

A1 ICT Distribucija

Dobrodošli na A1 ICT BRUNCH

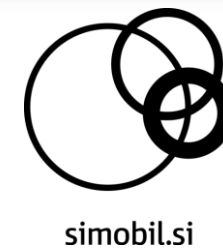


Spoznat ćete zašto su WithSecure i Labyrinth pravi izbor u borbi protiv kibernetских napada.

Hotel Antunović,
Zagrebačka avenija 100a, Zagreb
13. svibnja 2025. u 9:00



A1 Slovenija



| A¹ ICT Distribucija

Početak

Amis ulazi na tržište distribucije sa tadašnjim F-Secure antivirusom

Grupa Telekom Austria

Odvojene grupe po operaterima za distribuciju

Ulaz A1 Slovenija na Hrvatsko tržište

Odabrani vendori i preuzimanje aktivnosti za WithSecure

Ekipa



Sergeja Cvelfer

Voditeljica odjela za
distribuciju ICT rješenja



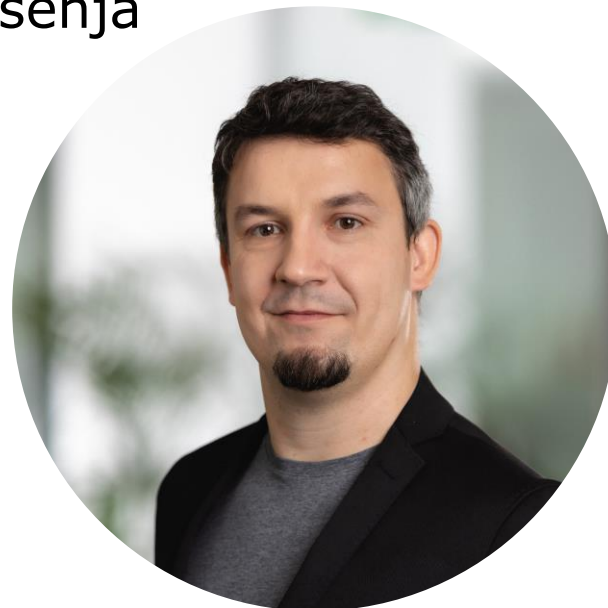
Tadej Križovnik

Ekspert za distribuciju
ICT rješenja



Maja Milojević

Ekspert za distribuciju
ICT rješenja



Marko Kašić

Vodeći ICT inženir



Filip Šimonka

Ekspert za distribuciju
ICT rješenja



Amadej Blažinčić

Ekspert za
implementaciju ICT
rješenja

Value Added Distributor

- Partnerski program
- Široka mreža partnera u Adria regiji
- Prodajna i tehnička podrška partnerima
- Organizacija tehničkih treninga
- Promocija brandova na eventima
- Širok izbor europskih rješenja
 - Endpoint zaštita (EPP, EDR, XDR)
 - Zaštita za mrežu (NGFW/UTM, NDR, Deception)
 - Zaštita za emailove (Antispam/antiphishing)
 - Zaštita privilegiranih pristupa (PAM)
 - Višenivojska autentikacija (MFA)
 - Backup rješenja (online, offsite)
 - SIEM



Distribucija u HR





LABYRINTH

W / T H[®]
secure

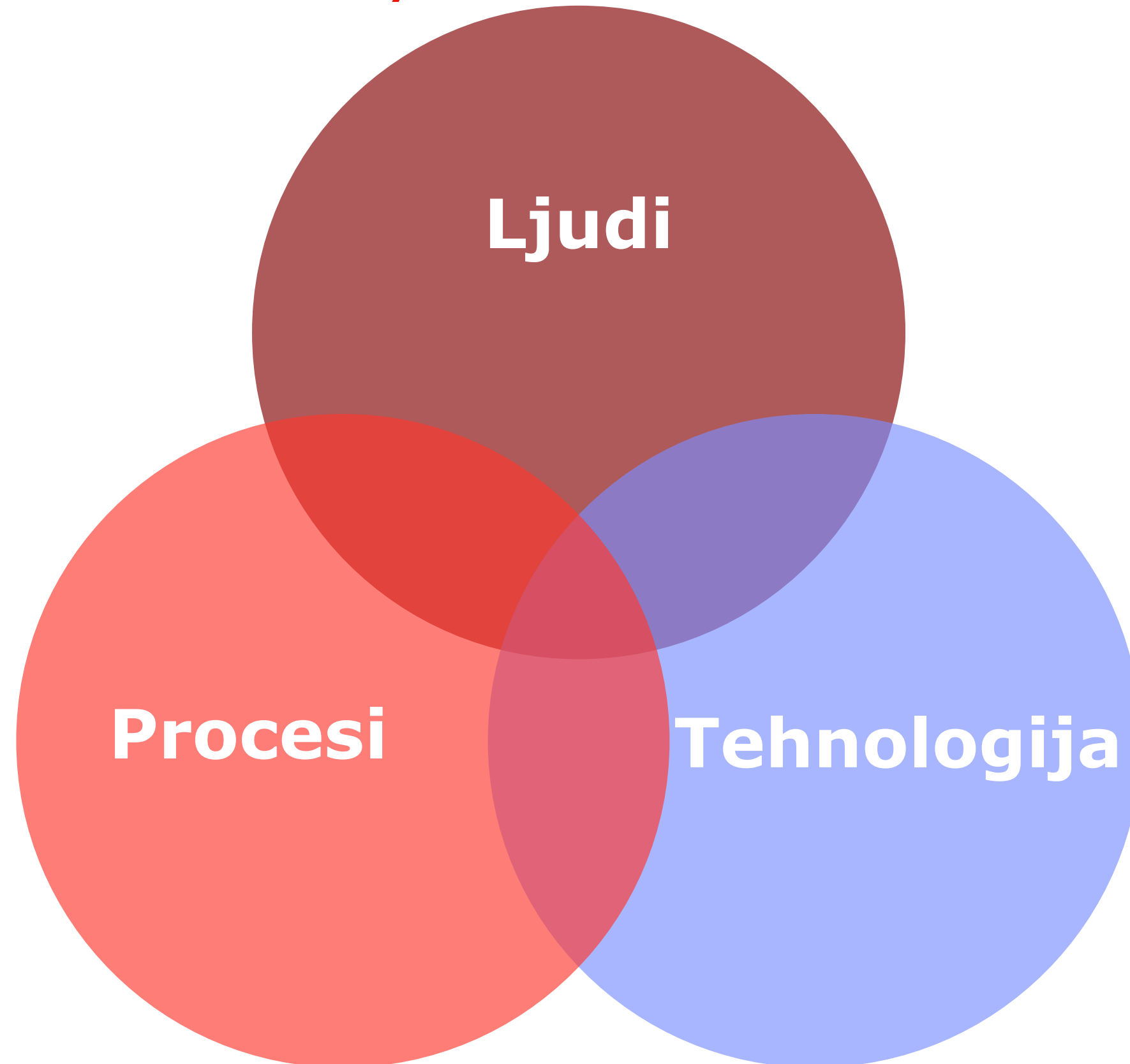
Cybersecurity izazovi





Kibernetska nevarnost: Ali ste pripravljeni na naslednji napad?

