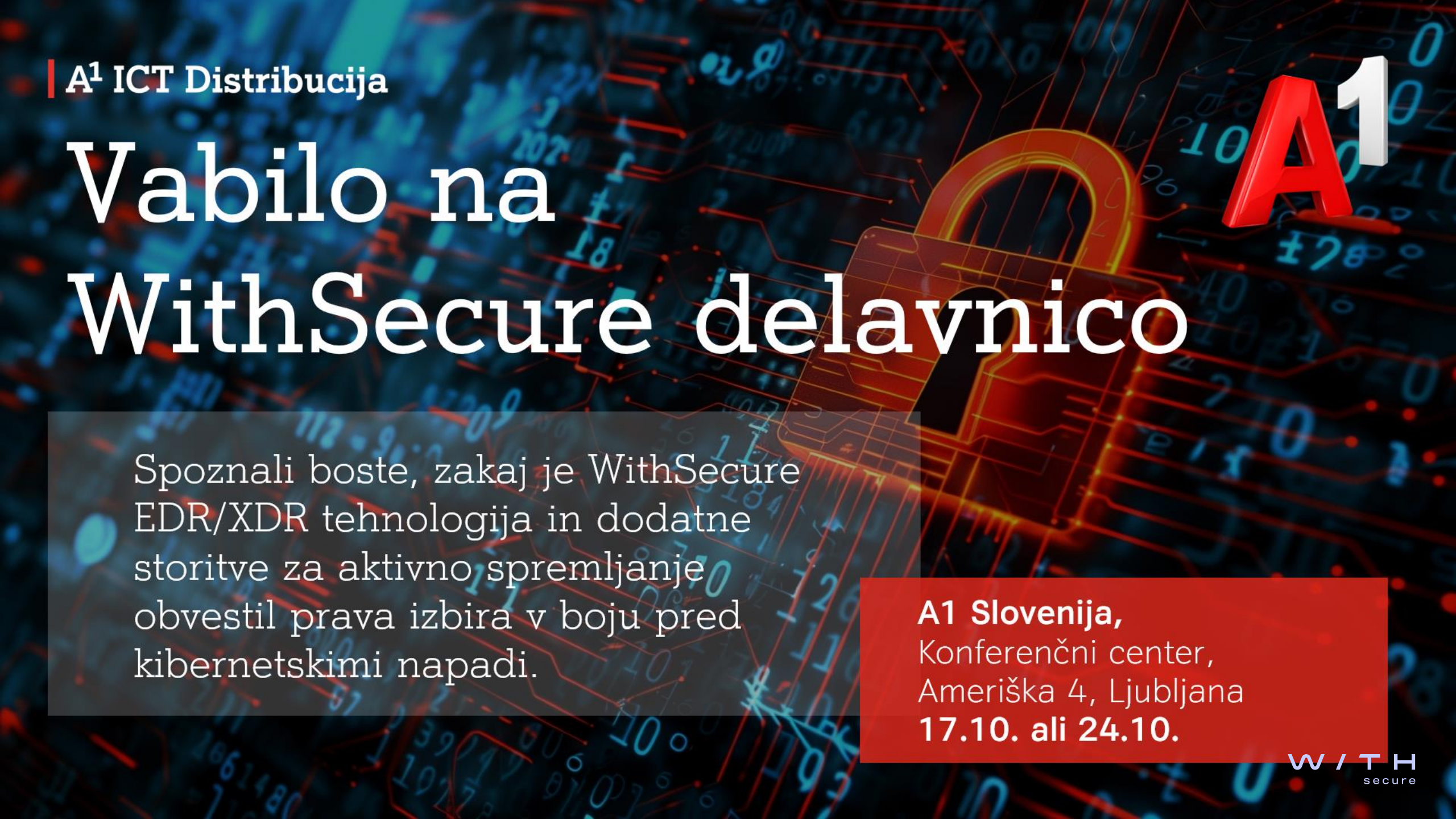

A1 ICT Distribucija
Vabilo na WithSecure delavnico
Spoznali boste, zakaj je WithSecure EDR/XDR tehnologija in dodatne storitve za aktivno spremljanje obvestil prava izbira v boju pred kibernetskimi napadi.
A1 Slovenija,
Konferenčni center,
Ameriška 4, Ljubljana
17.10. ali 24.10.
WITH secure

Potek delavnice

09.00 – 10.30 – Uvod v WithSecure in nove rešitve

10.30 – 10.45 – kratka pavza

10.45 – 12.00 – WithSecure Co-Security in A1 storitve

12.00 – 13.00 – KOSILO

13.00 – – WithSecure EPP in EDR novosti (tehnično)

– Q&A

Protecting businesses in 100+ countries out of 30+ offices

WITH secure

We exist to build and sustain digital trust

150,000
Customers

A leading European
Cyber security company

6,000
Partners

70
Nationalities

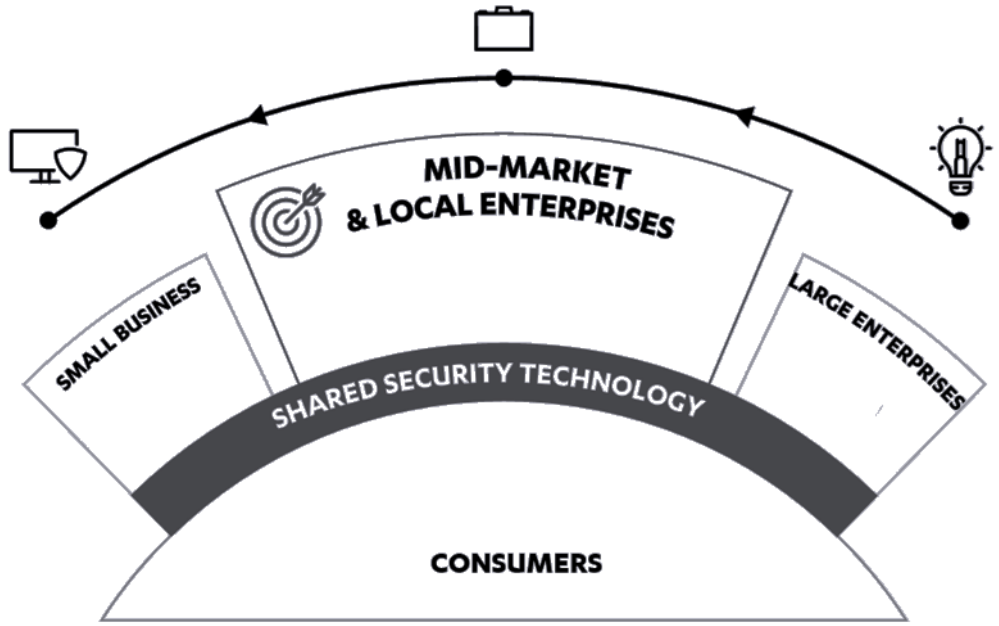
1000
Employees

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

IT
RESELLERS
6000+

Telia Frontier vodafone
LIBERTY GLOBAL

OPERATORS
200+ globally

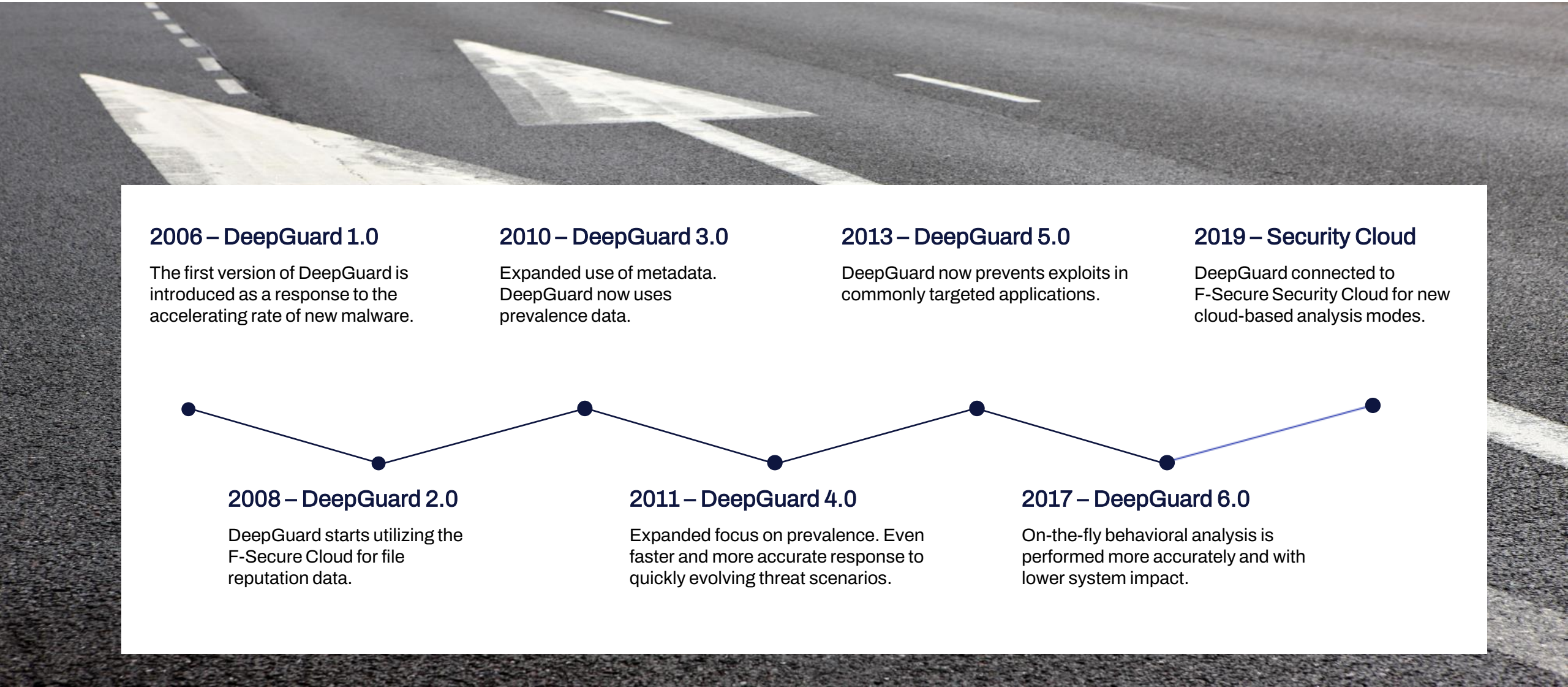
100,000+
companies

Tens of millions
of consumers

We sell our solutions through
a global network of channel partners

WITH secure

“NEXT-GEN” FOR 10+ YEARS



2006 – DeepGuard 1.0

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

2008 – DeepGuard 2.0

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

2010 – DeepGuard 3.0

Expanded use of metadata. DeepGuard now uses prevalence data.

2011 – DeepGuard 4.0

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

2013 – DeepGuard 5.0

DeepGuard now prevents exploits in commonly targeted applications.

2017 – DeepGuard 6.0

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

2019 – Security Cloud

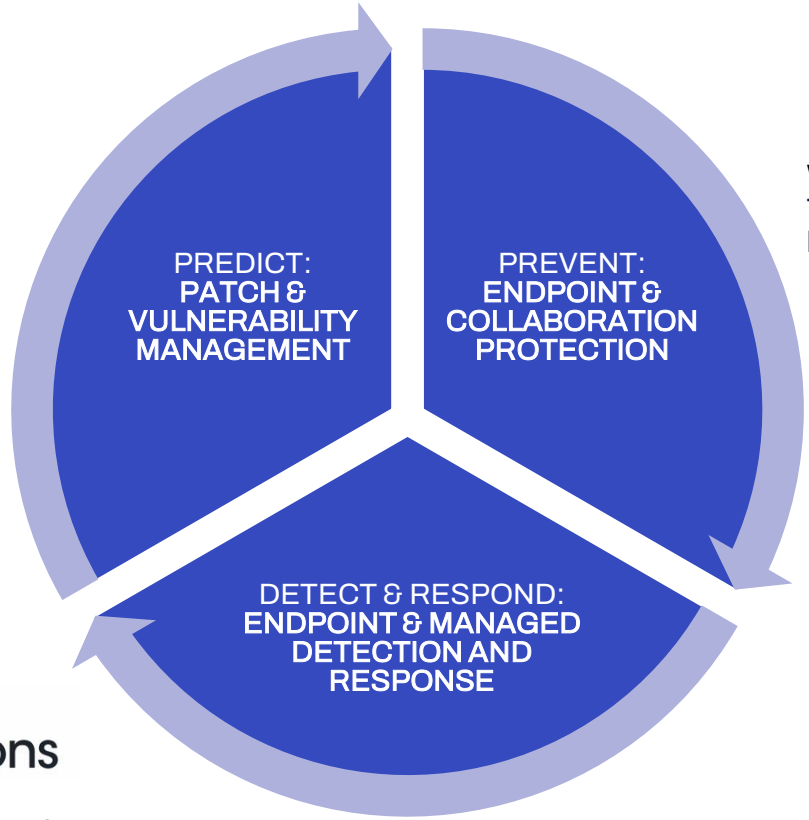
DeepGuard connected to F-Secure Security Cloud for new cloud-based analysis modes.

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



6 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

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!

WITH secure

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

WITH secure

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

- Amis, d.o.o. 2005 postane distributer za F-Secure
- 2015 združitev s Si.mobilom v A1 Slovenija
- Širok portfelj evropskih ponudnikov
  - Stormshield Network Security (NGFW / UTM)
  - iStor Backup
  - Vade Email Defense (M365 and Cloud Gateway)
  - WALLIX Privileged Access Management (PAM)
  - Labyrinth Deception
  - Censornet (MFA)
  - Energy LogServer (SIEM)

W / T H
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

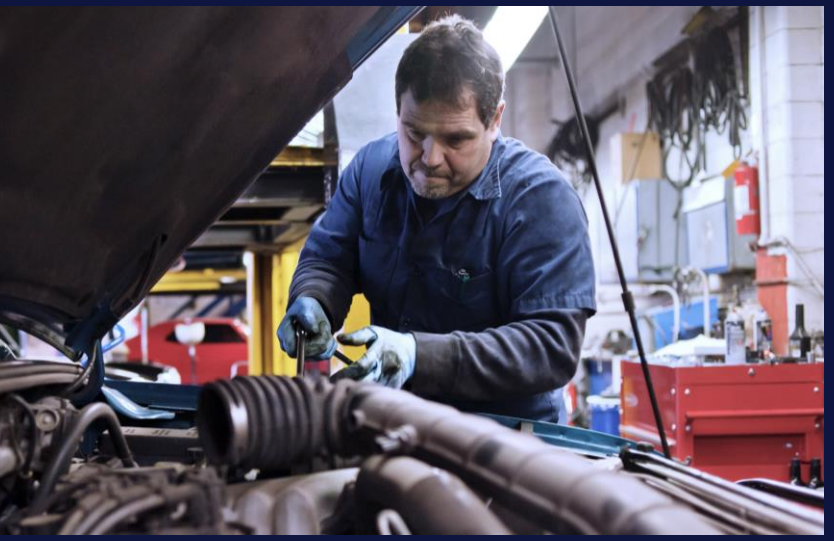
Lack of trained personnel

Increasing complexity & cost

Lack of understanding what is enough security

WITH secure

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



W/TH secure

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

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

- Exposure Management
- Extended Detection and Response
- Co-Security Services

WITH secure

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

- Endpoint Security
- Identity Security
- Collaboration Protection

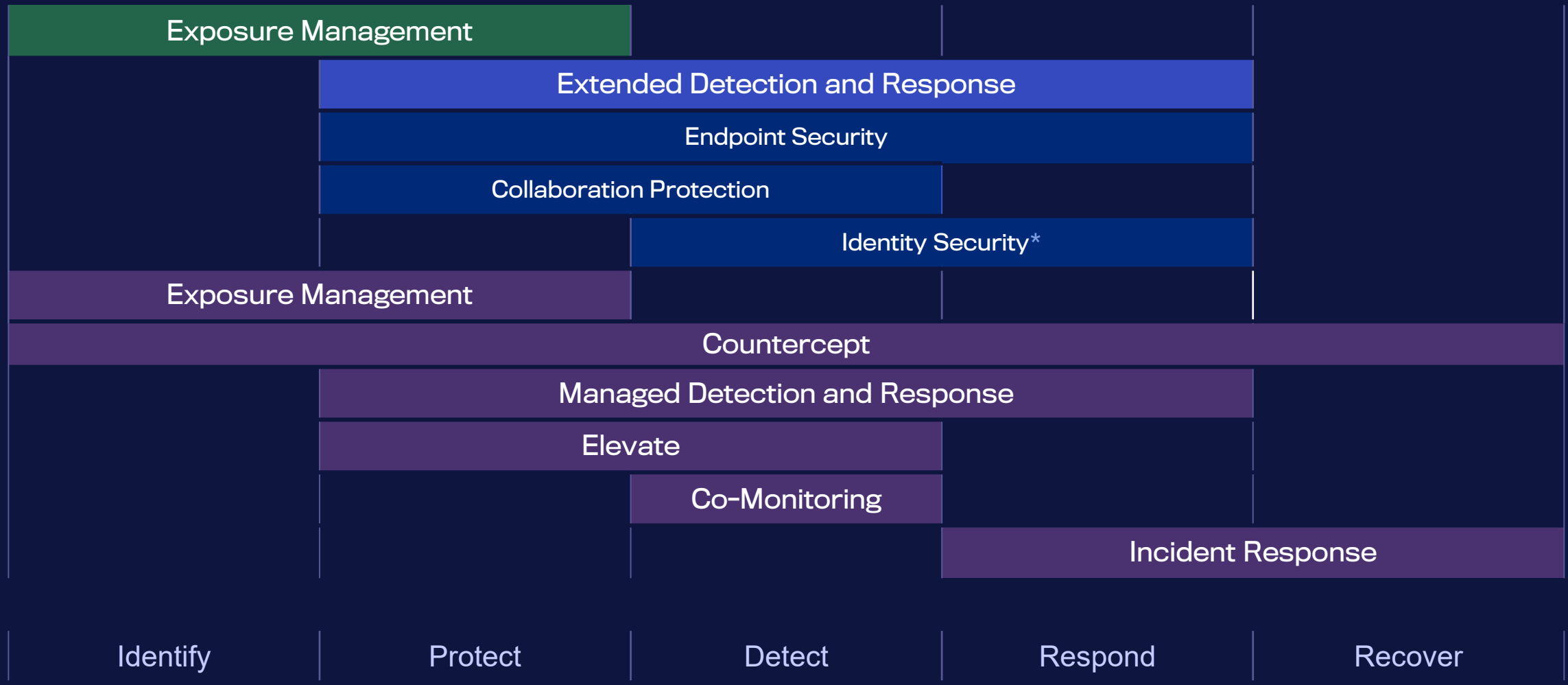
Co-Security Services

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

WithSecure™ Support Services

WITH secure

WithSecure™ Elements Cloud – NIST



*Identity Security will be extended to respond capability later in 2024

WITH secure

WithSecure™ Elements Exposure Management

WITH secure

Pain points of today's attack surface

Hybrid environment with unclear borders

Lack of visibility across cloud and on-premises environments

Identities as the weak link

Powerful attack acceleration points, easily phished and stolen

Dynamic threat landscape

Constant threat landscape changes and AI-enabled cyber attacks

WITH secure

Organizations face many challenging questions

What is my external attack surface?

What risks is my organization causing to the supply chain?

What shadow IT do I have in my environment?

Are there risks in users' identities that make those easy to breach?

How can I keep my business risk low with limited resources?

What is the business context of the identified exposure?

WITH secure

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

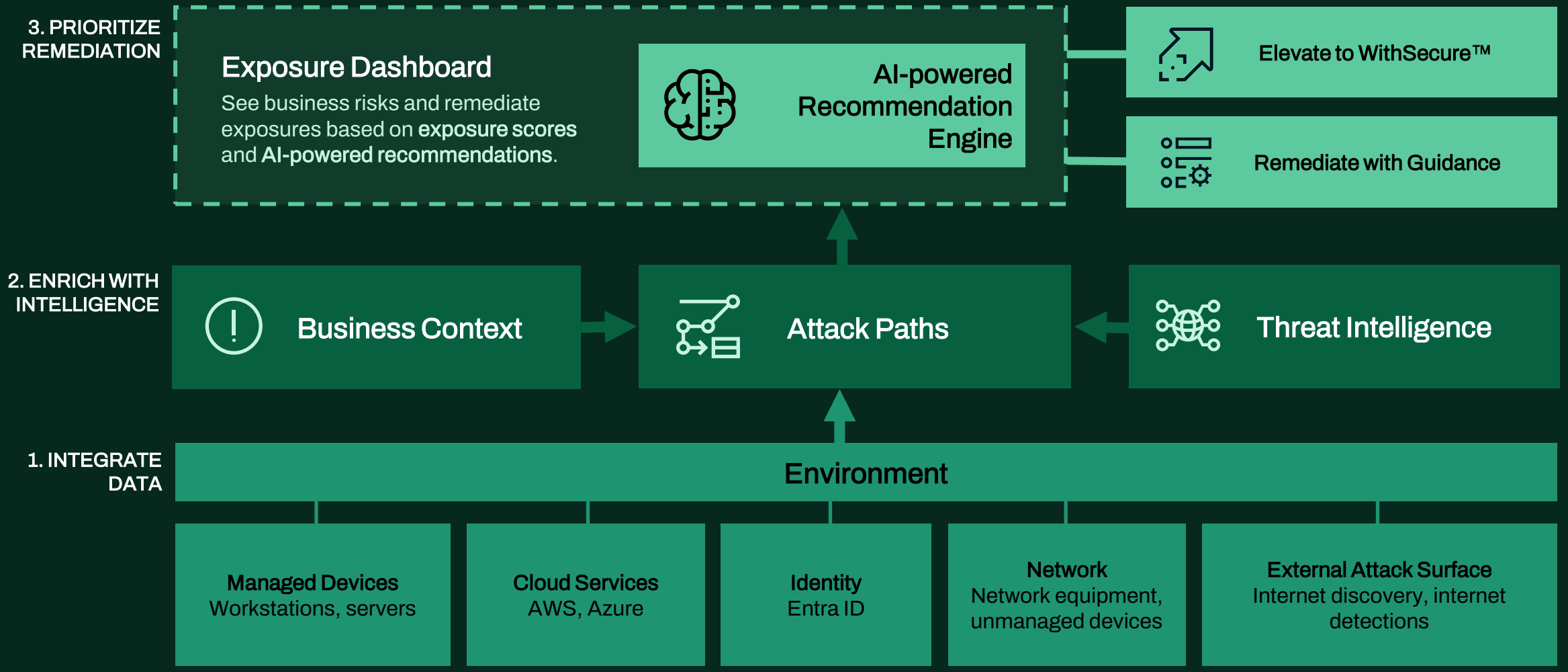
WithSecure™ Elements Exposure Management (XM)

A continuous proactive solution to predict and prevent breaches against your company's assets and business operations.

