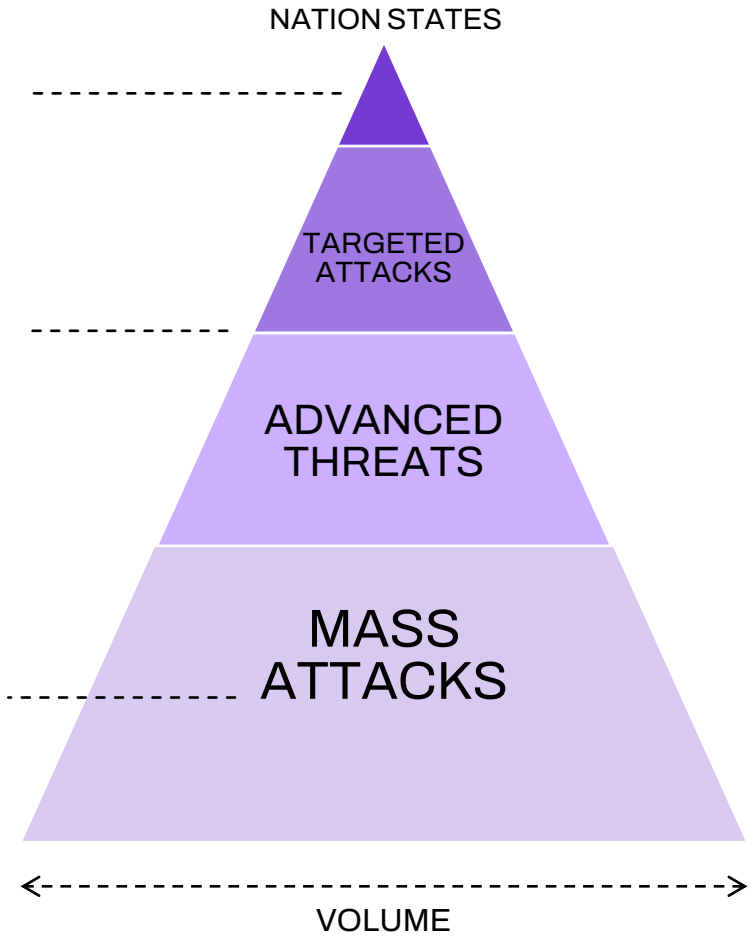
- Detecting is not the same as preventing threats.
- Traditional endpoint prevention will never stop 100 percent of all threats. This is especially true of targeted attacks.
- For full data security, both detection and prevention are required.
- The goal of WithSecure EDR is to detect and identify unknown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

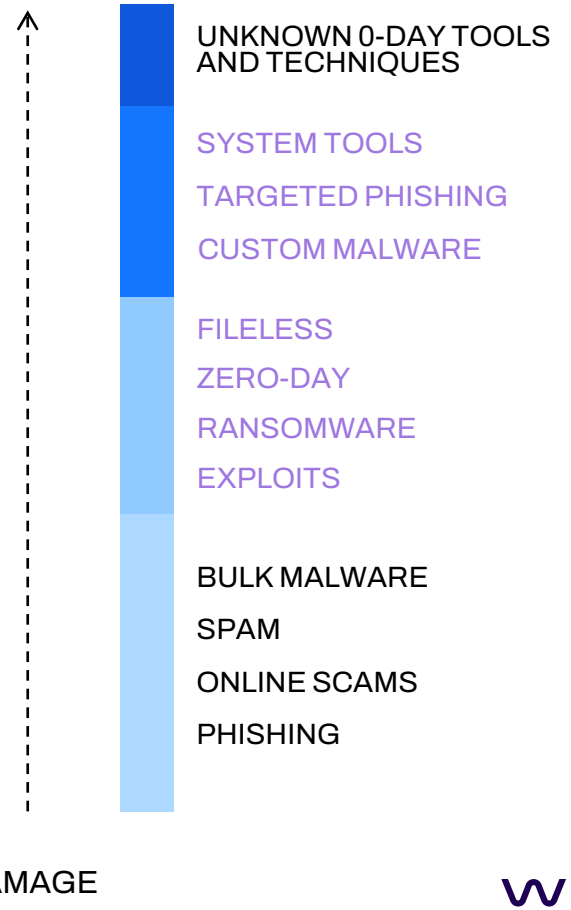
Understanding
The Threat Landscape

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.





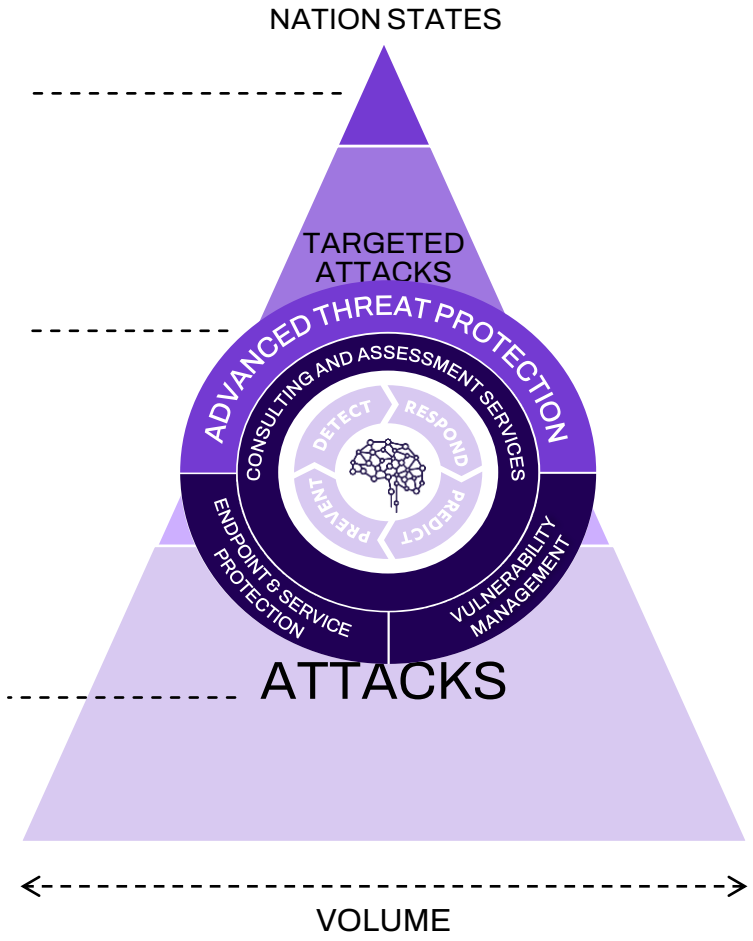
WITH secure

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.



WITH secure

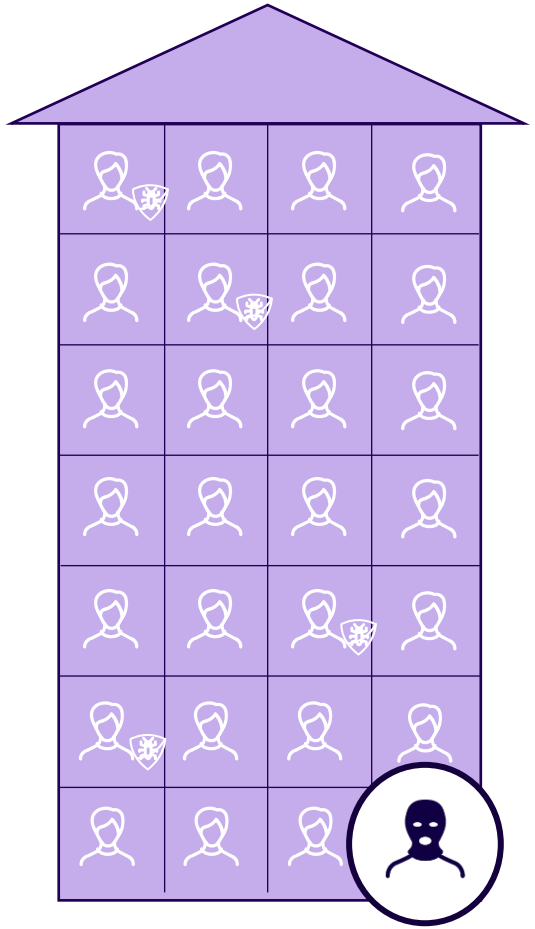
99,9 % DO LITTLE DAMAGE

0,1 % DO THE MOST DAMAGE

COMMODITY THREATS ⟷ TARGETED ATTACKS

Usually well covered

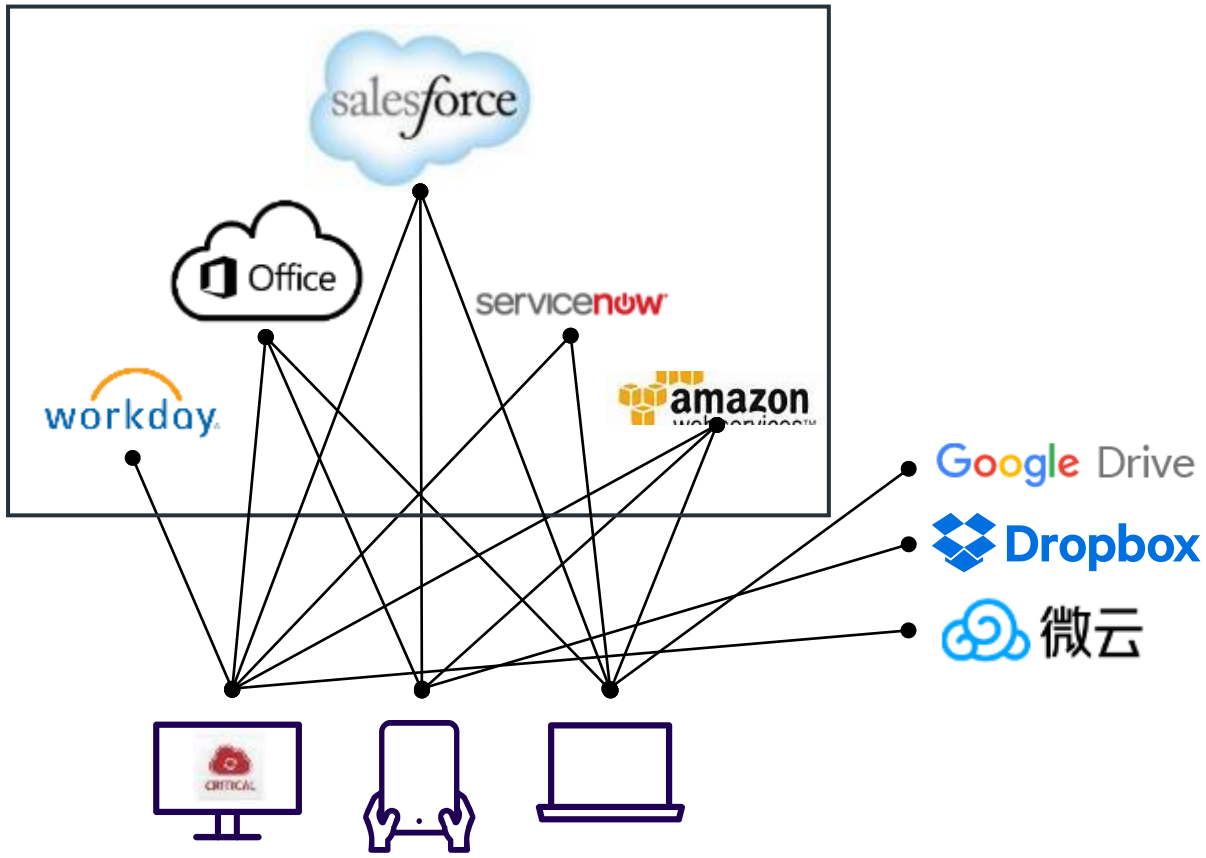
- Commodity threats
  - Machine conducted attacks
  - Malware, such as ransomware etc.
  - Spam and phishing campaign
  - >100 million new malware samples added each year (AV-TEST database)
- Addressed by preventive security:
  - Firewall
  - Email security
  - Endpoint protection
  - Other preventive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

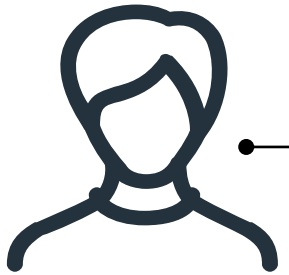
Modern IT Infrastucture Increases Exposure To Threats



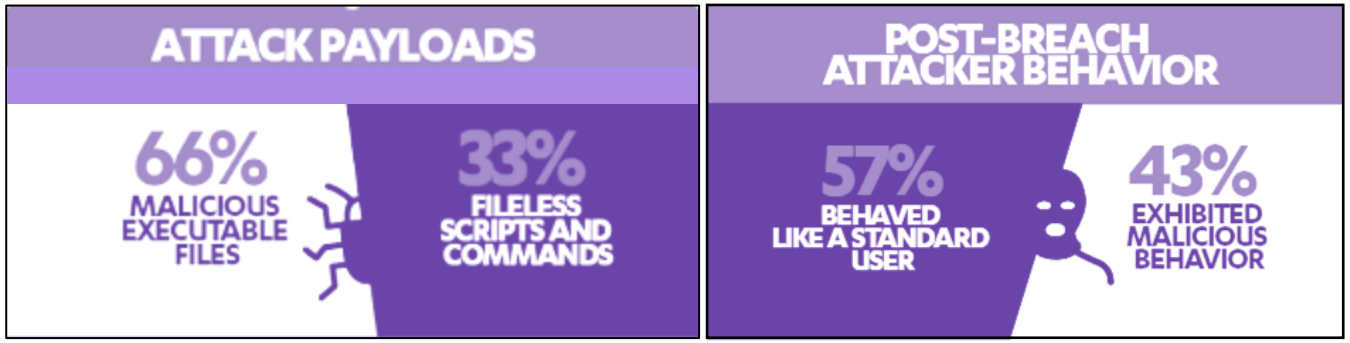
What assets do we have ?
How critical are they ?
Who can access them ?
What services are being used by our employees ?
How do they connect to those services ?
... etc.

WITH secure

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.

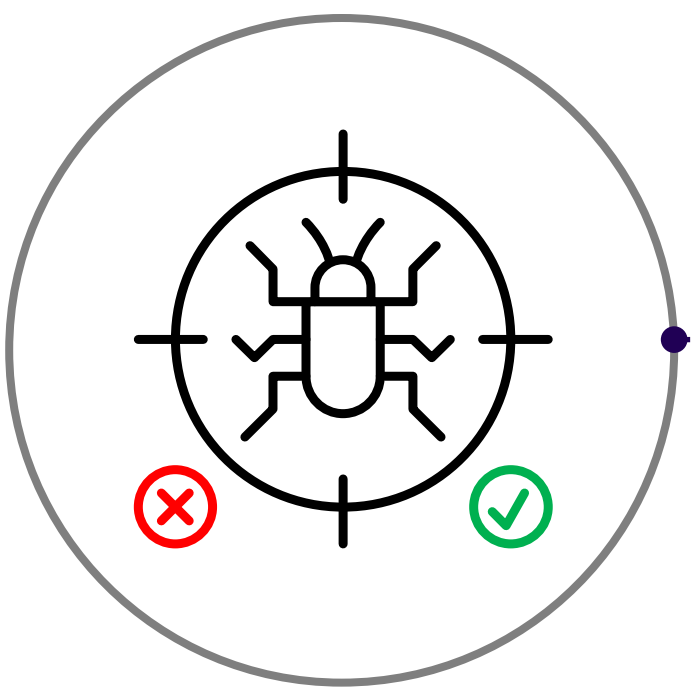
WITH secure

ON AVERAGE IT TAKES 100+ DAYS TO DETECT A BREACH

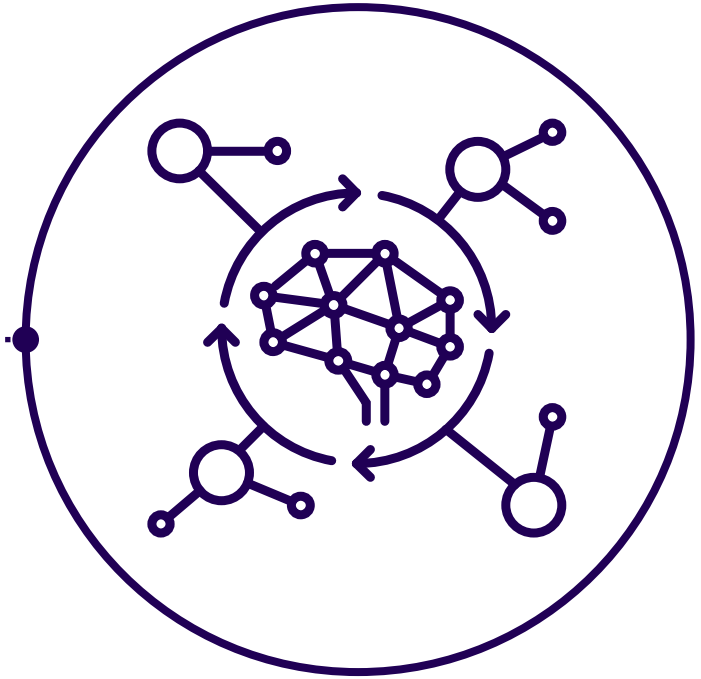
Source: 2019 Cost of Data Breach Study by Ponemon Institute indicated the days to identify the data breach varied between 131 to 279 days

WITH secure

Call For A Paradigm Shift

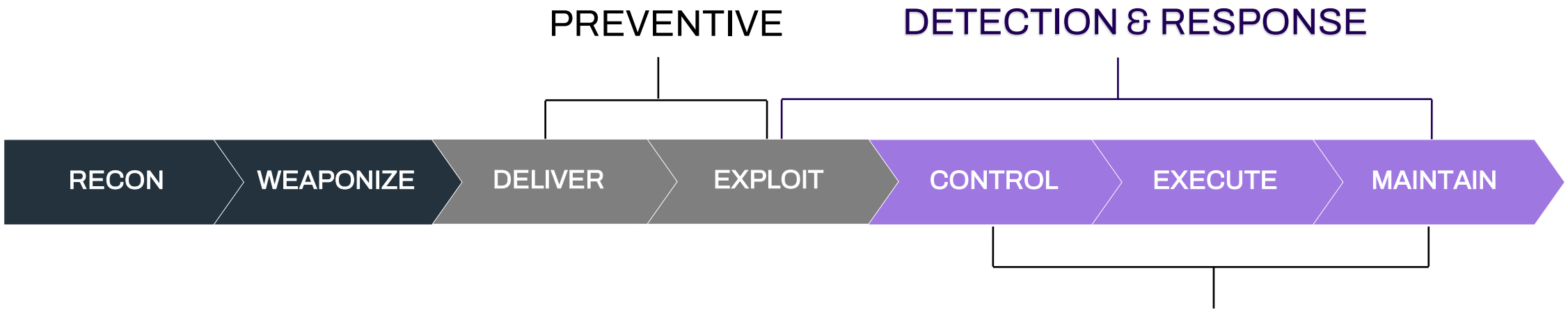


From single-shot, point detections and binary (ON/OFF) responses



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

Answering The Paradigm Shift



MITRE ATT&CK™

TACTICS, TECHNIQUES AND PROCEDURES

Persistence	Discovery	Exfiltration
Privilege Escalation	Lateral Movement	Command
Defense Evasion	Execution	and Control
Credential Access	Collection	

WITH secure

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

WITH secure

Detection & Response In Action

YOUR INFRASTRUCTURE

Workstations Laptops Servers Swarm Intelligence

EVENTS

REAL-TIME BEHAVIORAL ANALYSIS @WITHSECURE'S EDR BACKEND

Expert Insights

Global Threat Intel

Broad Context Detections

Data enrichment & correlation

AI analytics

Data analytics

DETECTION

ELEVATE TO WITHSECURE

Your own IT team OR WithSecure Partner/MSP

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

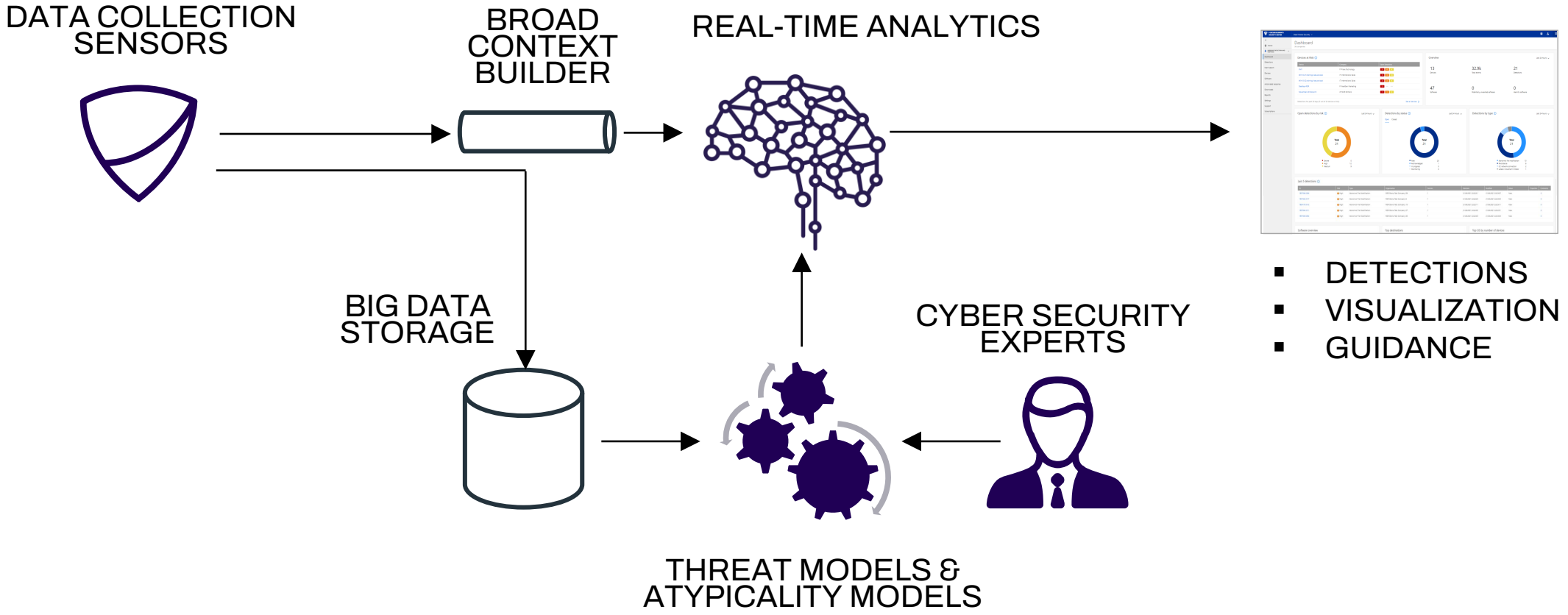
Retrieve logs, tasks

Memory dump

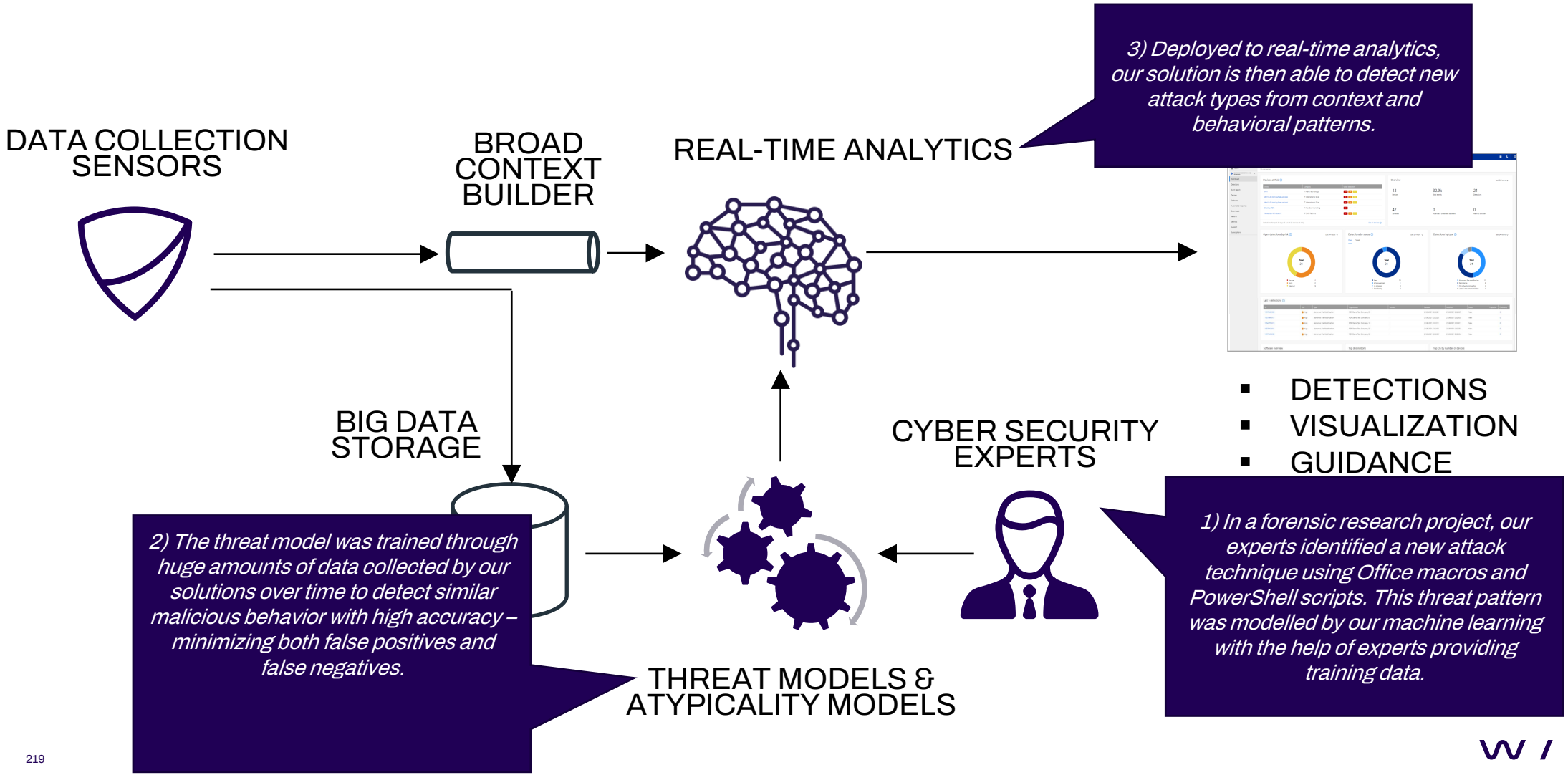
Event Search

Map network connections

AI And Machine Learning At the Heart of the Solution



Threat Model Training
In Action



WITH secure

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.