Glavne stvari cyber security-a



Prijetnje i sigurnost se mijenjaju

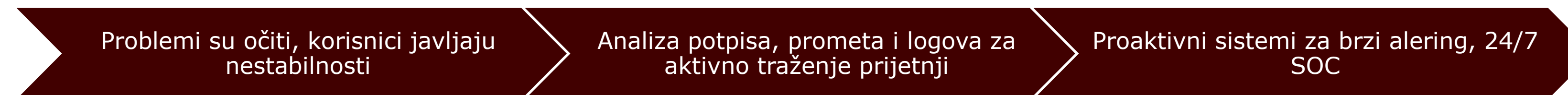
Naprednost prijetnji



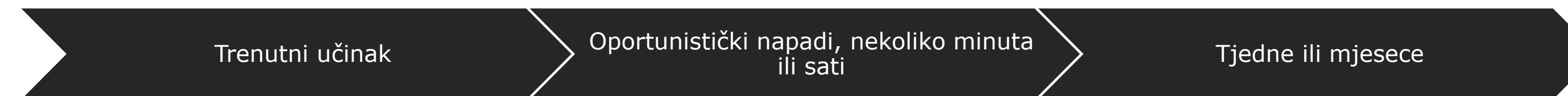
Potencijalna šteta



Sposobnost detekcije



Dužina napada



Koraci kibernetičkog napada



Uvijek korak iza

- Virus
- Spyware
- Spam
- Phishing
- Ransomware
- ...



- Antivirus
- Antispyware
- Antispam
- Antiphishing
- Antiransomware
- ...

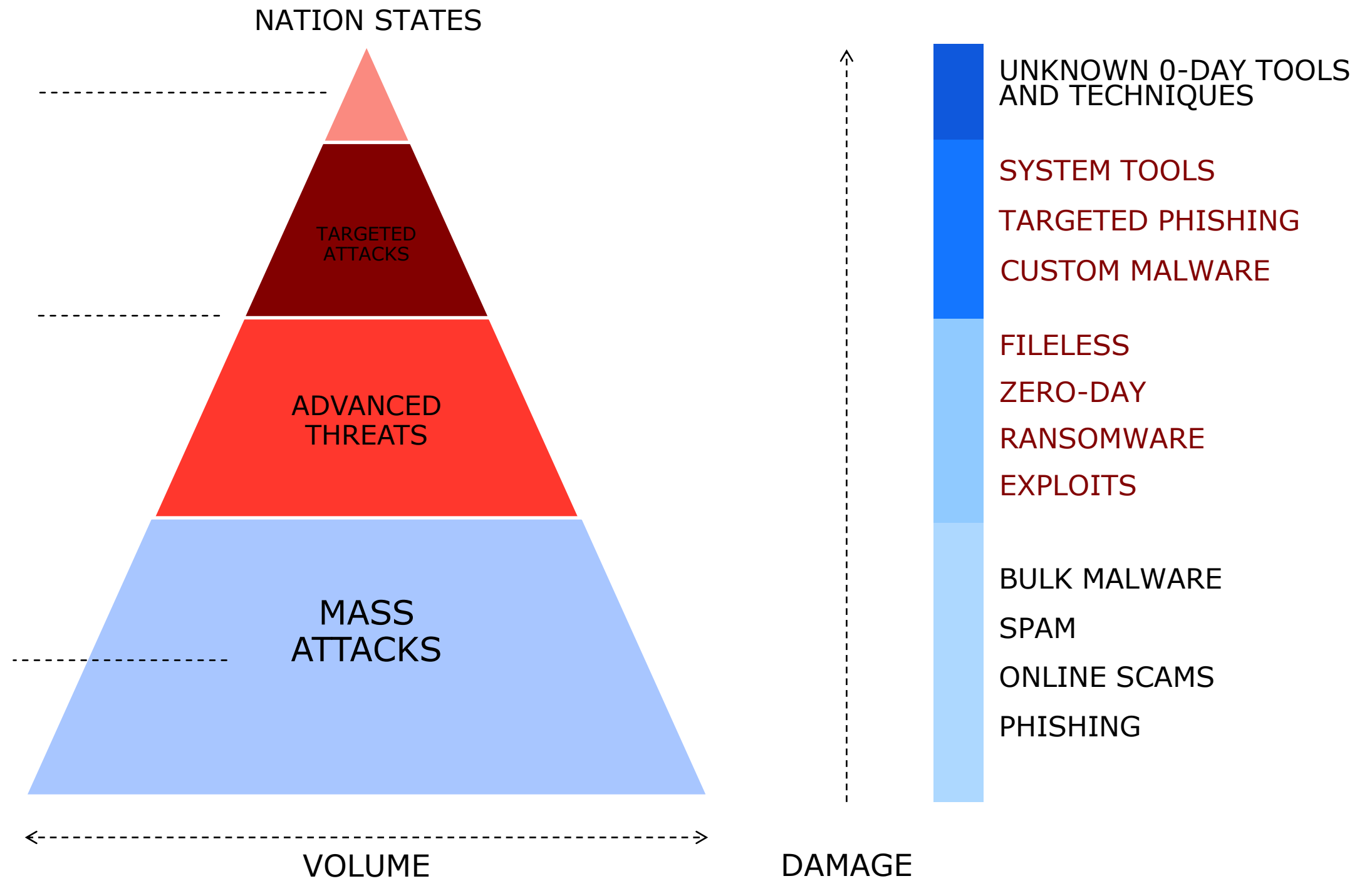
Kibernetska nevarnost: Ali ste pripravljeni na naslednji napad?