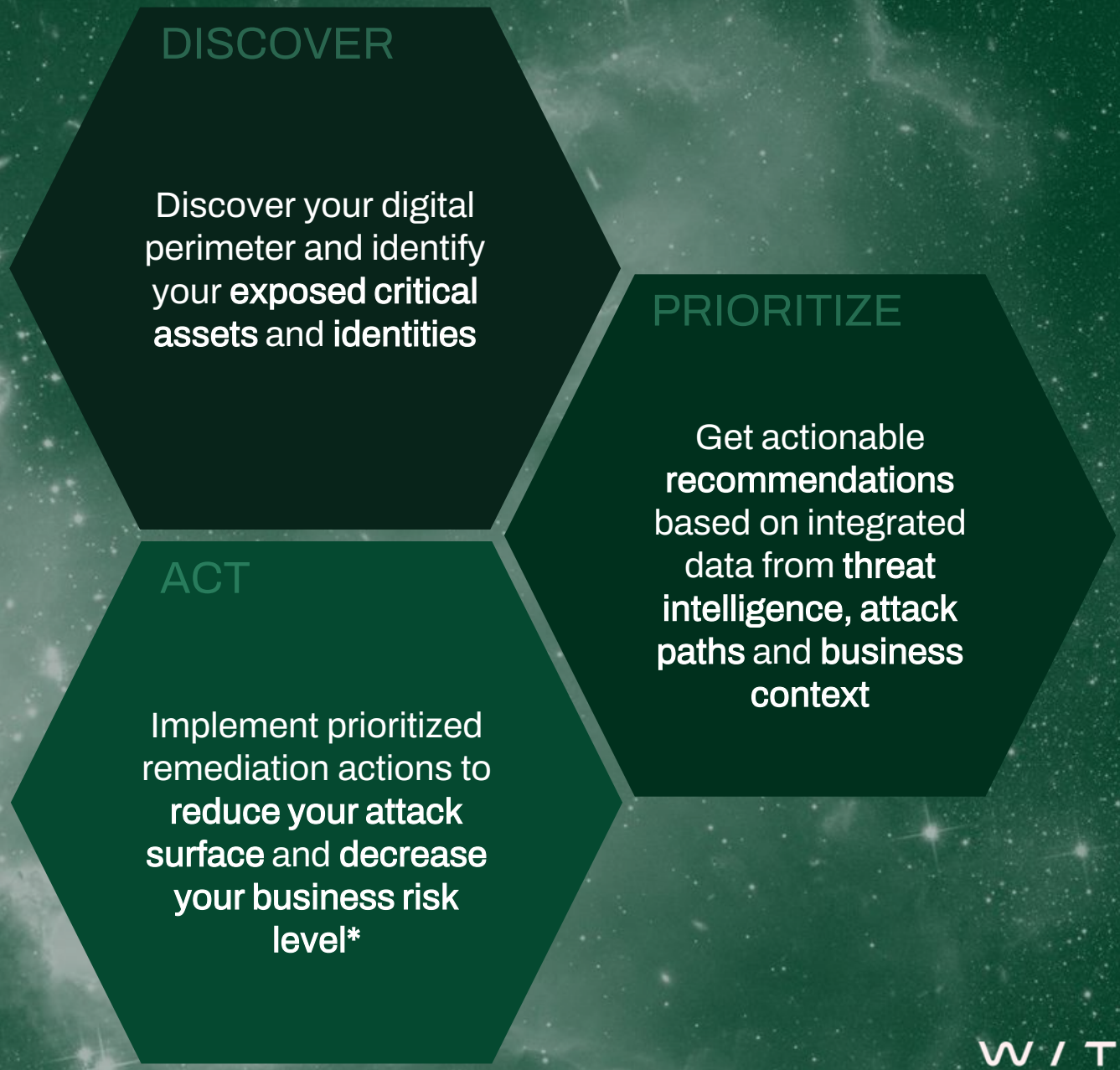
WITH secure

WithSecure™ Elements Exposure Management

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



Key outcomes:



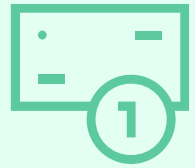
Note: *NIS 2 art. 21.2(e) mandates companies to have security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

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

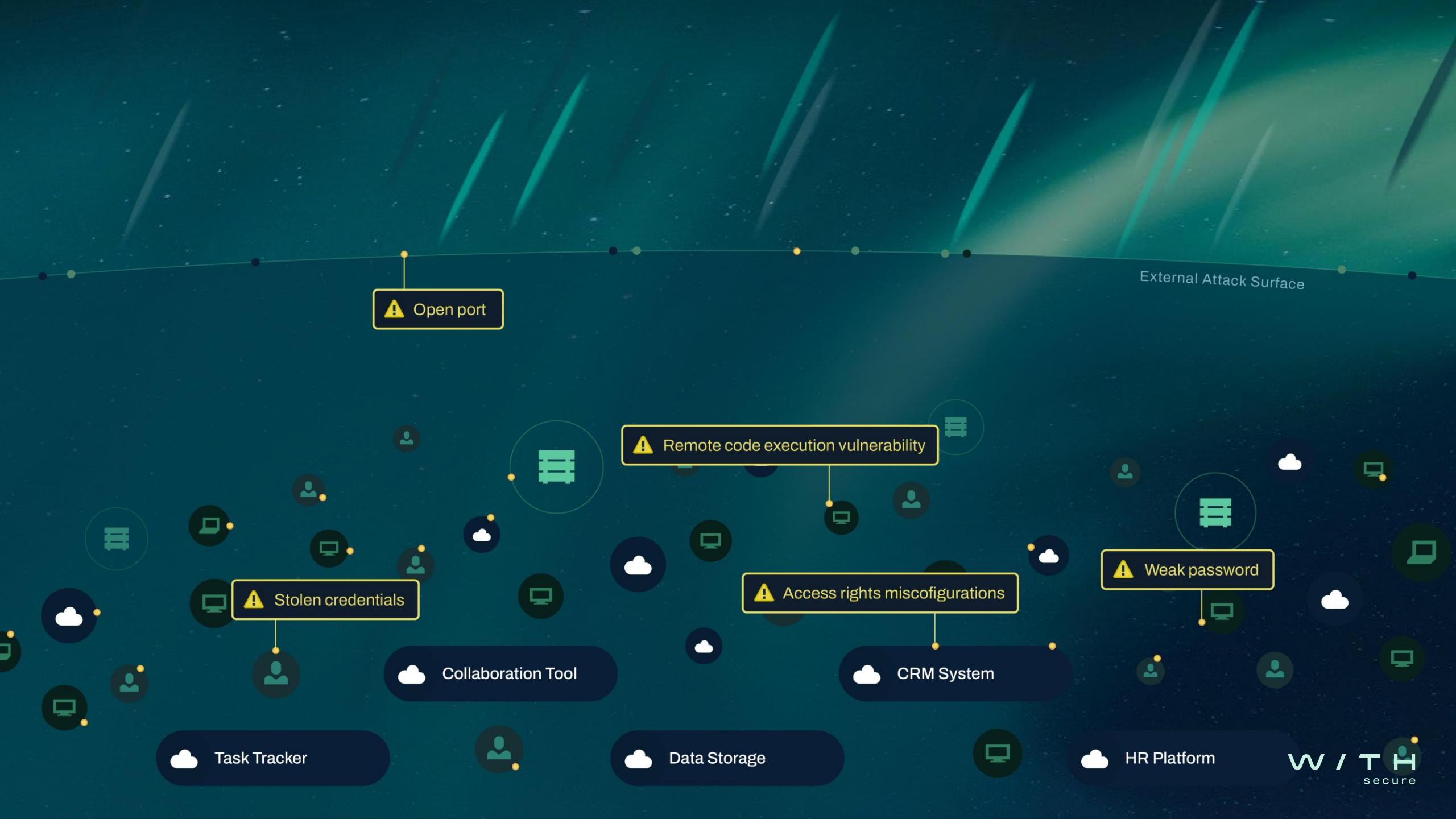
Many exposures, one solution
Tackle vulnerabilities, exploits & misconfigurations without silos

AI-powered recommendation engine
for efficient prioritization with actionable guidance

WITH secure

How it works

WITH secure

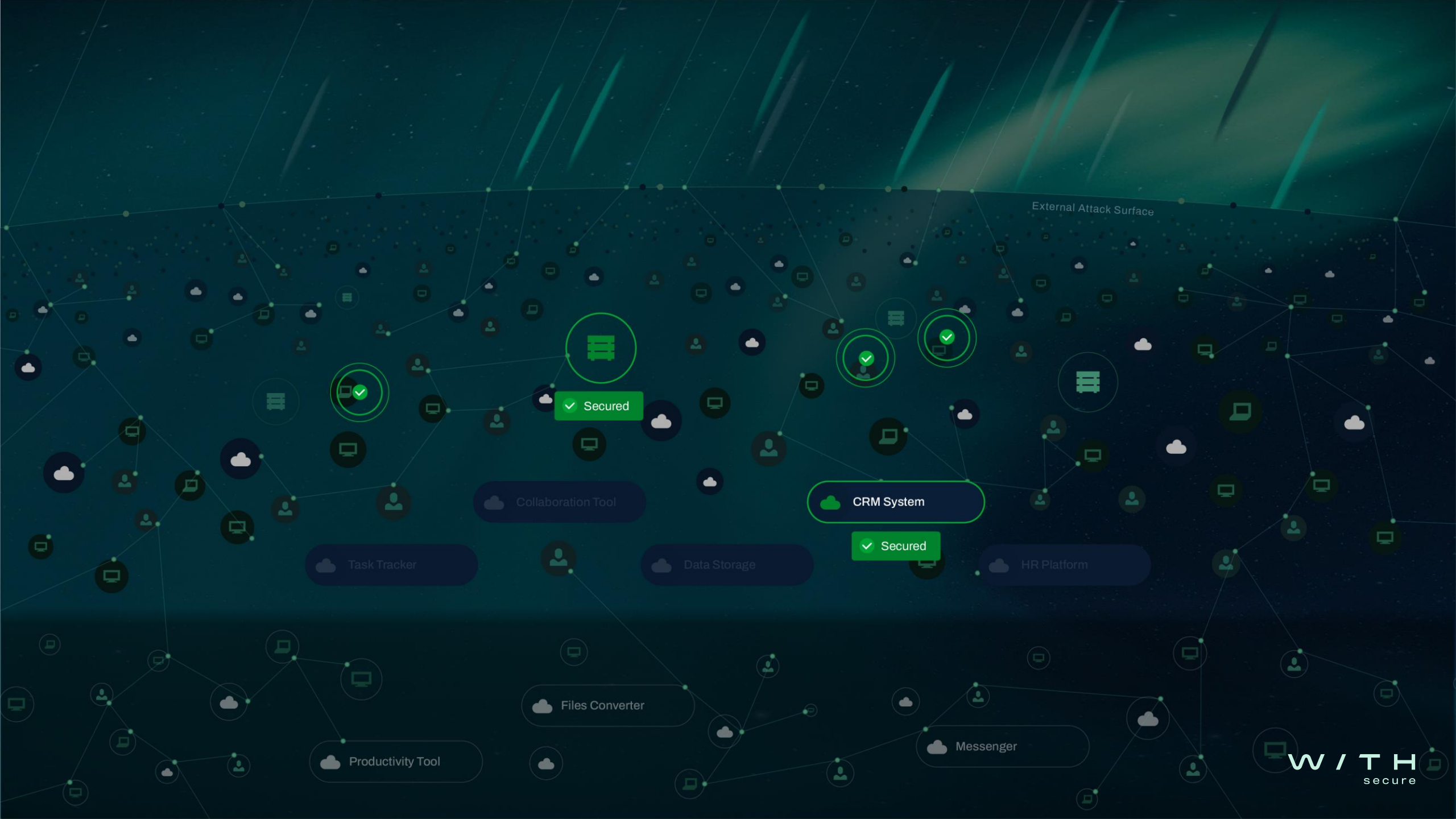

External Attack Surface
Open port
Remote code execution vulnerability
Stolen credentials
Access rights miscofigurations
Weak password
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
WITH secure


External Attack Surface
Collaboration Tool
CRM System
Task Tracker
Data Storage
HR Platform
WITH secure


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


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

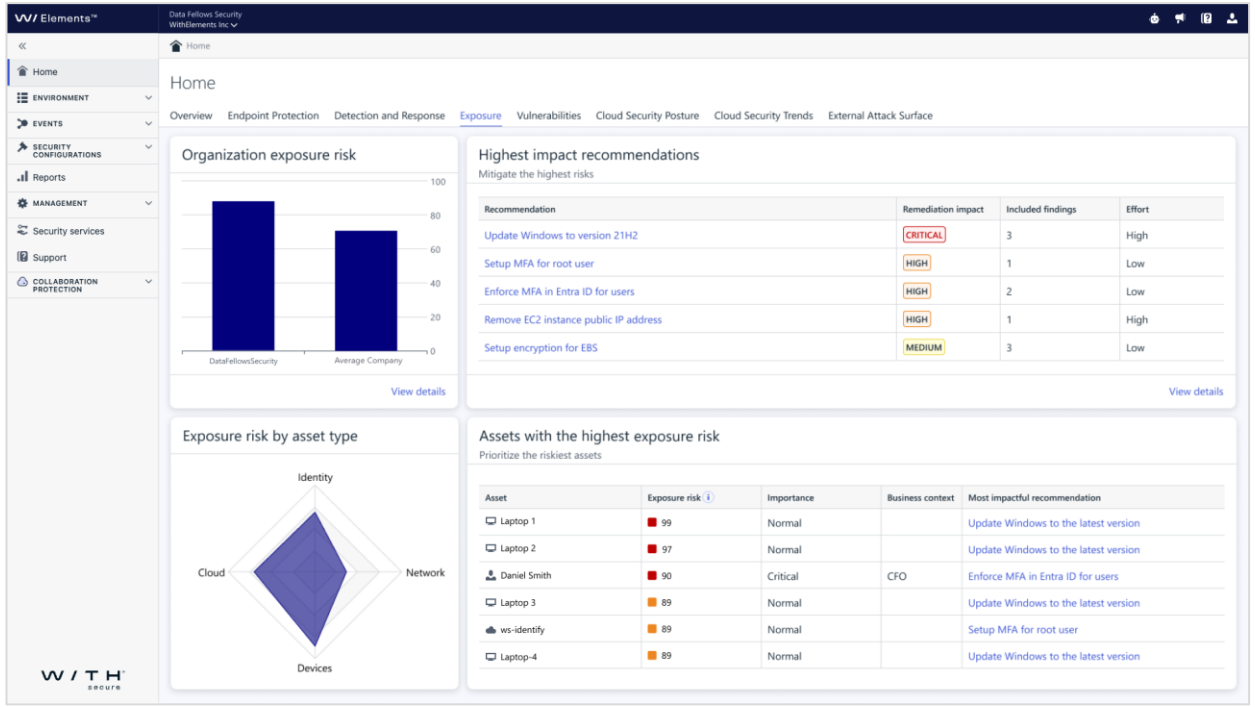

External Attack Surface
Secured
Collaboration Tool
CRM System
Secured
Task Tracker
Data Storage
HR Platform
Files Converter
Messenger
Productivity Tool

Key Features

WITH secure

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.

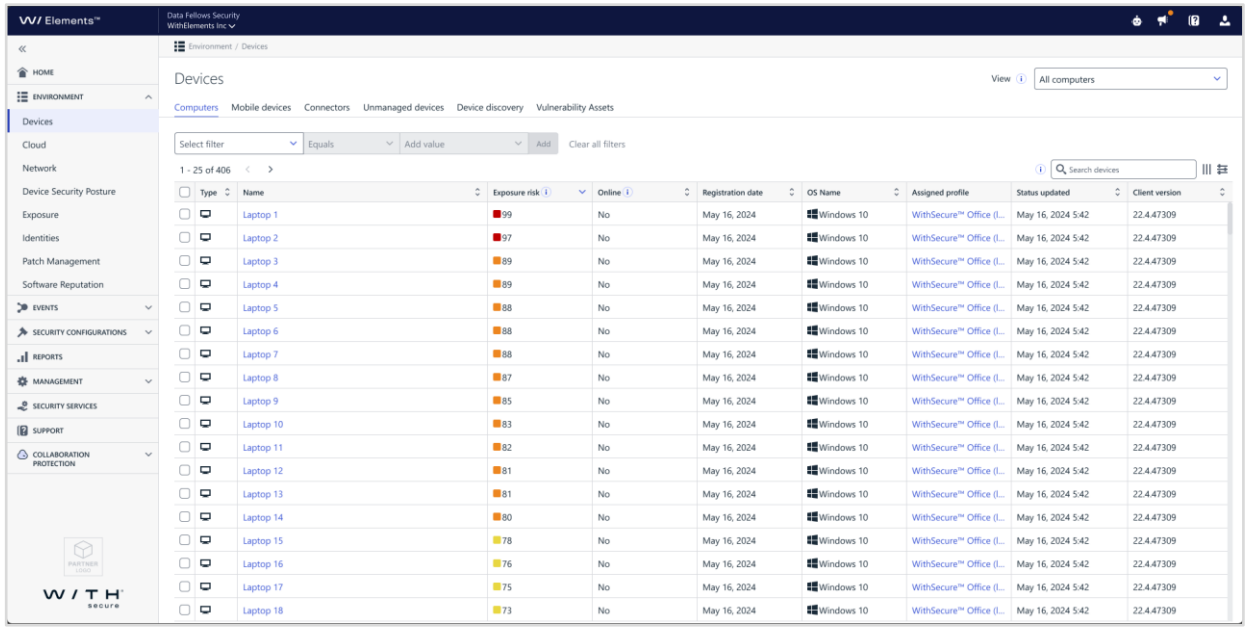
3. Know the next actions to improve exposure

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

WITH secure

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

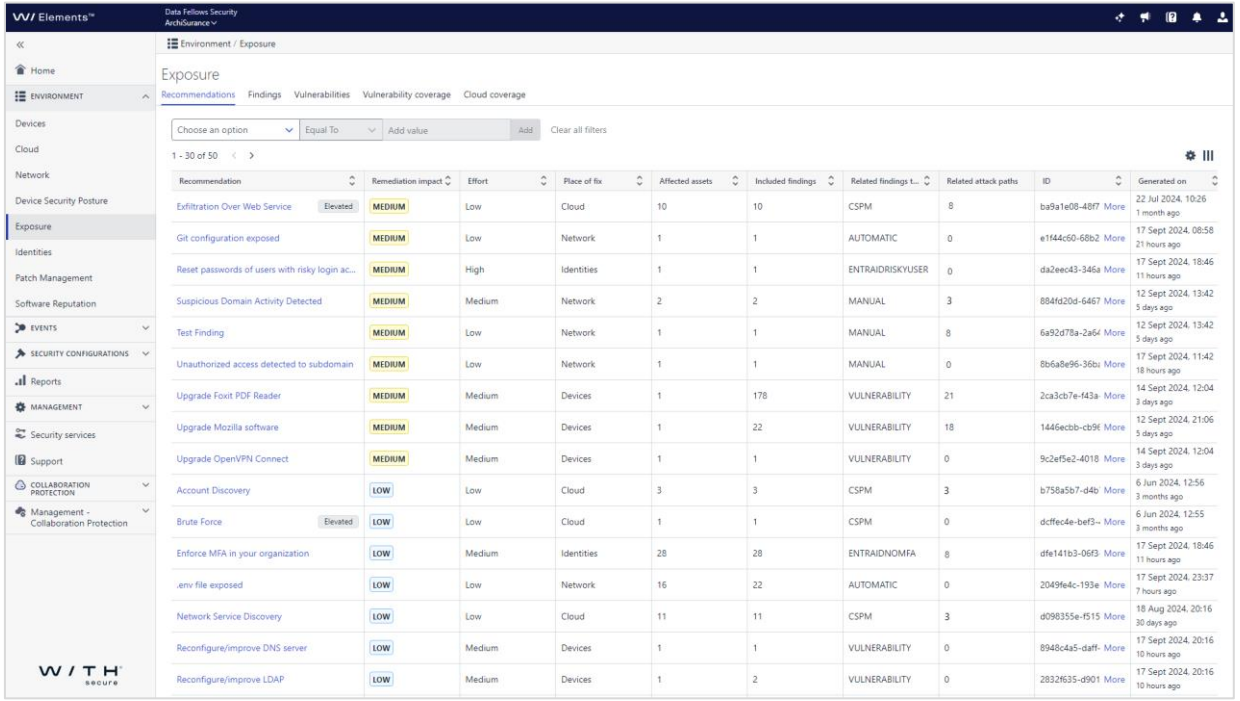
See the exposure risk level of your company and assets

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.