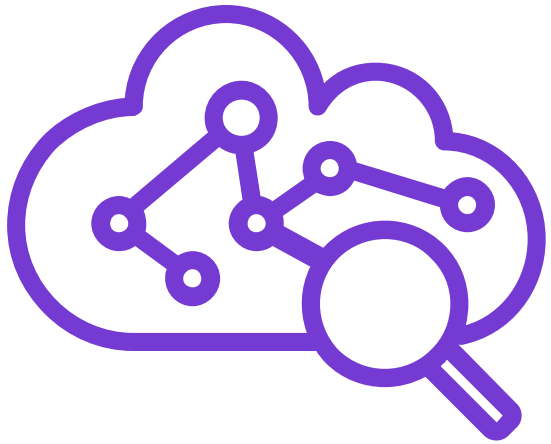
- Privacy and security restrictions (i.e. what it does **not** do):
  - Elements EDR is not intended for monitoring or profiling non-security related activities, including but not limited to employees' habits, interests, or interactions.
  - The focus of data collection is not on individuals or on business 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

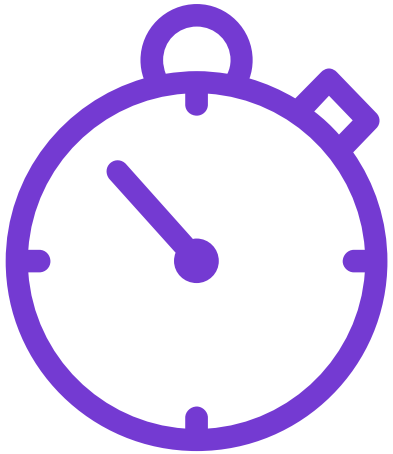
WITH secure

#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



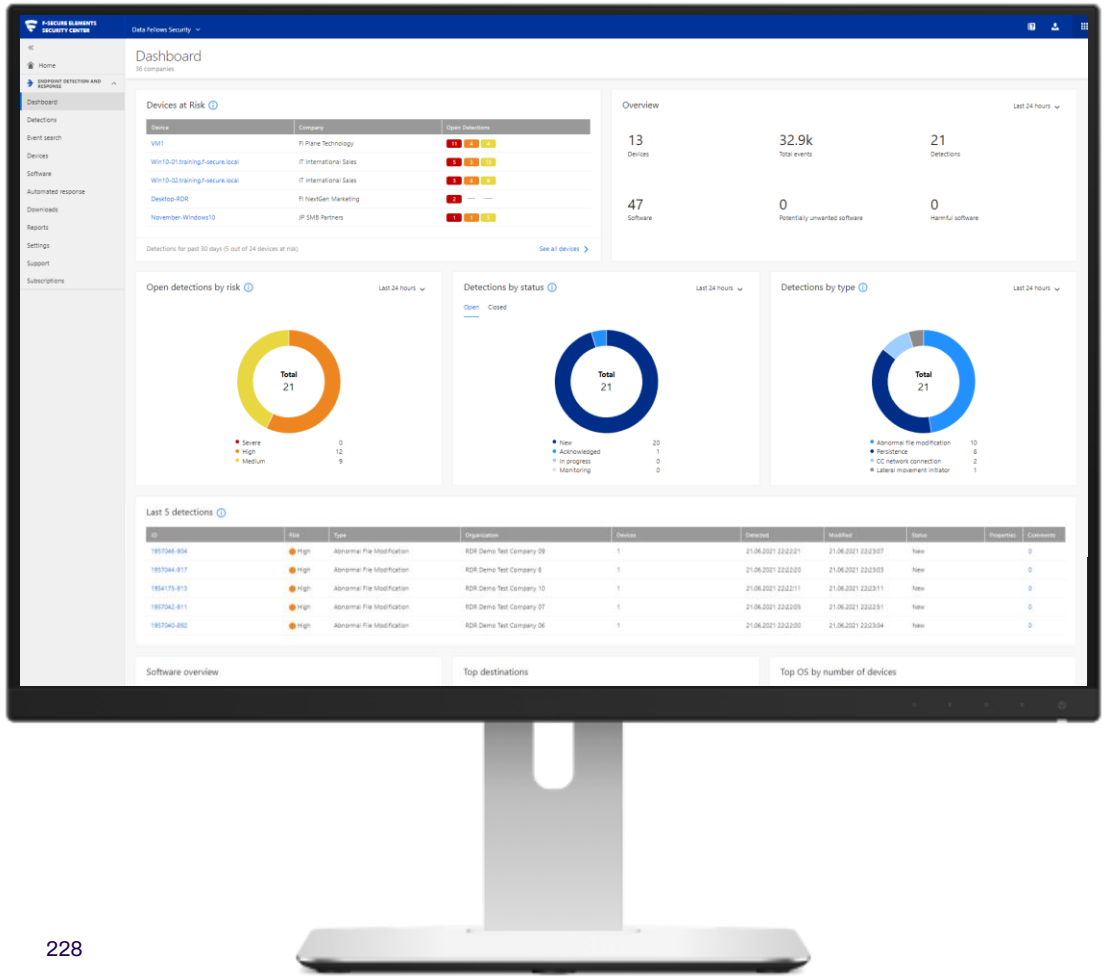
- Detect and stop targeted attacks quickly to **prevent business interruptions** and **impact on brand reputation**
- The detection & response service is **available within days** to have you prepared even before breaches happen
- Meet the regulatory requirements of PCI, HIPAA, and GDPR that requires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

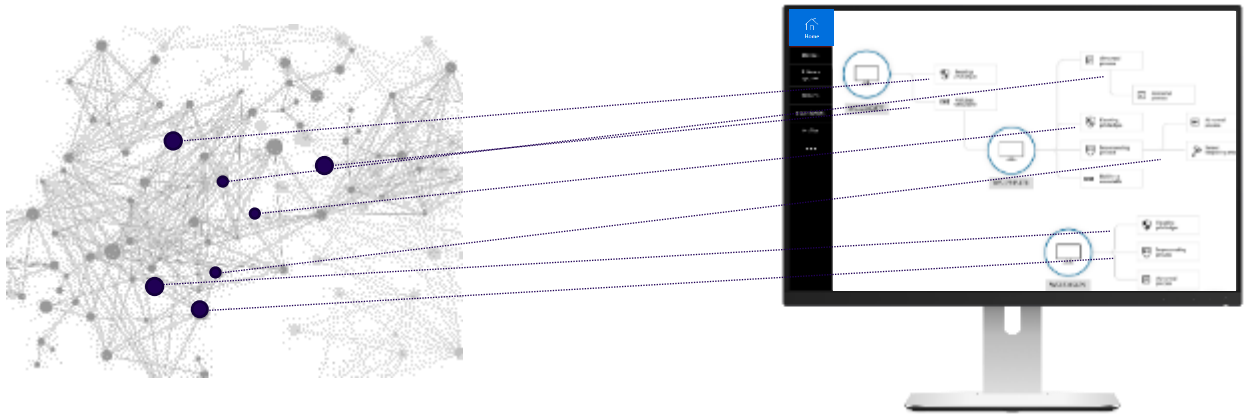
- BROAD CONTEXT DETECTION™
- INCIDENT MANAGEMENT
- GUIDANCE TO RESPOND
- APPLICATION INVENTORY
- CENTRALIZED MANAGEMENT
- HOST ISOLATION
- ELEVATE TO WITHSECURE
- AUTOMATED RESPONSE

WITH secure

Why Broad Context Detection?

YES

NO

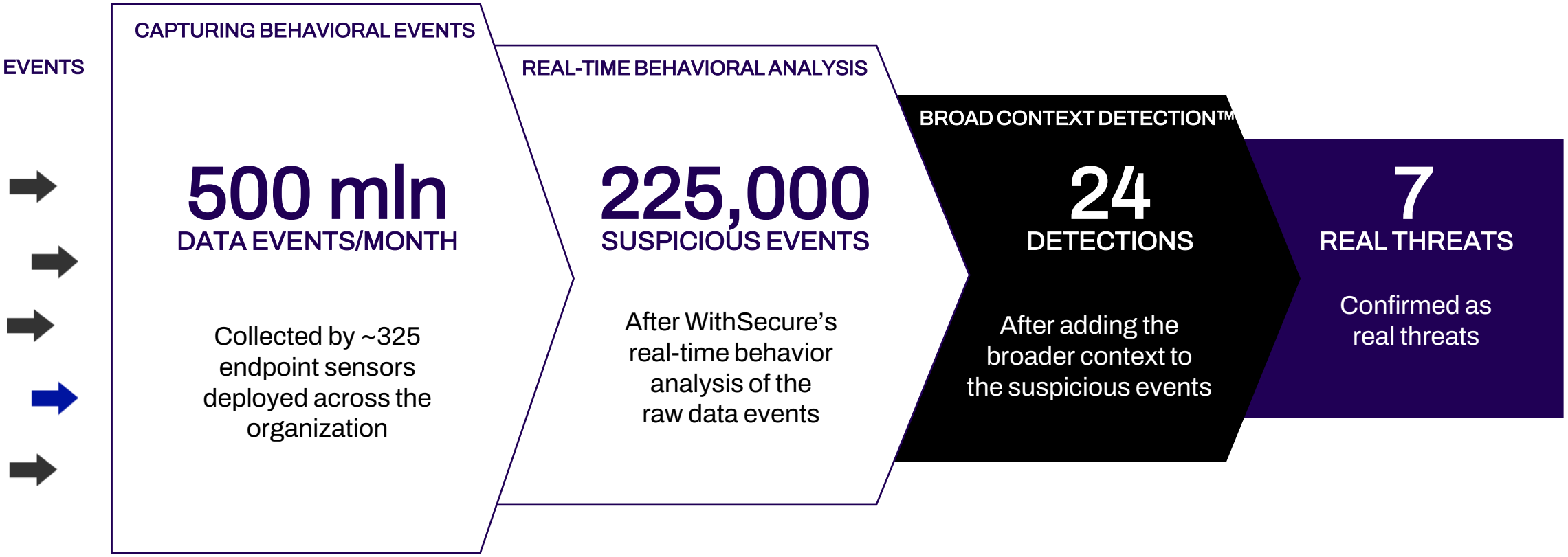


From single-shot, point detections and binary (ON/OFF) responses common for endpoint protection platforms.

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

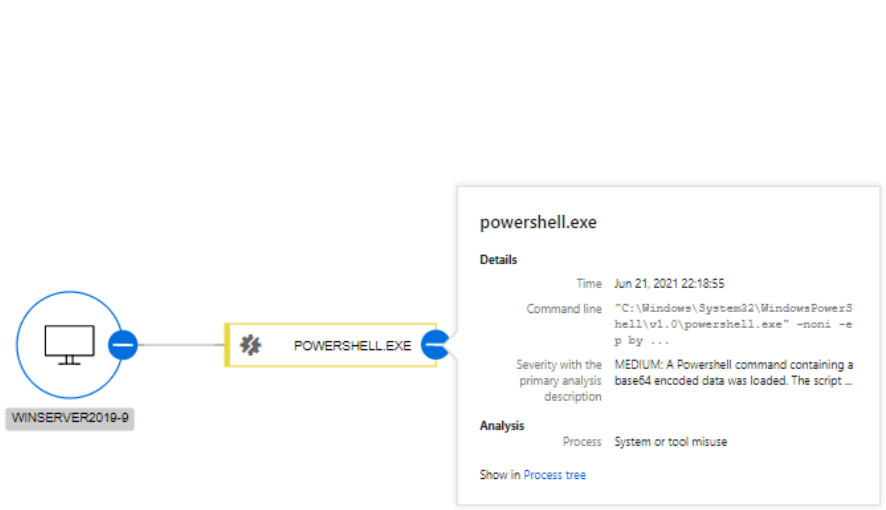
Presents only relevant detections with actionable visualization for risk-based and multi-faceted response.

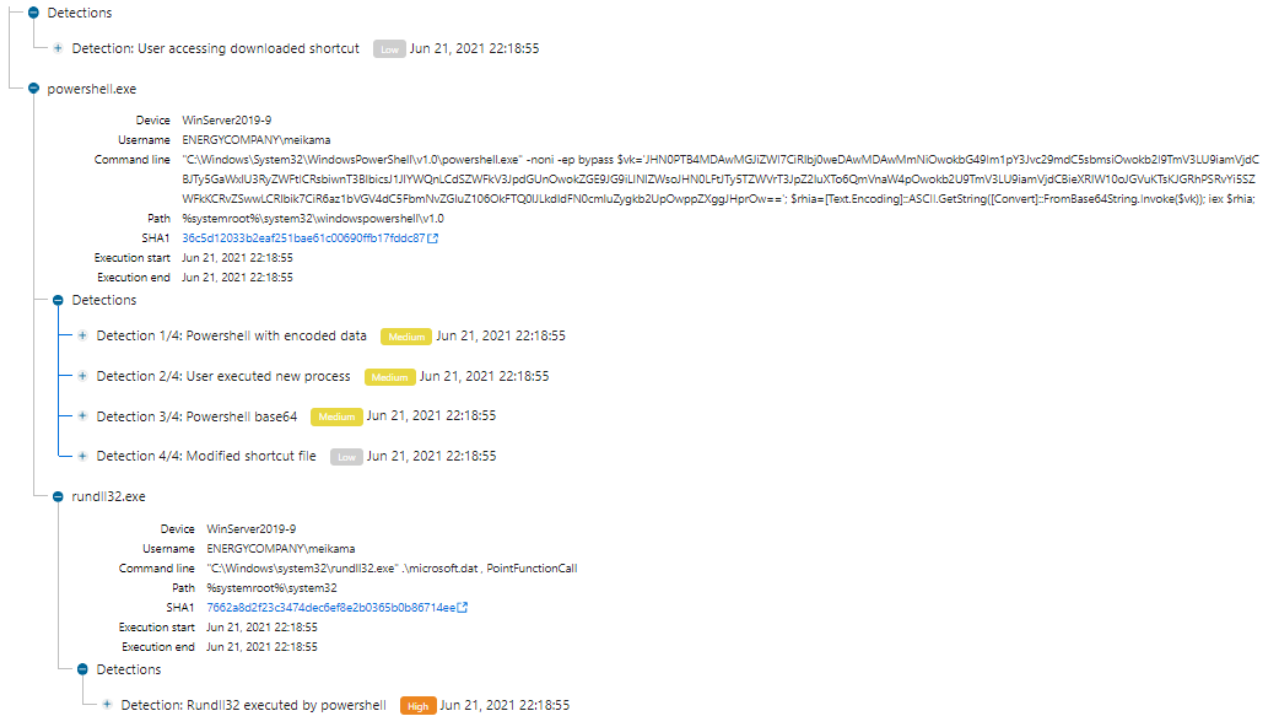
Broad Context Detection In Action



WITH secure

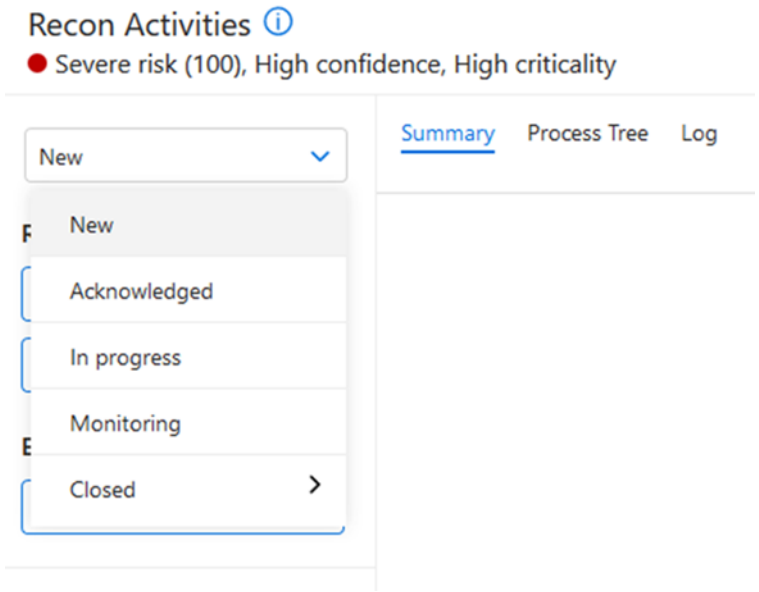
Feature Highlights:
Broad Context Detection





WITH secure

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

WITH secure

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

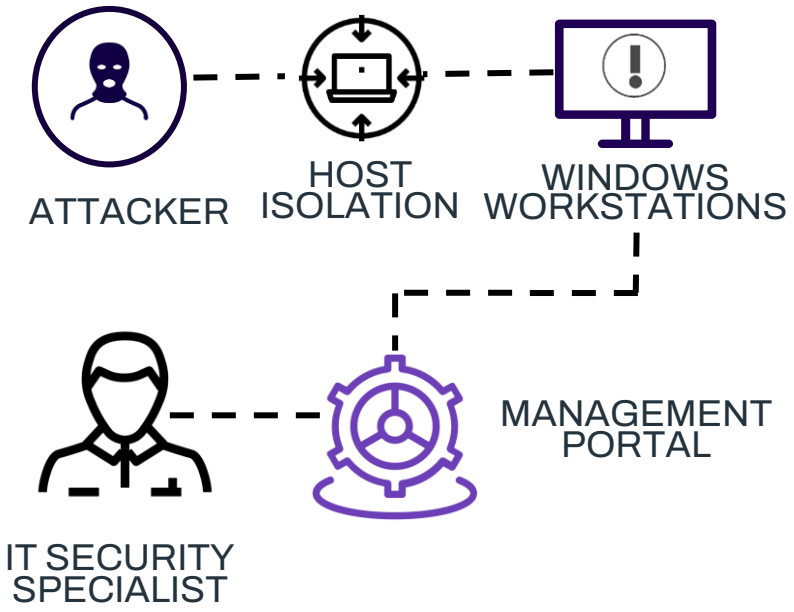
CONTAIMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

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

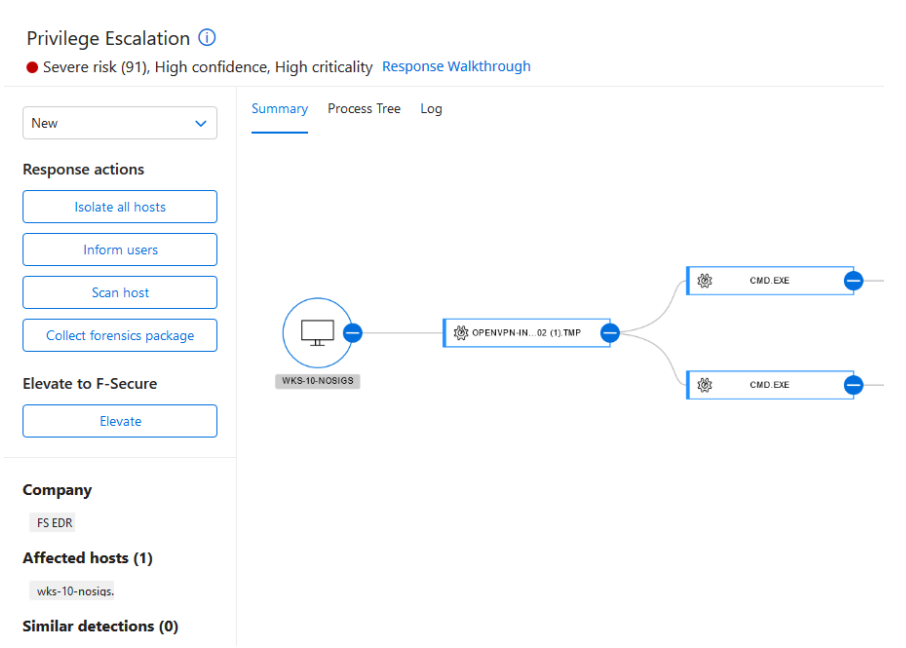
Feature Highlights:
Host Isolation



- 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

WITH secure

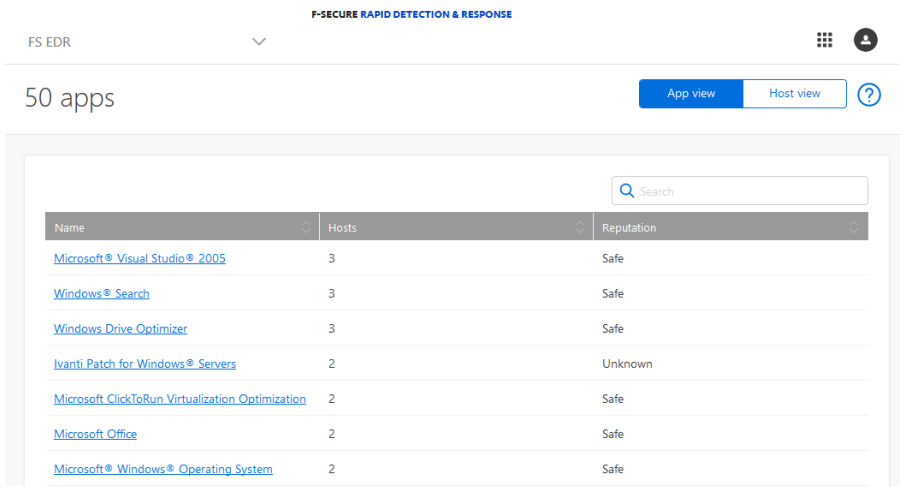
Feature Highlights:
Guidance To Respond



- 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

WITH secure

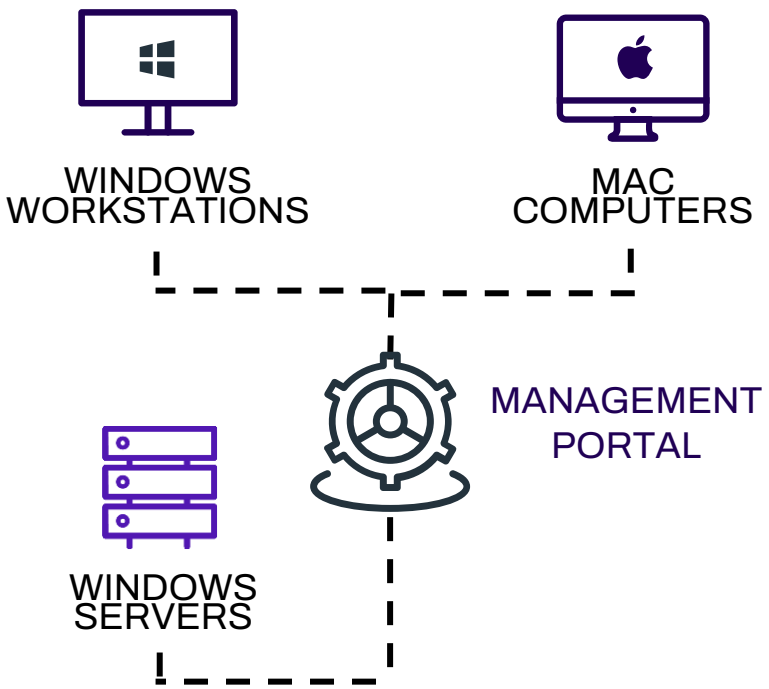
Feature Highlights:
Application Visibility



- 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

WITH secure

Feature Highlights:
Centralized Management

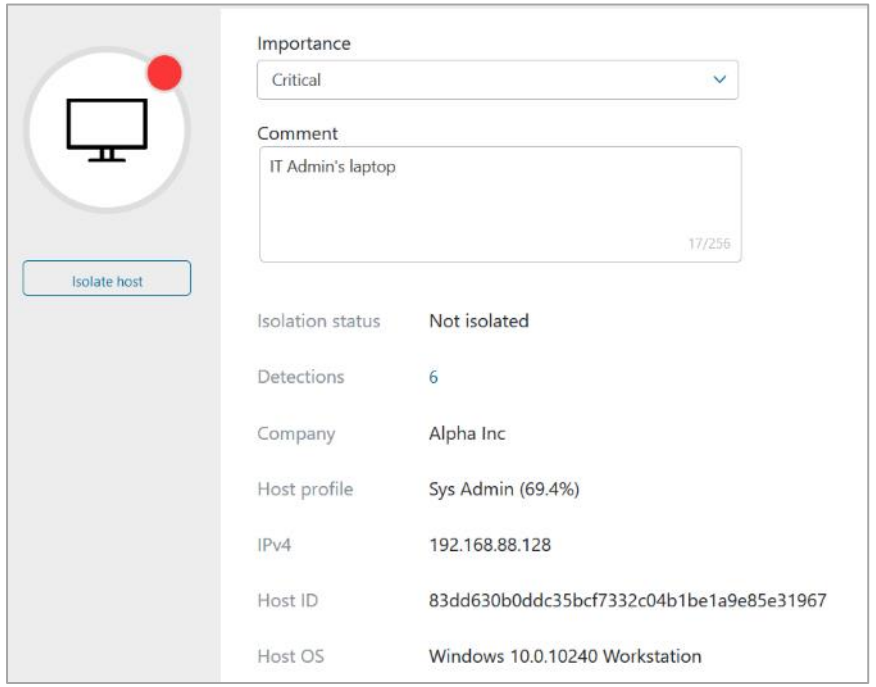


- Unifies visibility and control with cloud-based centralized management portal
- Unites WithSecure's endpoint protection*, detection and response into a single client
- Works with any endpoint protection solution as a lightweight sensor

*WITHSECURE ELEMENTS ENDPOINT PROTECTION (ELEMENTS EPP)