Razumijevanje napada

Praktički **nemoguće** braniti i preskupo

Napadači s **ogromno iskustva** koji koriste **kompleksne tehnike** napada

Prioritetni napadi zbog **velike frekvence** i **utjecaja** na svakodnevno poslovanje



99,9 %

**MALO
STETE**

0,1 %

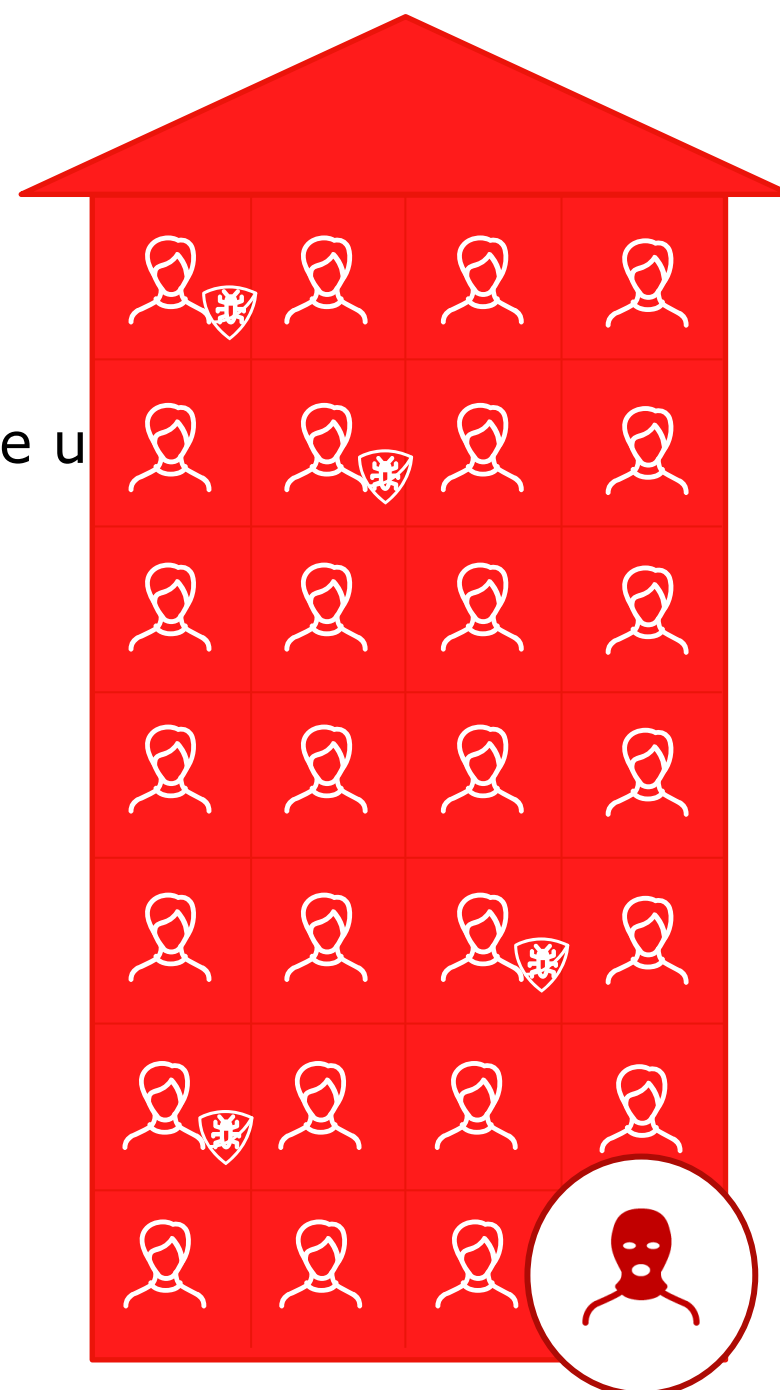
**VELIKA
STETA**

MASOVNI NAPADI

USMERJENI NAPADI

Obično dobro pokriveno

- Masovni napadi
 - Avtomatizirani
 - Malware, npr. u obliku ransomwarea
 - Kampanje slanja neželjene pošte i phishing poruka
 - >100 milijuna novih uzoraka godišnje u bazi (AV-TEST database)
- Rješavamo s preventivom:
 - Firewall
 - Zaštita e-maila
 - Zaštita radnih stanica i servera (antivirusna zaštita)
 - Ostala preventivna rješenja

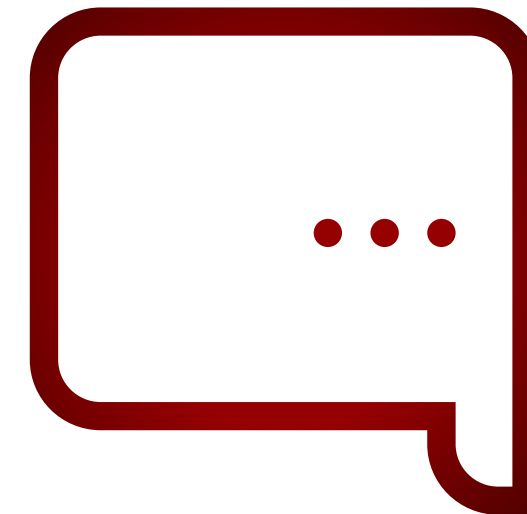


Uglavnom ne dajemo pažnje...

- Napredni i ciljani kibernetički napadi
 - Prilagođeni phishing i zloupotreba korisnika (email kao ulazni vektor)
 - Korištenje internih sustava (powershell, WMIC, komande za pokretanje servisa)
 - Korištenje alata za daljinsku administraciju (Remote Access Tools – RAT) i alata za hekanje (Orcus, Litemanager, VNC, Mimikatz, ...)
 - Prikrivanje prometa za nadzor radne stanice (preko M365, Gmail, HTTPS)
- Rješavamo s naprednih alatima
 - Managed Detection & Response (MDR)
 - Endpoint Detection & Response (EDR)
 - Network Detection & Response (NDR)
 - ...

Izazovi IT stručnjaka

- Nema 100% zaštite
- Nema pogleda u cijeli IT ekosistem zbog stalnog širenja (IoT, cloud, više uređaja po osobi, distribuirana mreža)
- Stalno nove prijetnje
- Potreba po standardima i regulativi (EU: NIS2, DORA, GDPR, ISO ...)
- Premalo stručnjaka
- Povećana kompleksnost & troškovi
- Nerazumijevanje koliko je dovoljno sigurnosti



Europska rješenja za cybersecurity

Discover cybersecurity solutions from Europe with Cyberhive

Cyberhive EUROPE® offers a unified matchmaking tool specialised to promote and discover cybersecurity solutions beyond your local borders. Increase your digital business resilience today, discover the Cyberhive Matrix and build towards a secure and stronger Europe!