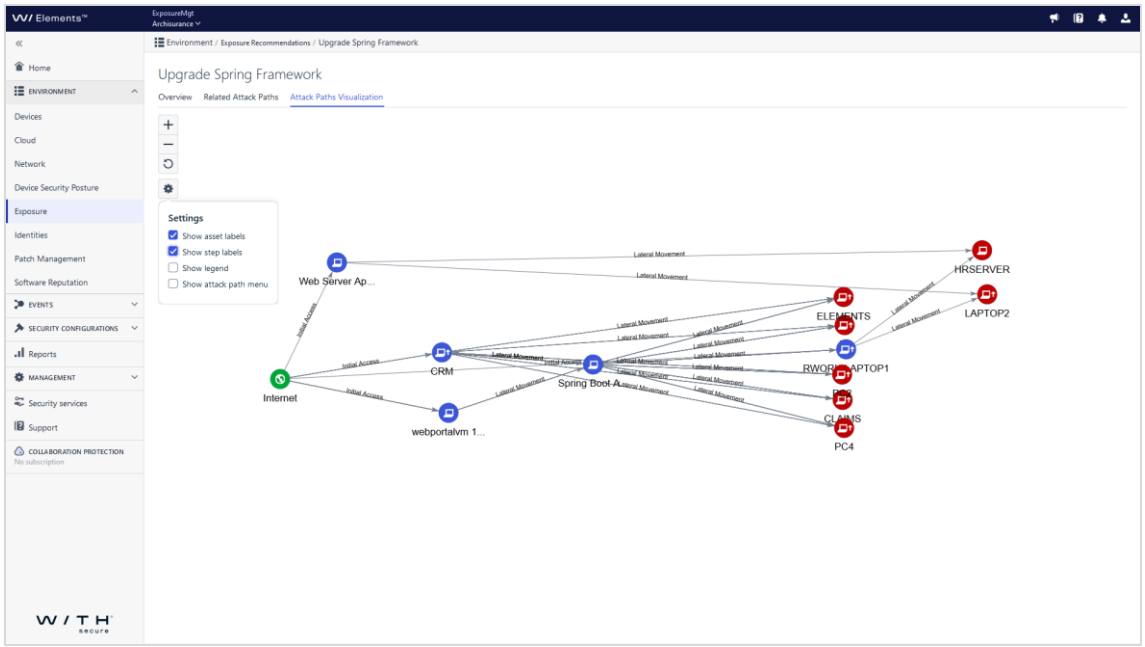
Benefit from our unique **threat intelligence data:**

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

W / T H 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.

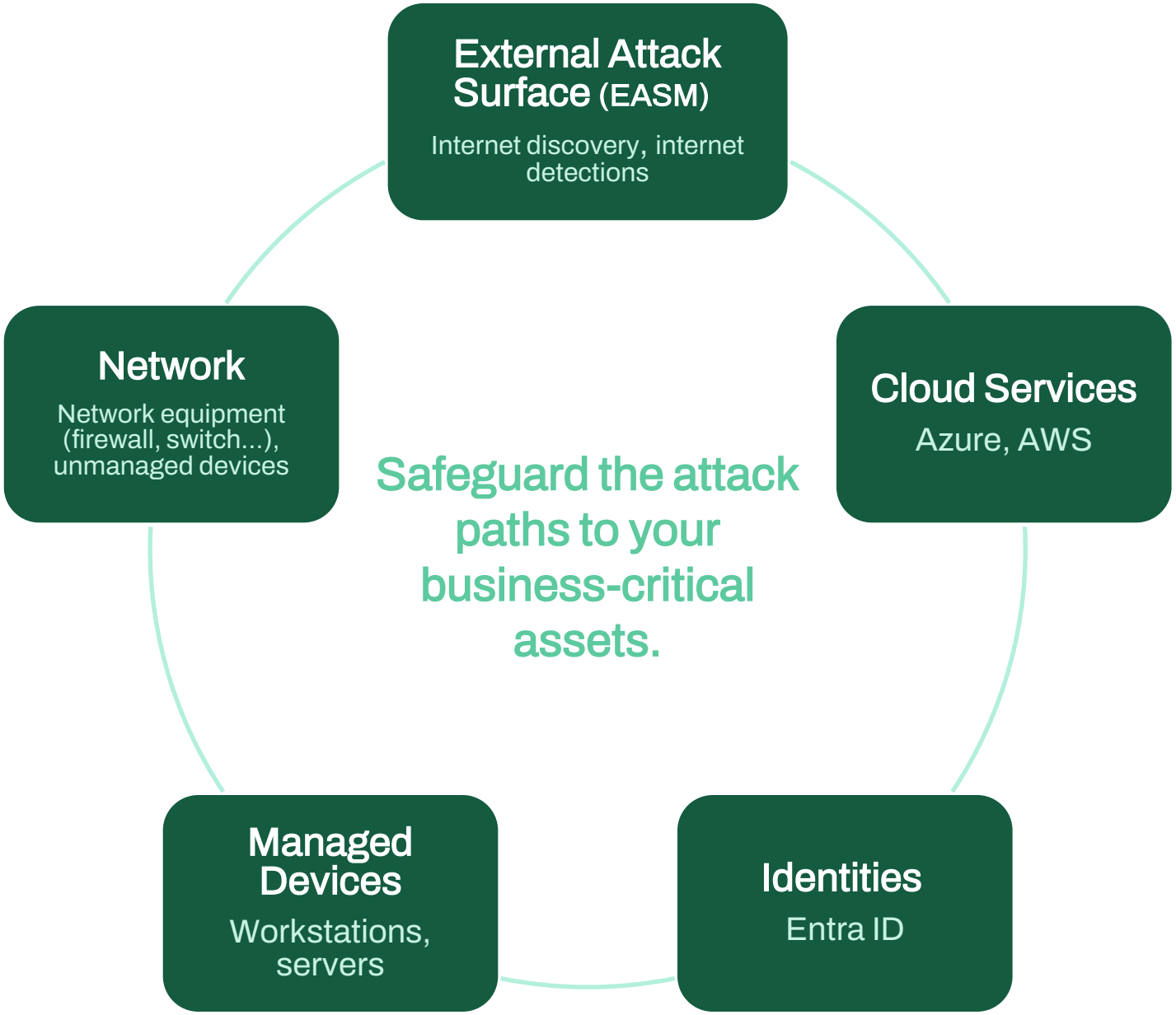
W / T H secure

Supported Assets

WITH secure

360° view of cyber risks

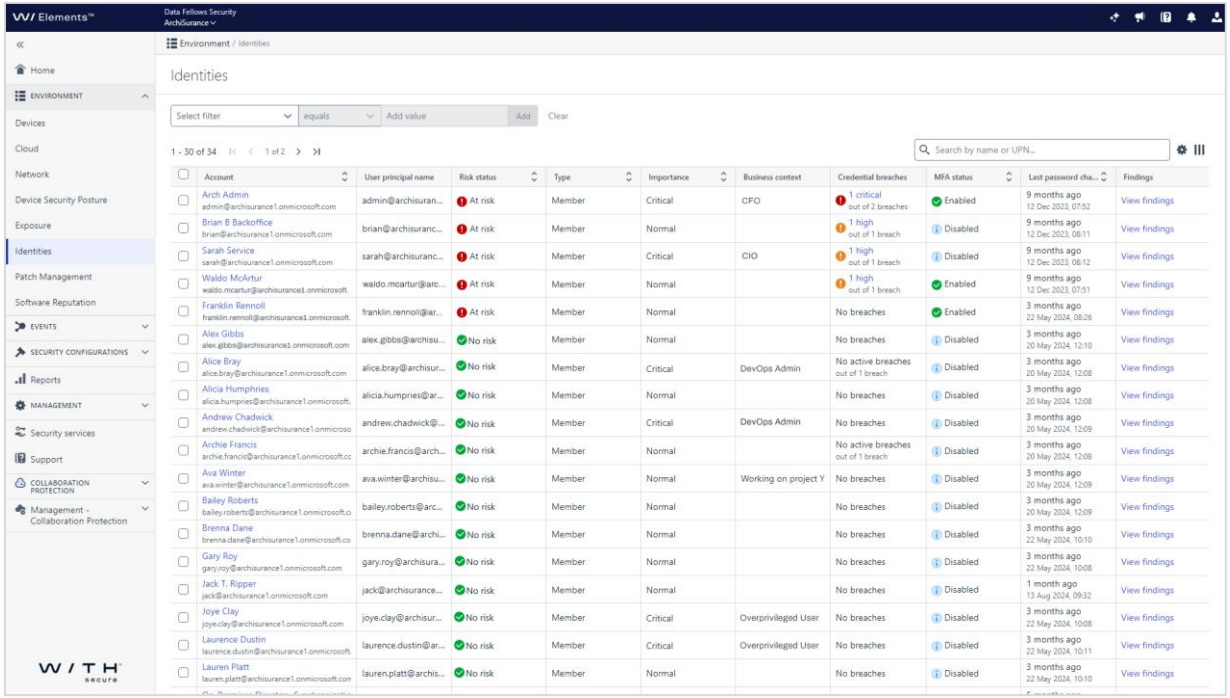
See your complete attack surface and remediate the highest-impact vulnerabilities that pose the most risk of intrusion to your organization efficiently from a unified view – thanks to our AI-powered recommendation technology.



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

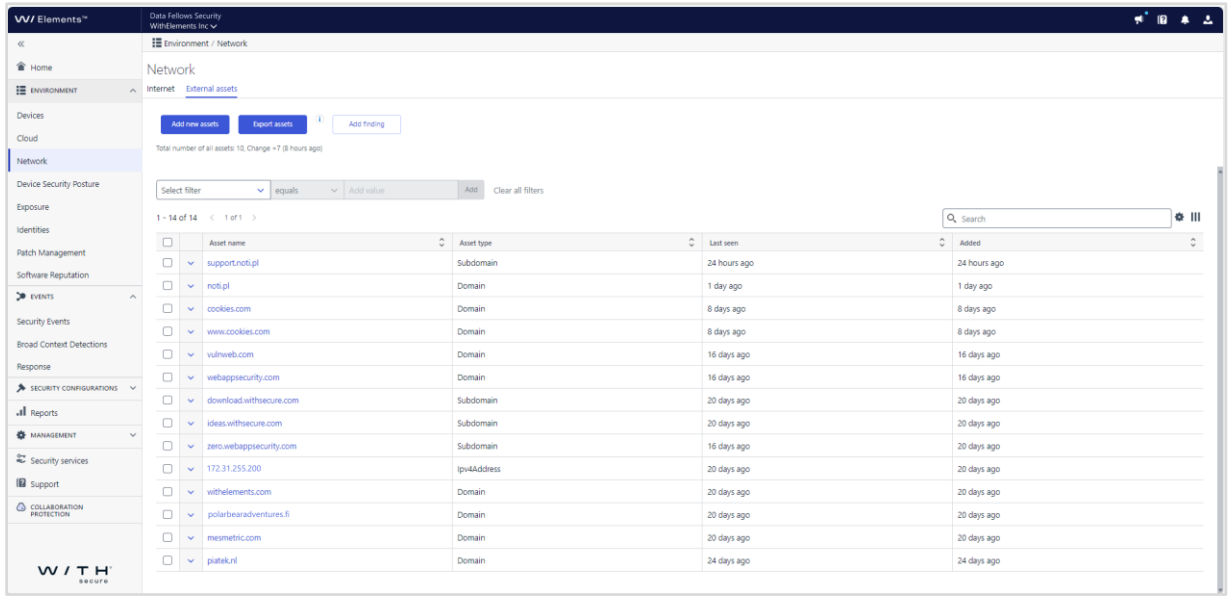
Exposure for Identity Risk

- 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.

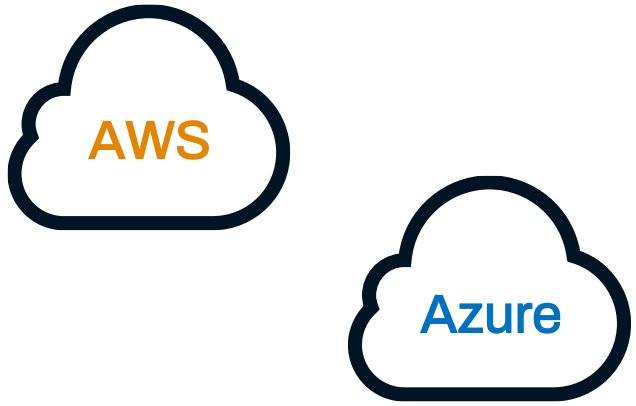
Internet detections

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

W / T H secure

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.

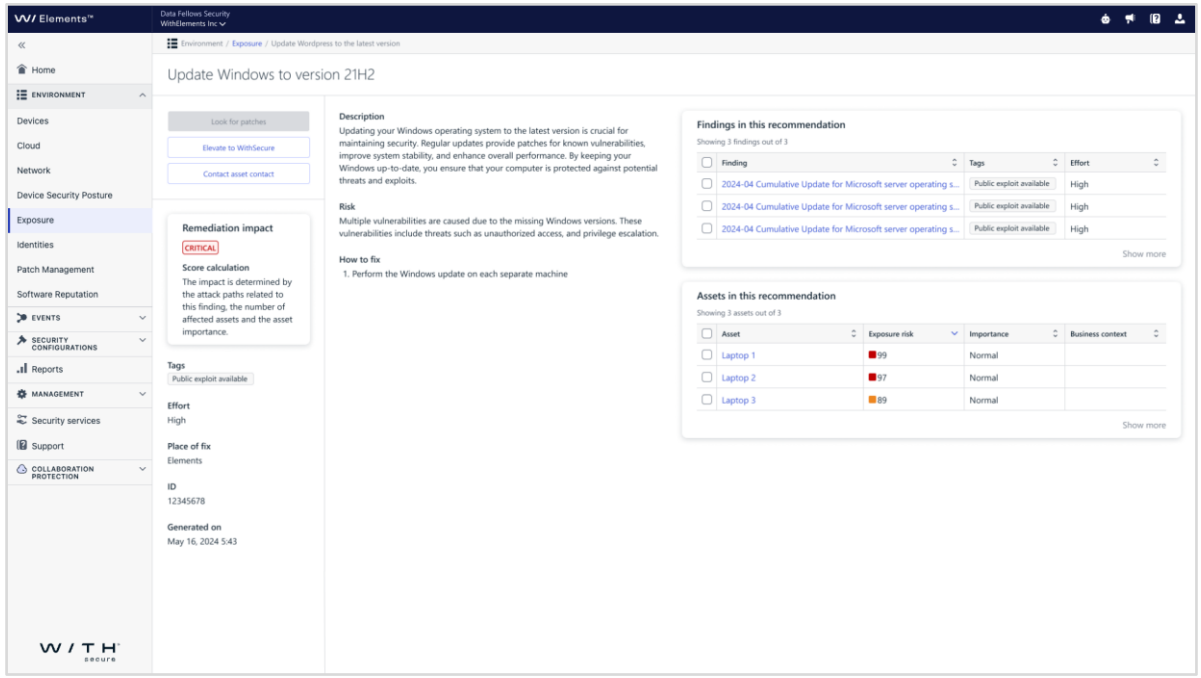
WITH secure

Remediate Exposures & Elevate Tough Cases

WITH secure

Remediation

Get actionable remediation guidance and track remediation

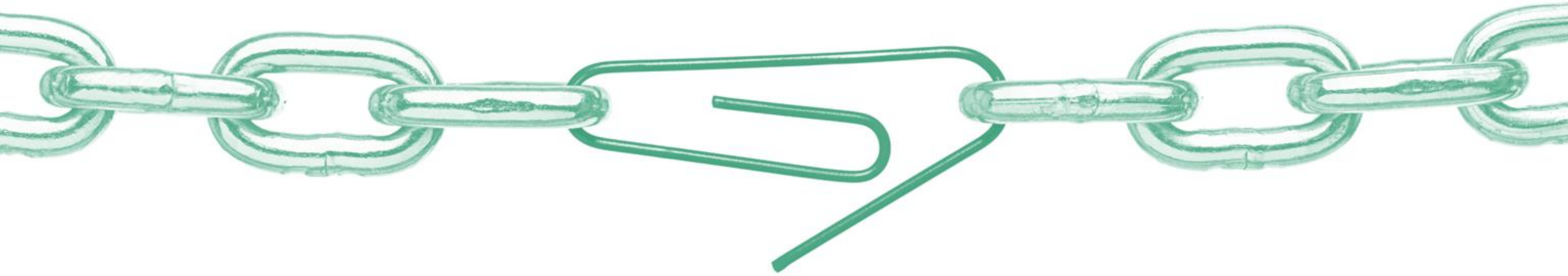


- Get **unified instructions** for remediation action, no matter the exposure type.
- Our actionable **remediation guidance** focuses on the top priority findings for you to work on.
- **Communicate** about the remediations for smooth collaboration.

Why choose WithSecure™ Elements Exposure Management?

WITH secure

Remediate business-critical exposures by focusing on the choke points in your attack surface.



WITH secure

Why choose Elements Exposure Management?

Thought-leading European Exposure Management with local threat intelligence, regulatory compliance, privacy, and decades of real-world attack experience

Actionable recommendations on what to remediate based on exposure scores that utilize our unique attack path modeling approach

AI-powered attack path simulation, where our reasoning engine and attack paths are built on heuristic scoring through the lens of the attacker

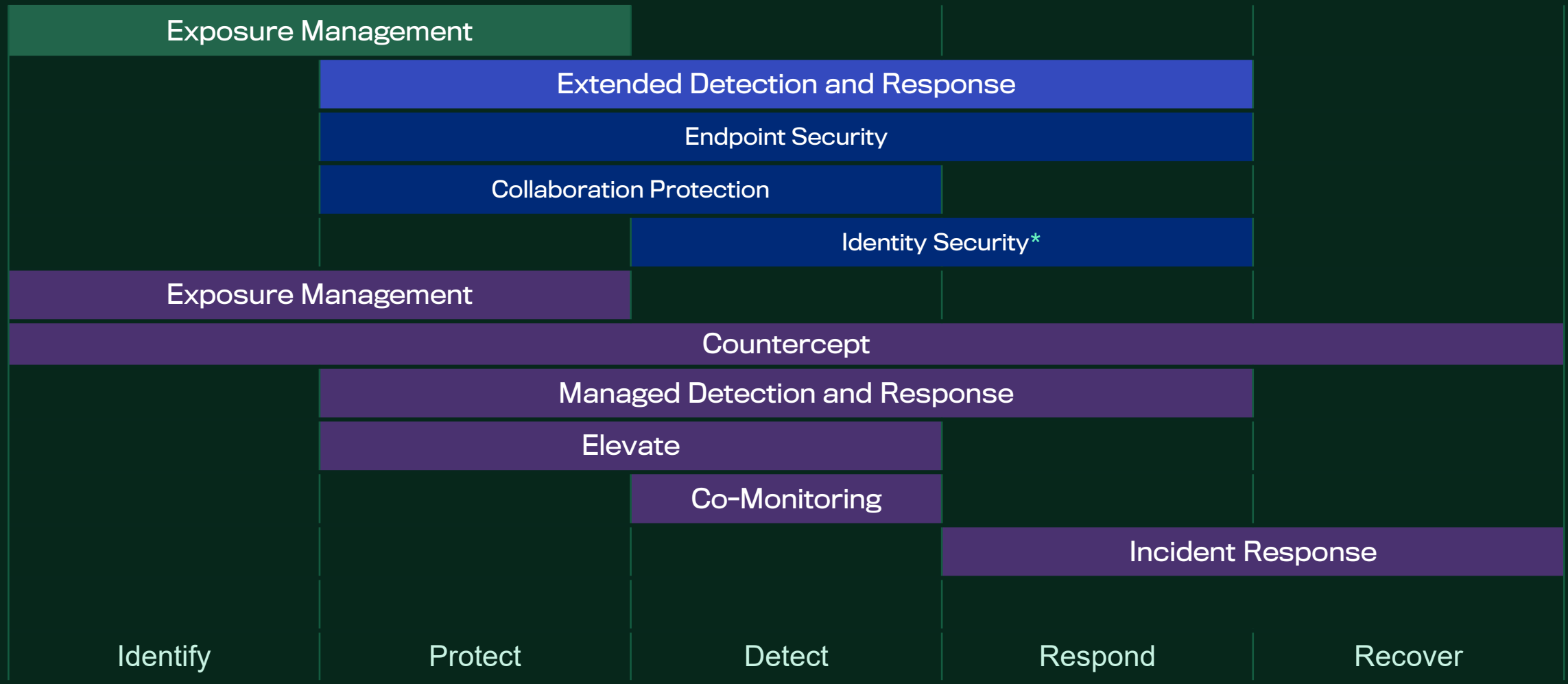
Covers identities, which can function as powerful attack acceleration points that are easily phished and stolen, in addition to covering the external attack surface

Optimized for minimum effective security and designed to offer democratized cyber security for mid-sized businesses, offering ease of use with limited resources

Unified security UX within a single pane-of-glass as part of the WithSecure Elements Cloud, complemented by Co-Security Services such as Elevate

WITH secure

WithSecure™ Elements Cloud – NIST



*Identity Security to be extended to respond capability later in 2024.