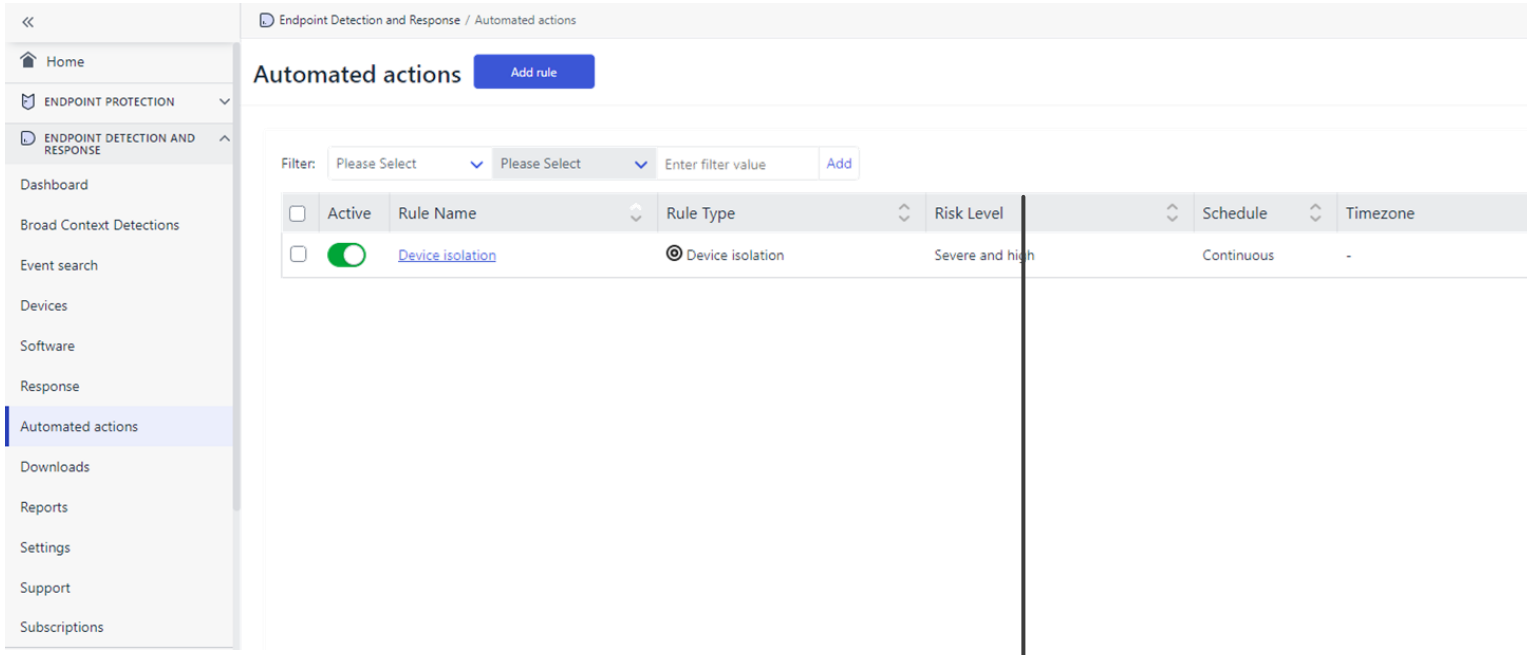
WITH secure

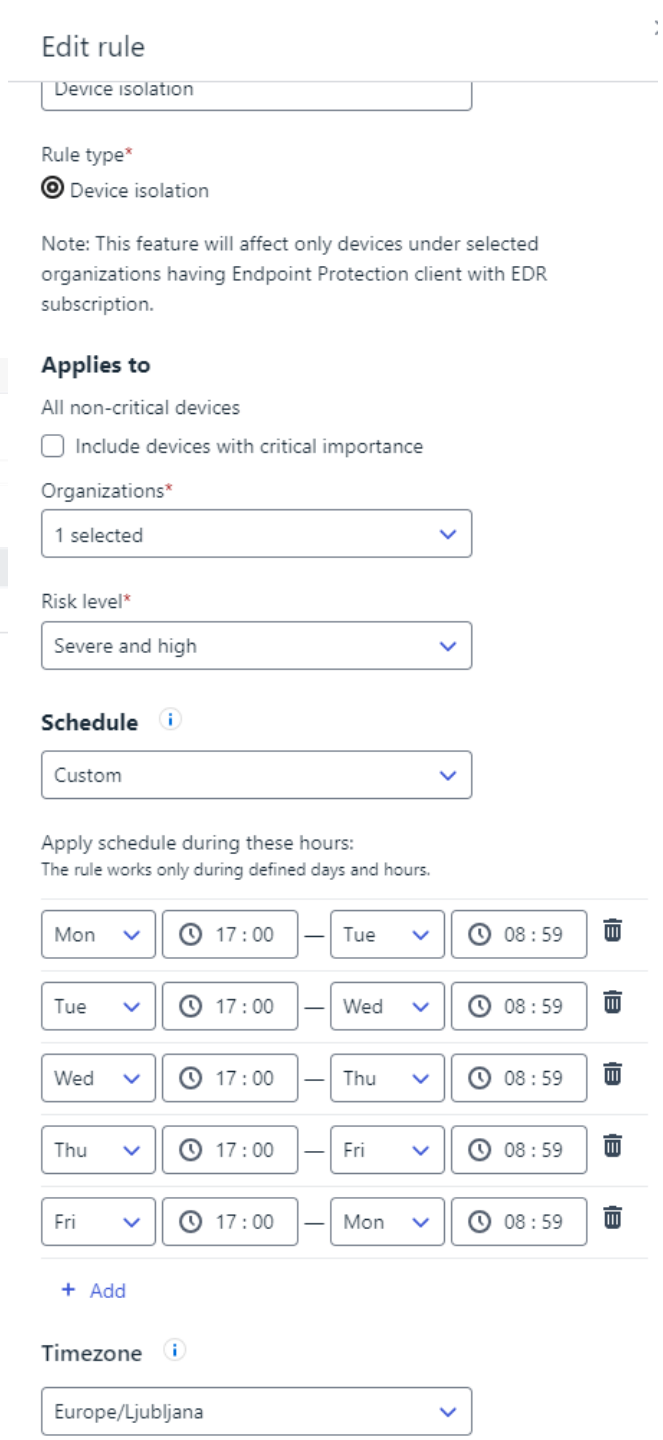
Feature Highlights:
User And Entity Profiling



- 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





- Automates risk-based response actions outside business hours
- Stops attacks quickly by isolating impacted hosts

WITH secure

Feature Highlights
Elevate To WithSecure

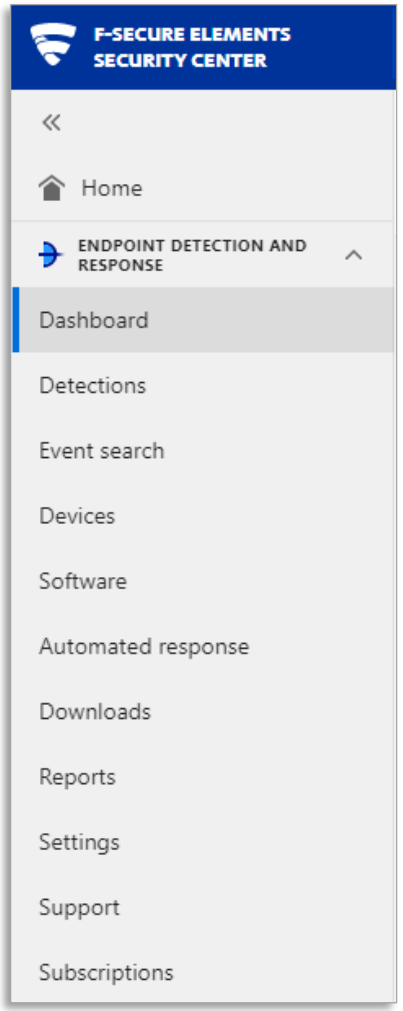
- Elevate to WithSecure feature for Partners when additional advice is needed
- WithSecure Detection & Response Team expertise is used for best knowledge and recommendations 24/7
- Trackable communication with experts

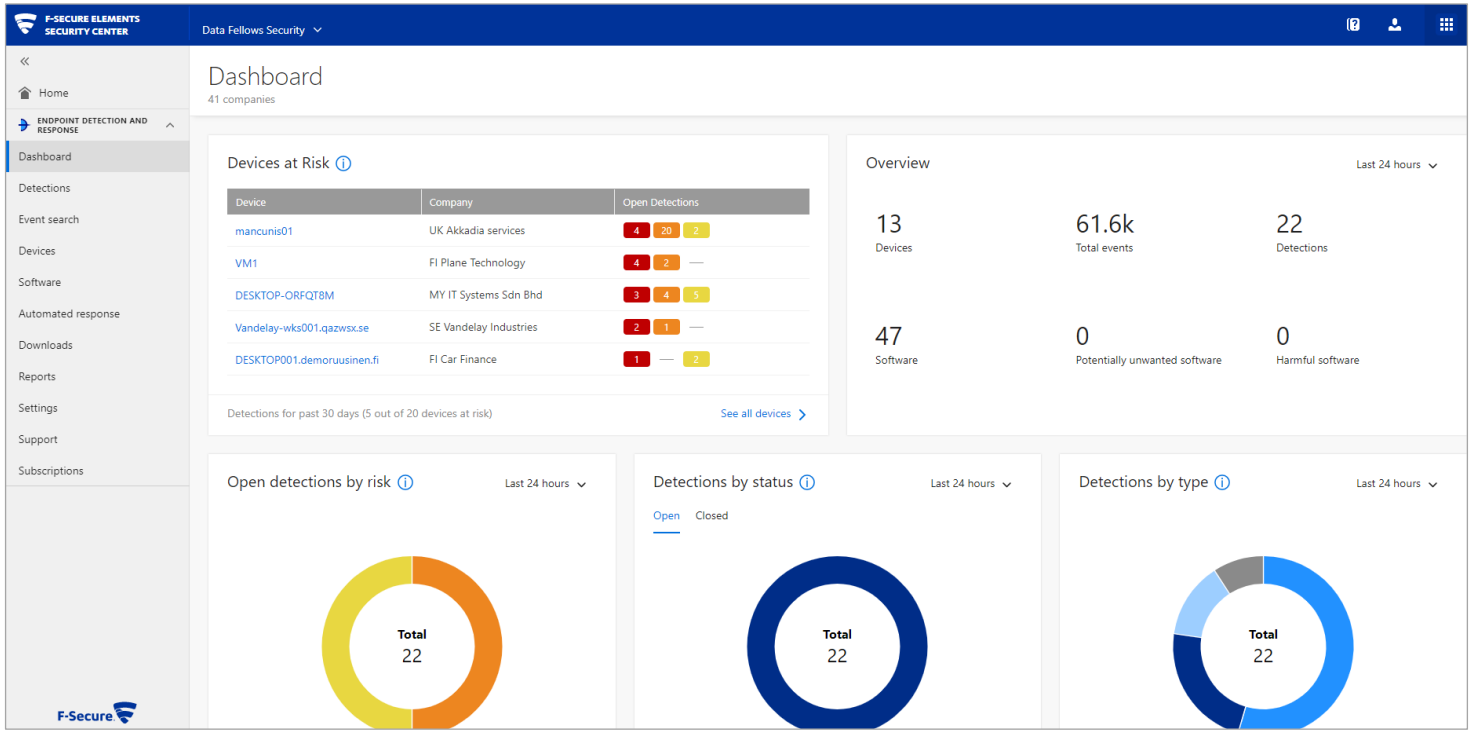
Using the ESC

Elements EDR

WITH secure

EDR in the ESC

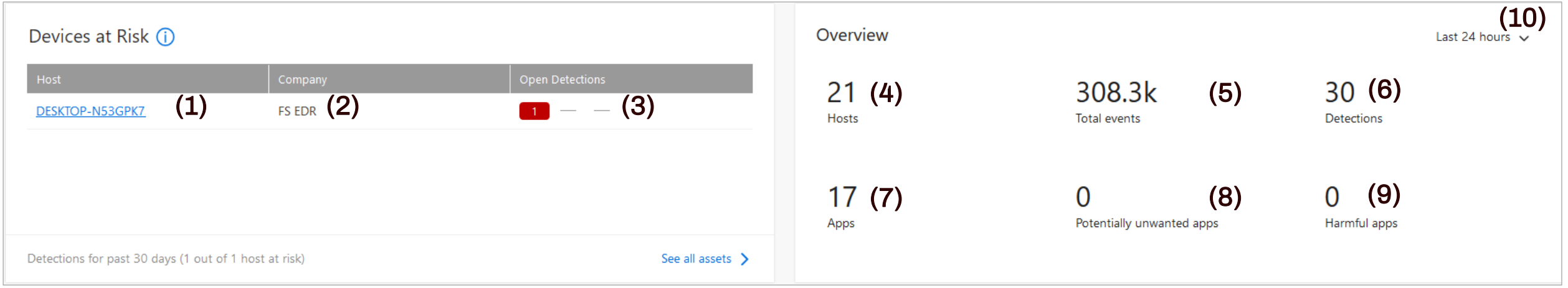




WITH secure

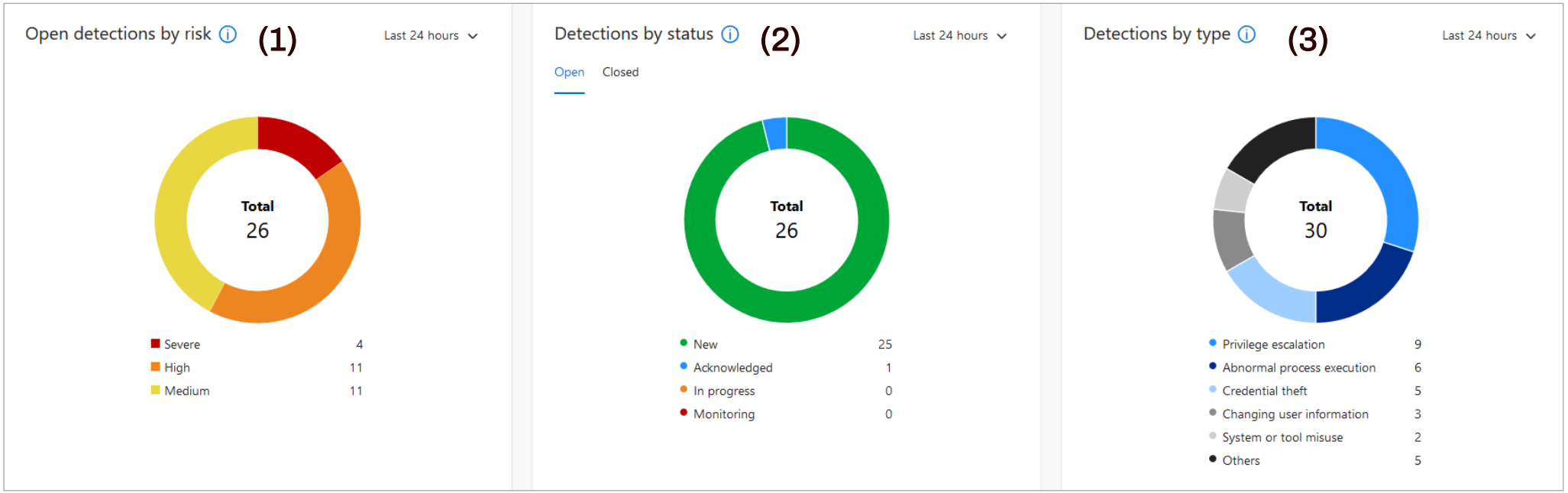
Checking The Overall Status Of Managed Devices And Events

- 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).



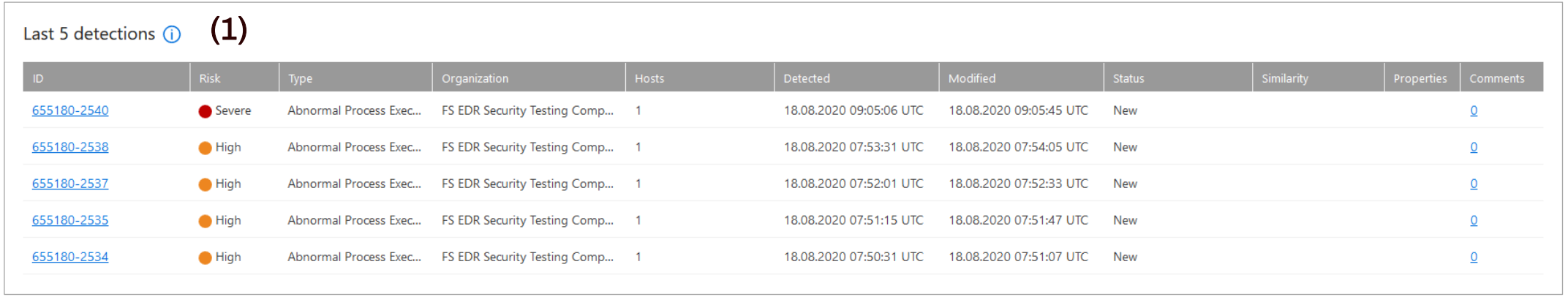
Checking Detections

- 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.

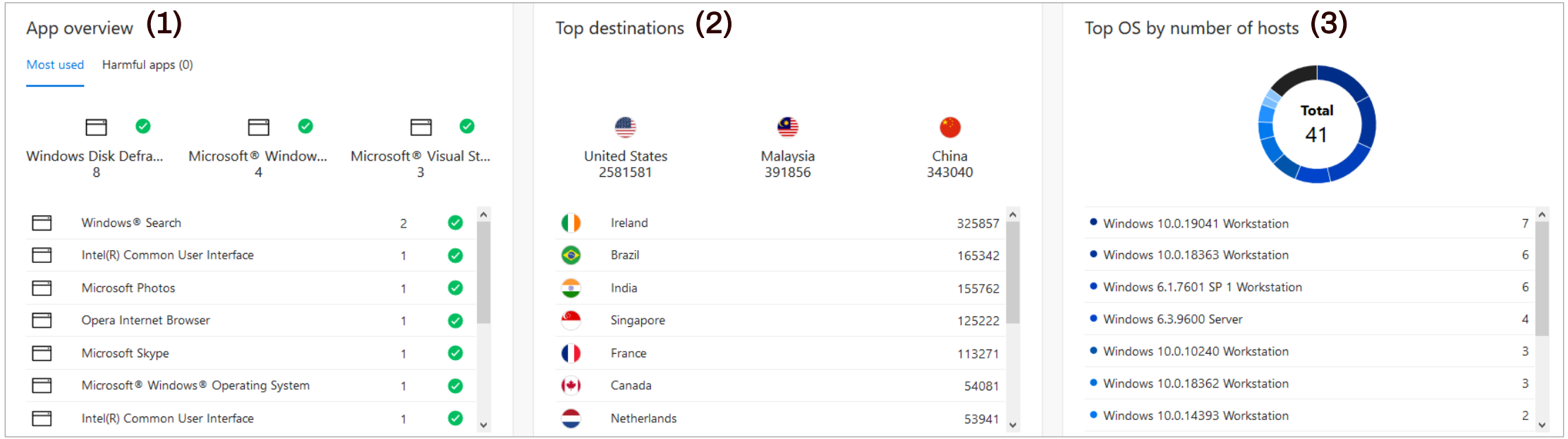


Last 5 detections (1)

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

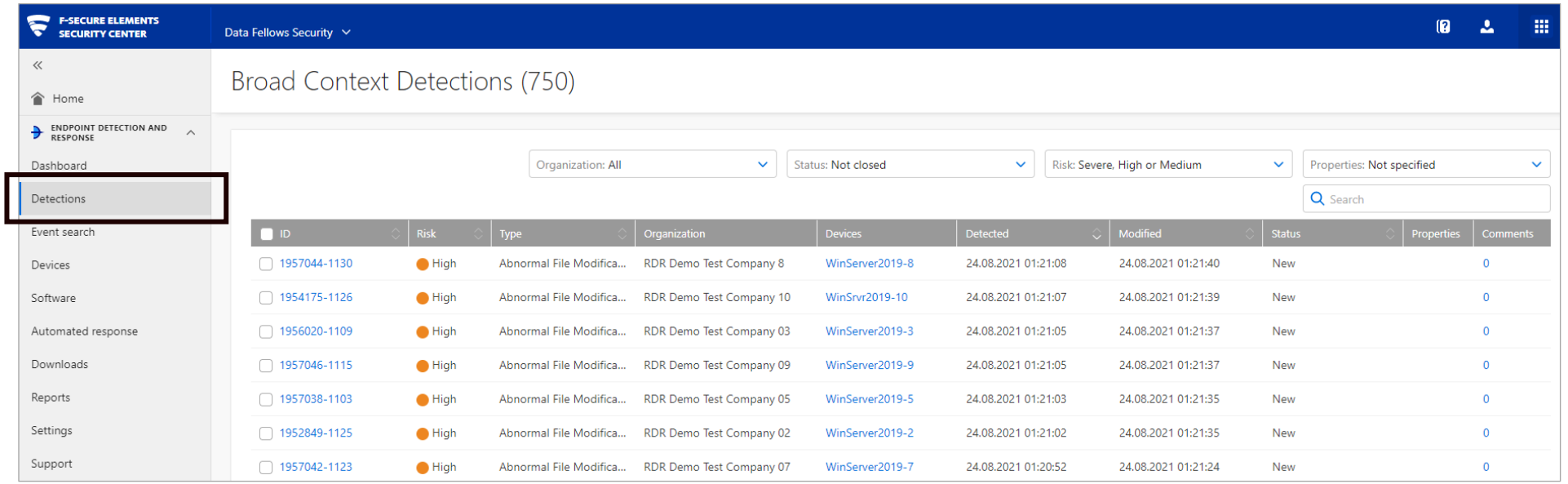
Checking The Application Overview

- 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).



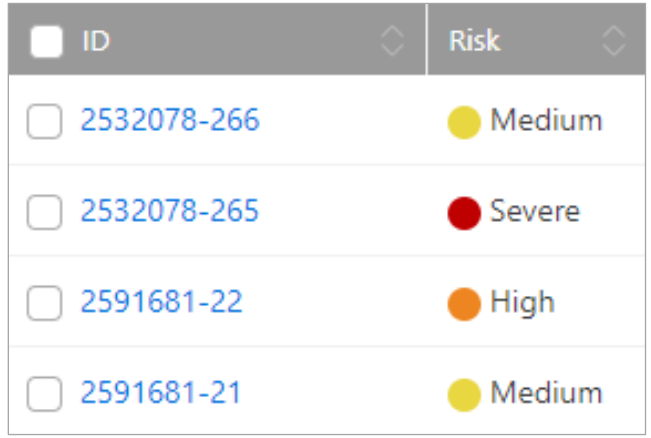
The Detections Page

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



The Detections Page
Detection List

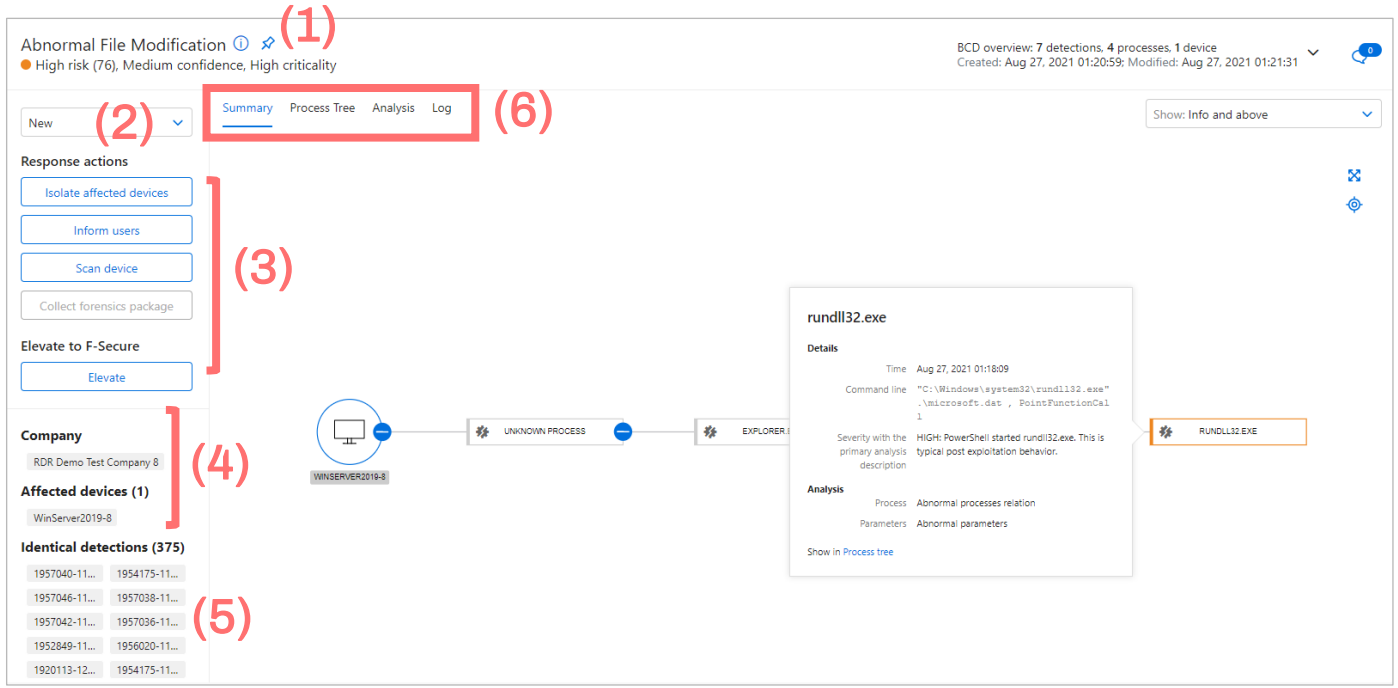
- On the Detections page, there is a list of Broad Context detections in your network that, by default, is organized from newest to oldest.
- All detections are color-coded based on criticality:
  - Red: Severe risk
  - Dark orange: High risk
  - Yellow: Medium risk
  - Grey: Low risk
- Open detections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



The Detections Page
Filter & 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