[Explore solutions](#)



Europska rješenja za cybersecurity

Discover
cybersecurity
solutions from
Europe with
Cyberhive



Cyberhive EUROPE® offers a UI tool specialised to promote and cybersecurity solutions beyond your local borders. Increase your digital business resilience today, discover the Cyberhive Matrix and build towards a secure and stronger Europe!

[Explore solutions](#)



Učinkovita i jednostavna rješenja





**Tu su rješenja za sve preopterećene
IT stručnjake s premalo resursa**



W / T H[™]
secure | Formerly
F-Secure Business

F-Secure Business
is now **WithSecure**

Protecting businesses in 100+ countries





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

150,000
Customers

**A leading European
Cyber security company**

6,000
Partners

70
Nationalities

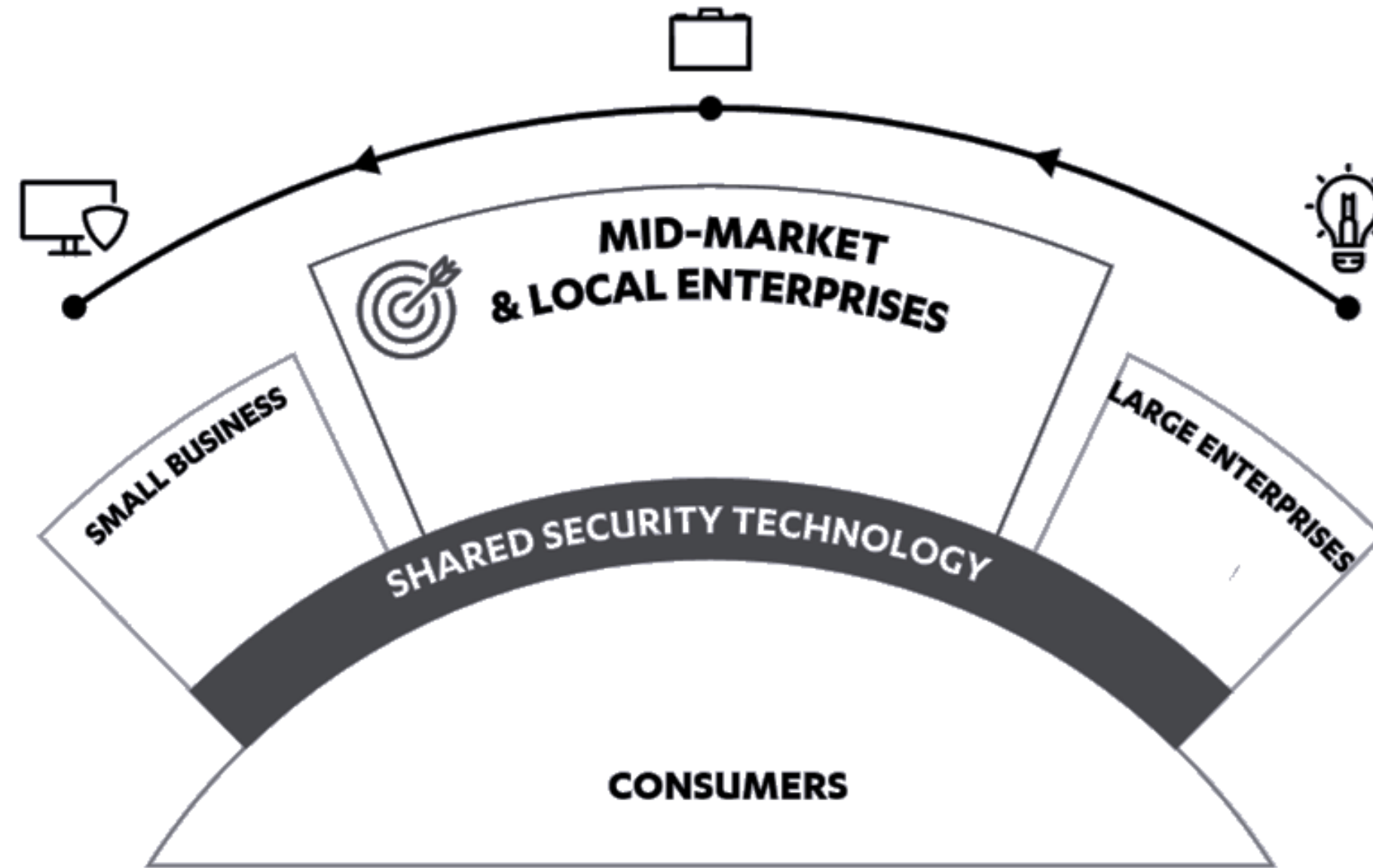
1000
Employees

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



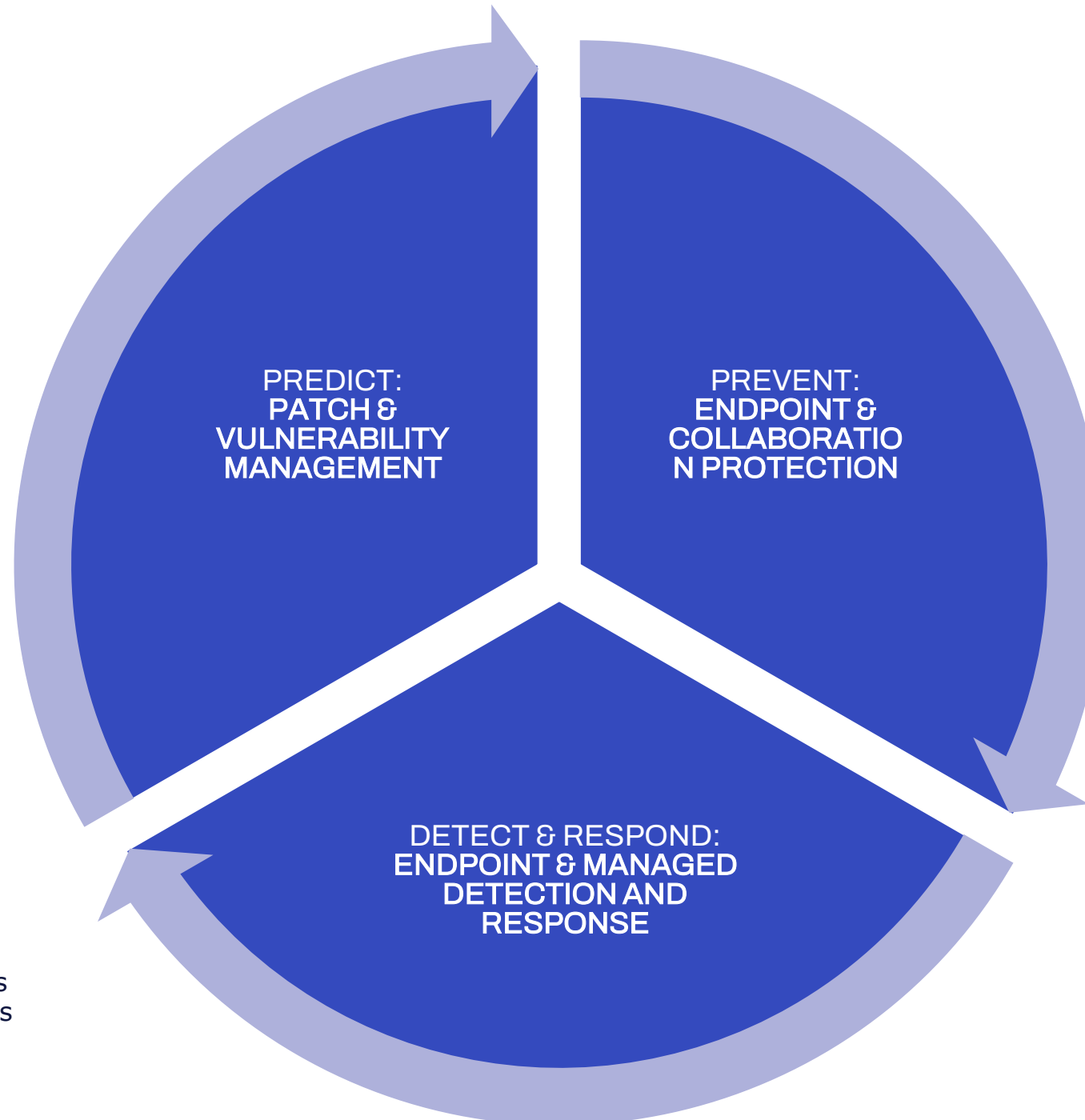
WithSecure™ named a 2020 Gartner Peer Insights Customers' Choice for Vulnerability Assessment



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



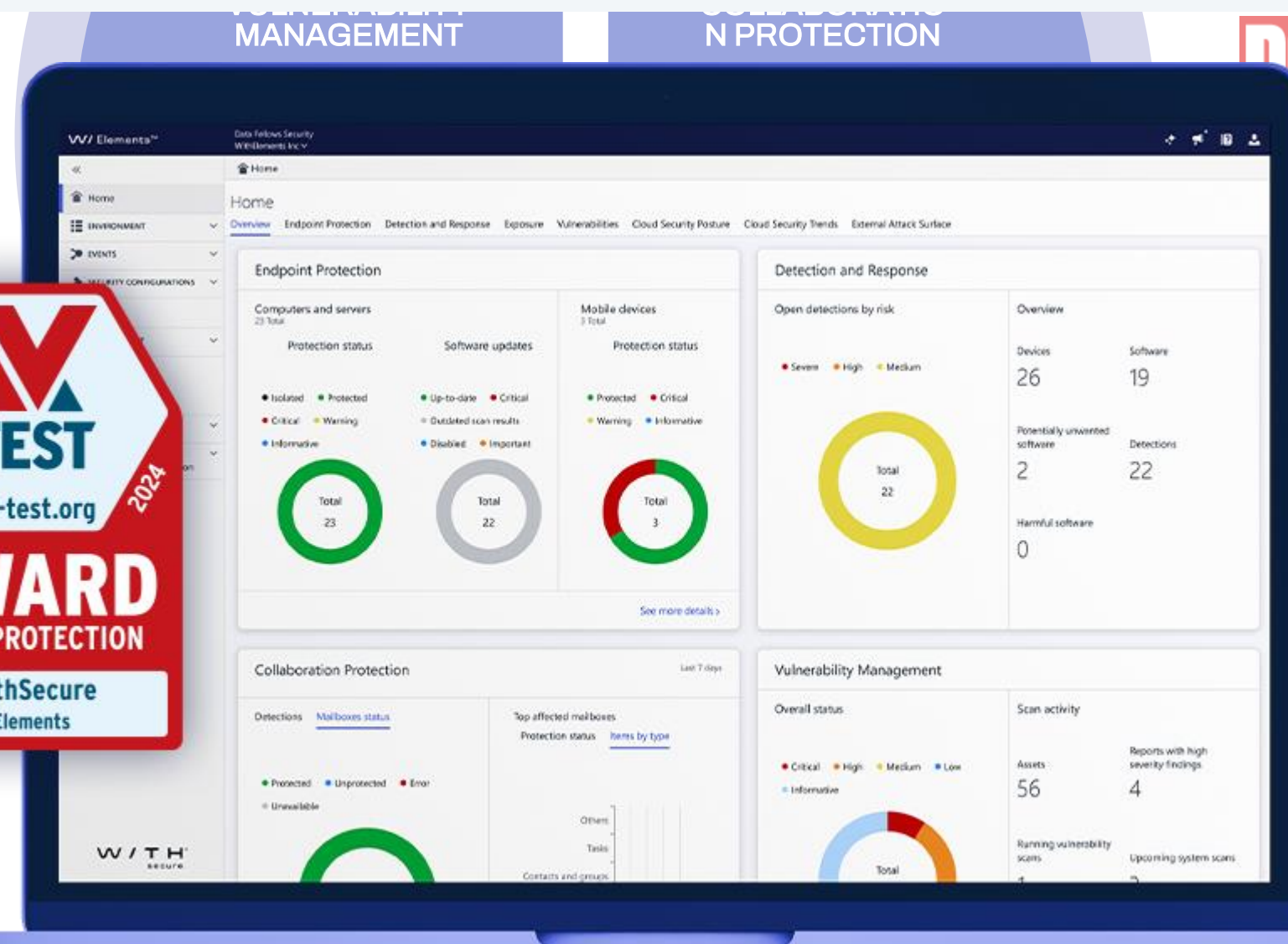
Qual 'Best Protection' AV-its inception, and the