WITH secure

How Elements XM vs XDR protects your environment?

Environment

	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.
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*

* Availability planned for 2025.

WITH secure


Don't get exposed.

Introducing Elements XDR with Identity Security

Protect your organization against modern threats

WITH secure

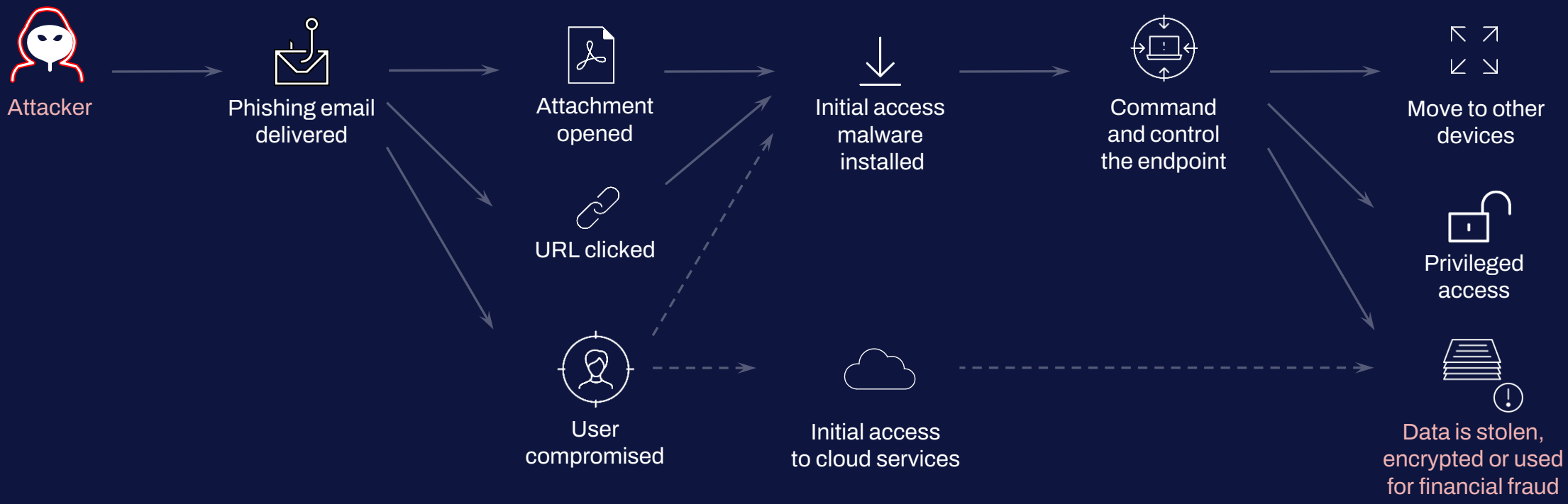
XDR is an evolution of EDR

Modern attacks no longer only start from malware on an endpoint, they stem from an attacker using an **identity** to gain access to business data.

Traditional EDR tools do not provide the visibility beyond the endpoint, **IT estates are now sprawling** across cloud hosted applications and emails.

Since **security skills are scarce** more tools doesn't necessarily mean you have the best security if you don't use them properly. **Need a low barrier to entry.**

XDR protection scenarios



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

WithSecure™ Elements | Extended Detection and Response

Preventive and reactive security

WITH secure

WithSecure™ Elements

Proactive and Modular. Made for Co-Security

- Exposure Management
- Extended Detection and Response
- Co-Security Services

WITH secure

WithSecure™ Elements

Proactive and Modular. Made for Co-Security

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

- Endpoint Security
- Identity Security
- Collaboration Protection

Co-Security Services

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

WithSecure™ Support Services

WITH secure

WithSecure™ Elements

Proactive and Modular. Made for Co-Security

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

- Endpoint Security
- Identity Security
- Collaboration Protection

Co-Security Services

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

WithSecure™ Support Services

WITH secure

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

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

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

Identity Security

Detect 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 phishing and other threats targeting users via email, Teams, OneDrive and SharePoint.

WITH secure

Introducing Elements Identity Security

Microsoft Entra ID

WITH secure

Same attacker, same goals, new target

Use of cloud-based Entra ID for remote workers and authentication to third party tools increases the attack surface

Attacks focus less on deploying payloads to endpoints, and more on abusing identities (user and entity) and their privileges.

Attacker goals have not changed, they are still trying to cause disruption and steal information.

WITH secure

Attacks targeting identities on the rise

71% spike in cyberattacks caused by exploiting identity – reported by **90% of organizations**

Attacks directly targeting Entra ID identities are on the rise based on our recent incident response engagements – **7 cases** in the last **6 months,** compared to 1 in the same period last year

Stolen or compromised credentials took the **longest to resolve** – nearly **11 months**

Source: Cost of a Data Breach Report 2023 by Ponemon,
Trends in Identity Security 2023 by Identity Defined Security Alliance

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 metadata anomalies.

Techniques to advance identity attacks

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

Attacks against privileged users' managed devices

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

WITH secure

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

Identity Security in Action

Protection against identity-based attacks

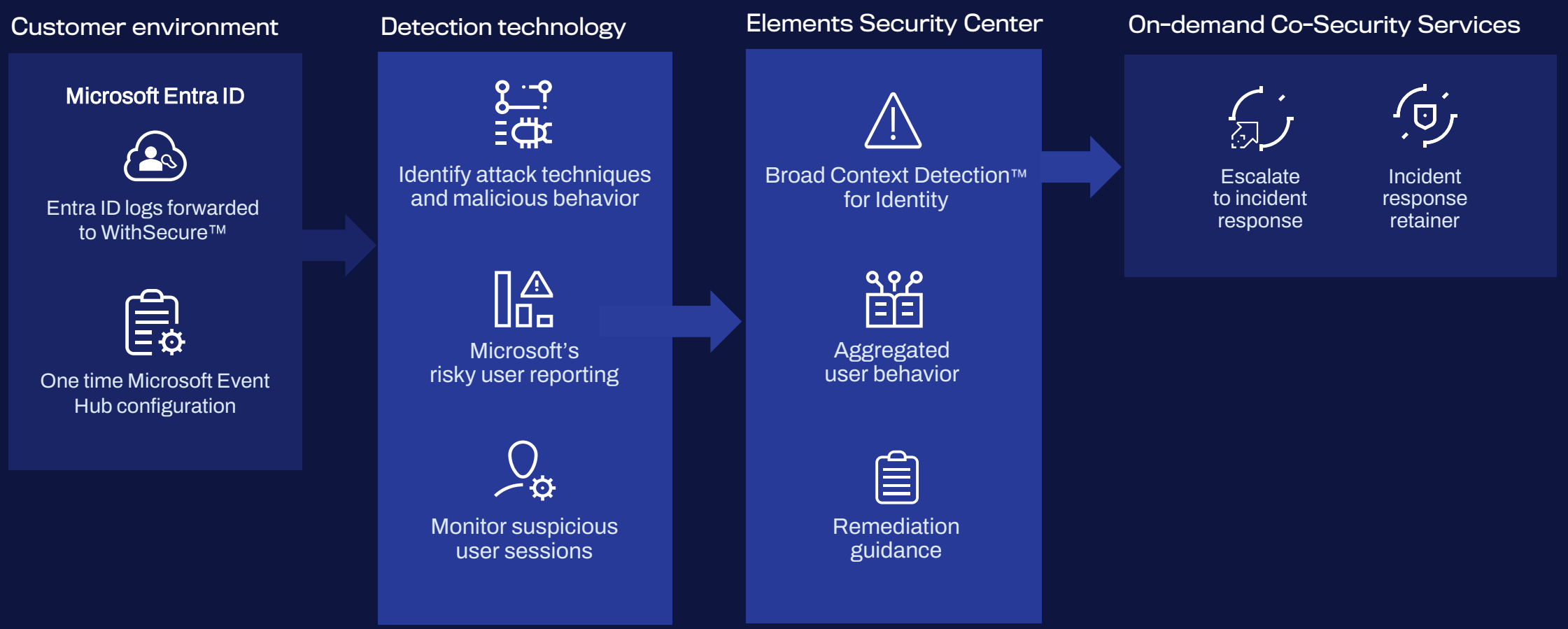
Capture relevant identity-based events to quickly detect suspicious user behavior **in one place**

Expand your existing endpoint focused toolset to quickly understand identity-based attacks in broader context

Reduce risk of data breaches by detecting potentially compromised users in modern cloud-based IT environments

WITH secure

WithSecure Identity Security for Entra ID



Monitoring, investigation and response

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

WITH secure

Detection coverage

Attacker abuses stolen credentials, tokens or sessions.

Stolen credentials are used to log into the Azure Tenant
We detection this by identifying atypical sign ins
e.g. rare country, impossible travel

Attacker creates an “application registration” that they can use from their own tenant to access the “target tenant”

Attacker disables or removes MFA

WITH secure

Configuration steps for Identity Security

1

Elements Security Centre guides through onboarding configuration

2

A script is downloaded from the portal

3

Customer runs the script

Each tenant requires one script

4

Customer configures cloud connection by entering the connection string

5

Final test of the configuration

6

Data collection begins and detections appear in the portal

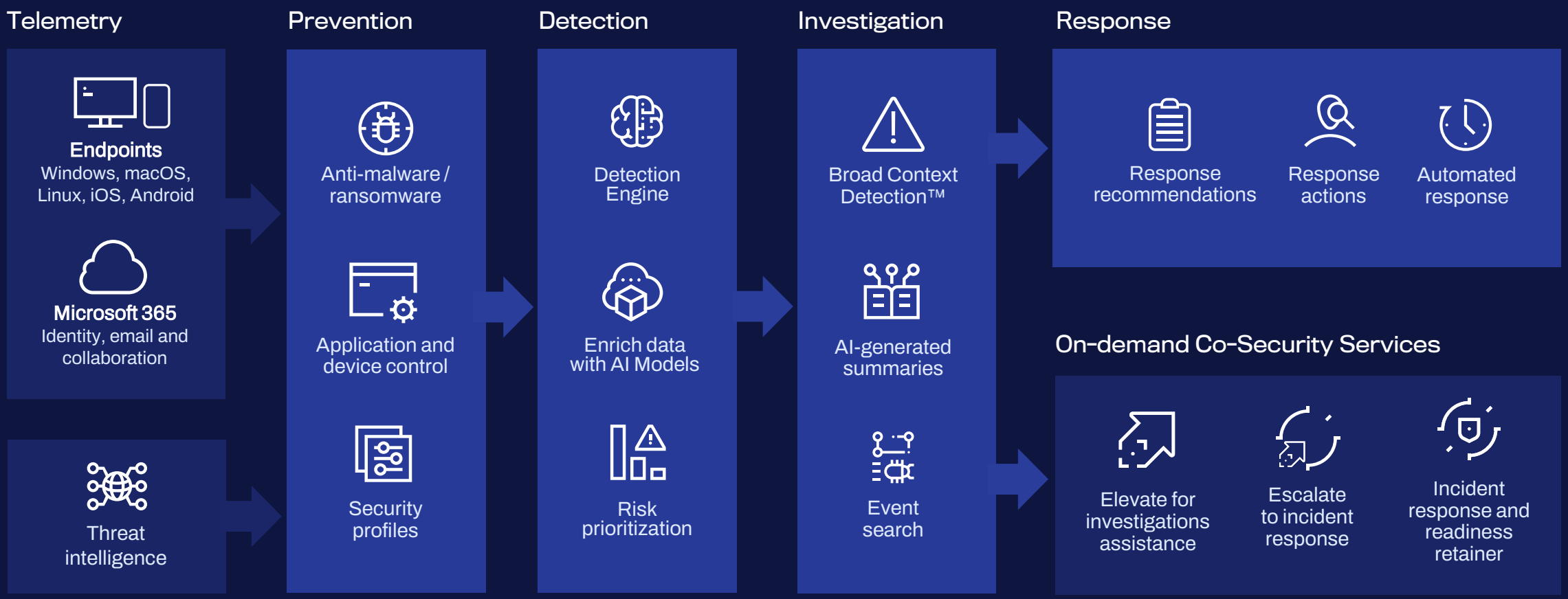
WITH secure

Elements 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

WITH secure

WithSecure Elements XDR in operation



Configuration, monitoring, investigation and response

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

WITH secure

Kako se podjetja branijo?

Podjetje M

- Proizvodno podjetje
- 100+ zaposlenih

- Varnostne rešitve:
  - Požarna pregrada
  - Windows Defender
  - Zaščita elektronske pošte za M365 okolje
  - Varnostno kopiranje podatkov s ključnih strežnikov

- Vodstvo je dalo prioriteto zadovoljstvu zaposlenih
  - Dovoljena ohlapna gesla
  - Malo ali brez omejitev pri dostopih do internih storitev
  - Pogosto omogočene administratorske pravice

- Aktivno testirali EDR rešitev

Podjetje M – potek incidenta

Začetni vstop

Nikoli odkrili pravega vektorja napada. Najbolj verjetna razlaga je vstop preko slabo zavarovanega RDP dostopa do strežnika

Širjenje okužbe po strežnikih

Postopno širjenje okužbe tudi na delovne postaje z najdenimi domenskimi gesli

KRIPTIRANJE

Začetek kriptiranja

Na omejenem obsegu EDR agentov sprožene prve zaznave zaradi širjenja okužbe

Poleg izključitve že okuženih naprav so urgentno pričeli z nameščanjem EDR agentov v celotno okolje

ČIŠČENJE

S pomočjo EDR in hitre reakcije so uspeli identificirati vse okužene naprave

EPILOG

Vodstvo je dovolilo investicijo v dodatne varnostne ukrepe: zdaj najemajo zunanje SOC storitve skupaj z EDR

Podjetje M cidenta

Ne vemo s kakšnimi orodji in kateri dostopni podatki so bili kompromitirani

Prvi indici, da se nekaj zares dogaja, pred tem so zaznavali le upočasnjene interne storitve

Nimamo podatkov o vstopni točki, zaradi česar bi lahko prilagodili tudi ostale varnostne sisteme

Najprej so se morali opeči, da so dokončno ukrepali

streznika

Širjenje okužbe po strežnikih

Postopno širjenje okužbe tudi na delovne postaje z najdenimi domenskimi gesli

KRIPTIRANJE

Začetek kriptiranja

Na omejenem obsegu EDR agentov sprožene prve zaznave zaradi širjenja okužbe

Poleg izključitve že okuženih naprav so urgentno pričeli z nameščanjem EDR agentov v celotno okolje

uspeli identificirati vse okužene naprave

ILOG

dstvo je dovolilo vesticijo v dodatne varnostne ukrepe: zdaj najemajo zunanje SOC storitve skupaj z EDR

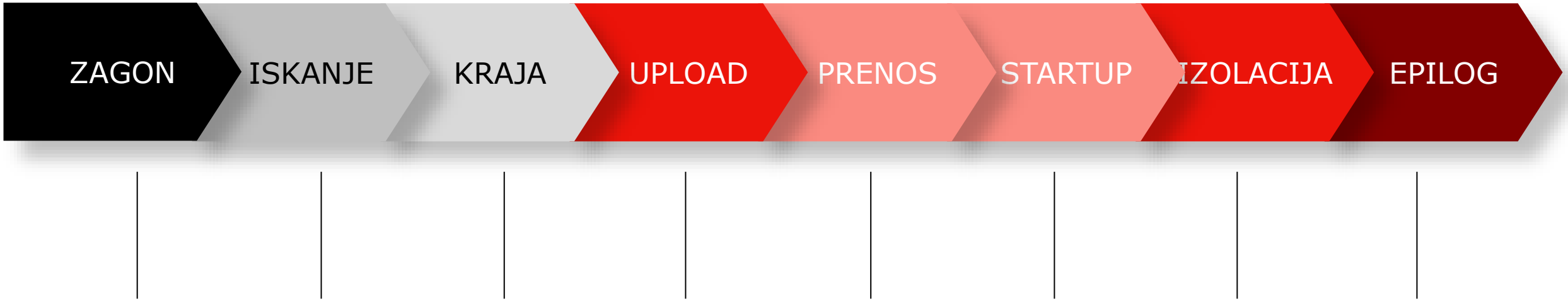
Podjetje K

- Storitveno podjetje
- 200+ zaposlenih

- Varnostne rešitve:
  - Požarna pregrada
  - Zaščita elektronske pošte
  - Varnostno kopiranje podatkov
  - Napredna zaščita delovnih postaj in strežnikov z vključenim EDR
  - Nadzor omrežja s postavljenimi vabami
  - Omejene pravice uporabnikov
  - Redno izvajanje varnostnih pregledov
  - Izobraževanje zaposlenih na področju informacijske varnosti

- Vodstvo podpiralo investicije v informacijsko varnost

Podjetje K – potek incidenta



midjourney.exe
Uporabnik je ob raziskovanju orodij za AI kreacijo fotografij neprevidno zagnal datoteko

Proces je takoj zbral vse podatke o trenutnem uporabniku, sistemu in omrežju ter dosegljivih strežnikih

Proces je iz pomnilnika poiskal vsa gesla, enako je pobral vsa gesla, ki so bila shranjena v brskalnikih

Credential theft

Zbrane podatke je proces naložil na javno dostopne spletne storitve (twitter oz X, reddit in pastebin)

Iz istih spletnih storitev je proces prenesel delčke datotek, ki so se lokalno združili v nov proces

Nov proces je bil vstavljen na lokacijo za samodejni zagon ob naslednjem zagonu ali prijavi na lokacijo „startup“

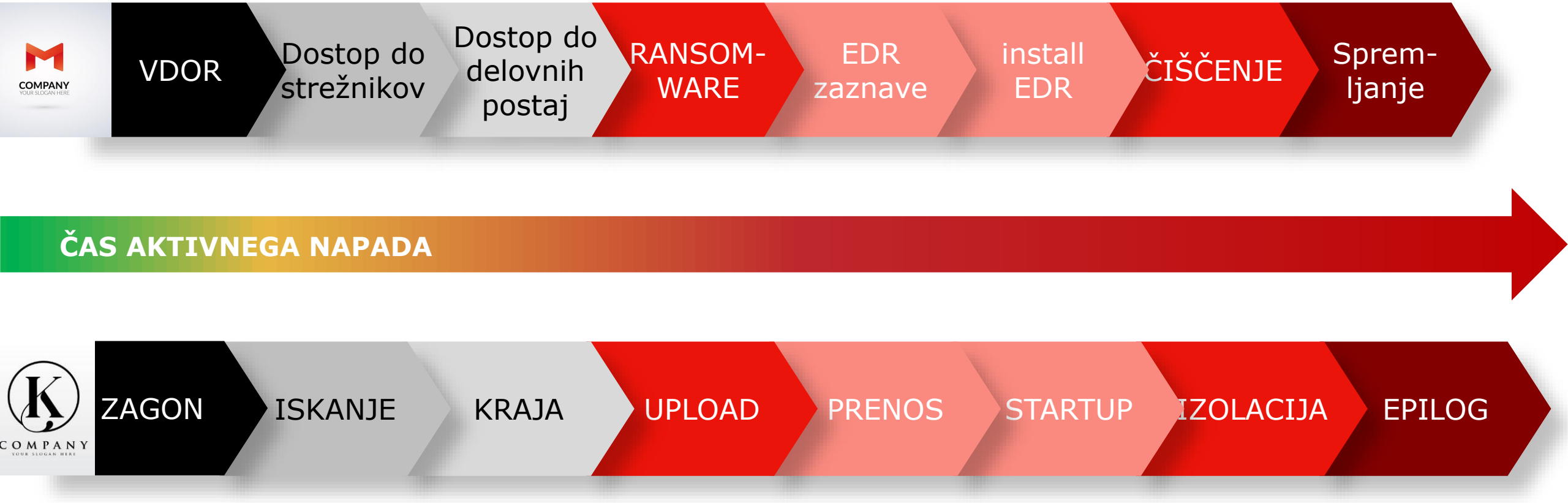
Reakcija EDR

EDR je na podlagi analize omenjenih dogodkov samodejno klasificiral grožnjo najvišje stopnje in sprožil samodejno osamitev naprave

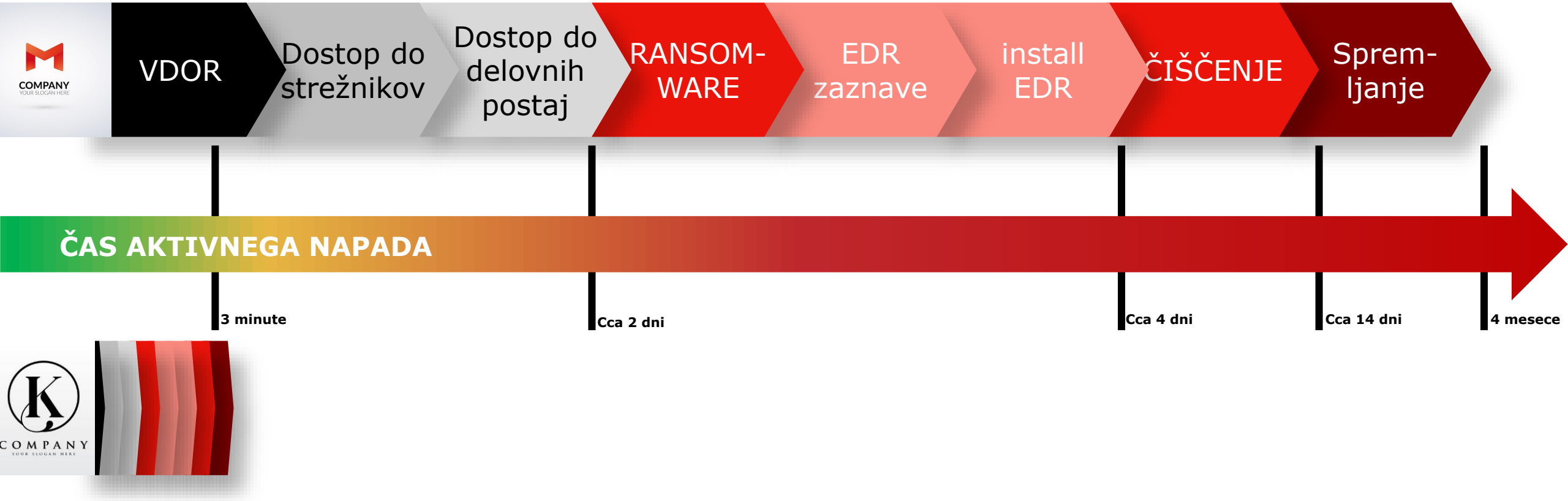
Ocena škode

Poslovna škoda je omejena na zamenjavo gesel, ki so bila lokalno dosegljiva, drugih podatkov napadalcu ni uspelo odtujiti

Primerjava incidentov



Primerjava incidentov



Why choose Elements XDR?