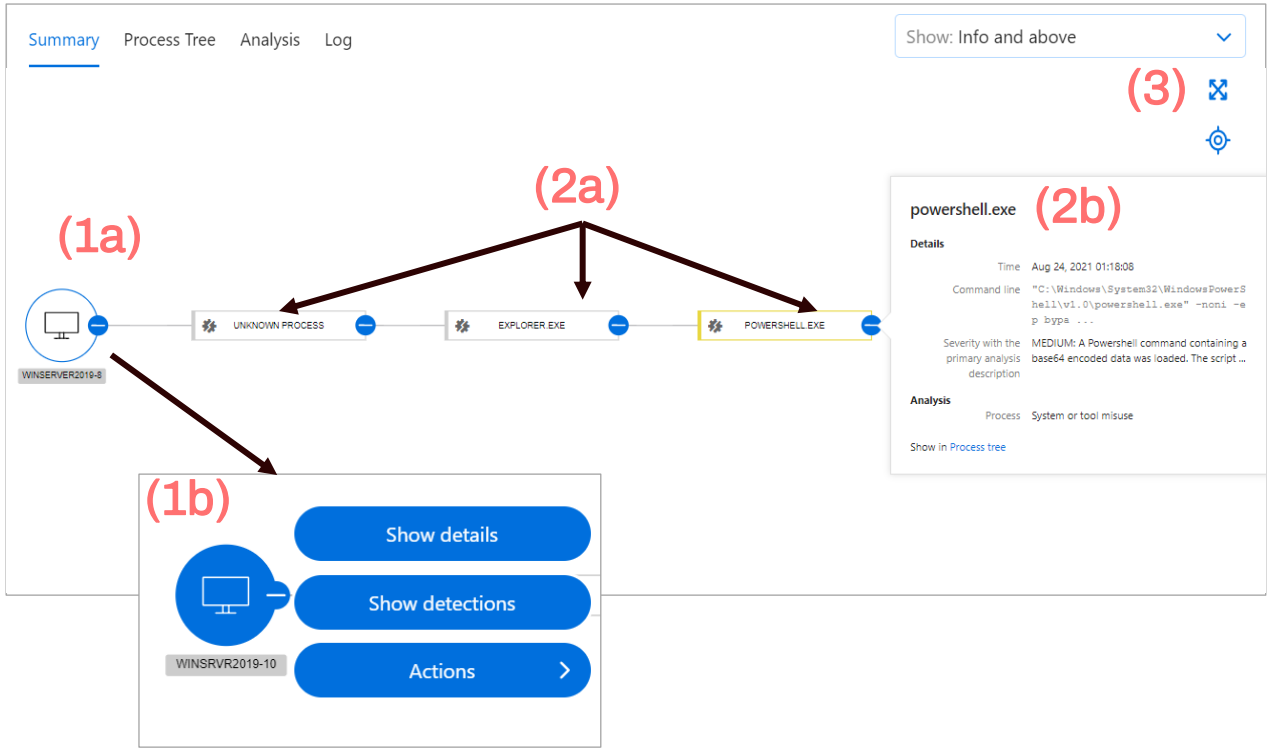
When viewing a specific detection, you are presented with the following information:

- 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

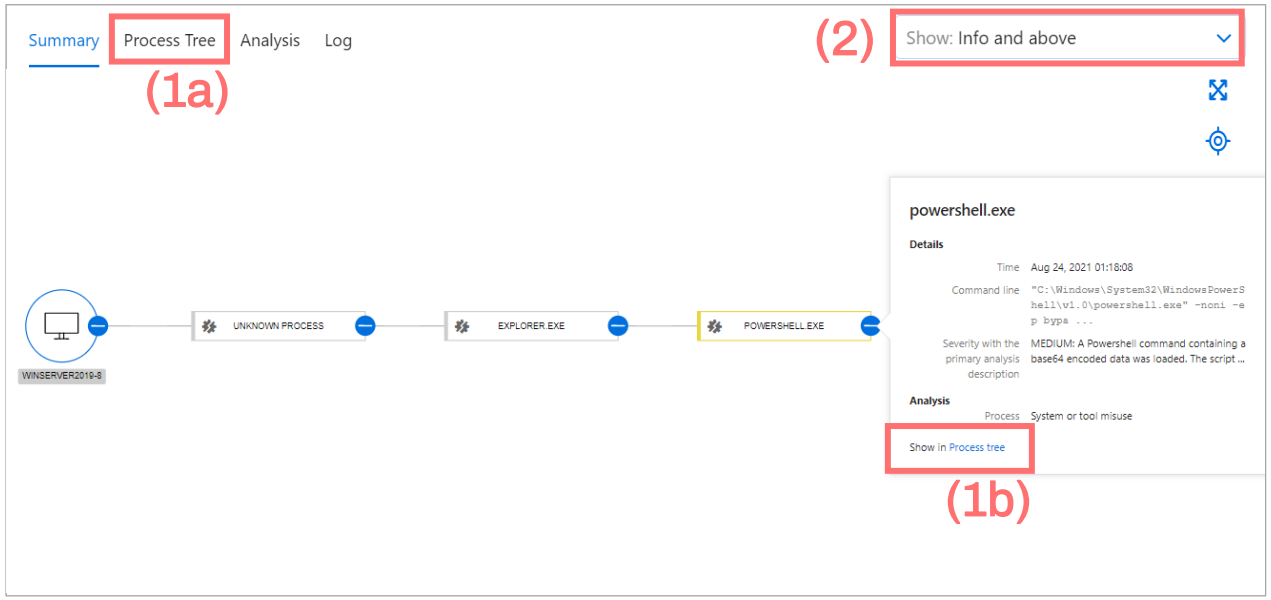
- The right side of the Summary tab shows you how the Broad Context Detections are connected in a graphical way.
- Click the Computer (1a) to view more details and possible actions available (1b).
- You can also click any of the detections in the Process (2a) to get more detailed information (2b).
-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



WITH secure

The Detections Page
Summary View Continued

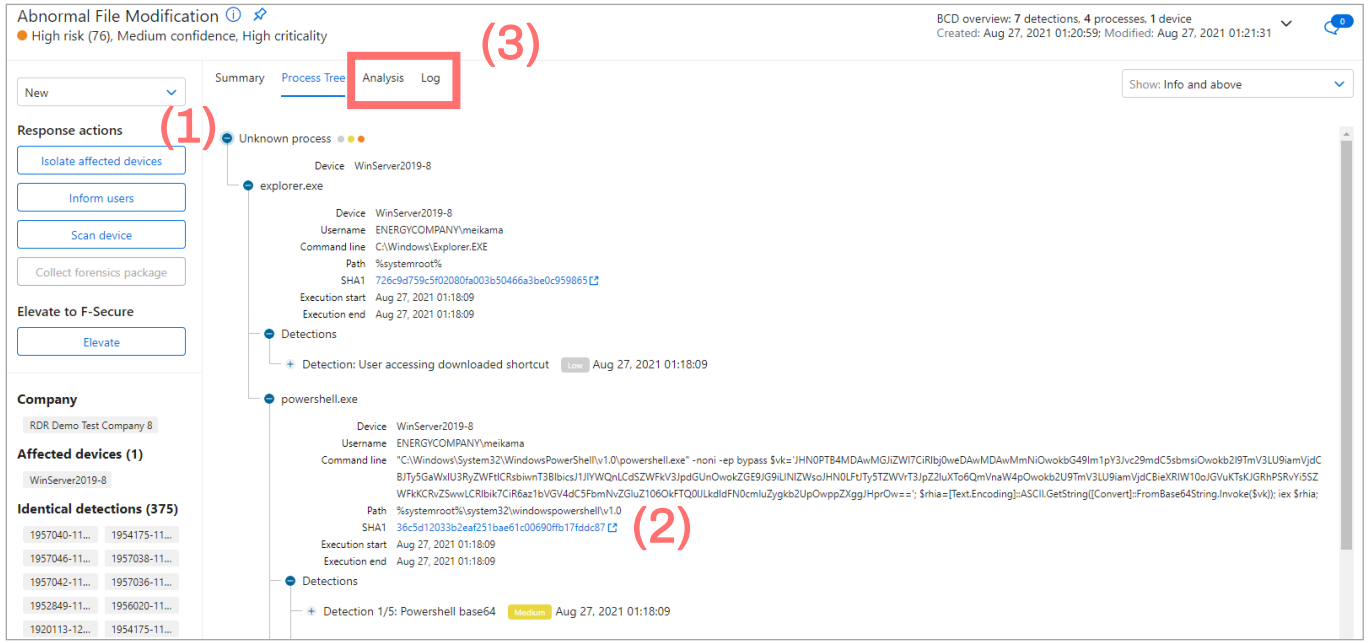
- The full command line is visible from the Process Tree view (1a, 1b) if further analysis is needed. We'll look at this tab next.
- Note that the processes are color-coded the same way as detections.
  - Red for severe, dark orange for high, yellow for medium, and grey for low
- You can also filter 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.



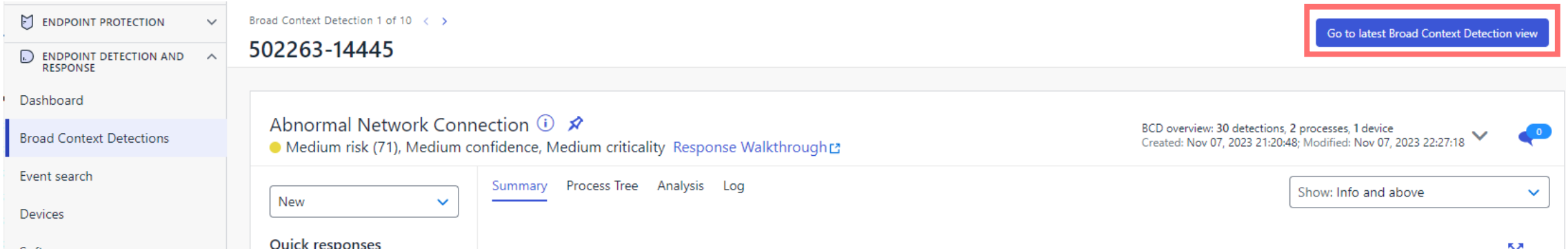
WITH secure

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.

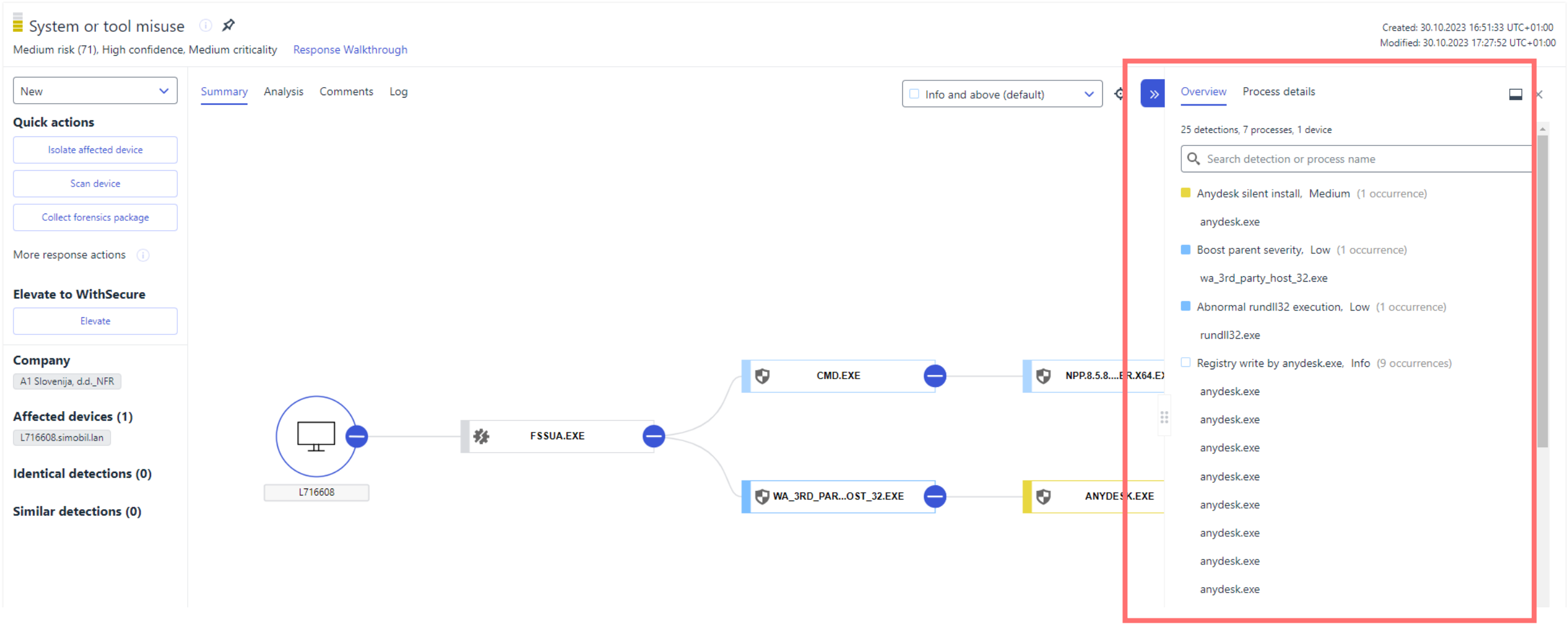


The Detections Page
New Broad Context Detection view



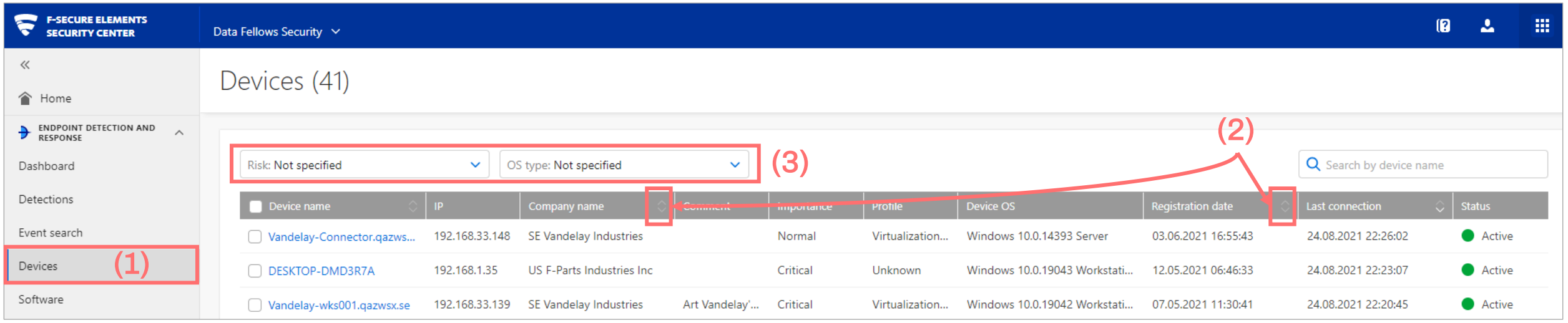
WITH secure

The Detections Page
New Broad Context Detection view



The Devices Page

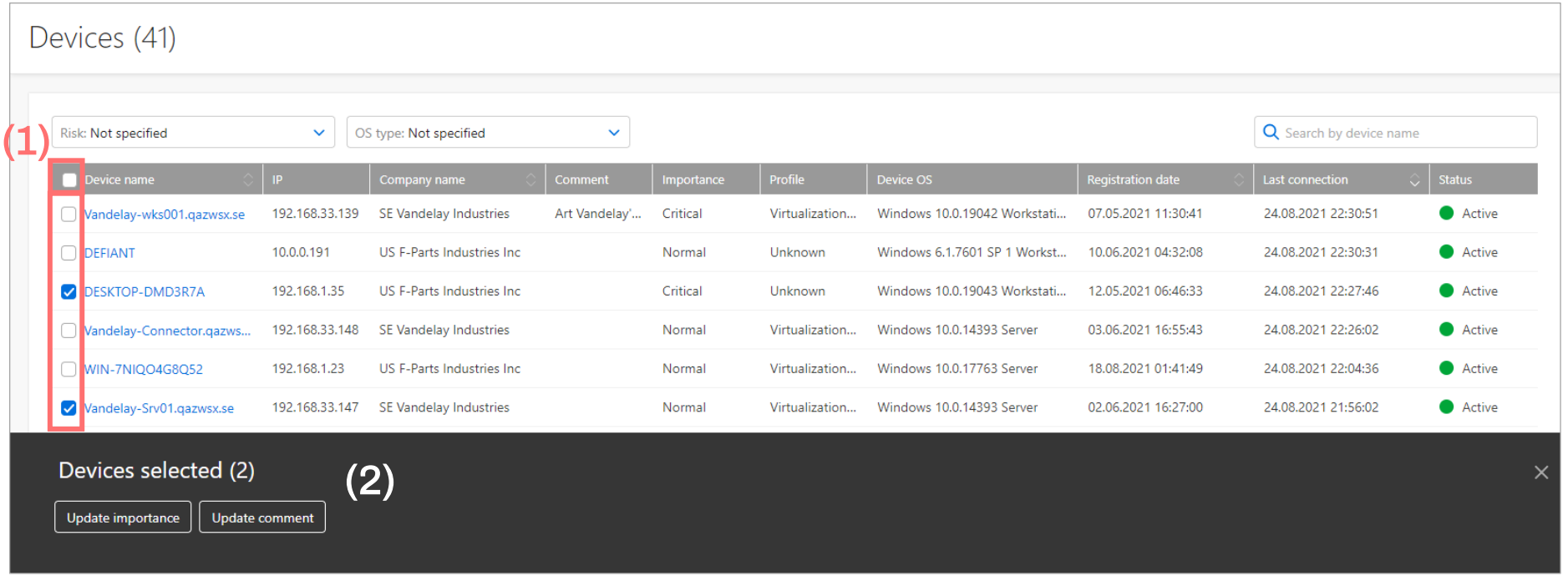
- The Devices page contains all devices with EDR sensors installed in your network (1).
- By default, the page is organized by last connection, however, click the up/down arrows next to a category (2), like company, to change how entries are organized.
- You can also filter these by risk or device OS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



WITH secure

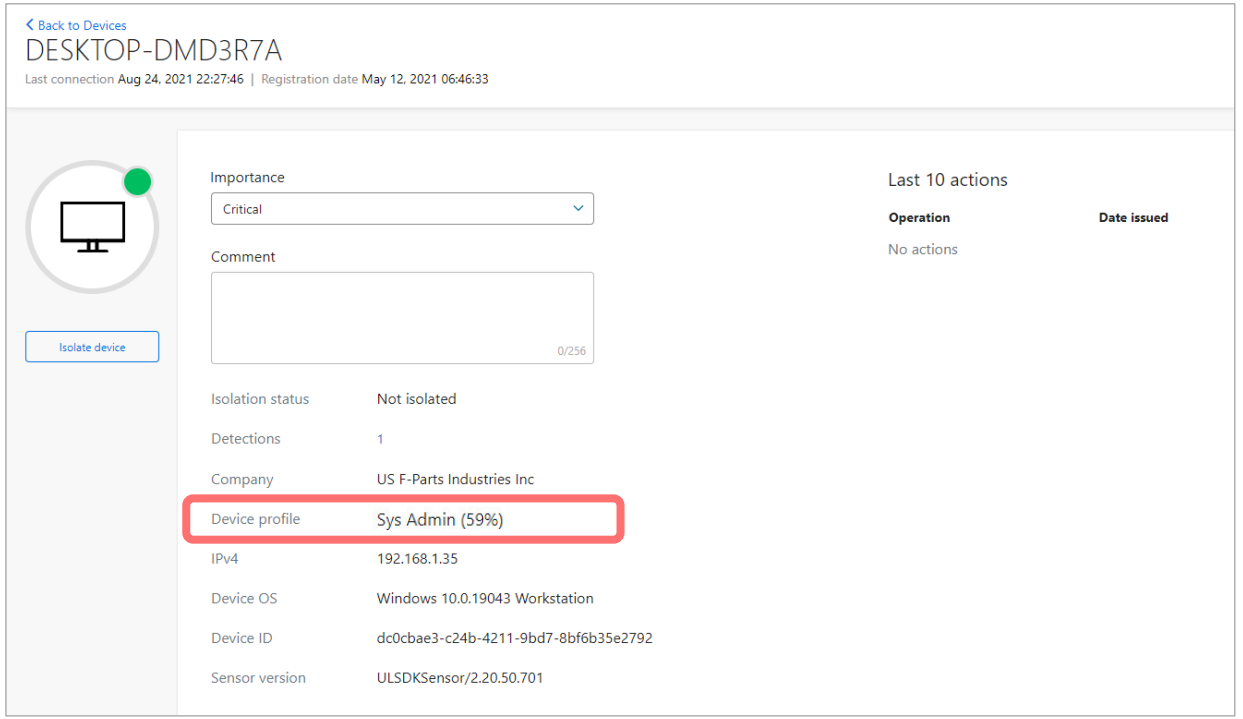
The Devices Page
Operations

- 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).



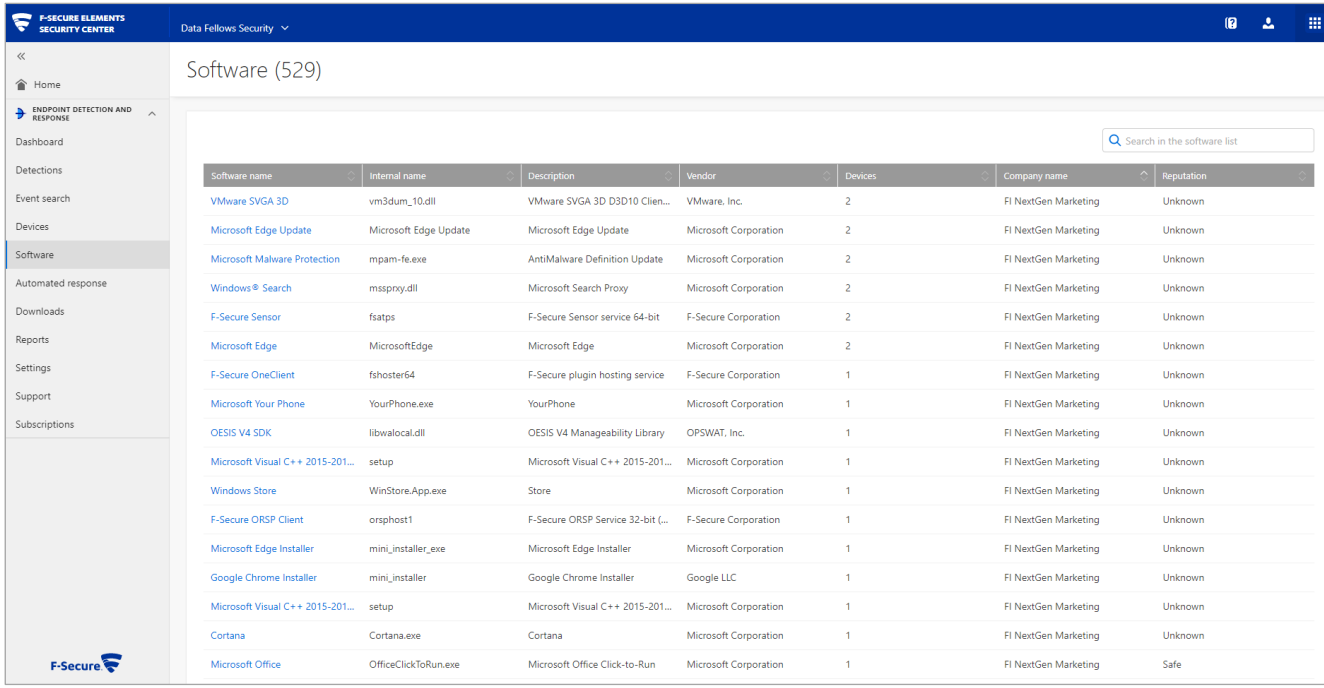
The Devices Page
Device Profile

- 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.



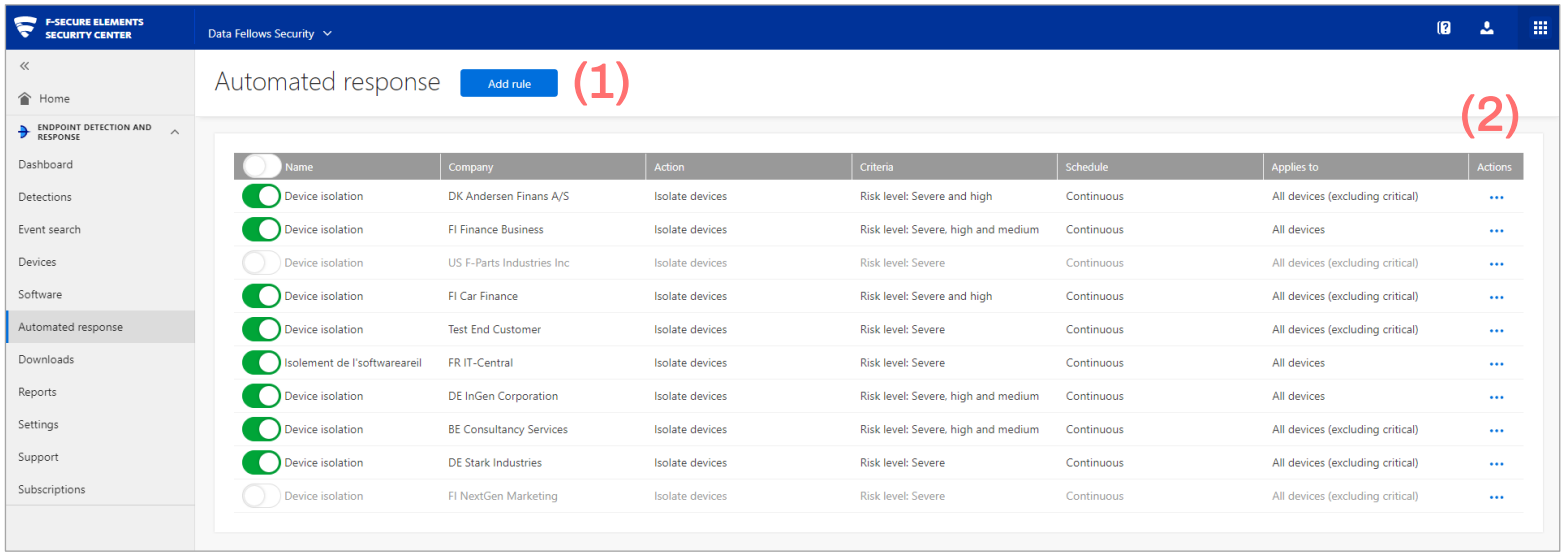
The Software Page

- 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.



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.