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 threats



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



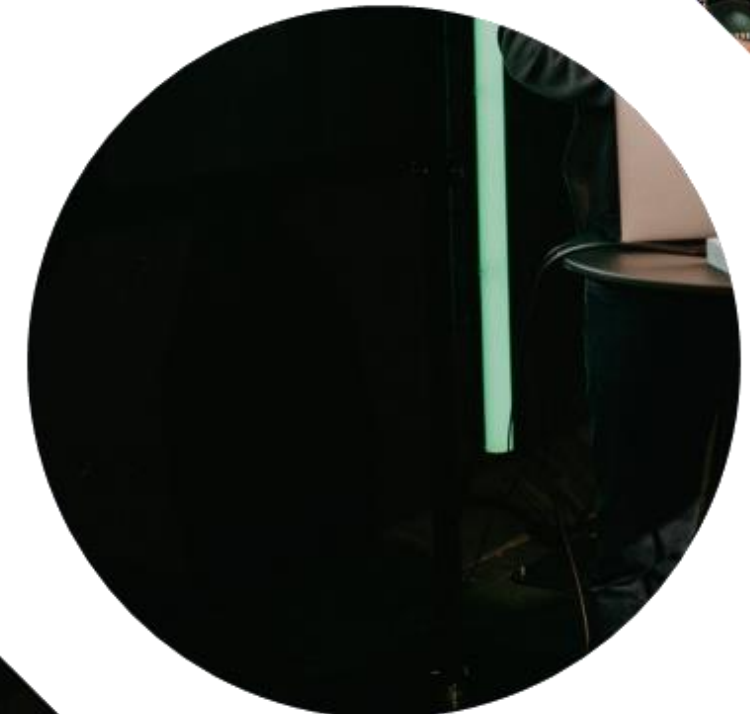
Gartner noted WithSecure's **new innovations** Exposure Management, Identity Security, ease of use and MDR service augmentation