A unified solution to gain visibility

to protect modern IT estates and minimize impact of attacks

Advanced prevention

with award-winning protection that enables XDR to be effective

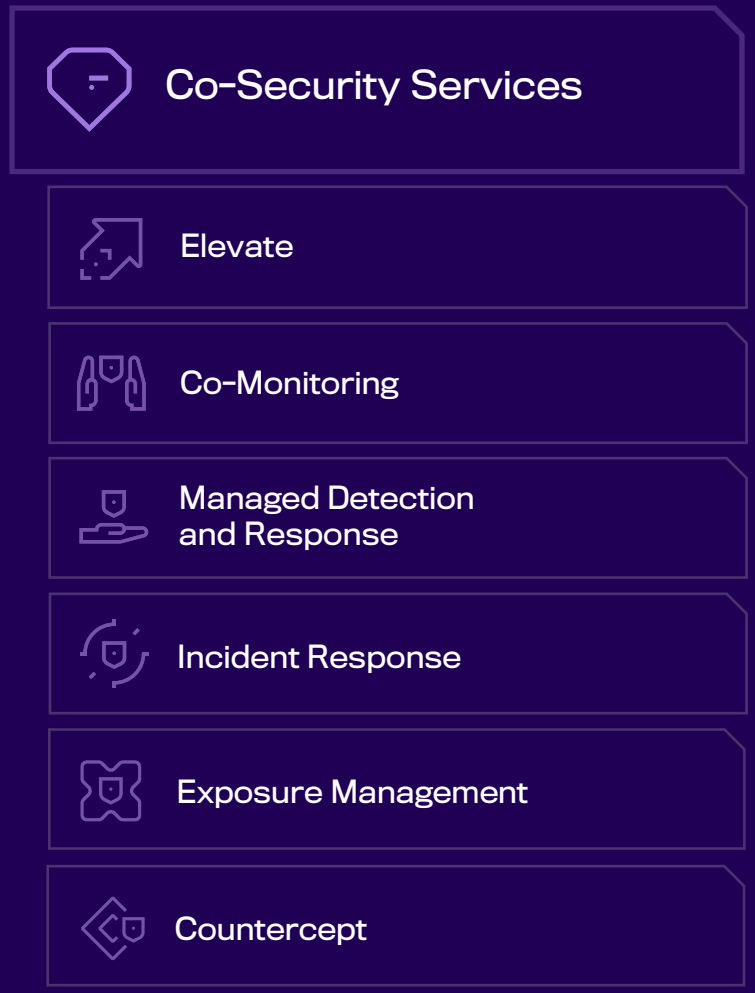
AI-powered tooling

for fast detection, investigation and response to threats in broader context

Easy access to augment your team

with flexible, round-the-clock expert services

WITH secure



WithSecure™ Co-Security Services

World's best experts behind a click of a button, co-delivered with partners

WITH secure

For mid-market companies seeking assistance for their cyber security operations

Strong defenses are built on teamwork

Experience, Expertise and Effortless Experience

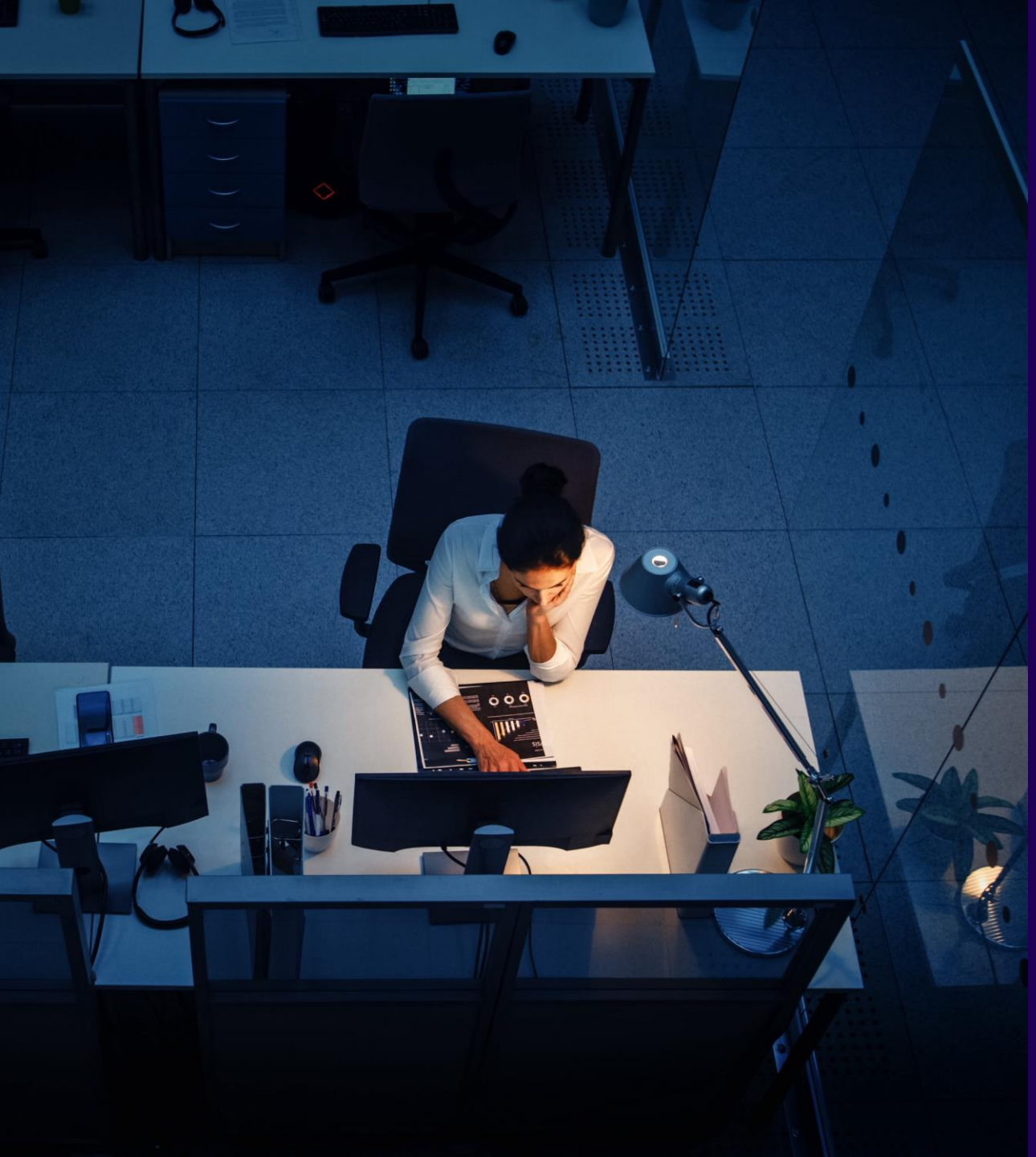
Cyber criminals don't keep office hours

Empowering partners to offer cyber security

WITH secure

Strong defenses are built on teamwork

- We join forces with customers and partners to protect business outcomes against cyber risks and threats.
- Together with our partners we combine expertise and knowledge to amplify the security outcomes to customers.



Cyber criminals don't keep office hours

- We monitor your IT environments around the clock.
- WithSecure expert analysts are “one-click away” to detect and respond.
- Services range from on-demand Elevate to 24/7/365 Managed Detection and Response services.

WITH secure

Experience, Expertise and Effortless Experience

- Detection and Response Team (DRT) with deep expertise and real-world experience
- Supported by researchers and developers
- Highly professional Incident Response team handles emergency incidents.

Empowering partners to offer cyber security

- Our technology empowers partners to enhance their cybersecurity capabilities, even if they don’t provide full security services.

- By leveraging Elements Cloud, partners efficiently deliver value to customers with existing staff and establish security services within their IT service offering.

WITH secure

WithSecure™ human expertise

- Detection and Response Team (DRT) members with the help of the combined wisdom of ~100 researchers, developers, and operators.
- Over 60 experts work exclusively on attack detection and incident response.
- Offensively minded threat hunters with experience of real-world attacks daily.
- Highly professional and certified Incident Response team handles emergency incidents.
- Teams located in the United Kingdom, Poland and Kuala Lumpur, providing a follow-the-sun approach that ensures a high level of service delivery 24x7x365 and zero ‘skill downtime’.

20 years of IR experience tells us...

The cost of a cyber security incident is 70-90% lower...

...contained within 72 hours of detection

WITH secure

Enhance your security operations team with flexible access to combat-fit defenders

Detection and Response service need and risk profile

Extended Detection and Response

Elements Software

Elevate

On-Demand Assistance, Investigation & Guidance

Co-Monitoring

Outsourced Monitoring, Investigation & Guidance

Managed Detection and Response

Managed Detection and Response

Countercept

'Premium MDR' with continuous security posture improvement.

Incident Response

Incident Response service

Exposure Management

Elements Software

Exposure Management

Exposure Management service

Amount of human-delivered service

WITH secure

Co-Security Services

Elevate

WithSecure™ Elevate is a threat analysis and guidance service available to Elements Endpoint Security (EDR) customers that validates and investigates difficult detections.

Co-Monitoring

The WithSecure Co-Monitoring Service provides Elements EDR (Endpoint Detection and Response) users with 24/7 validation, investigation, and remediation guidance. Also possibility for monitoring during Out-of-Office times and expanded with seamless escalation to our Incident Response (IR) retainer services.

Managed Detection and Response

WithSecure MDR is a continuous 24/7 detection and response service, in which WithSecure cyber security experts protect your IT environment by investigating and remediating cyber security attacks on your estate using data collected by WithSecure Elements EDR. Includes also Incident Response service.

Exposure Management

Exposure Management service includes three options: Elevate service for escalating tough cases in Exposure Management to WithSecure to get help with prioritization and validation, Proactive Threat Hunting service and Exposure Review service.

Incident Response

WithSecure Incident Response service is an insurance-like service, which provides SLA-backed, on-demand access to skilled IR resources during a cybersecurity incident, whose primary objective is to ensure the business continuity of the client.

Countercept

Countercept is a full MDR service that deals with cyber threats to your organization in minutes. WithSecure Countercept MDR acts as an extension of your cyber security team, sharing out threat hunting expertise, helping your team learn and grow, and continuously improving your security.

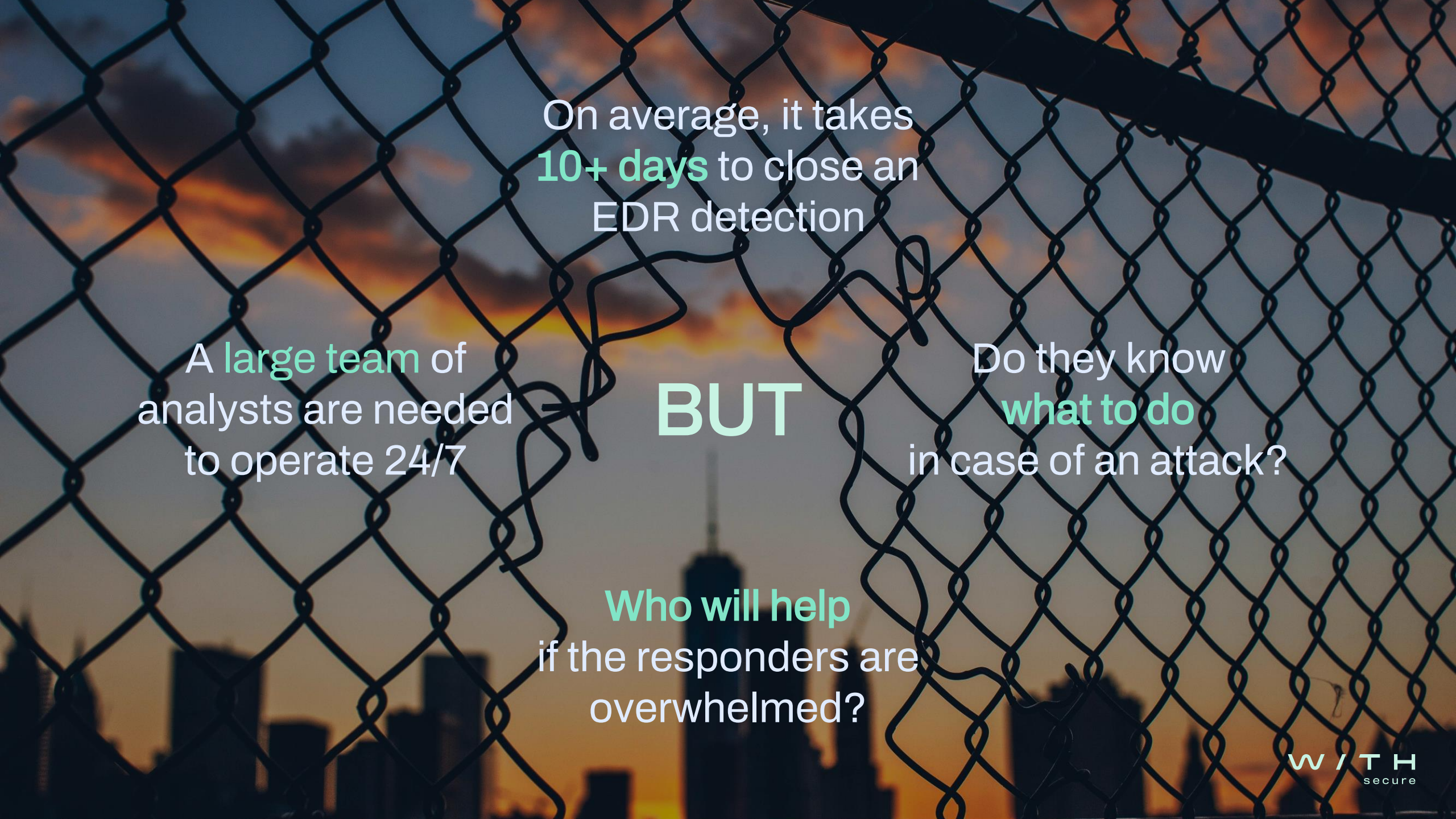
WITH secure

WithSecure™ Elevate

- If deeper threat analysis and guidance by specialized cyber security experts is required, the solution has a unique **built-in Elevate to WithSecure™ service***.
- Sometimes you might want to ask for more information about a detection from our security experts, for example to analyze or follow-up on unusual activity.
  - For example, we receive requests to analyze suspicious attachments or links, which we can do with some of the forensic utilities available to us.
- Offers professional incident analysis of methods and technologies, network routes, traffic origins, and timelines of a Broad Context Detection™ to provide expert advice and further response guidance.

* **Note:** Full WithSecure Elevate service availability planned for the General Availability of WithSecure MDR.

WithSecure Co-Monitoring Service


On average, it takes
10+ days to close an
EDR detection
A large team of
analysts are needed
to operate 24/7
BUT
Do they know
what to do
in case of an attack?
Who will help
if the responders are
overwhelmed?
WITH
secure

WithSecure Co-Monitoring service

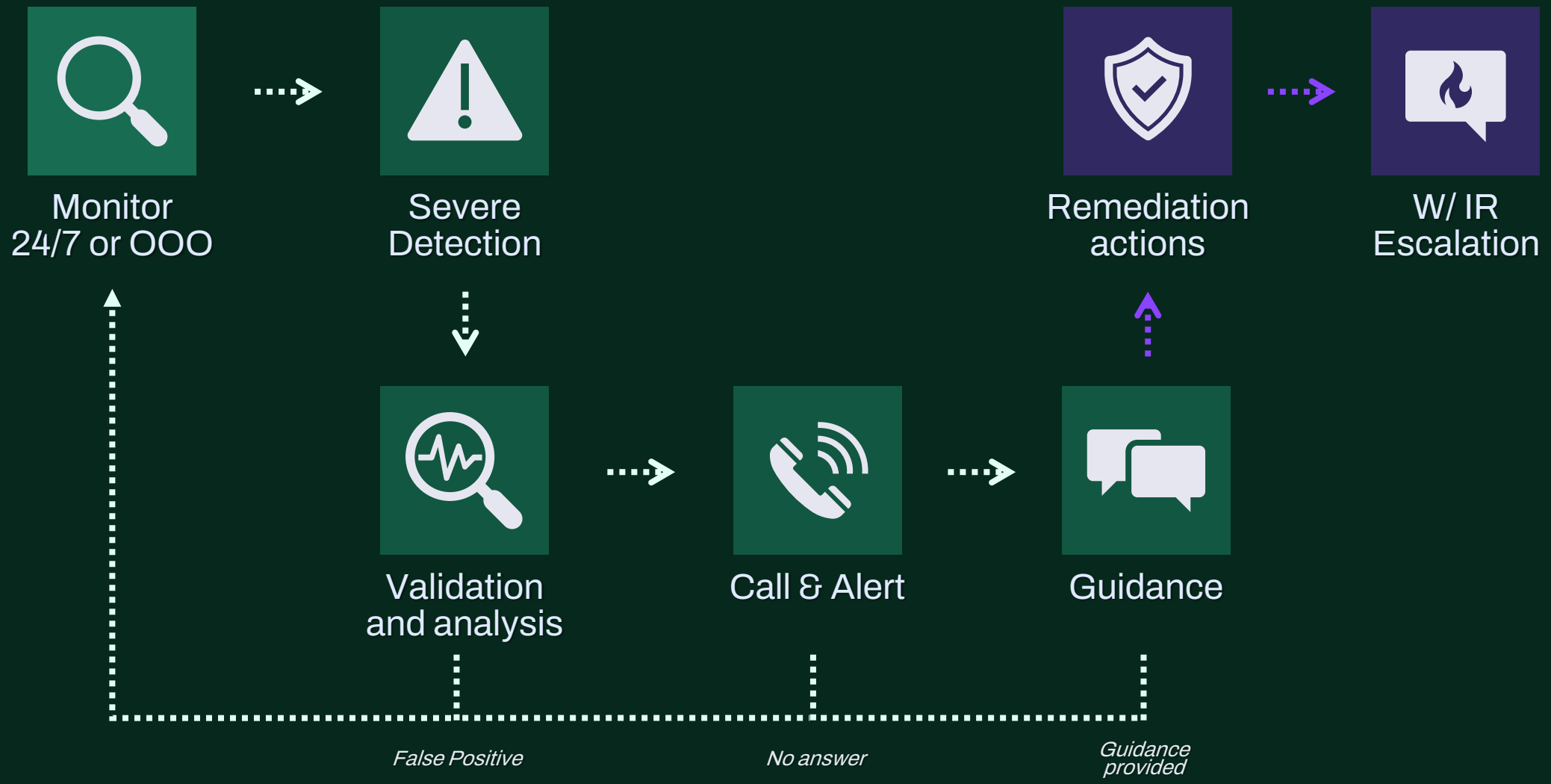
- Monitoring (24/7 or out-of-hours) of severe-risk detections by WithSecure
- Validation and investigation of severe-risk detections by a human threat analyst
- Confirmed attacks are escalated directly to customers or partners on-call
- Threat Analyst provides containment advice for fast and effective remediation
- Possible to escalate to Incident Response services with or without IR Retainer