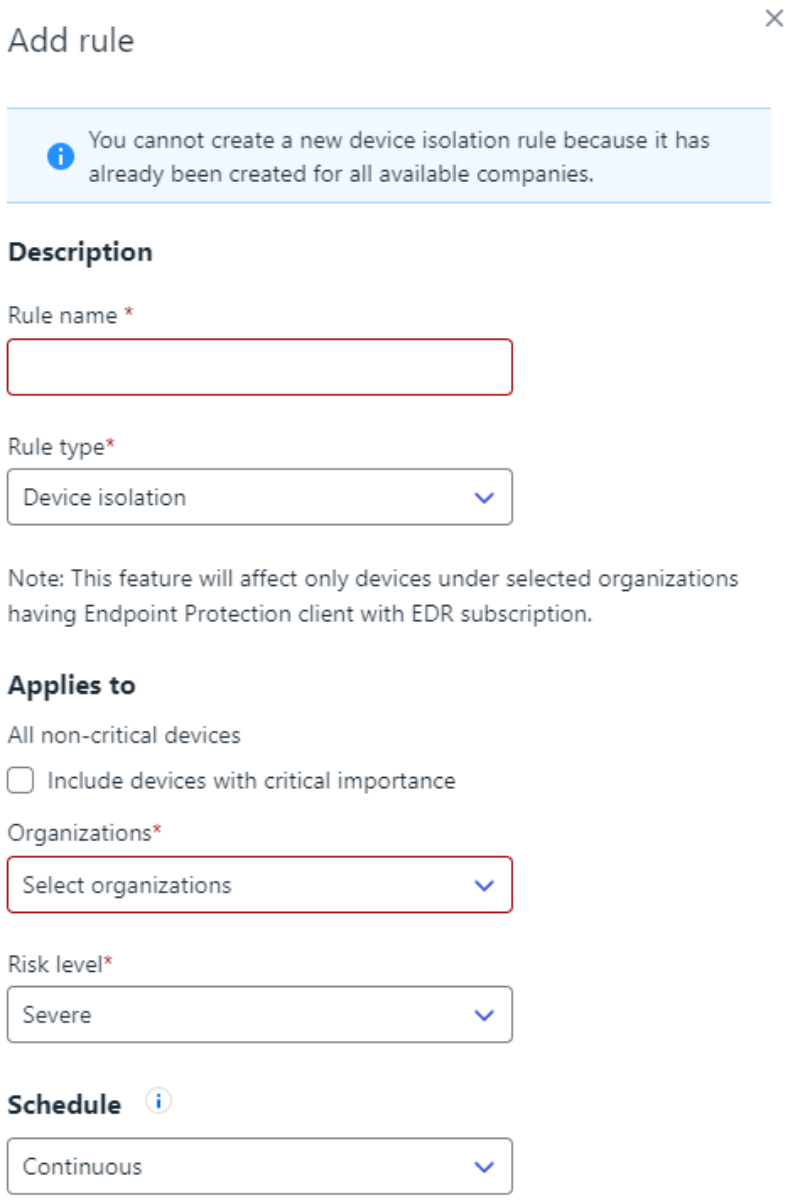


WITH secure

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

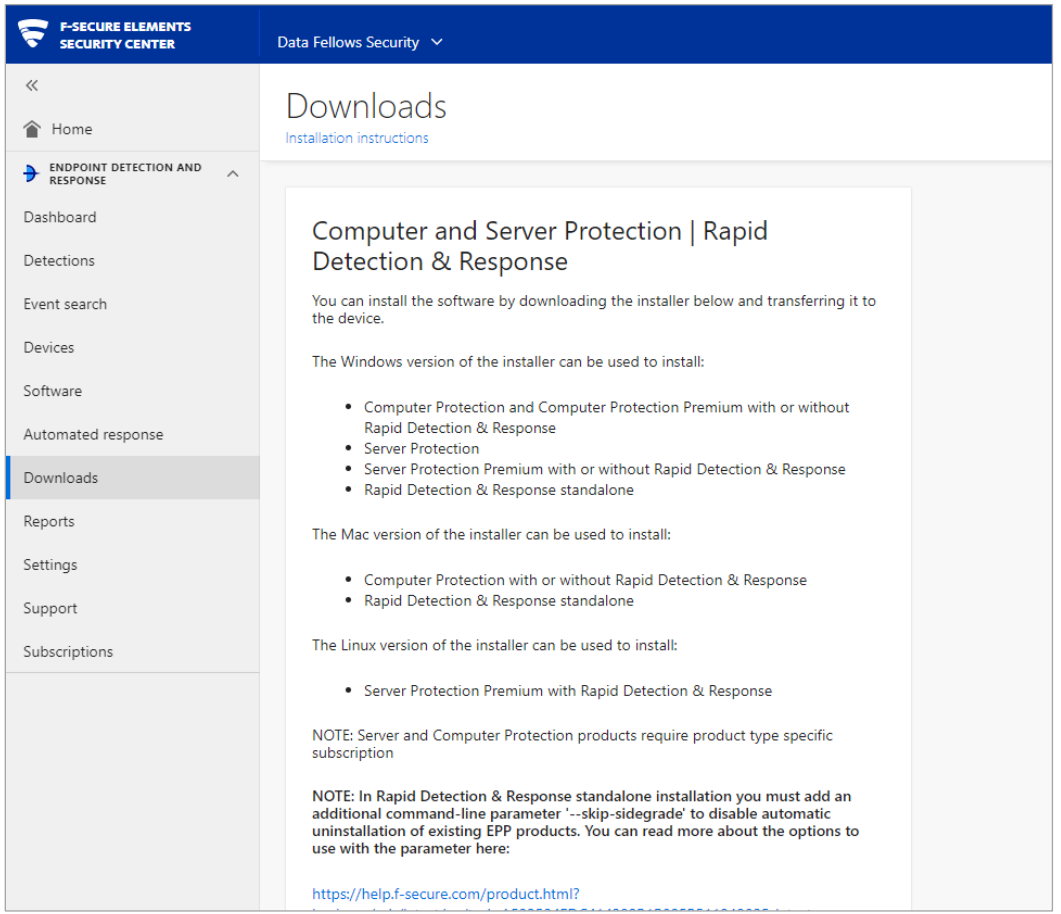
- The schedule is continuous or on a custom schedule and will remain in effect so long as the rule remains enabled.



WITH secure

The Downloads Page

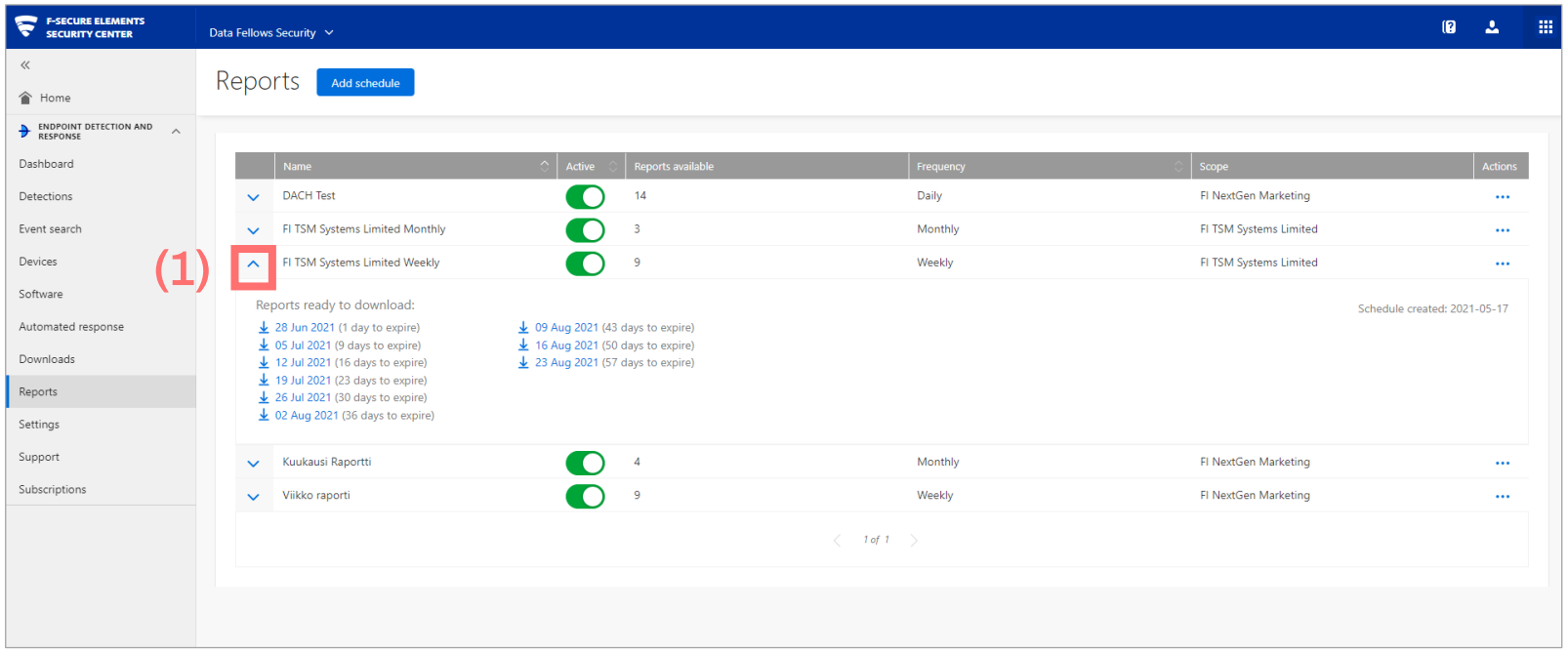
- The Downloads page contains the sensor installers for both server and computer clients.



WITH secure

The Reports Page

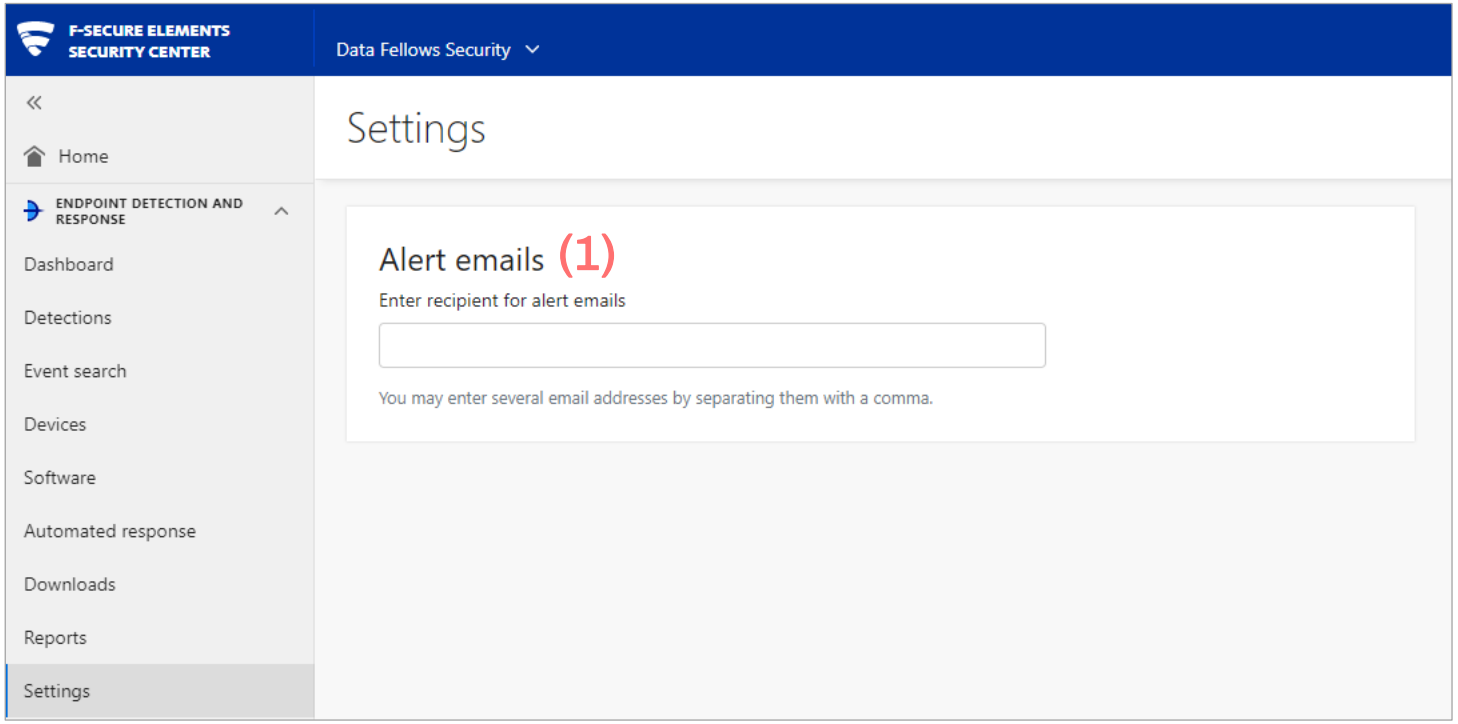
From the Reports page it is possible to Schedule reports to be made automatically. Click the downward arrow or chevron (1) to see the reports that have already been compiled.



WITH secure

The Settings Page

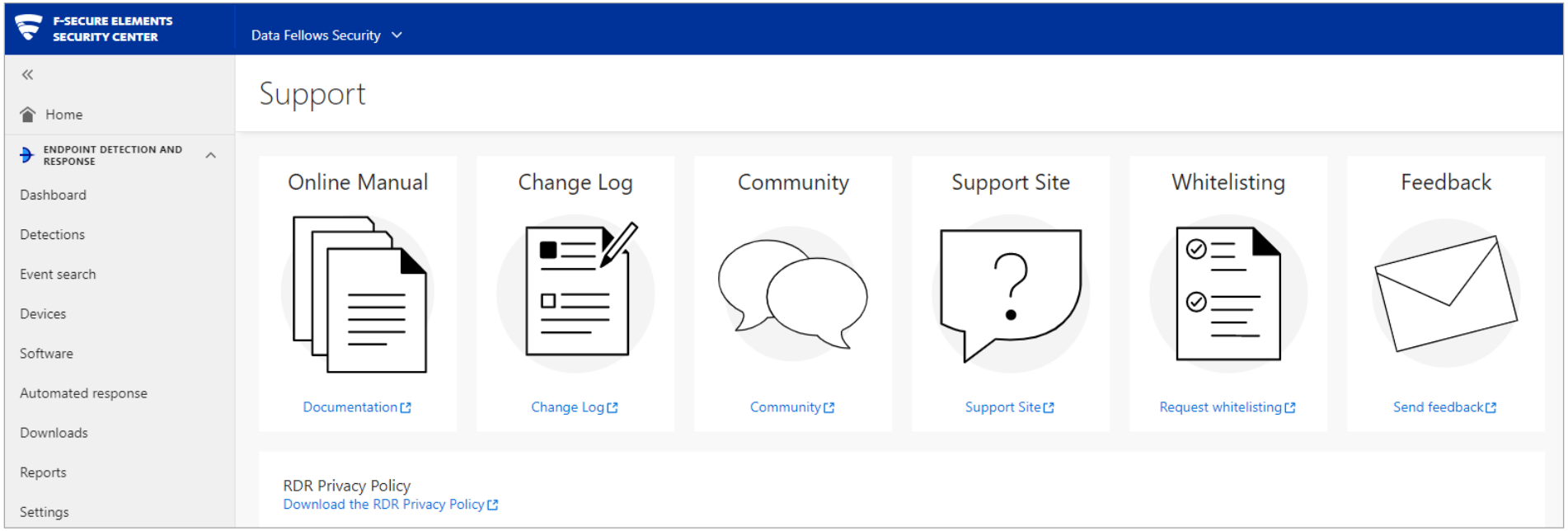
- On the Settings page, you can set the alert email addresses (1).
- Note that it is critically important to input at least one email here, as all alerts will be sent to the address (or addresses) listed here. **If there is no email provided, you will not receive any alerts.**
- Separate emails with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



WITH secure

The Support Page

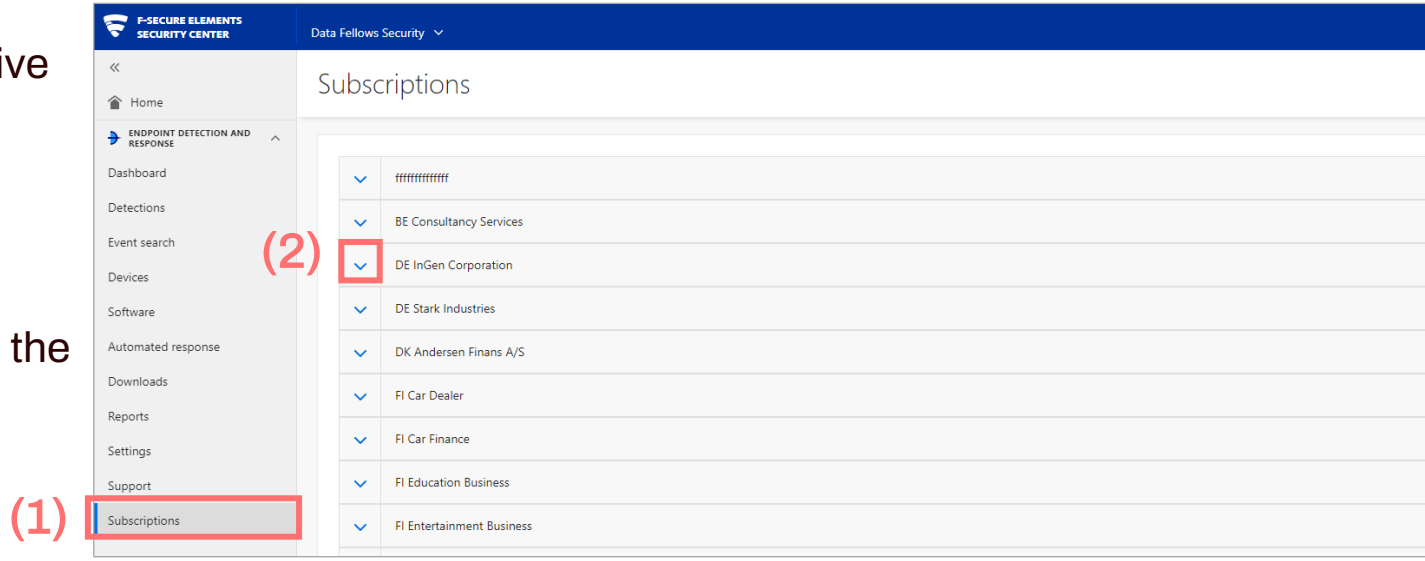
- The Support page contains links to the user guide, changelog, WithSecure community, WithSecure support page, whitelisting request link, feedback form, and EDR Privacy Policy. We'll look more at each in the Troubleshooting module.

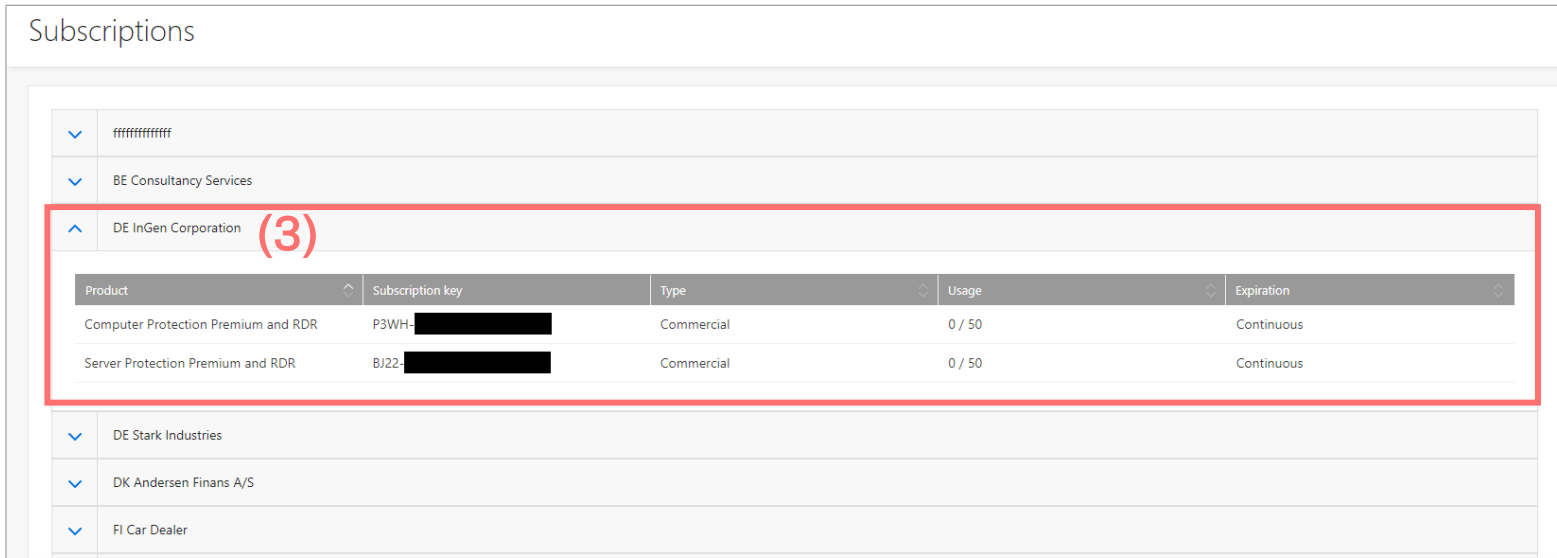


WITH secure

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

WITH secure

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.

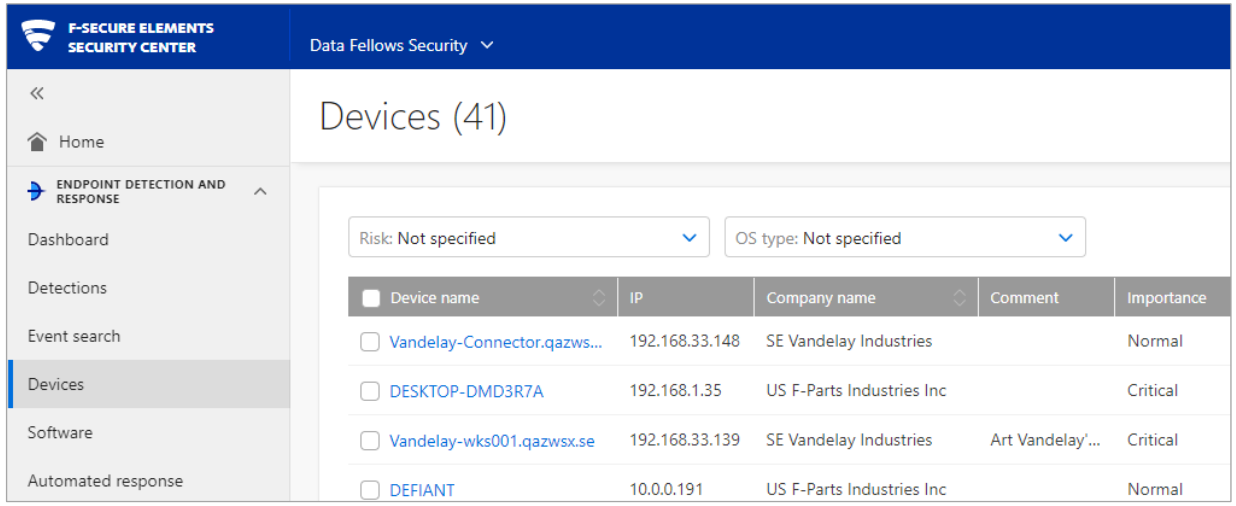
OR

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.