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

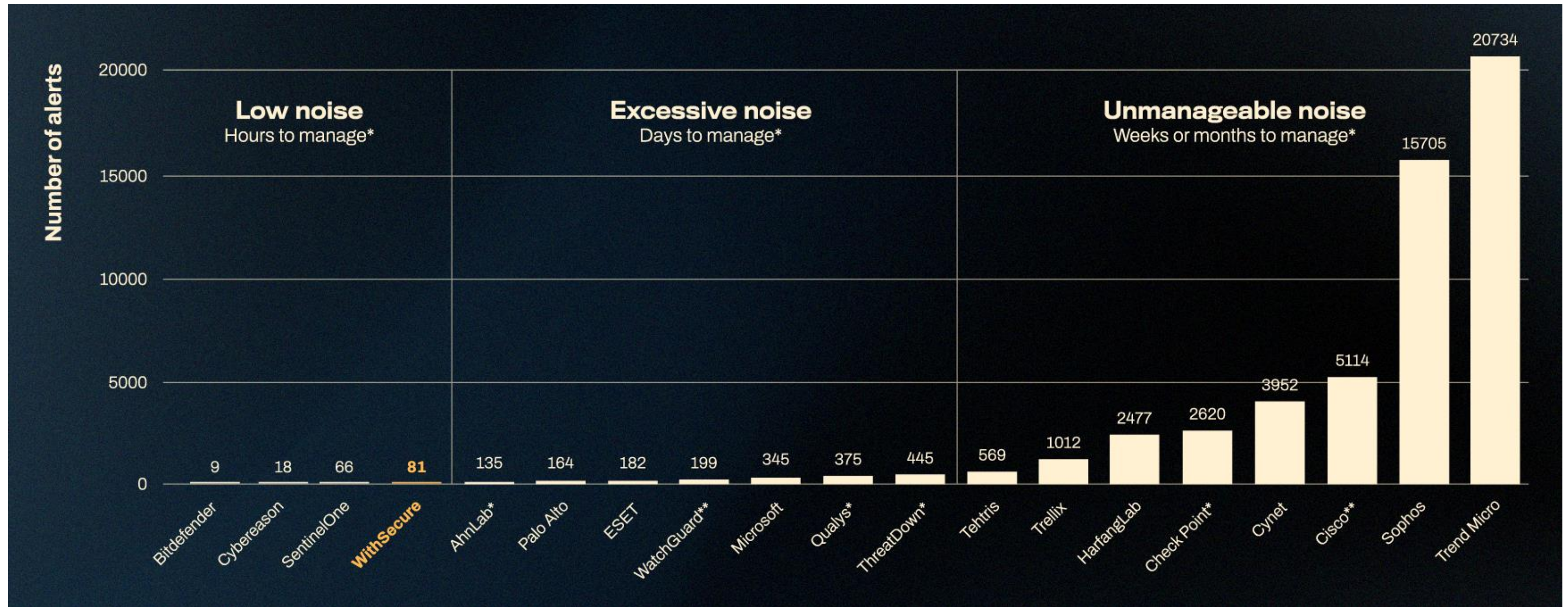


WithSecure is a good fit for small and midsize businesses

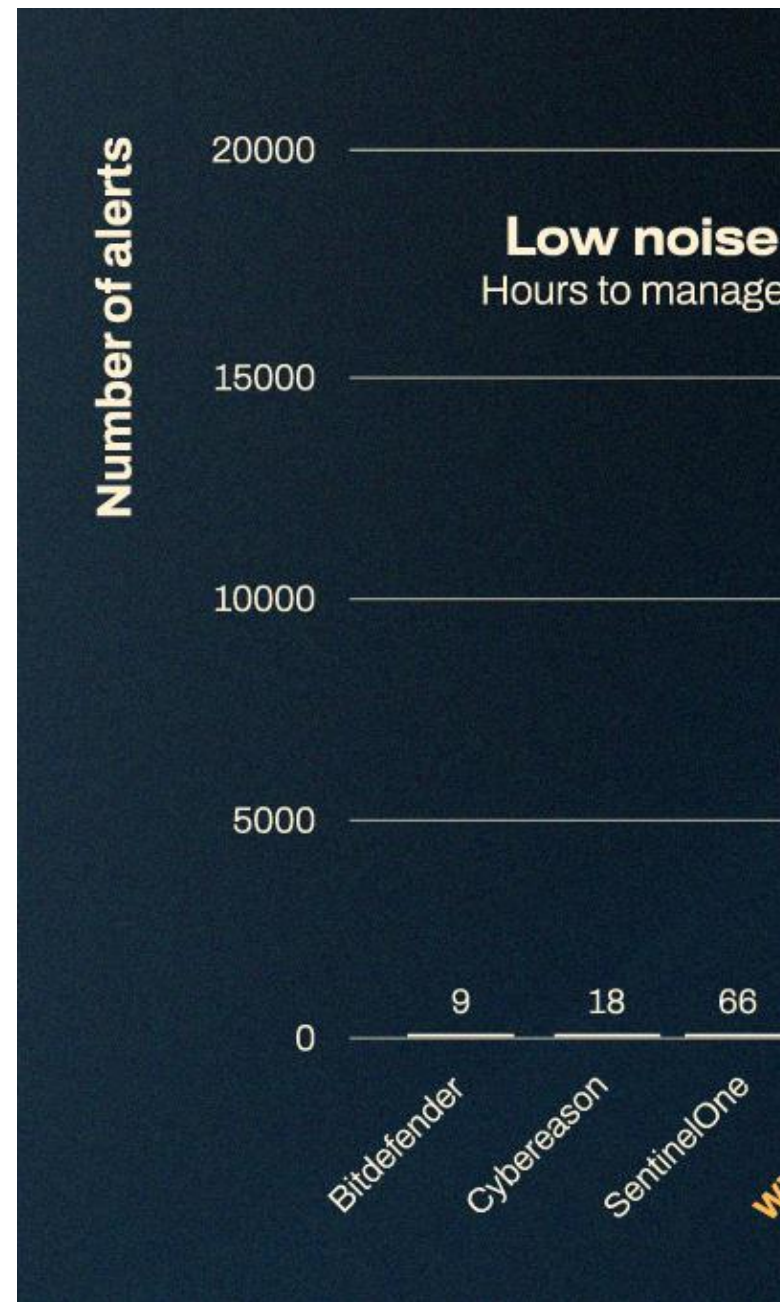
WithSecure's strengths:

- **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

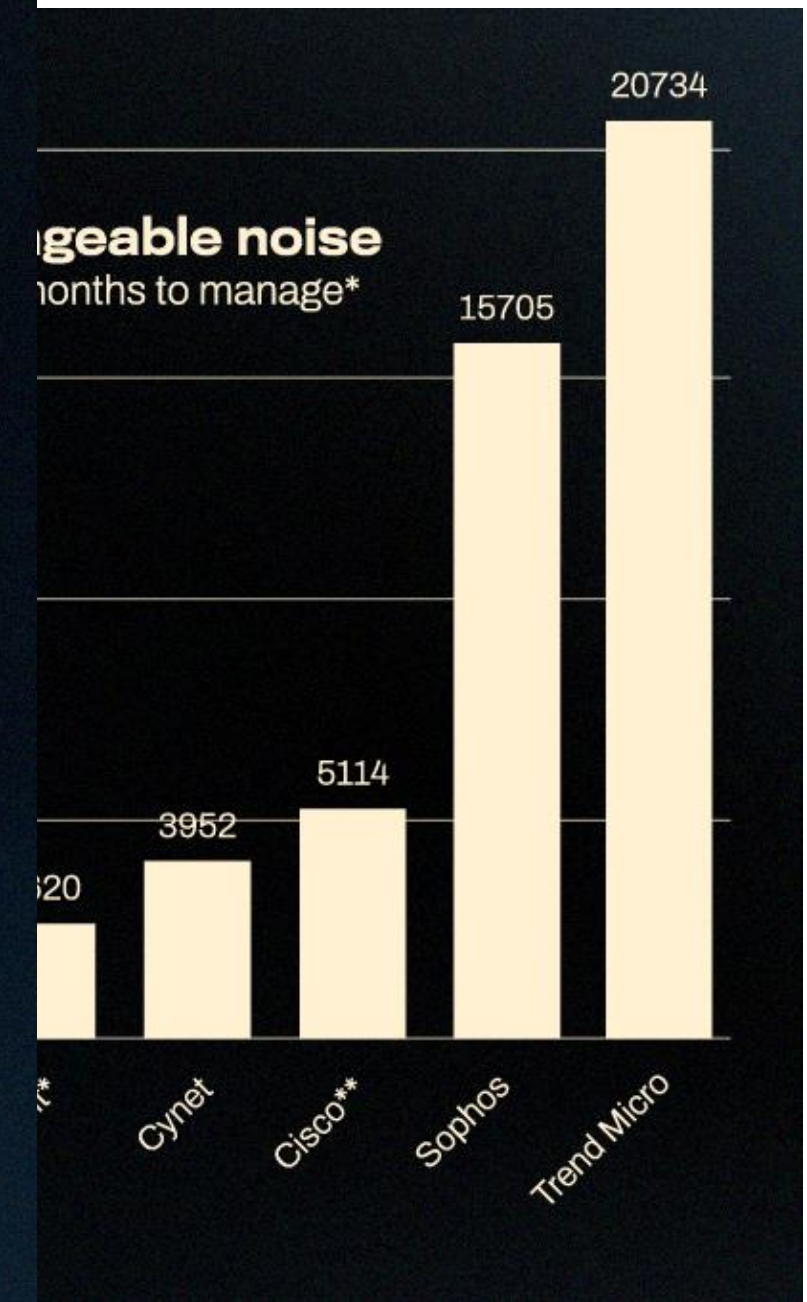
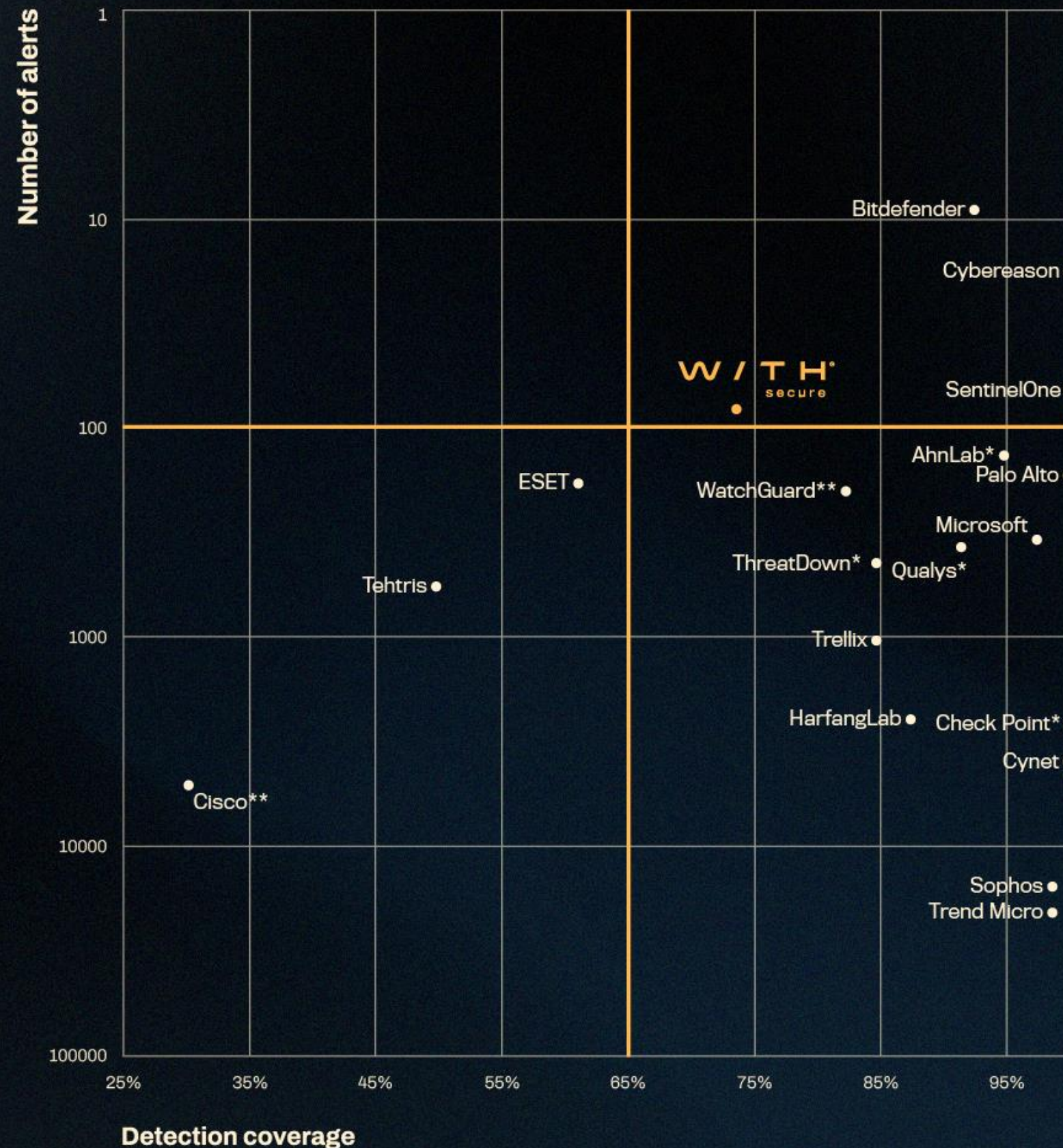
WithSecure sets new standards in detection-to-alert ratio for the mid-market