Outcome

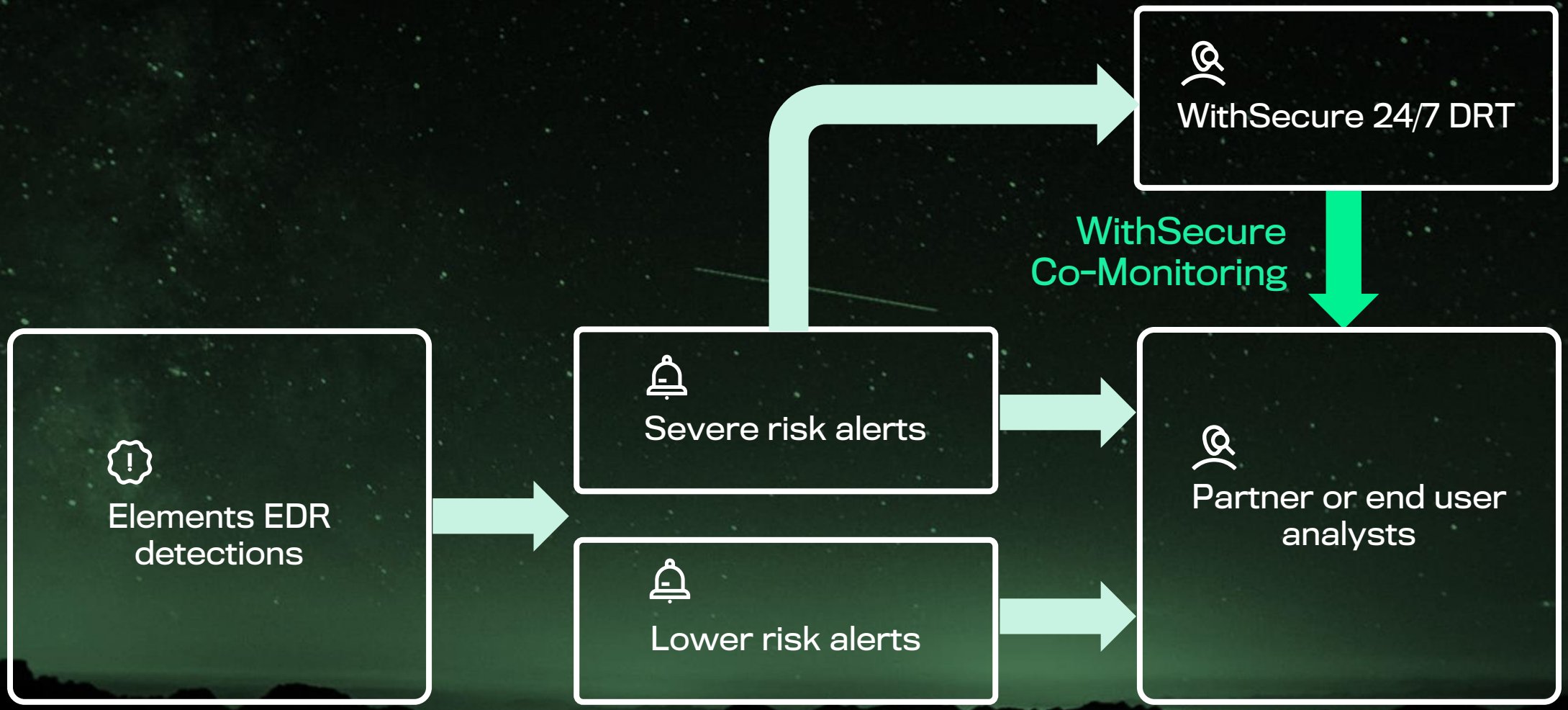
- Improved resilience
- Minimized disruption and unplanned expense
- Customer trust

WITH secure

WithSecure Co-Monitoring Service



WithSecure Co-Monitoring



Co-Monitoring (OOO) Service Hours

MONDAY to FRIDAY

00:00-09:00 and 17:00-23:59

SATURDAY to SUNDAY

00:00 - 23:59

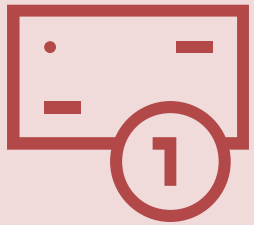
W / T H
secure

WithSecure™ Managed Detection and Response (MDR)

WITH secure

Detection and Response (D&R) to cyber threats is challenging

Successful D&R requires extensive monitoring capabilities and advanced threat analysis



For most companies, acquiring these security capabilities is prohibitively expensive

NIS 2

EU's member states must incorporate the measures introduced by NIS 2 into their national laws*

***Note:** NIS 2 Directive in Europe poses capability requirements that an MDR solution can help with, including: 1) Establish capabilities to detect and handle cyber security incidents (NIS2 10 Minimum Requirements: Article 21.2(b)) and 2) Establish capabilities to ensure business continuity during cyber security incidents (NIS2 10 Minimum Requirements: Article 21.2(c)).

WITH secure

WithSecure™ Co-Security Services:

Find the right level of D&R for your organization

Detection and Response service need and risk profile →

Extended Detection and Response

Elements Software

Elevate

On-Demand Assistance, Investigation & Guidance

Co-Monitoring

Outsourced Monitoring, Investigation & Guidance

Managed Detection and Response

Managed Detection and Response

Countercept

'Premium MDR' with continuous security posture improvement.

Incident Response

Incident Response service

Amount of human-delivered service →

Products Services

WITH secure

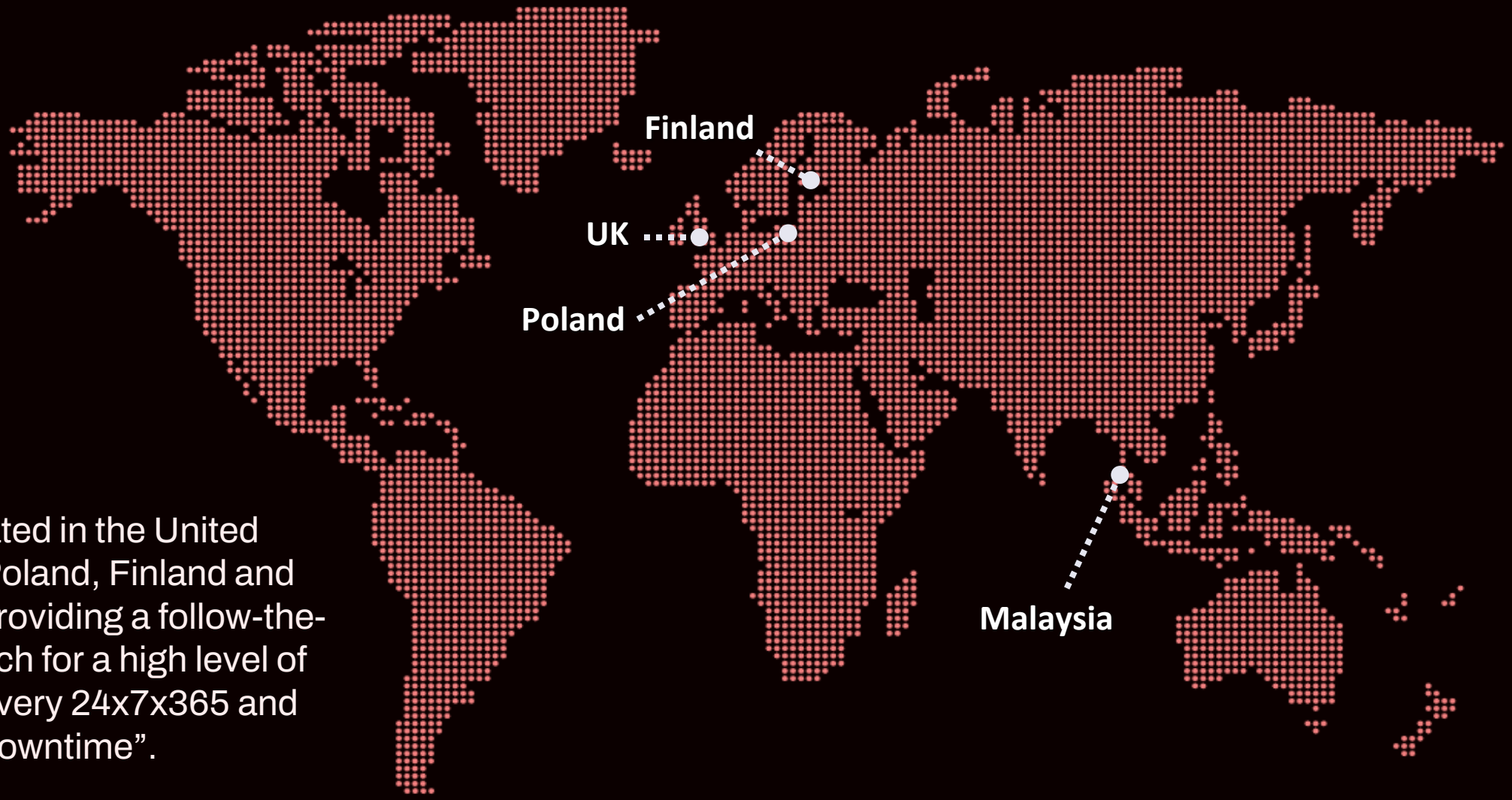
WithSecure™ human expertise:

Superior service, delivered by the best in the industry

- **Detection and Response Team (DRT)** helps customers with the combined wisdom of ~100 researchers, developers, and operators.
- Highly professional and certified **Incident Response (IR) team** handles emergency and large-scale incidents.
  - Our IR team and DRT are used to collaborating, enabling them to take the optimal fast response actions together.
- Incident Response team's services are government-assured:
  - Assured by the **UK National Cyber Security Centre since 2013**, as one of only 9 IR organizations competent to handle the most complex incidents.
  - Assured by the **German Federal Office for Information Security**.

Some of the accreditations and certificates our company holds:

CREST CSIR CREST STAR National Cyber Security Centre a part of GCHQ



- ✓ Teams located in the United Kingdom, Poland, Finland and Malaysia, providing a follow-the-sun approach for a high level of service delivery 24x7x365 and “zero skill downtime”.

WITH secure

Solution overview

WithSecure™ MDR

WithSecure™ Managed Detection and Response (MDR)

WithSecure™ MDR is a continuous 24/7 Detection and Response (D&R) service, in which WithSecure's cyber security experts protect your IT environment by investigating and remediating cyber security attacks across your estate. The service is delivered based on our WithSecure™ Elements Endpoint Detection and Response (EDR) tooling.

WithSecure™ MDR key benefits

24/7 monitoring by experts:

Detect and respond to threats like ransomware attacks and data breaches 24/7/365.

Incident Response included:

Shorten the time it takes to respond* to incidents, in a cost-effective manner and around the clock.

Less pressure on your staff:

In addition to extensive visibility of your environment via Elements EDR, our Detection & Response experts have got your back.

*** Note:** The Incident Response included in WithSecure MDR covers one (1) device. Incidents are handled by our experienced and offensively-minded Threat Analysts in Detection and Response Team (DRT). Major incidents where multiple devices are affected require additional Incident Response services.

WITH secure

Overview of service elements

01 Monitoring
Maintaining constant watch over suspicious detections in customers' IT environments.

02 Investigation
Identifying potential security incidents from detections by validating and investigating them to establish if they are true positive incidents that require action to remediate, or false positives that can be closed.

03 Escalation
Ensuring that true positive incidents are escalated in a timely fashion to the correct contact customer representative(s) and/or the customer's IT partner managing their environment.

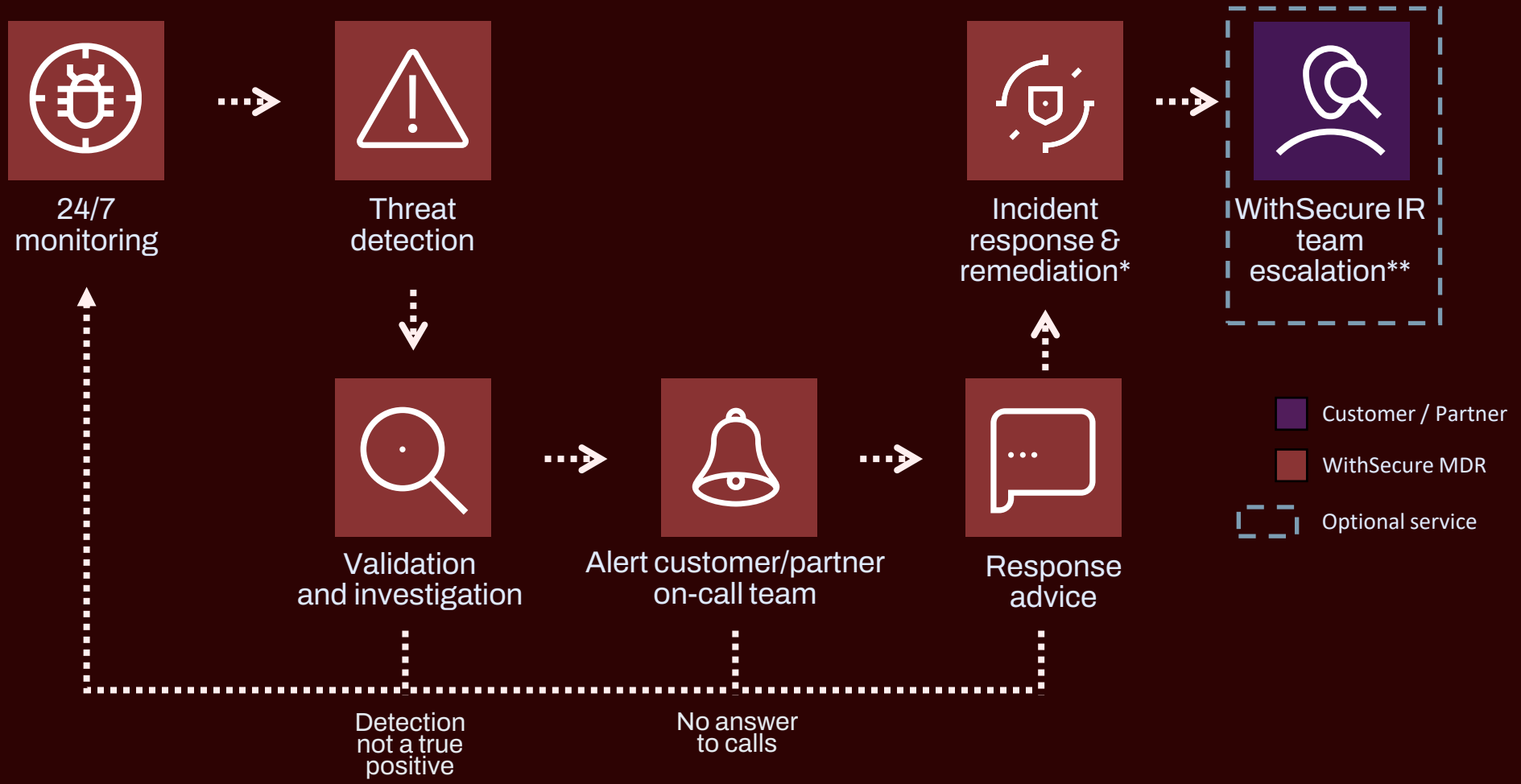
04 Response
Taking decisive and appropriate investigation, containment, and eradication actions on behalf of the customer according to the authorizations given.

05 Retainer
Customer can purchase access to additional skilled and SLA-backed Incident Response resources, in case a major cyber security breach occurs, via Incident Response Retainer*.

***Note:** WithSecure's additional IR services which MDR customers can access have been assured by the UK National Cyber Security Centre since 2013, as one of only 9 IR organizations competent to handle the most complex incidents. They are also assured by the German Federal Office for Information Security.

WITH secure

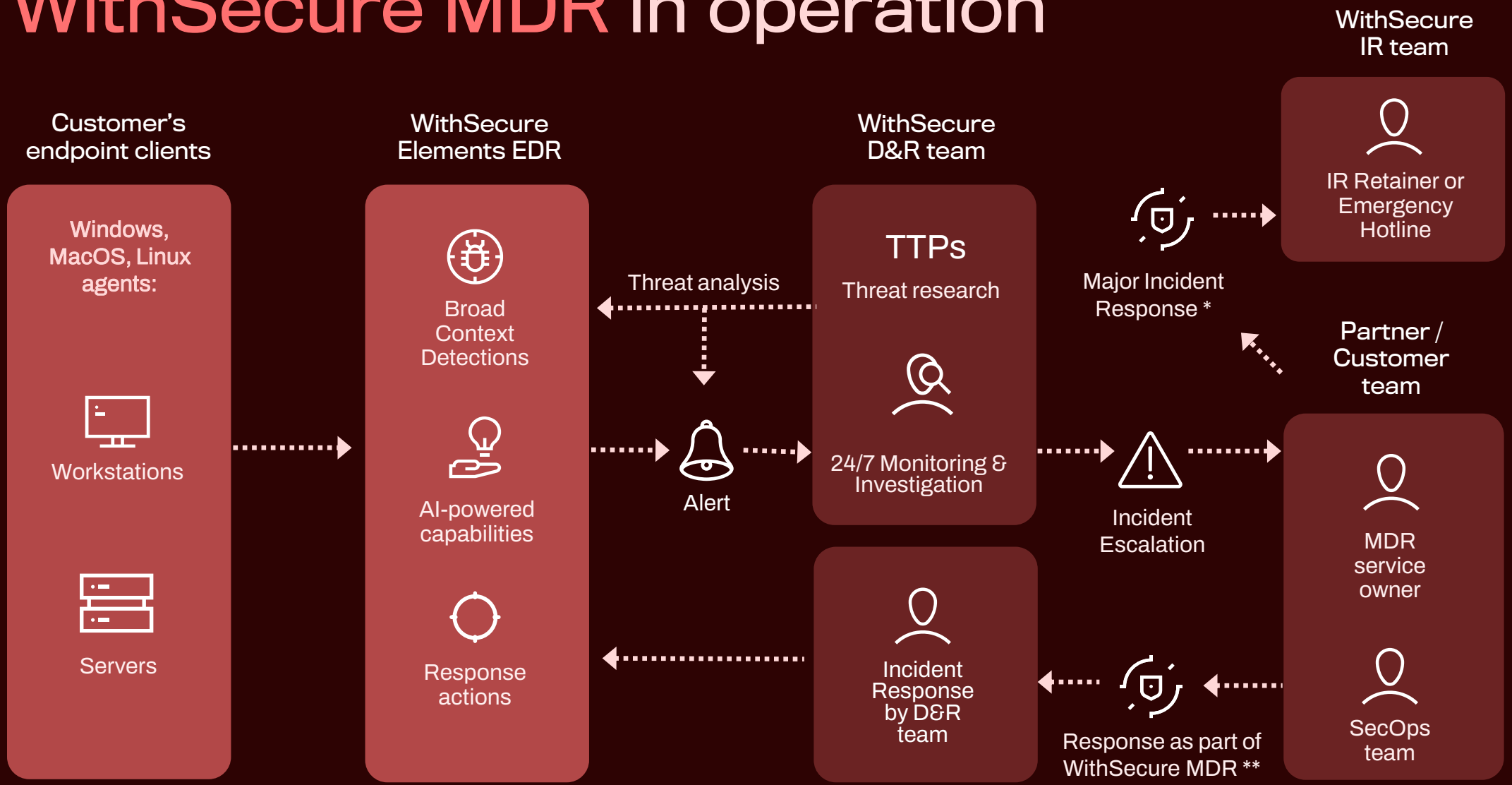
How WithSecure MDR works



* Response actions taken for the affected device according to agreed authorization for servers and workstations (Pre-authorization / Explicit / None).
** Requires customer's consent or an existing IR service like Incident Response Retainer.

WITH secure

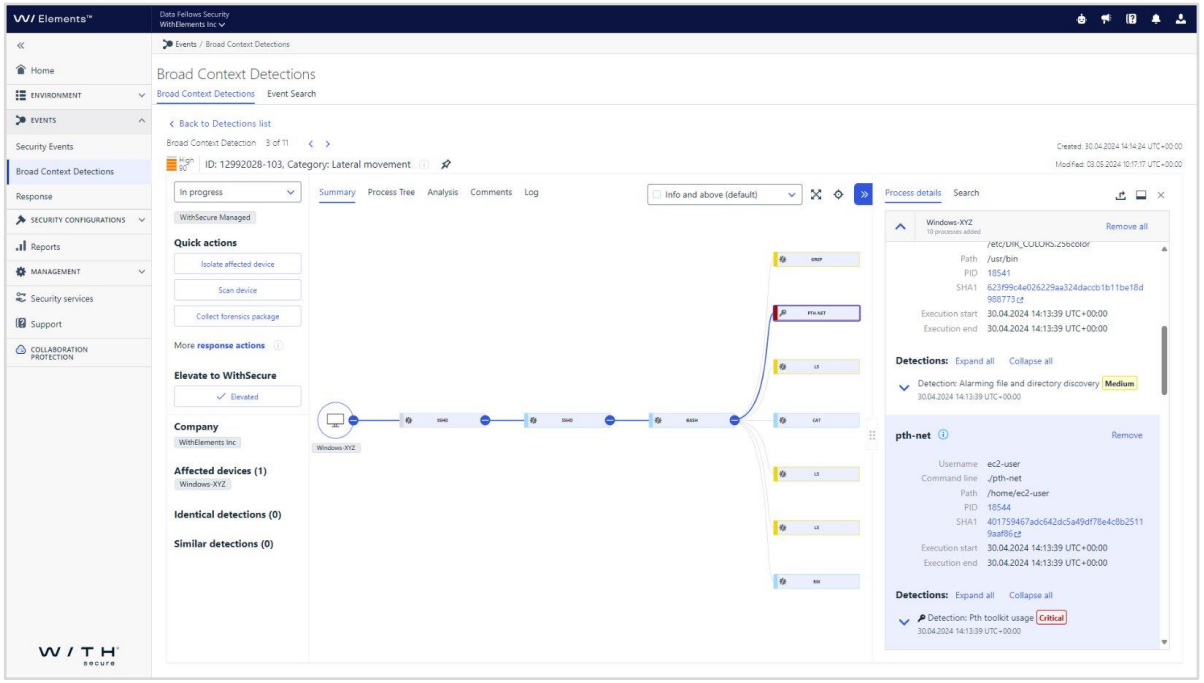
WithSecure MDR in operation



* Requires customer's consent or an existing IR service like Incident Response Retainer.
** Response actions taken for the affected device according to agreed authorization for servers and workstations (Pre-authorization / Explicit / None).