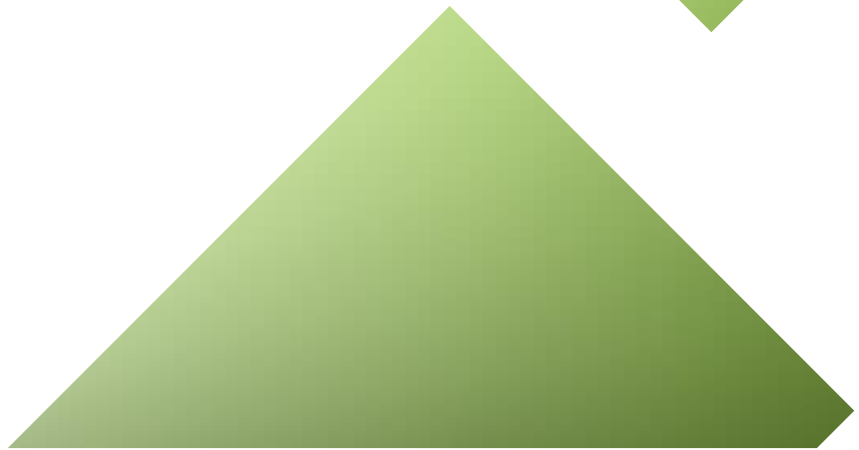


Administrating EDR

WITH secure

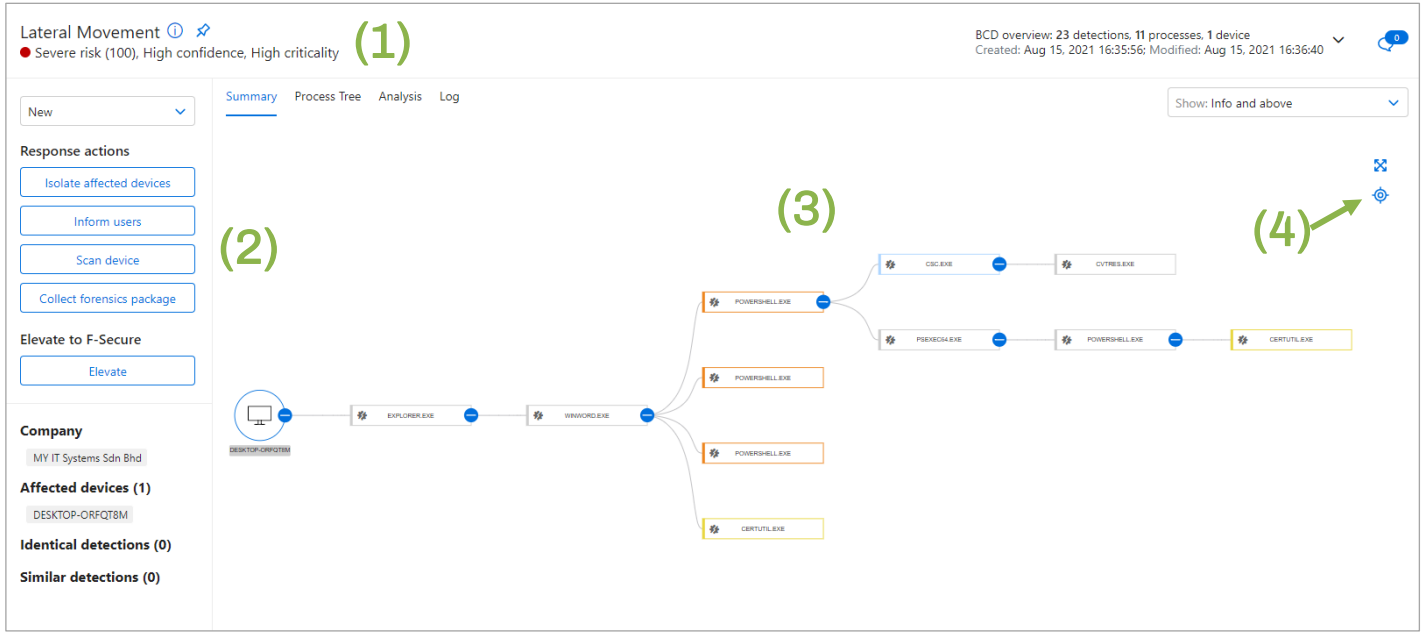
Gathering information

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



Gathering Information
Detection Information

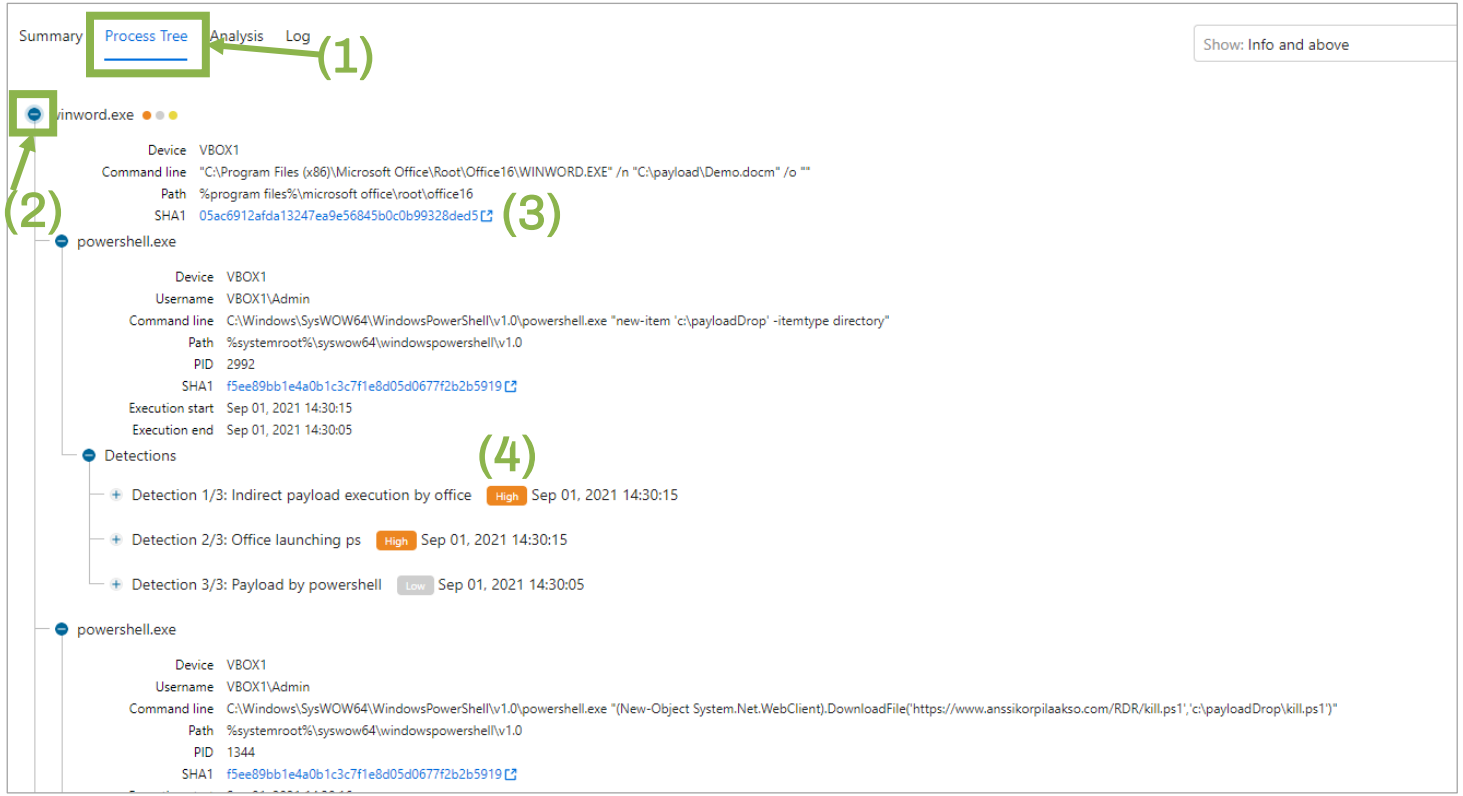
1. Check the detection severity (1).
   Is this something you should act on?
   - How high is the confidence?
   - What is the criticality rating?
2. The Response actions (2) provides various options for handling the detection. We'll look at them soon.
3. Finally, check the Summary view on the right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



WITH secure

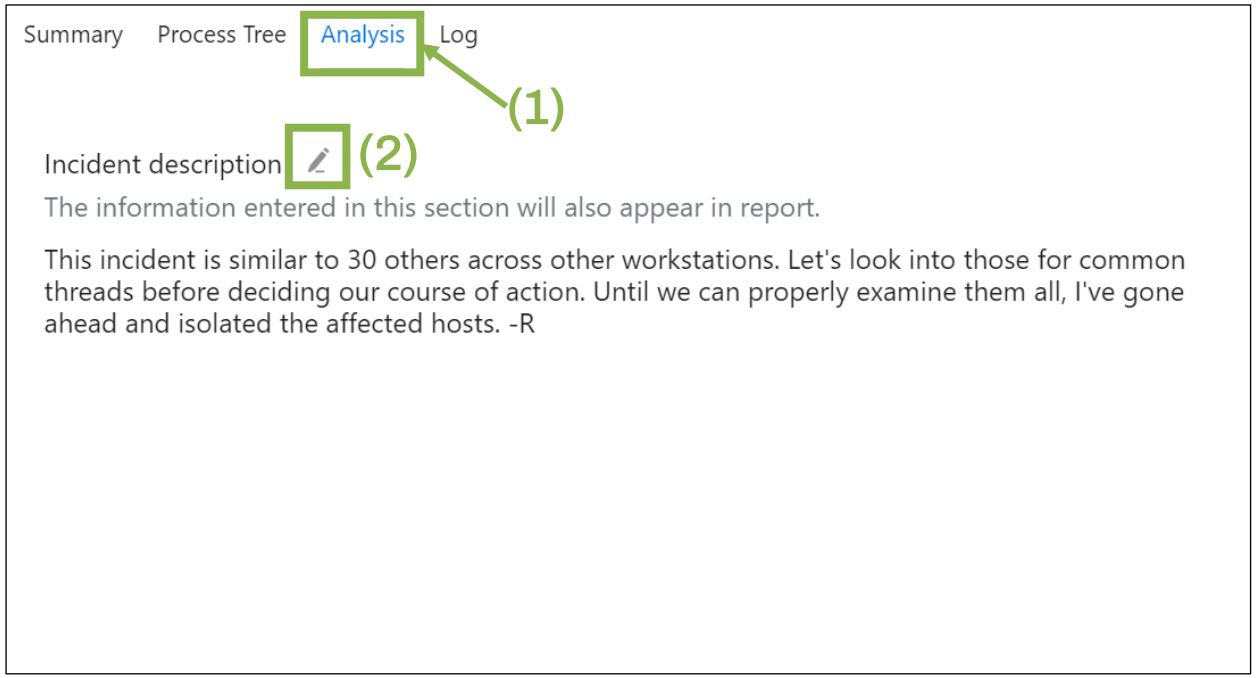
Gathering Information
Process Tree

- 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.



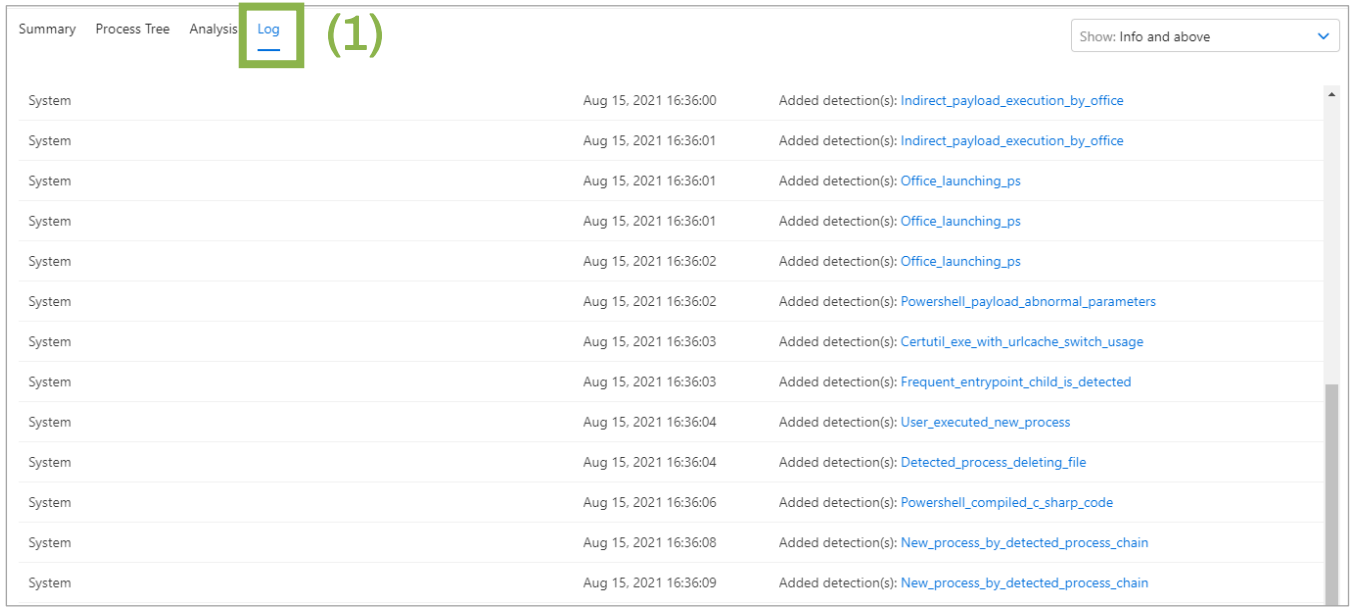
Gathering Information
Analysis

- 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.



Gathering Information
Detection Log

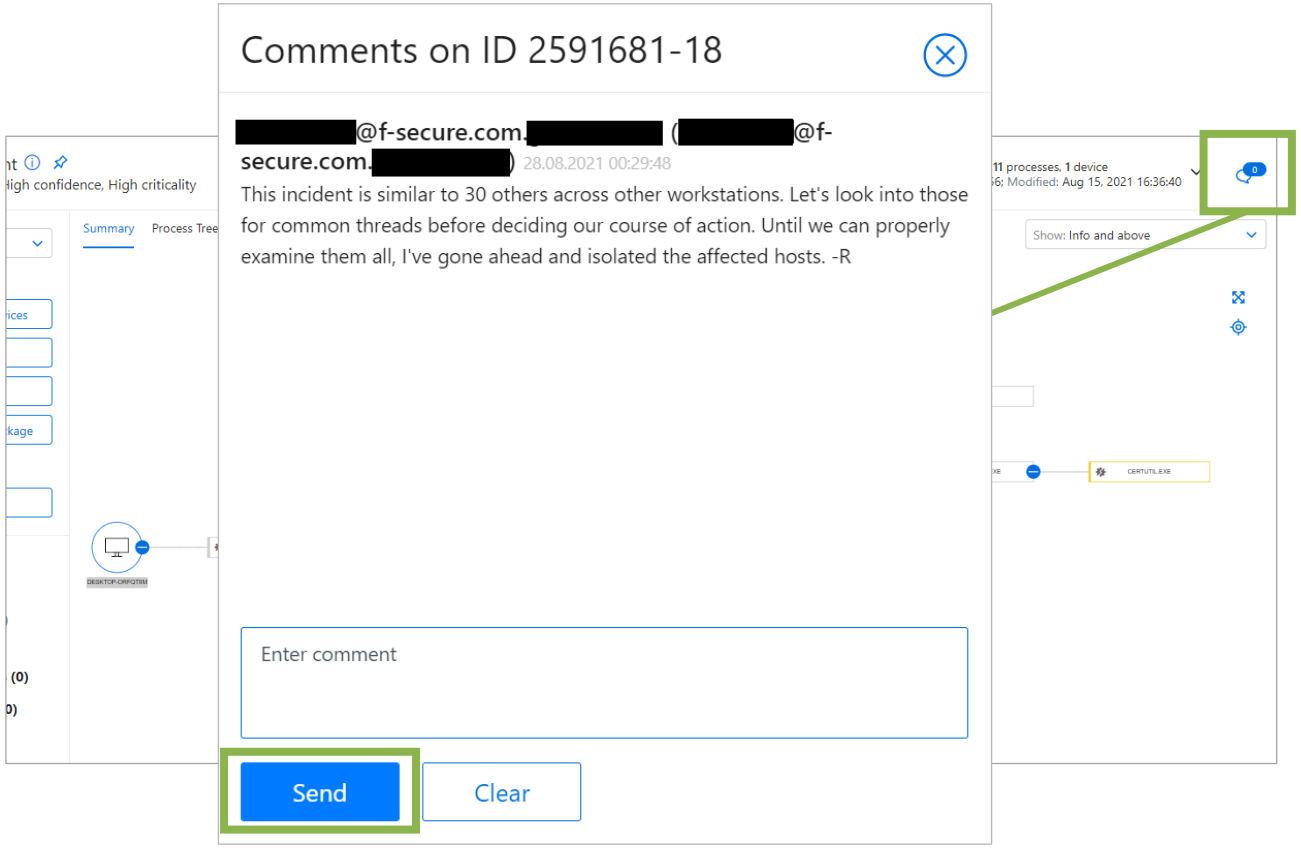
- Finally, the Detection log (1) view offers insight into the remediation efforts taken.
- Where Summary & Process Tree provides a context-based approach of the detection, the Log provides an event breakdown, showing how the detection was created, modified, and handled by users in the system.



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.

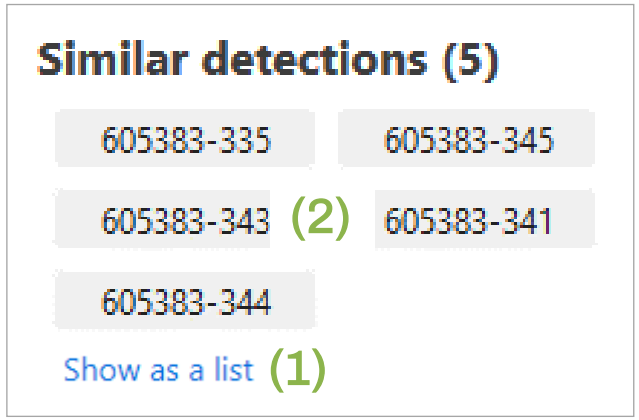
- Clicking the icon will open a pop-up, as shown. Click Send to post your comment.
- Clear will empty the textbox so you can start over. However, it will not clear previous comments that have been made.
- What separates comments from the Analysis tab is that comments are not published to reports.



WITH secure

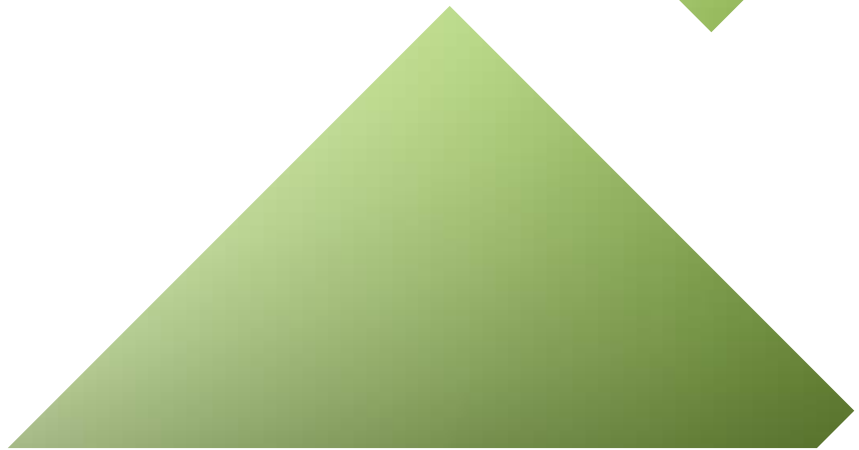
Gathering Information
Similar Detections

- 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.



Managing detections

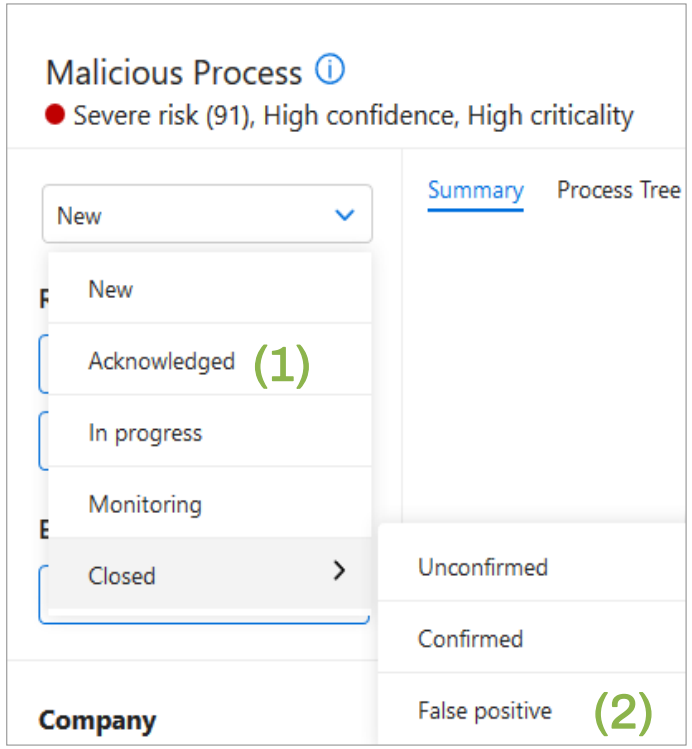
1. Confirming an incident
2. False positives
3. Progress updates
4. Event search



W / T H
secure

Managing Detections
Confirming An Incident

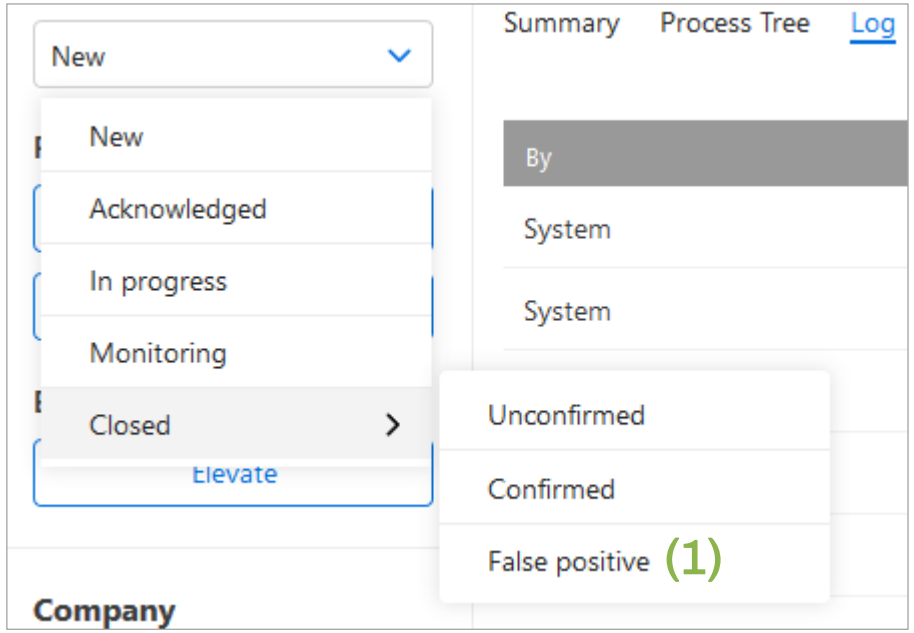
- If the detection is New (i.e. it has not been assigned one of these status already), you can choose to Acknowledge it (1) or report it as a False positive (2) by clicking the menu.
- Acknowledging the incident allows you to begin showing the handling status of the detection while marking the incident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



WITH secure

Managing Detections
False Positives

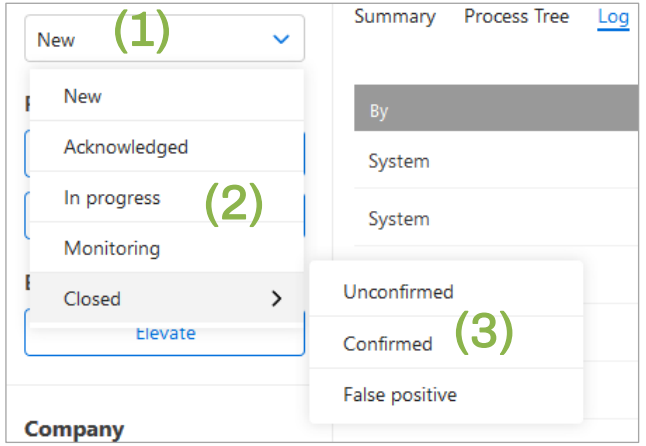
- When you evaluate an incident as a False Positive (1), it will be closed and marked as non-malicious.
- There is also a Closed: Auto False Positive state, which is triggered when all the following conditions are met:
    1. An incident is NEW and UNCONFIRMED.
    2. System admins have archived identical 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.



WITH secure

Managing Detections
Progress Updates

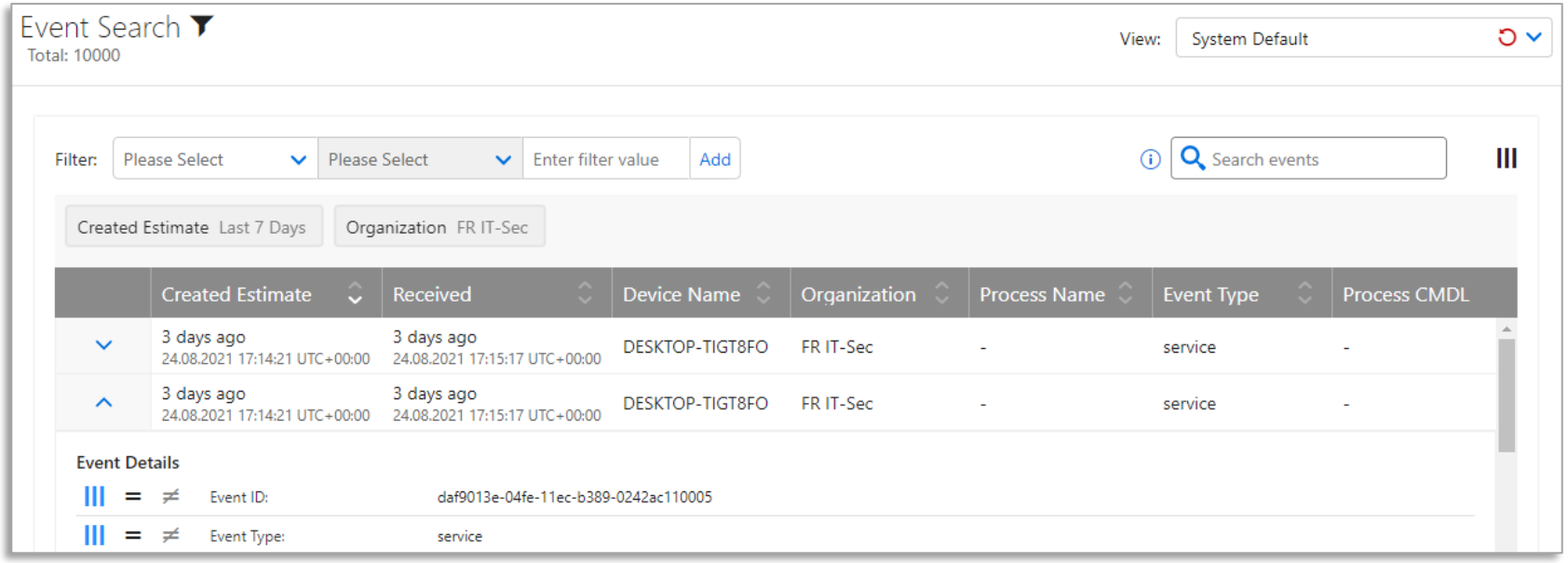
- As you progress in handling the incident with your customer, remember to update the incident status in the Detection view.
    1. Click the incident status field (1).
    2. Select the new status for the incident (2), such as In-Progress or Acknowledged.
    3. Once the incident has been handled, select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



WITH secure

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.



Response actions

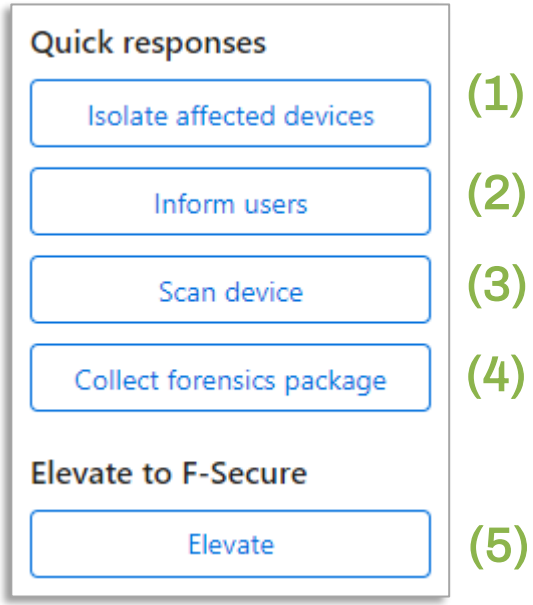
1. Quick response
2. Response actions
3. Host isolation
4. Elevate

Quick Response

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

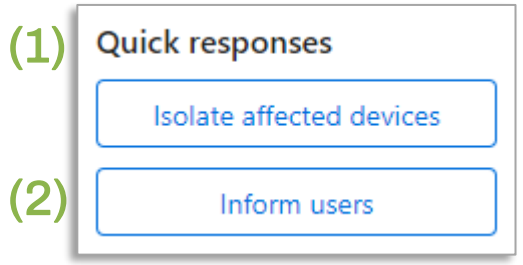
- Clicking Isolate all hosts (1) removes the computer from the network, prohibiting any access to or from it. Only connections to the WithSecure cloud are allowed. Clicking Inform users (2) guides you through sending an alert email to the customer.
- Clicking Scan host (3) sends a scanning request to 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.

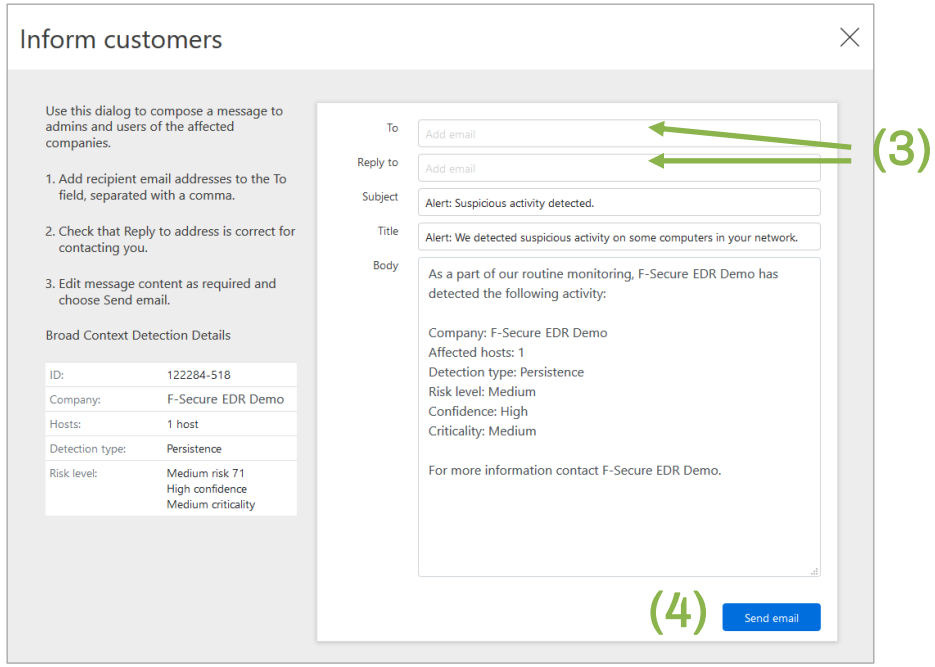
Let's go through these individually, starting with the alert email.



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).

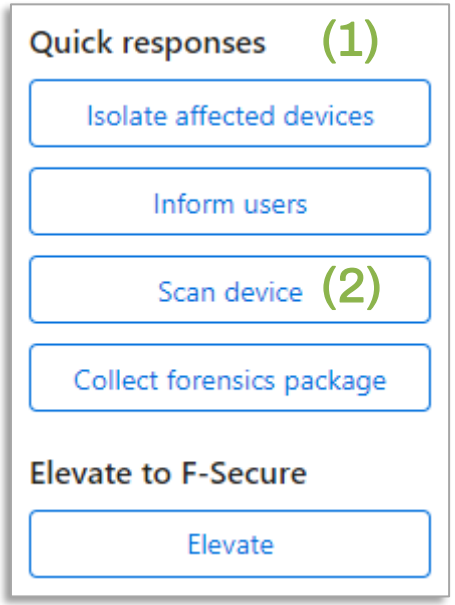


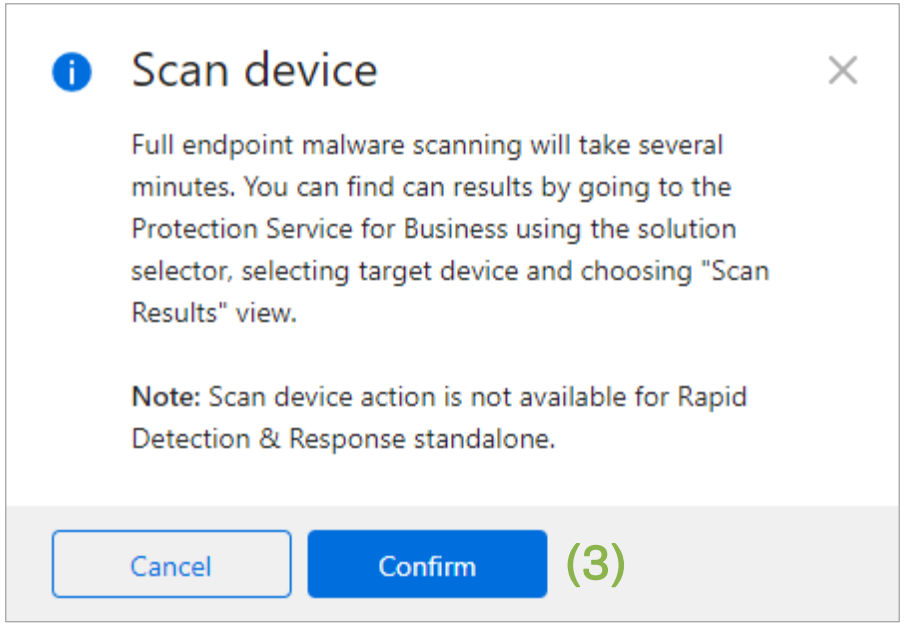


WITH secure

Quick Response
Scan Host

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

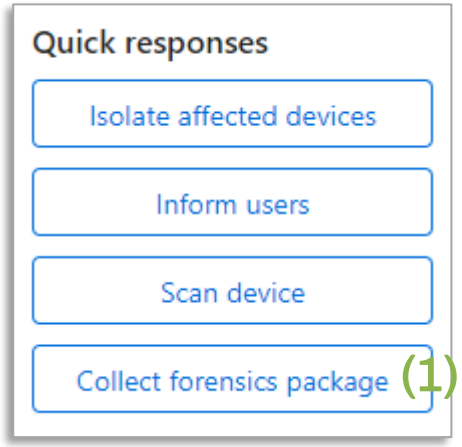


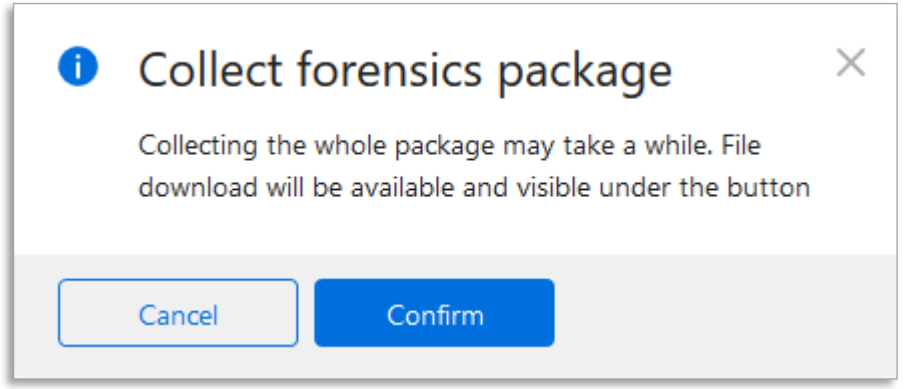


NOTE: *This feature is only available for the Elements EPP and EDR combined licenses on Computers and Servers. This feature is also available for standalone instances of EDR on Windows computers.*

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

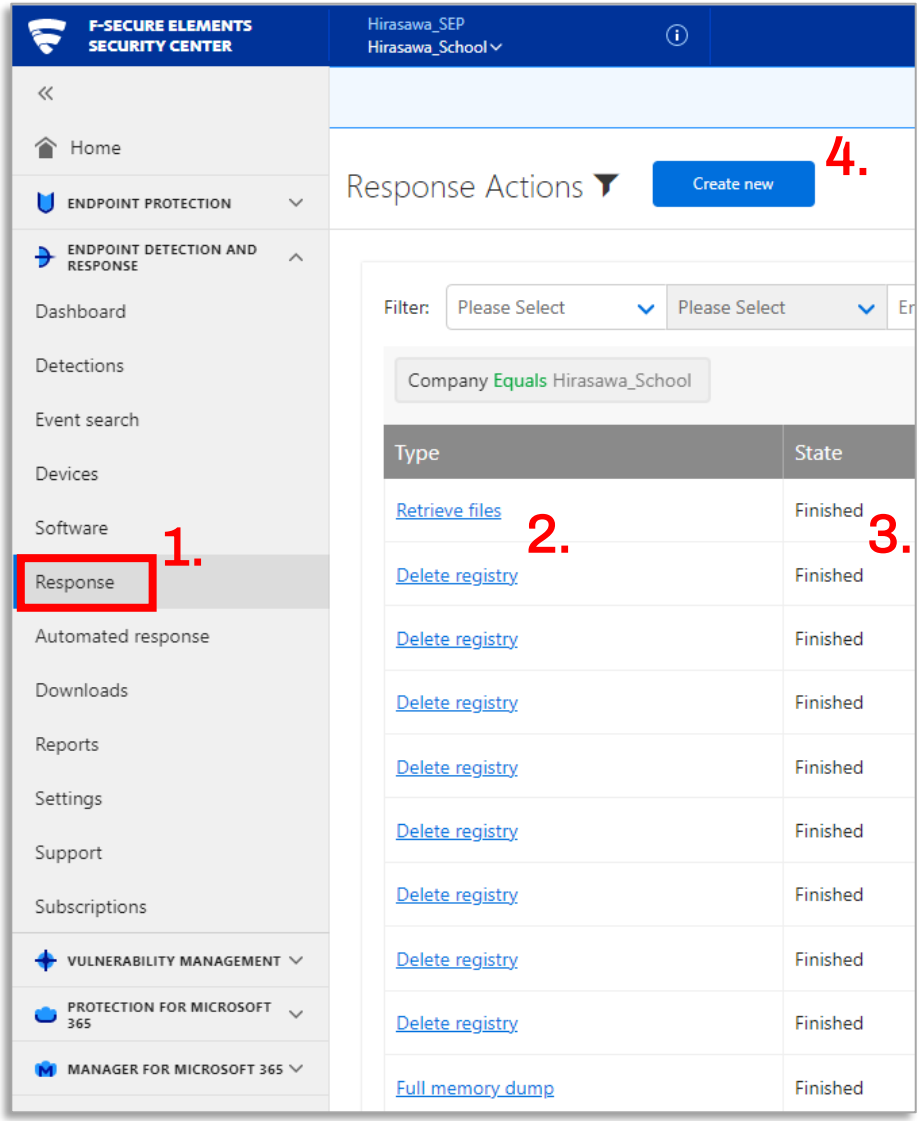
CONTAIMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

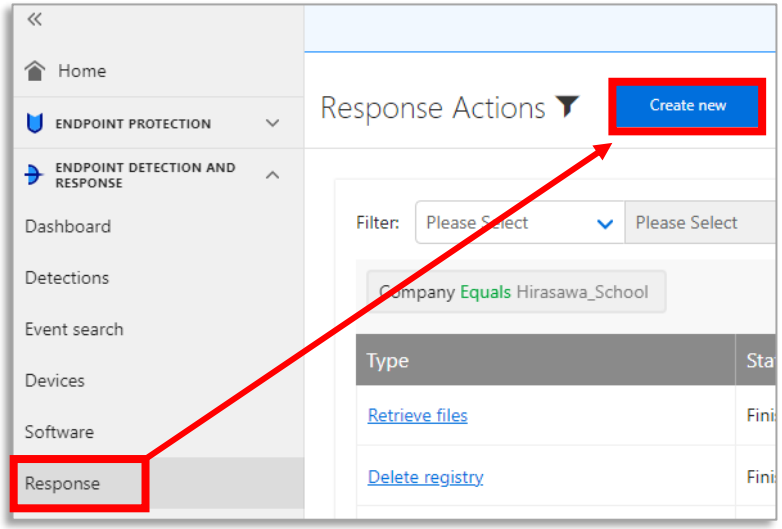
- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

Accessing Response Actions

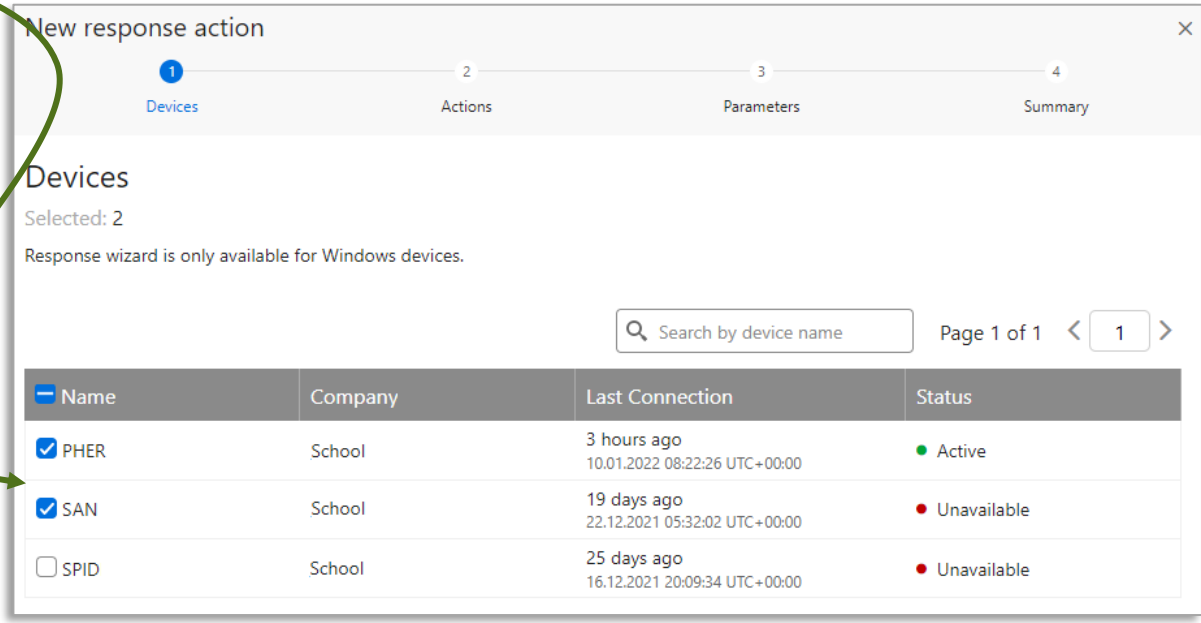


- You can access response actions by clicking **Response** (1.) on the navigation pane. Note that you need to be on the company level.
- Once you have opened the **Response** page, you can see a list of response actions (2.) that have been performed, as well as their state (3).
- You can click on an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

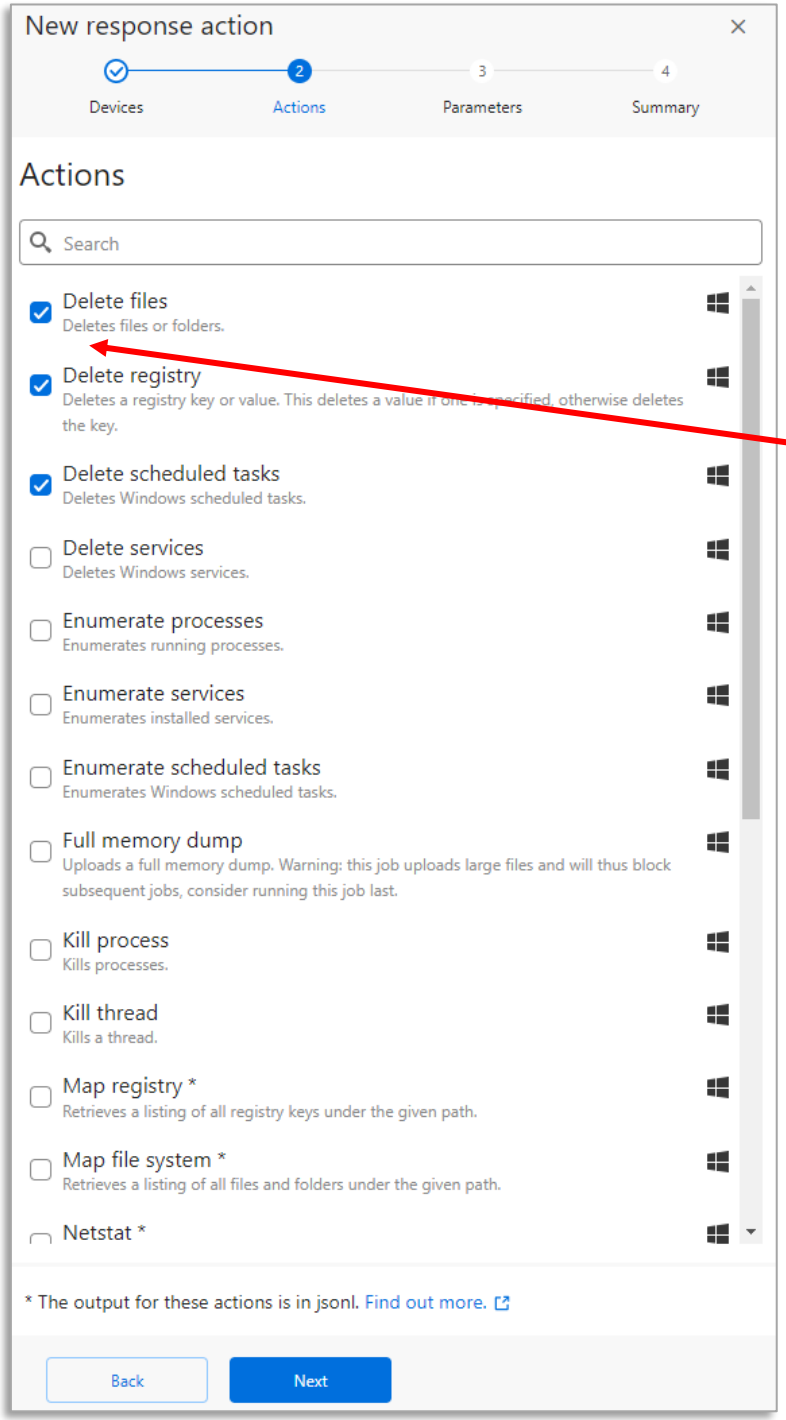
Creating New Response Action



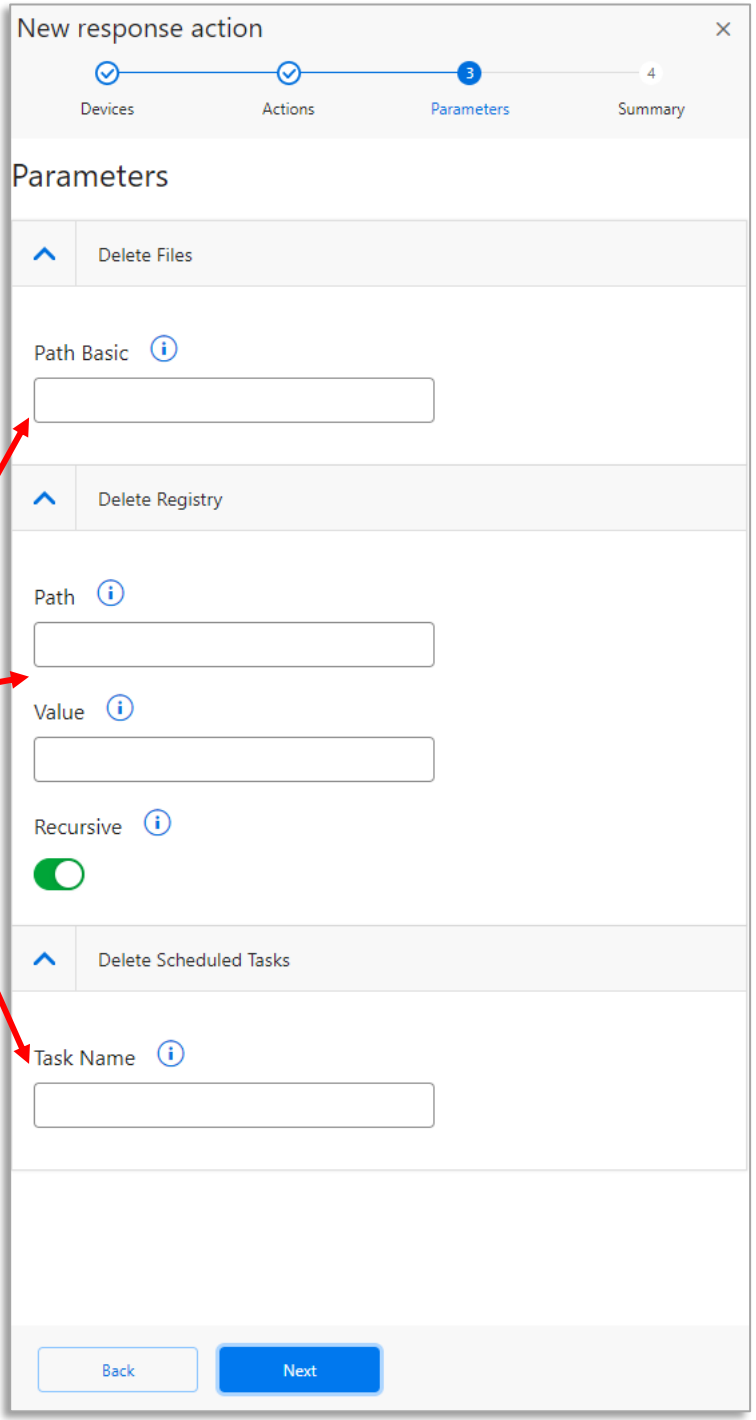
- To create a new response action, click the **Create new** button on the **Response** page.
- Select the devices you want to create the response action for.
- Remember to click **Next** to proceed.

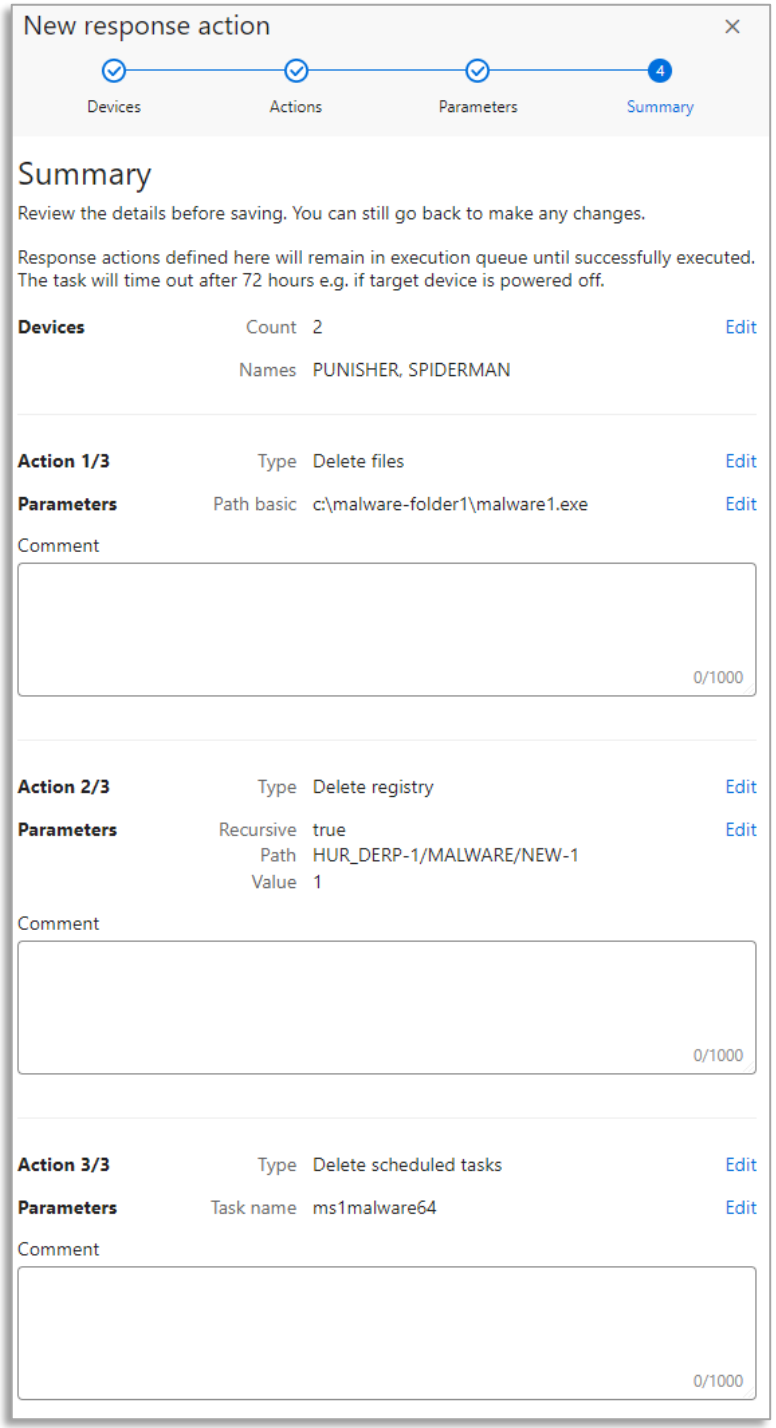


Creating New Response Action #2



- 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.