WITH secure

Stay informed via Elements EDR while we take care of your Detection and Response

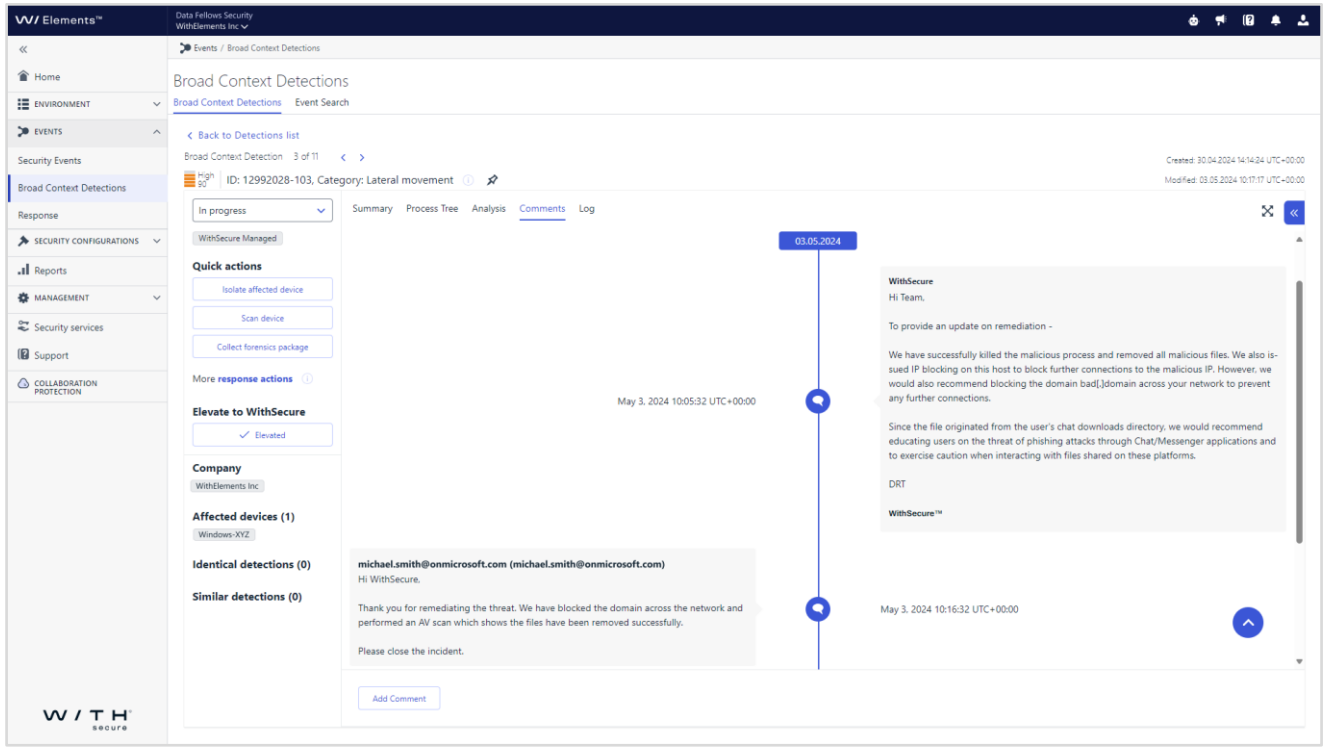


See a Broad Context Detection summary within our WithSecure Elements Cloud platform, with options for quick action.

- WithSecure™ MDR is an operationally efficient and cost-effective service for continuous monitoring, detection and response.
- Incidents are handled by our experienced Detection and Response Team (DRT) members, utilizing the combined knowledge of our industry-recognized researchers, developers, operators, and incident responders.
- Uses WithSecure™ Elements EDR's Broad Context Detections™ (BCD), telemetry and response capabilities.
  - You can use Elements EDR for extensive visibility into your digital estate without having to worry about missing security incident related alerts.

WITH secure

Includes Incident Response



A customer is alerted about a security incident, and our Detection and Response Team (DRT) remediates it and provides further guidance on next steps.

- In our 24/7 Managed Detection and Response service, WithSecure™ experts from DRT contain and remediate incidents on your device* before those have a chance to impact your business.
- Incident Response is automatically included in your WithSecure™ MDR subscription*, beyond automatic isolation.
- If a large-scale incident affecting multiple devices occurs, customers are advised on additional Incident Response (IR) services.**

* The Incident Response included in WithSecure MDR covers one (1) device. Incidents are handled by our experienced and offensively-minded Threat Analysts in Detection and Response Team (DRT). Major incidents where multiple devices are affected require additional Incident Response services.
** WithSecure's additional IR services by our Incident Response team have been assured by the UK National Cyber Security Centre since 2013, as one of only 9 IR organizations competent to handle the most complex incidents. They are also assured by the German Federal Office for Information Security.

WITH secure

Varnostno operativni center A1

Zakaj se vključiti v Varnostno operativni center?

Varnostno operativni center A1 Slovenija d.d.

Varnostno operativni center A1 Slovenija d.d.

Krovna predstavitev varnostno operativnega centra

- Pričetek delovanja: 2020
- Število strank: 50+
- Število oseb: 7 + 6 + 3
- Geografsko pokrivanje: Slovenija

1.nivo, 24/7 dežurstvo na lokaciji

Sprejem alarmov
Osnovna triaža

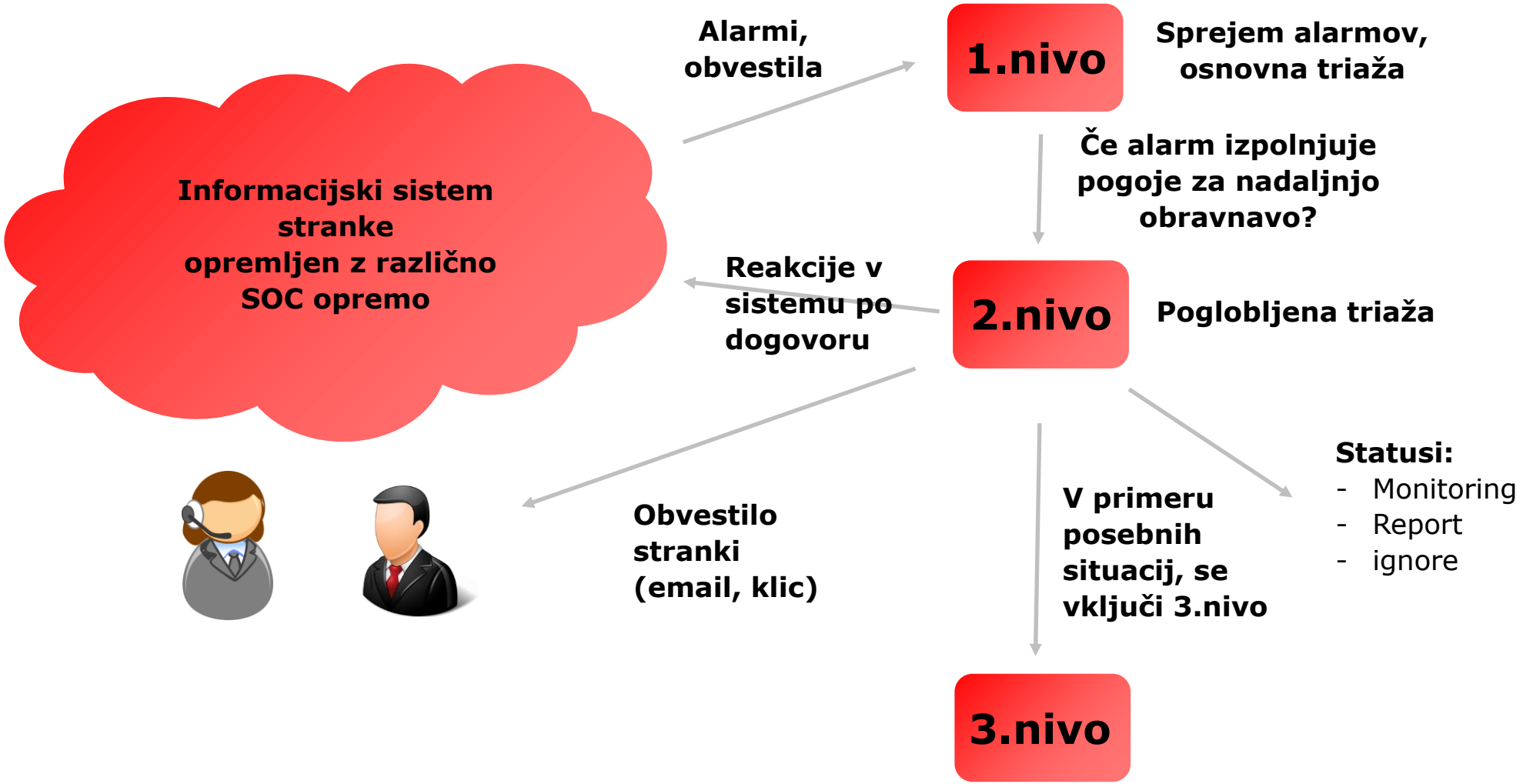
2.nivo, 24/7, dežurstvo na klic

Poglobljena triaža
Odredba nadaljnjih aktivnosti do stranke

3.nivo

Specifična znanja
Poglobljene varnostne storitve

Procesi/storitve v varnostno operativnem centru



- Obveščanje stranke ob dogodkih
  - Klic
  - Email
  - Zapis v rednem poročilu
- Tipične reakcije v sistemu po dogovoru
  - Deaktivacija AD uporabnika
  - Deaktivacija M365 uporabnika
  - Blokada prometa na požarni pregradi
  - Osamitev delovne postaje
  - Različne aktivnosti na delovni postaji/strežniku (AV scan, brisanje datoteke, deaktivacija servisa,…)
- Pomen Playbook definicij
  - Kdaj in kako obveščamo
  - Kaj in kako izvajamo tipične reakcije v sistemu
  - Možni različni scenariji za različne dele sistema, za različne čase v dnevu, za različne dneve,

Varnostno operativni center

Začetek

- Naredimo celovit sistemski varnostni pregled
- Onboarding (izmenjava informacij, definicija Playbookov, ipd.)

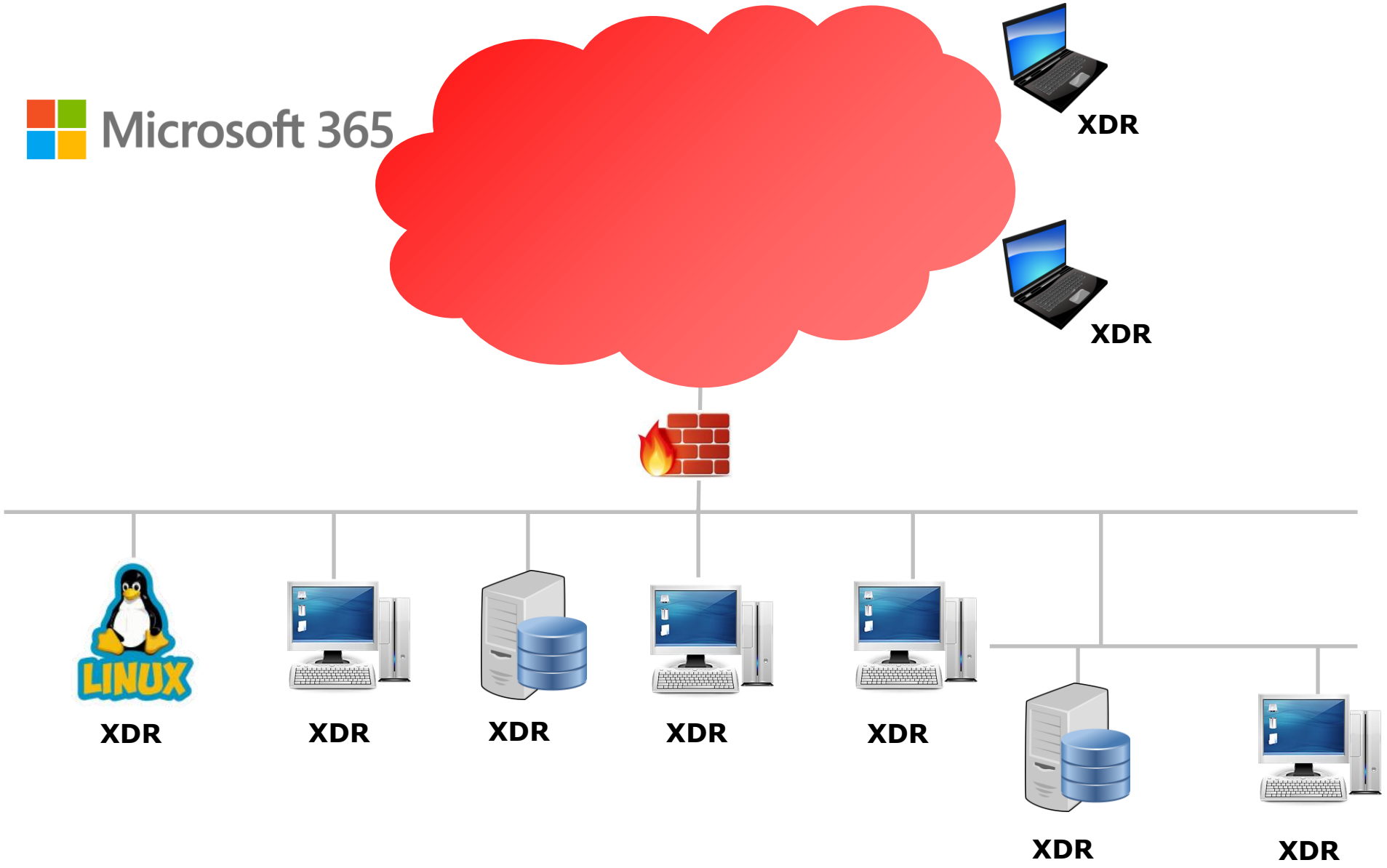
Med delovanjem

- Thread hunting aktivnosti
- Izmenjava podatkov z drugimi varnostno operativnimi centri (primer: znotraj A1 grupe)
- Redna mesečna poročila
- Redni kvartalni sestanki/obiski

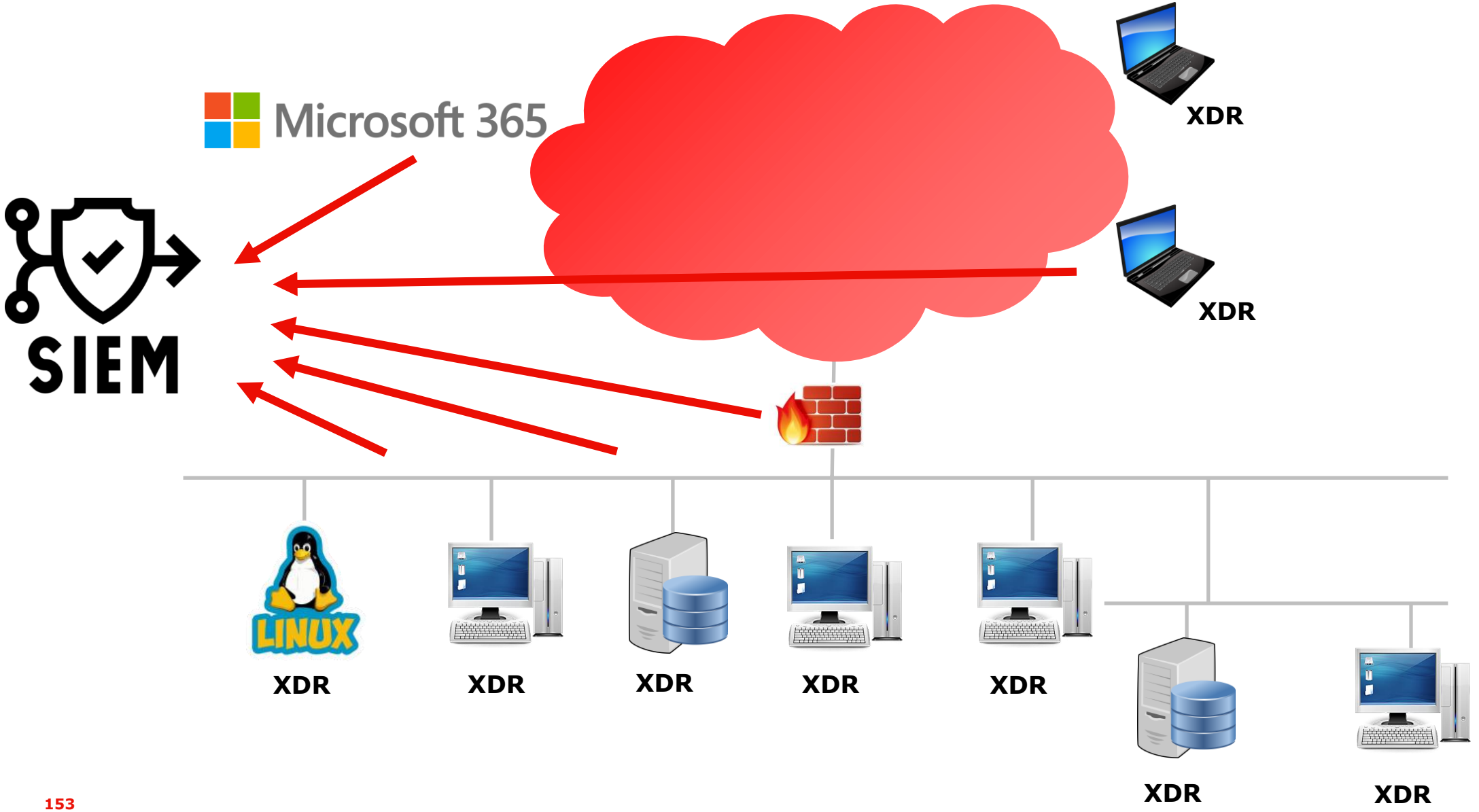
Ostale storitve **(*potencialno dodatno plačilo)**

- Komunikacija s tretjimi osebami (revizorji, Si-cert, ipd.)
- Sodelovanje pri analizi dogodkov, forenziki, odpravi posledic napadov
- Redno izvajanje varnostnih pregledov
- Redno izvajanje varnostnih testiranj za uporabnike
- Redno izvajanje varnostnih šolanj za uporabnike

Oprema v varnostno operativnem centru



- WithSecure, Cynet, SentinelOne
- Možna je uporaba lastne XDR opreme



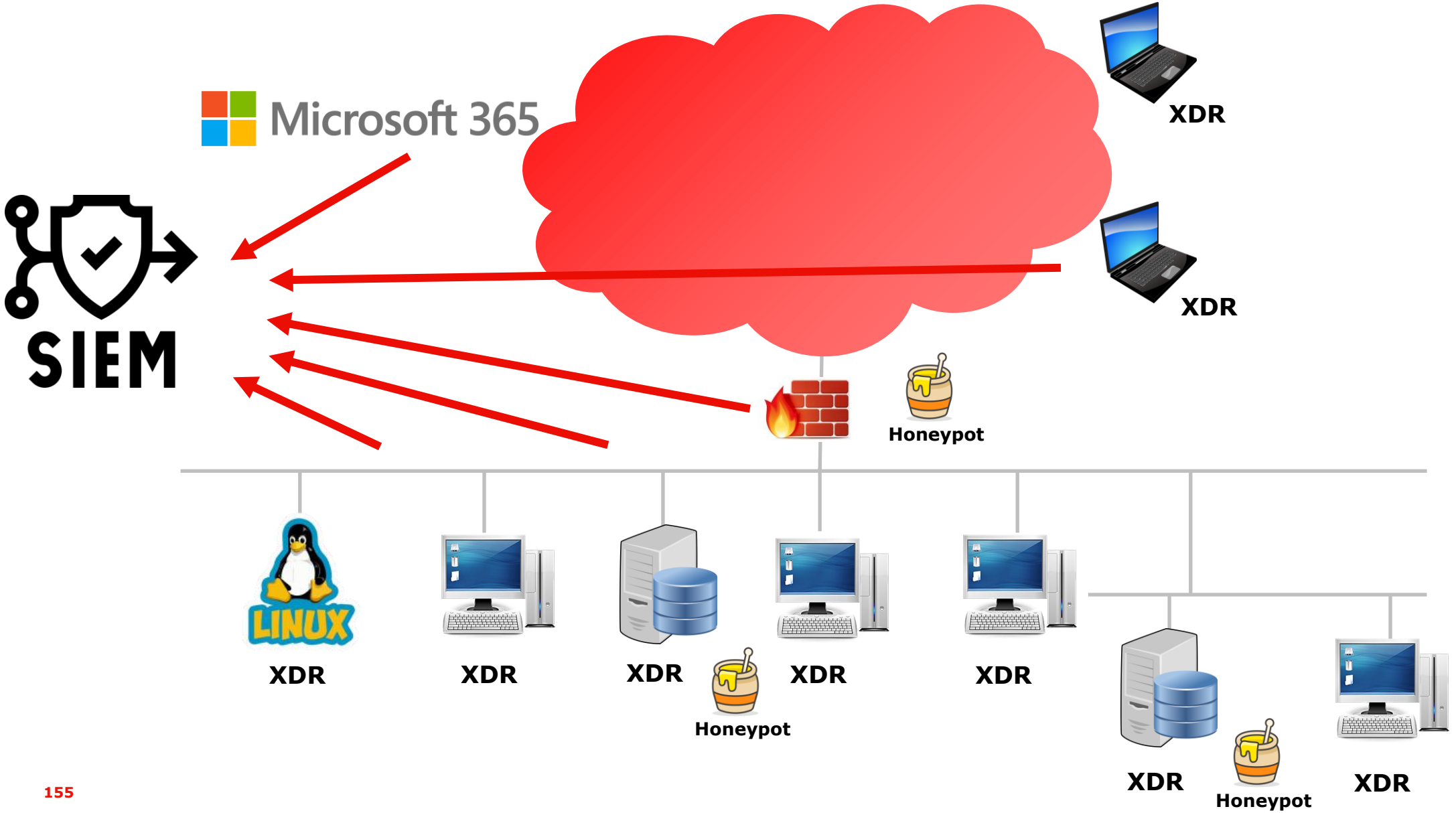
- Nujen, saj XDR ne vidi vsega

- Klasičen SIEM v oblaku A1 Slovenija

(vsaka SOC stranka je vključena v ta SIEM brez doplačila)