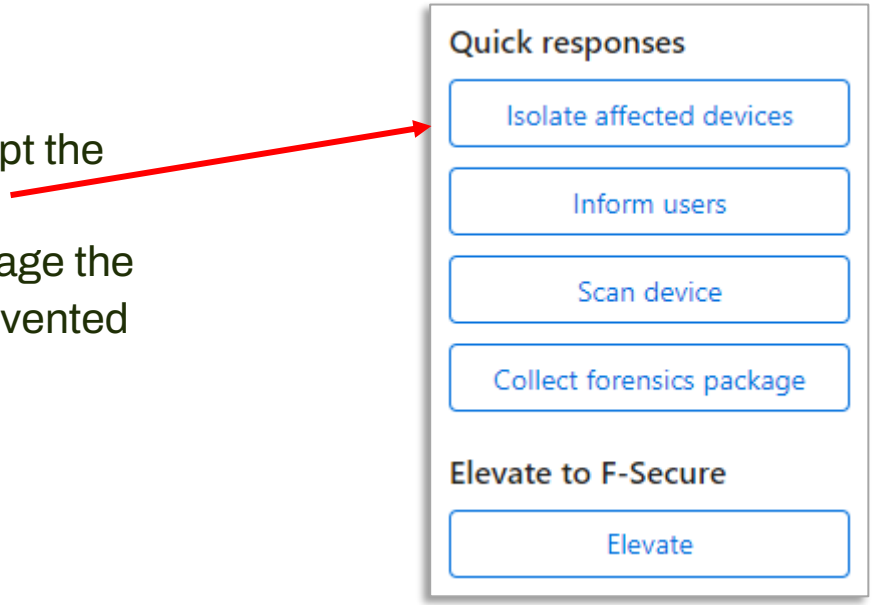


Creating New Response Action #3

- 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.

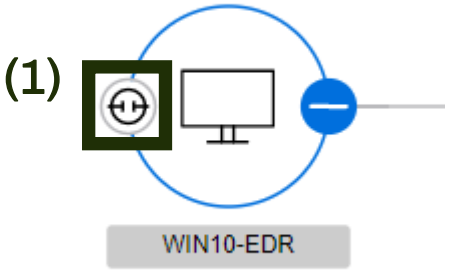
Isolating Affected Hosts

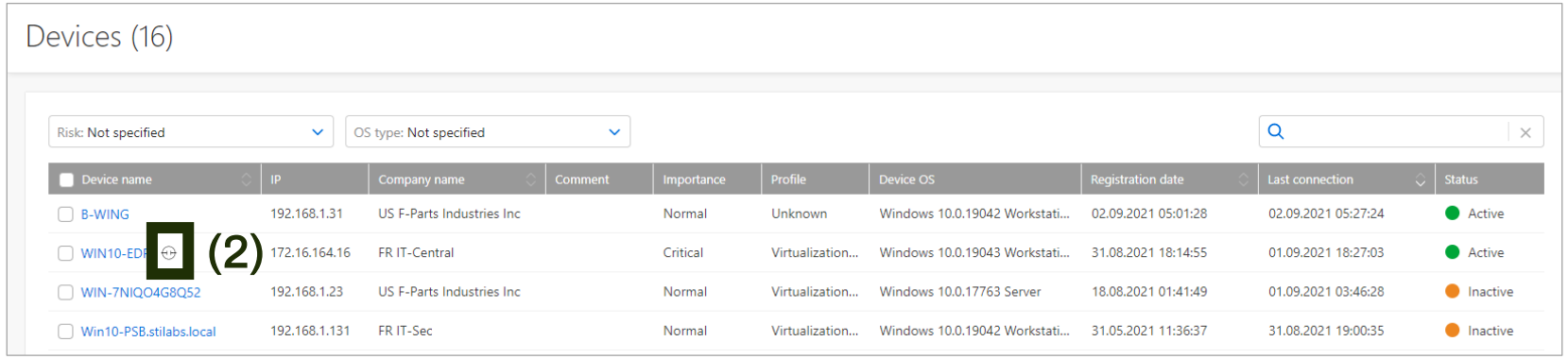
1. When you have evaluated the incident as real and actionable, you can choose to isolate the host from the network from the Quick responses.
2. Select Isolate affected devices from the options available.
3. The hosts will then disconnect from all active connections except the one established with the 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

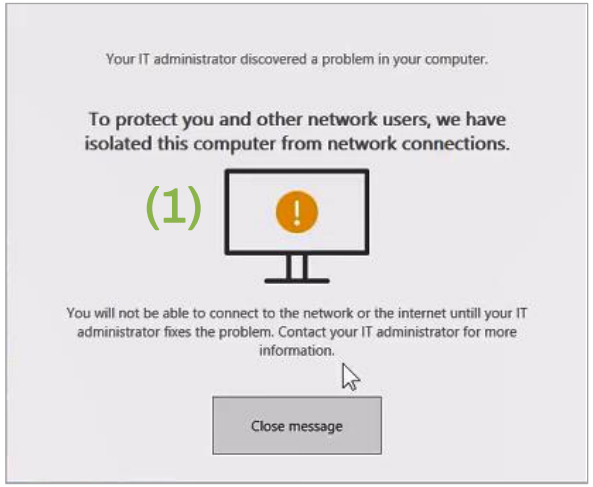
1. In the Summary view of the detection details, the device icon displays a smaller grey broken connection icon (1) to show that it is now isolated from the network.
2. This same icon appears next to the device name on the Devices page in the ESC portal (2).

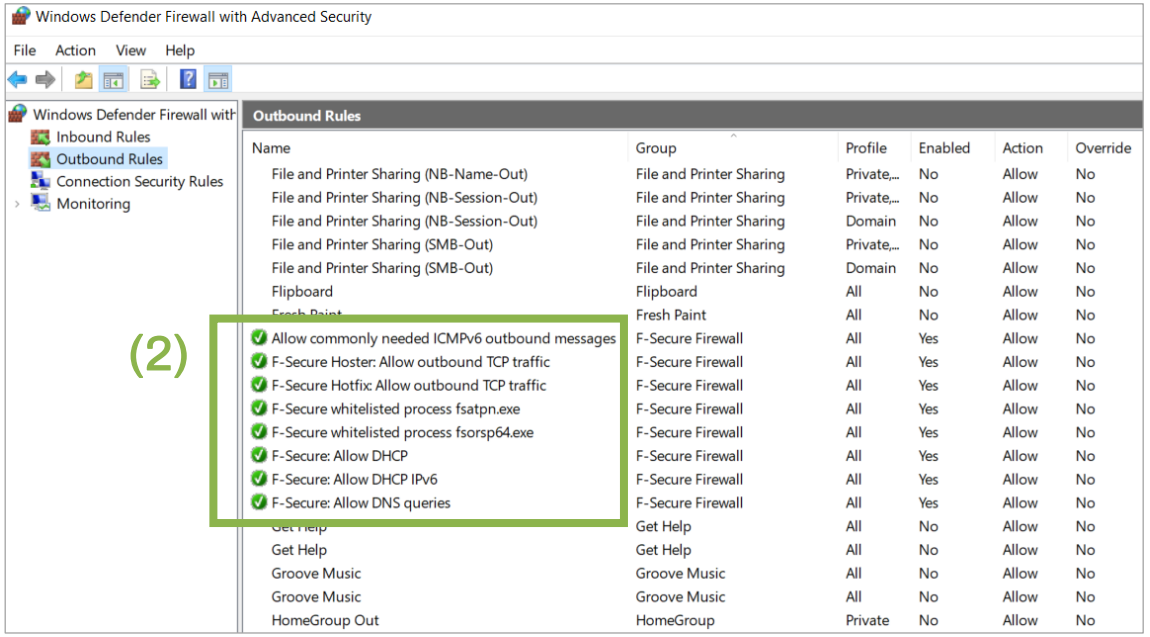




Isolated Host Notification

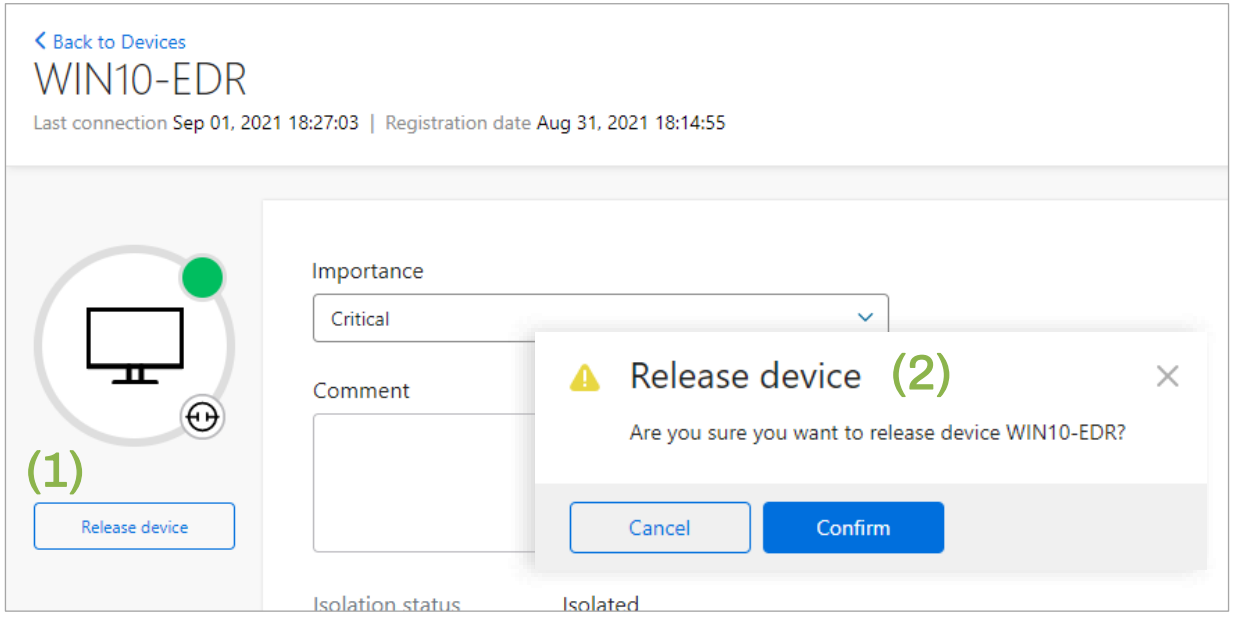
1. When a devices becomes isolated, a pop-up (1) is shown on the isolated host to explain the situation to the current user. This also occurs when the host is removed from isolation.
2. Isolation deactivates all rules from the Windows Firewall except connections to WithSecure, as shown in the Outbound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





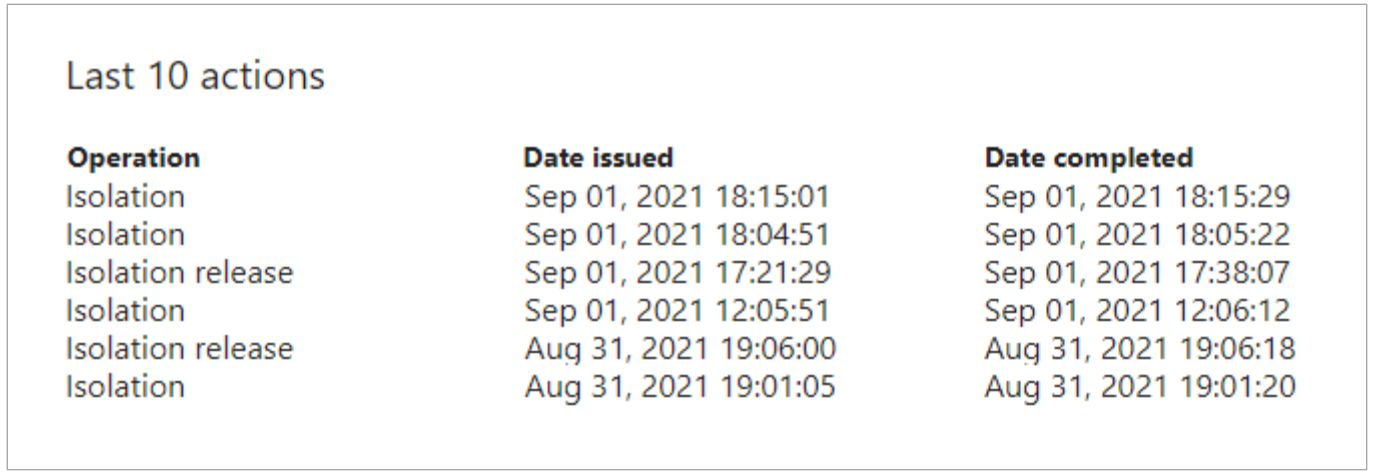
Releasing an Isolated Host

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).



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.



Our Experts Always Back You Up With Elevate To WithSecure

WithSecure Partner

WithSecure's experts respond 24/7 to the Elevate to WithSecure requests by analyzing the threat and providing actionable advice on attack containment and remediation

1. DETECTED ANOMALY

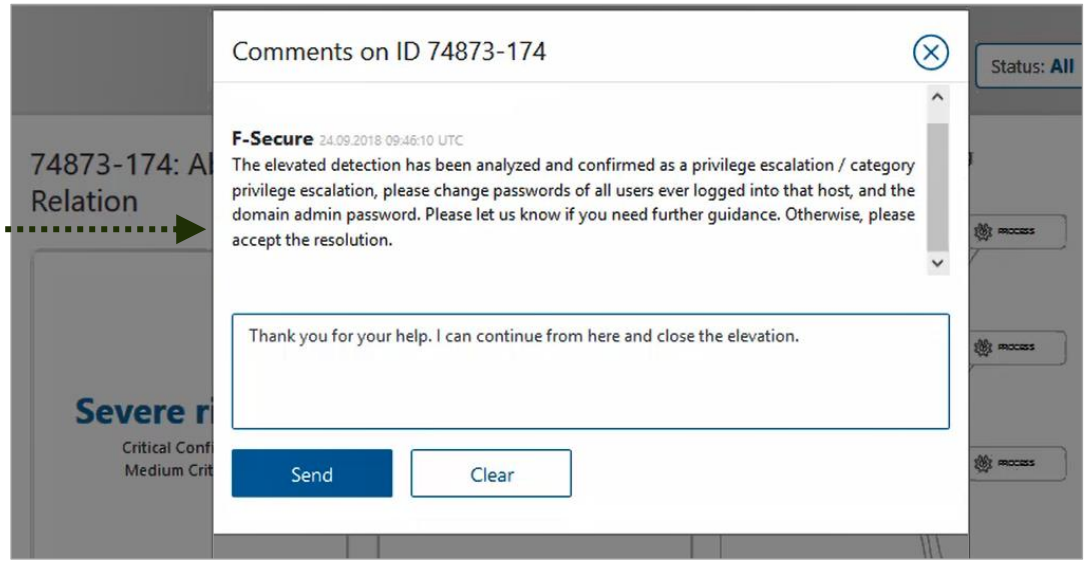
A potential targeted attack was detected but it cannot be confirmed by the WithSecure Partner

2. ELEVATED TO WITHSECURE

The Partner chose "Elevate to WithSecure" to request WithSecure's assistance

3. RESOLVED WITH EXPERT'S GUIDANCE

Actionable response guidance from cyber security experts helped with a quick response



EDR detekcije

Elements EPP+EDR for Computers Premium

WITH secure

EDR detekcije

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

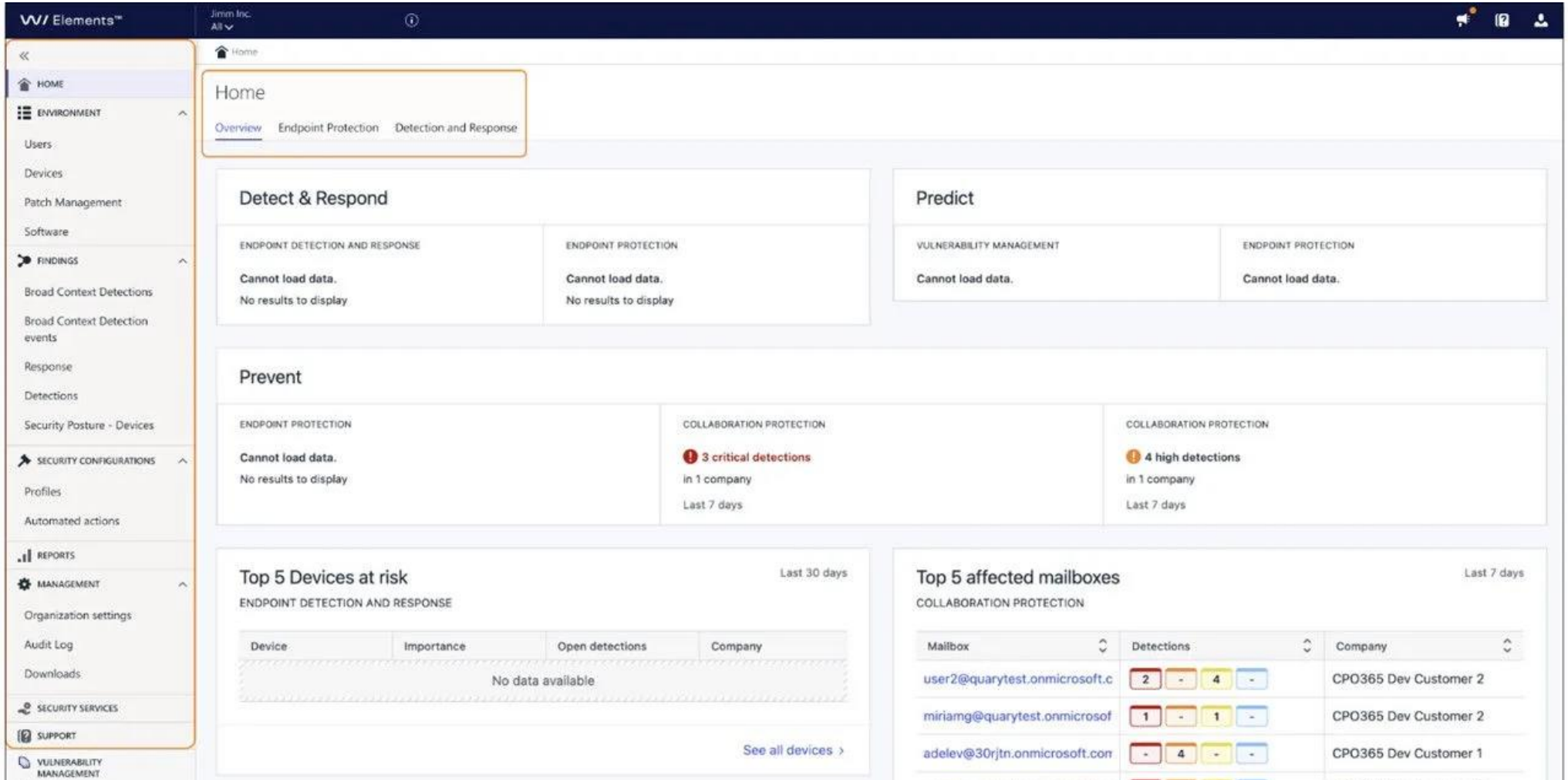
WITH secure

WithSecure Elements
Evolution of User Interface

WITH secure

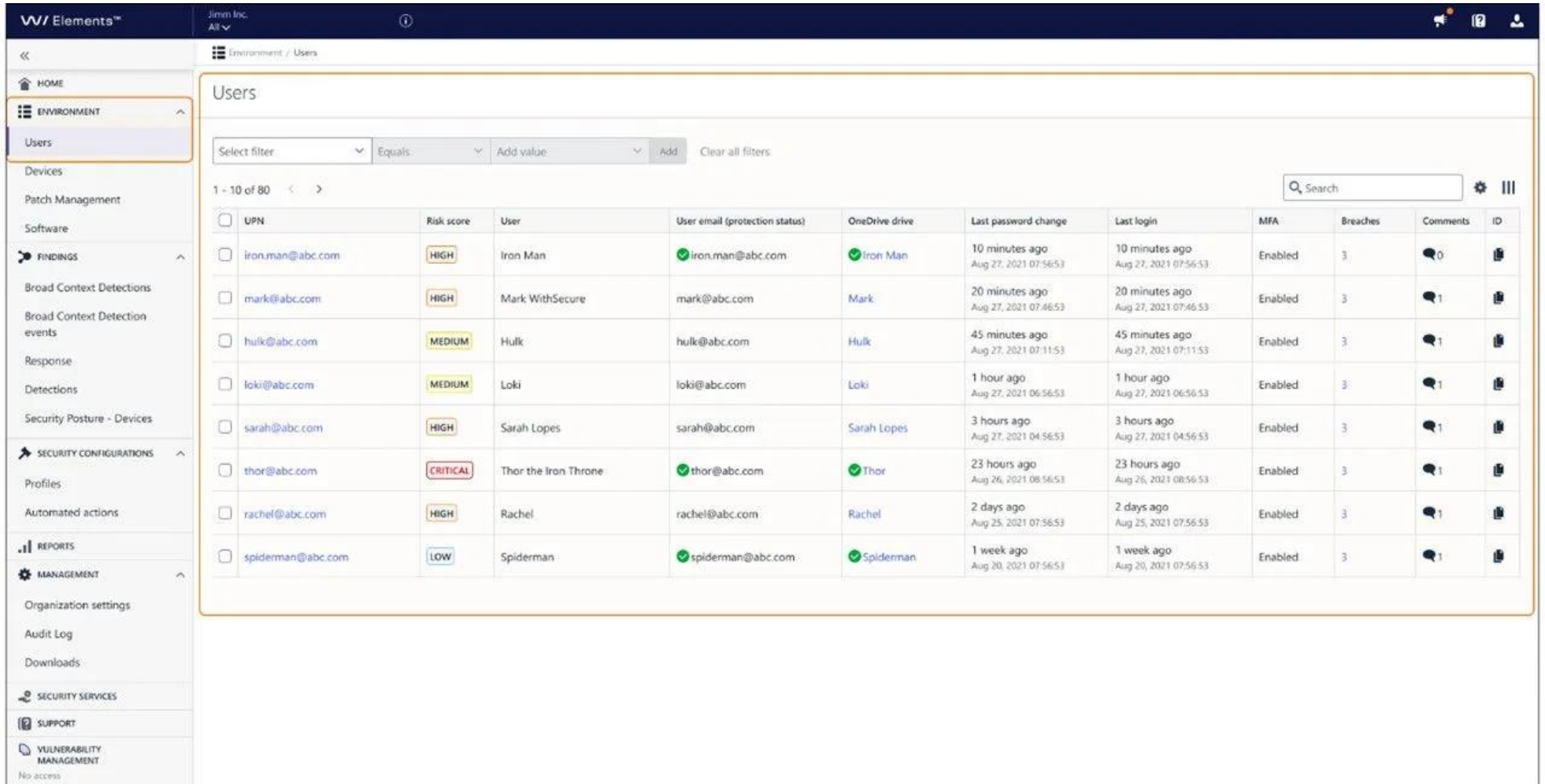
New Elements Experience

- Elements Security Center is receiving a facelift.



New Elements Experience

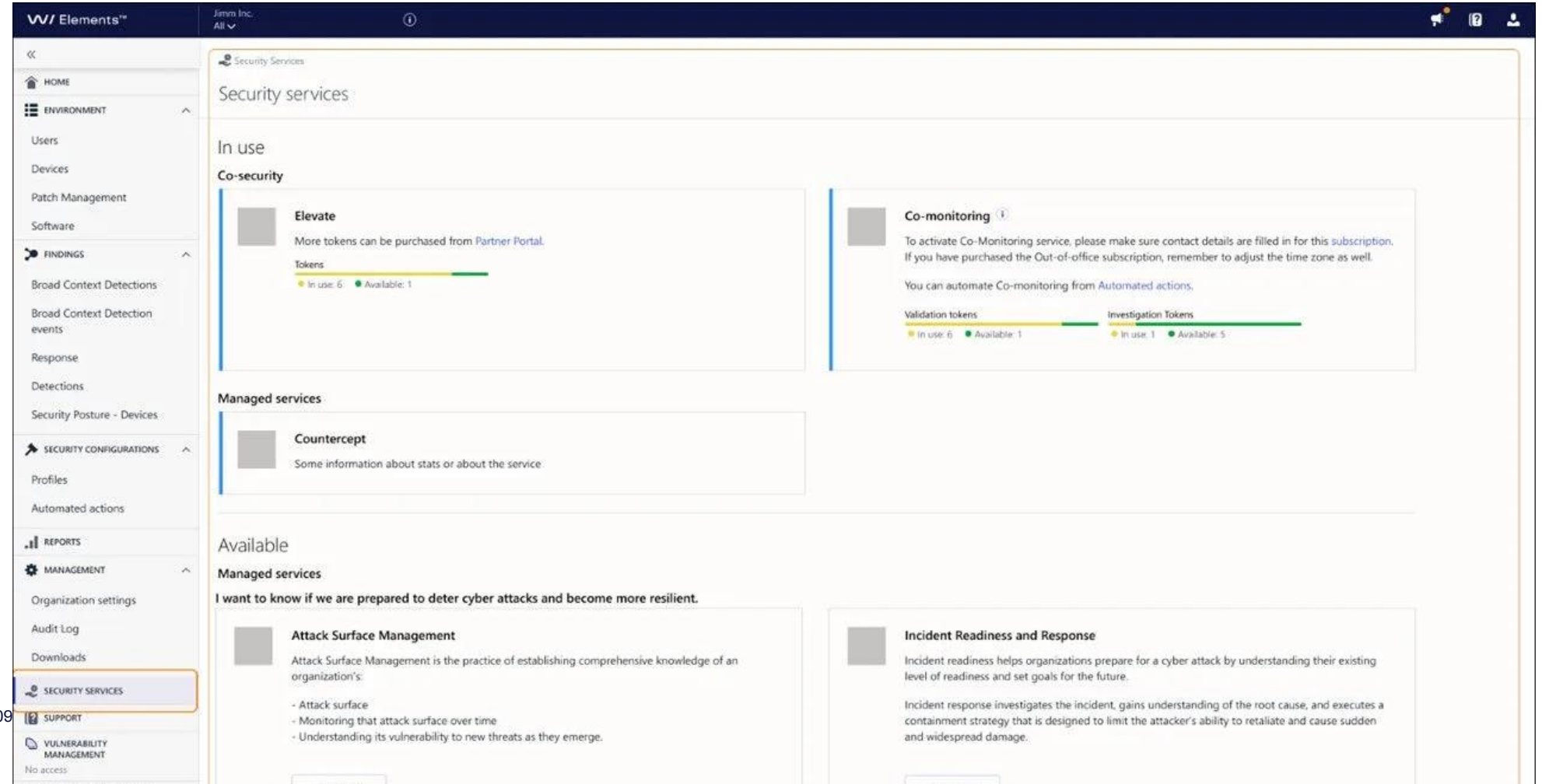
- Information will be based on users not subscription models



WITH secure

New Elements Experience

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



WITH secure