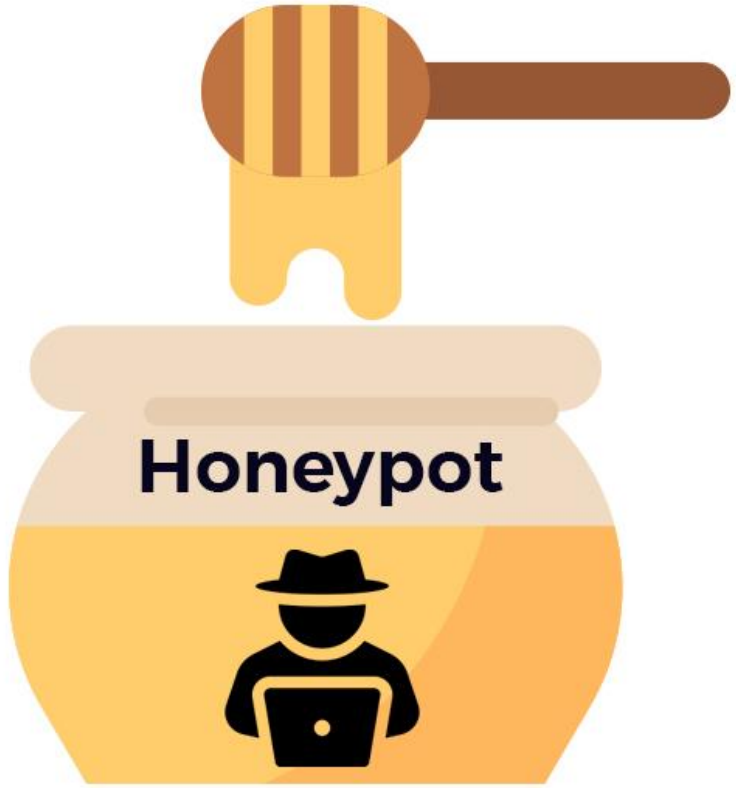
- Tipično vključimo v SIEM
  - Windows/Linux strežnike
  - VPN opremo
  - Sistem elektronske pošte
  - Požarno pregrado
  - Ostalo specifično opremo

- Tipična uporaba
  - Spremljanje login dogodkov
  - Spremljanje prometa
  - Pridobivanje informacij za oplemenitev podatkov iz XDR alarmov

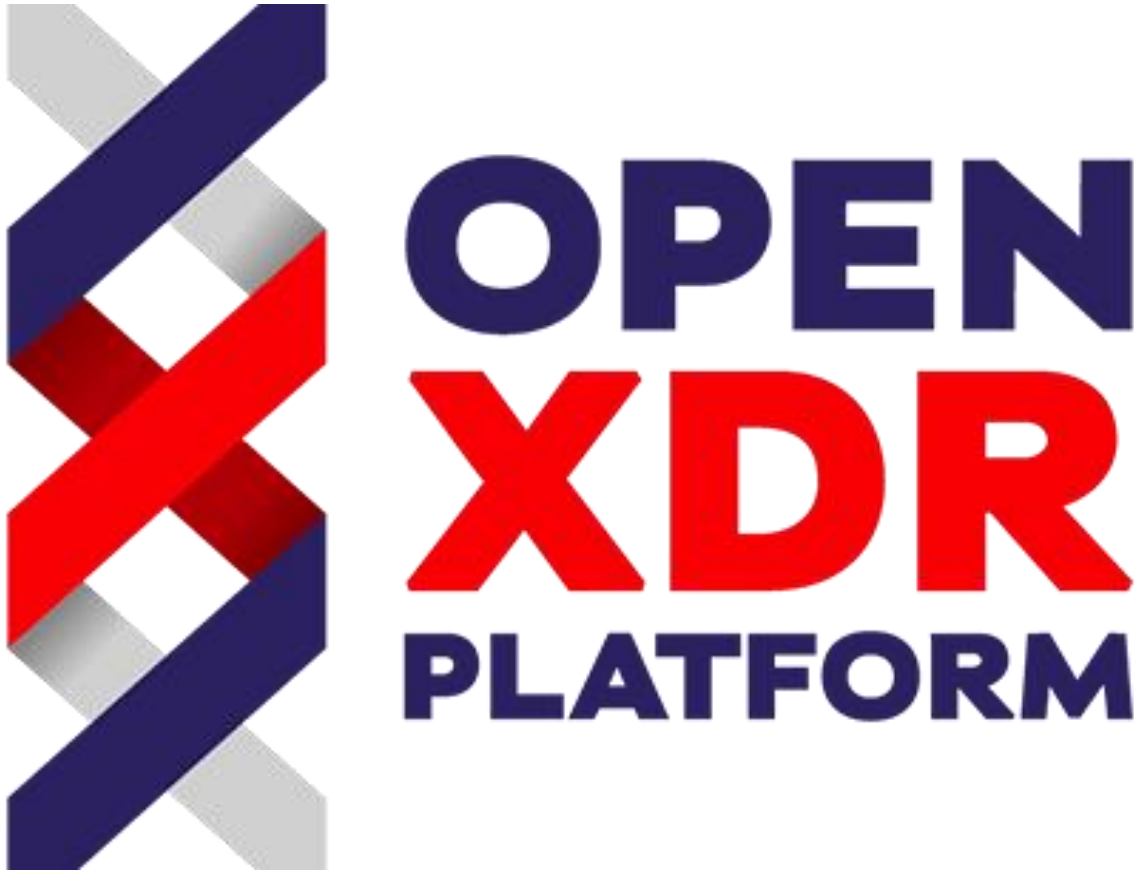


- Vsaka stranka ima vključene mehanizme Honeypot zaščite

- Tipični Honeypot mehanizmi
  - Lažni domenski skrbniki
  - Lažni lokalni skrbniki
  - Lažni „zanimivi" strežniki
  - Lažne datoteke na strežnikih

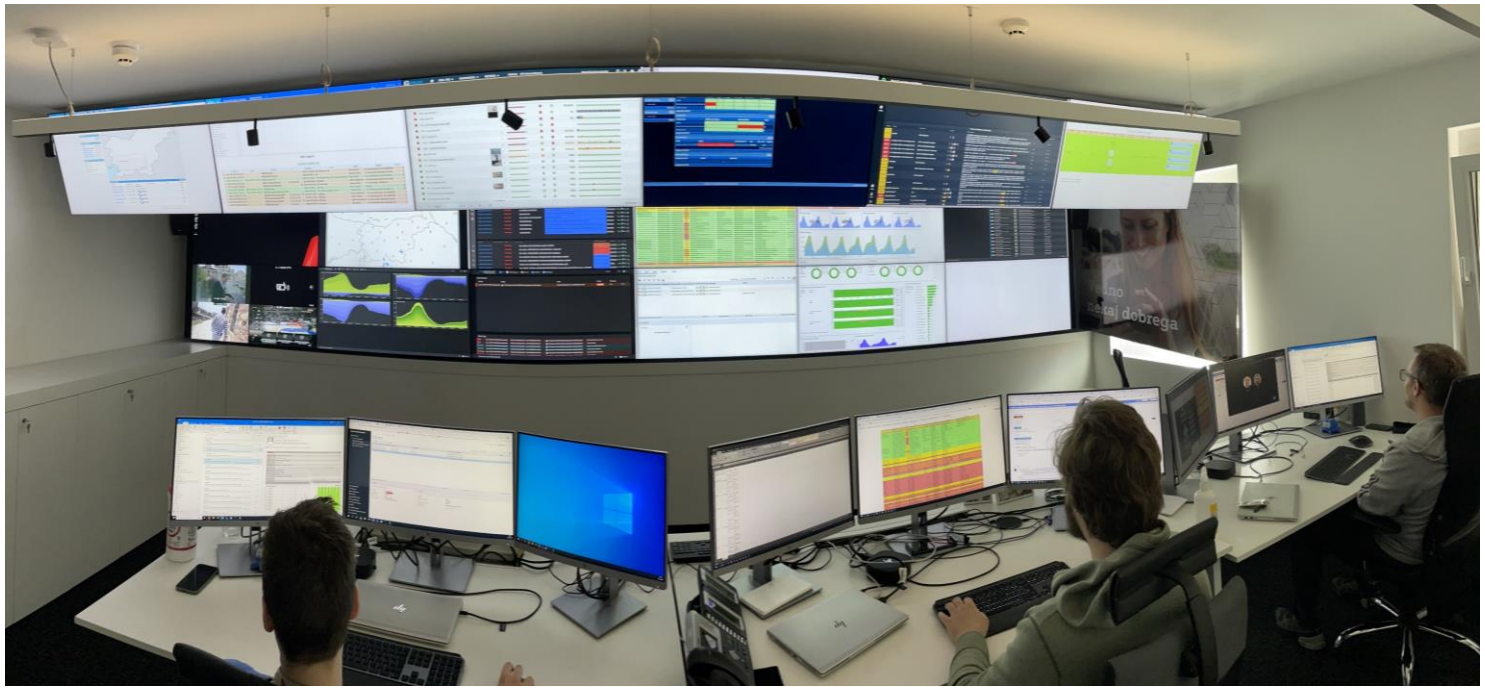


- Prinaša integracijo s celo vrsto sistemov v okolju naročnika (AD, M365, XDR, ipd)
- Prinaša možnost NDR detekcij (ščitimo okolja, kjer XDR ni instaliran)
- Prinaša možnost uporabe lastnega XDR okolja s strani stranke
- Prinaša enostavno in učinkovito integracijo s sistemi z možnostjo hitrih reakcij v teh sistemih
- Prinaša inteligentni SIEM v okolje
- Uporabljamo Stellar Cyber



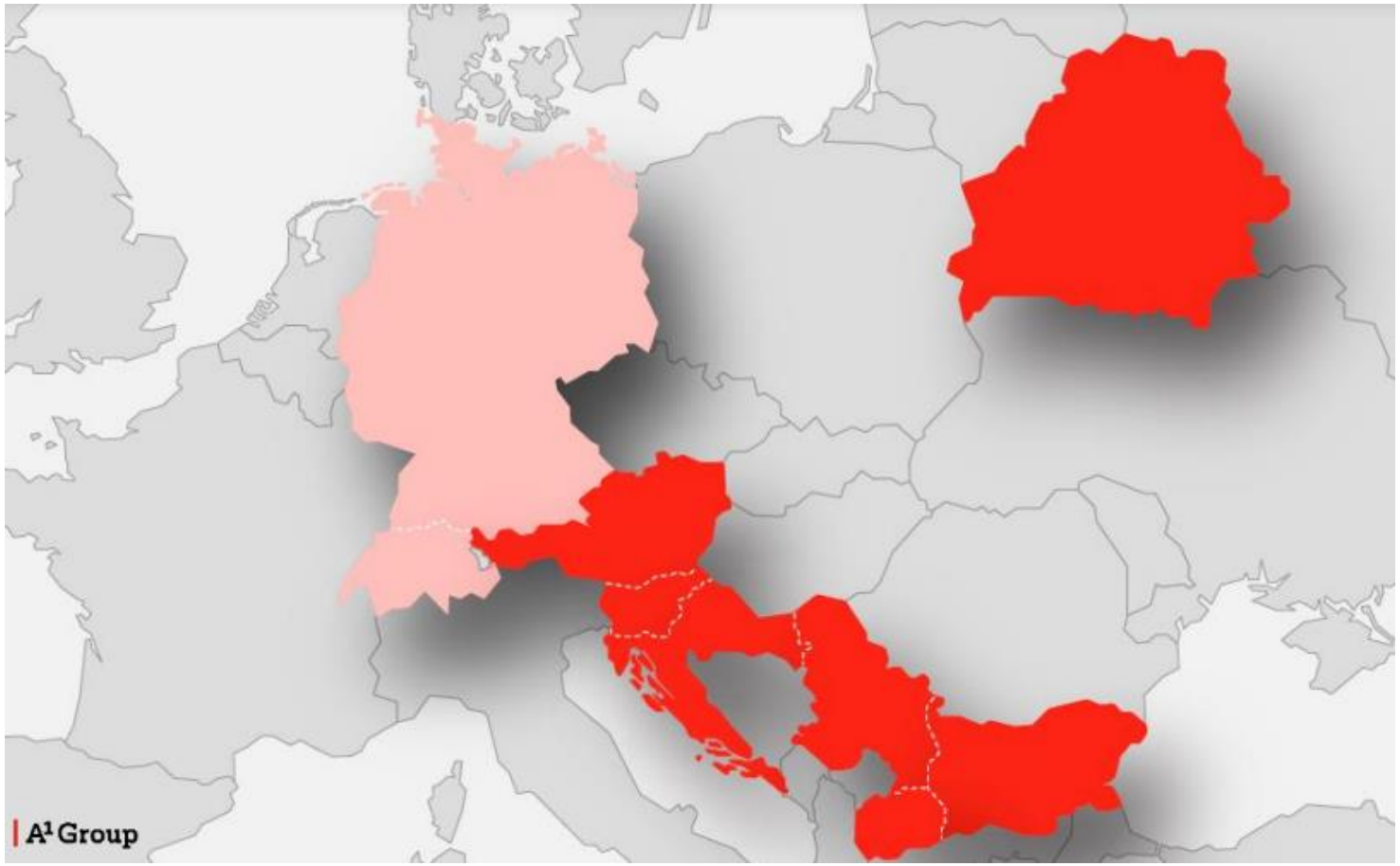
Zakaj A1?

Profesionalen, napreden in inovativen varnostno operativni center



Varnostno operativni center A1 Slovenija d.d.

Varnostno operativni center A1 Slovenija d.d.



+100

Št. Varnostnih pregledov, ki jih v 18 mesecih izvede A1 Slovenija d.d.

Kaj torej dobi WithSecure stranka?

- Uporaba cele vrste opreme (SIEM, HoneyPot, Threat Hunting)
- Storitve (detekcija, reakcija)
- Dodatne storitve (obveščanje v naprej, mesečna poročila, kvartalni sestanki)
- 1x letno varnostni pregled (vsebina pregleda je odvisna od stranke in se jo sproti določi, stranka nujno ne dobi pravega poročila)
- Možnost dodatnih storitve (potencialno dodatno plačljivo)
  - Pomoč pri varnostnih zadevah
  - Redna izobraževanja, redna testiranja uporabnikov
  - SIEM-as-a-service

- Profesionalen in učinkovit Varnostno operativni center
- Usmerjen v vsako stranko posebej
- Varnostno operativni center z najbolj napredno vizijo v Sloveniji
- Vsaka stranka dobi veliko opreme (SIEM, Honeypot, Threat hunting)
- Vsaka stranka dobi veliko storitev (detekcija, reakcija, varnostni pregledi)

Polni in brezplačni vklop vašega informacijskega sistema v naš Varnostno operativni center za 45 dni!

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

- Endpoint Security
- Identity Security
- Collaboration Protection

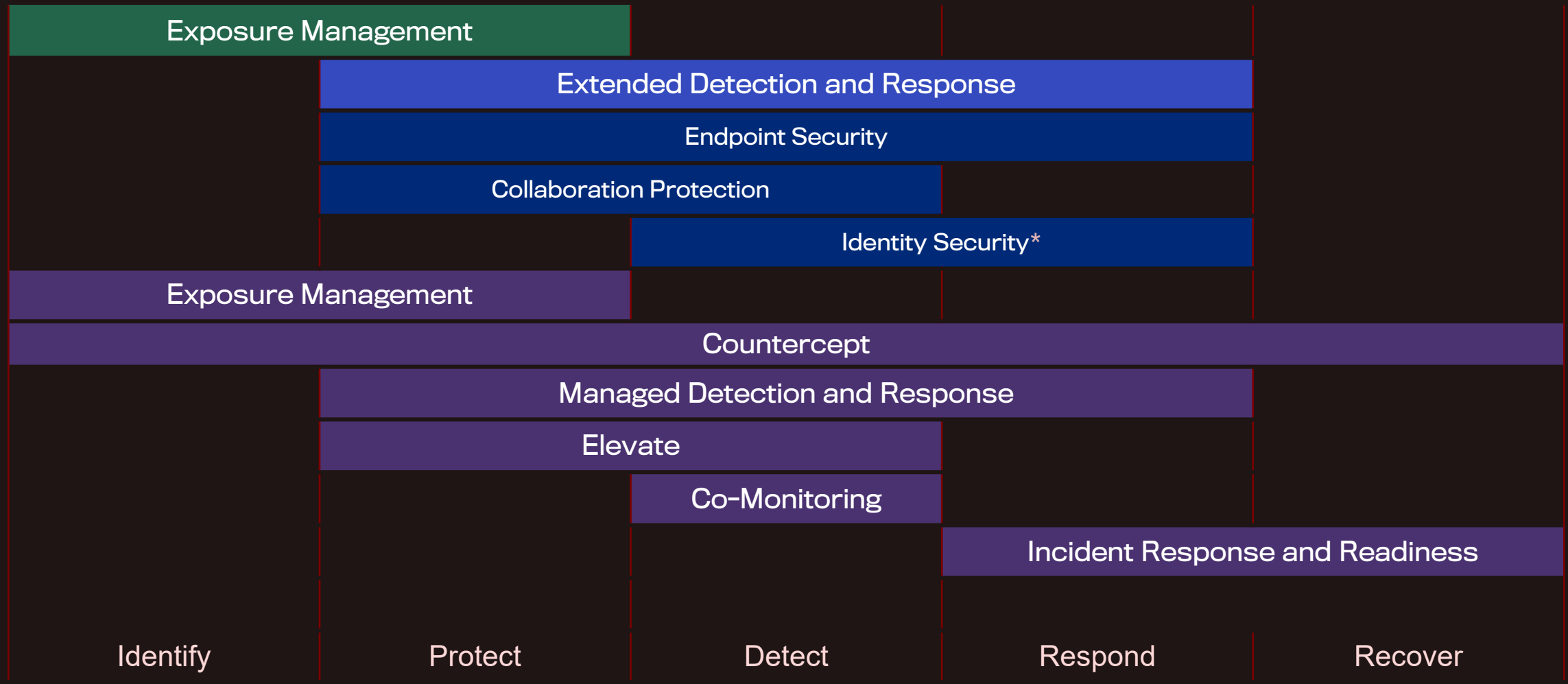
Co-Security Services

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

WithSecure™ Support Services

WITH secure

WithSecure™ Elements Cloud – NIST



*Identity Security will be extended to respond capability later in 2024

WITH secure

Ranked #1 in Software Reviews

WithSecure Elements ranked 1st overall as evidence to provide great service, a great product and great value.

The **Emotional Footprint** diamond is positioning vendors based on who's providing the best customer experience while still driving a highly valuable product.

"In our research we find the relationship a customer has with a vendor has a huge impact on satisfaction, even more so than features and price. That's why we have the emotional footprint component to our research which measures exactly that."

Source: 2024 Endpoint Protection Emotional Footprint Report by Software Reviews

WITH secure

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

- **WithSecure** is once again identified as one of the **15 recognized 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** positioned in the report for both **completeness of vision** and **ability to execute**
- We believe this recognition is due to our **latest innovations** in Identity Security, MDR services, Exposure Management and Luminen™ AI

> "A Niche Player may support your needs better than a market Leader
>
> Gartner

Gartner, Magic Quadrant for Endpoint Protection Platforms, September 2024, Evgeny Mirolyubov, Franz Hinner, Max Taggert, Nikul Patel. The Gartner document is available upon request from WithSecure.

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
Collaboration Protection
Identity Security
Endpoint Security
Flexible Software Modules

Zakaj je WithSecure EDR/XDR tehnologija in dodatne storitve za aktivno spremljanje obvestil, prava izbira v boju pred kibernetskimi napadi?

- **Evropska** rešitev
- V Sloveniji na voljo od **2005**
- Več kot **60.000 aktivnih licenc** (90% na Elements)
- Močan **partnerski ekosistem**

https://varnostne-resitve.si/

ict-partners@A1.si

WITH secure

A1 ICT Distribucija