WithSecure sets alert ratio for the



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.



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



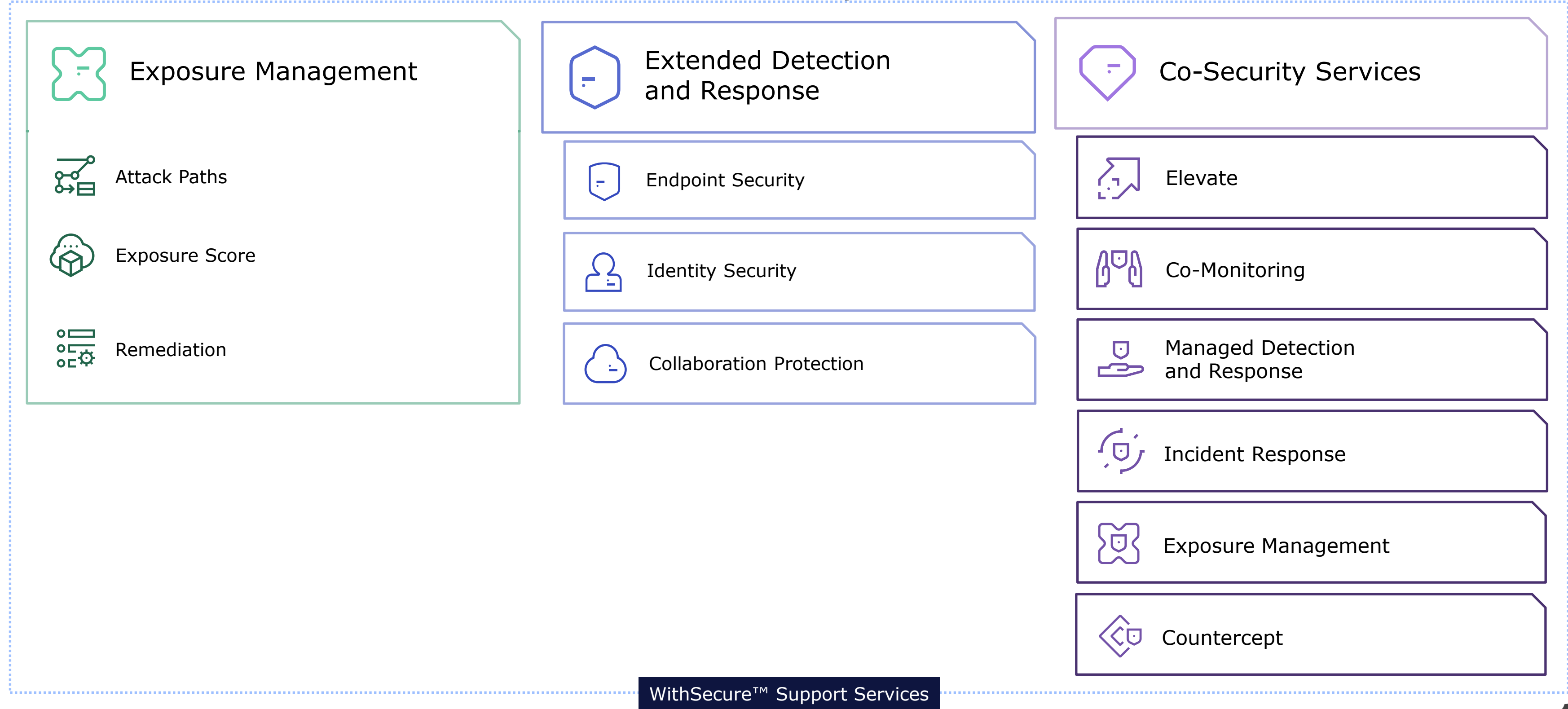
**Extended Detection
and Response**



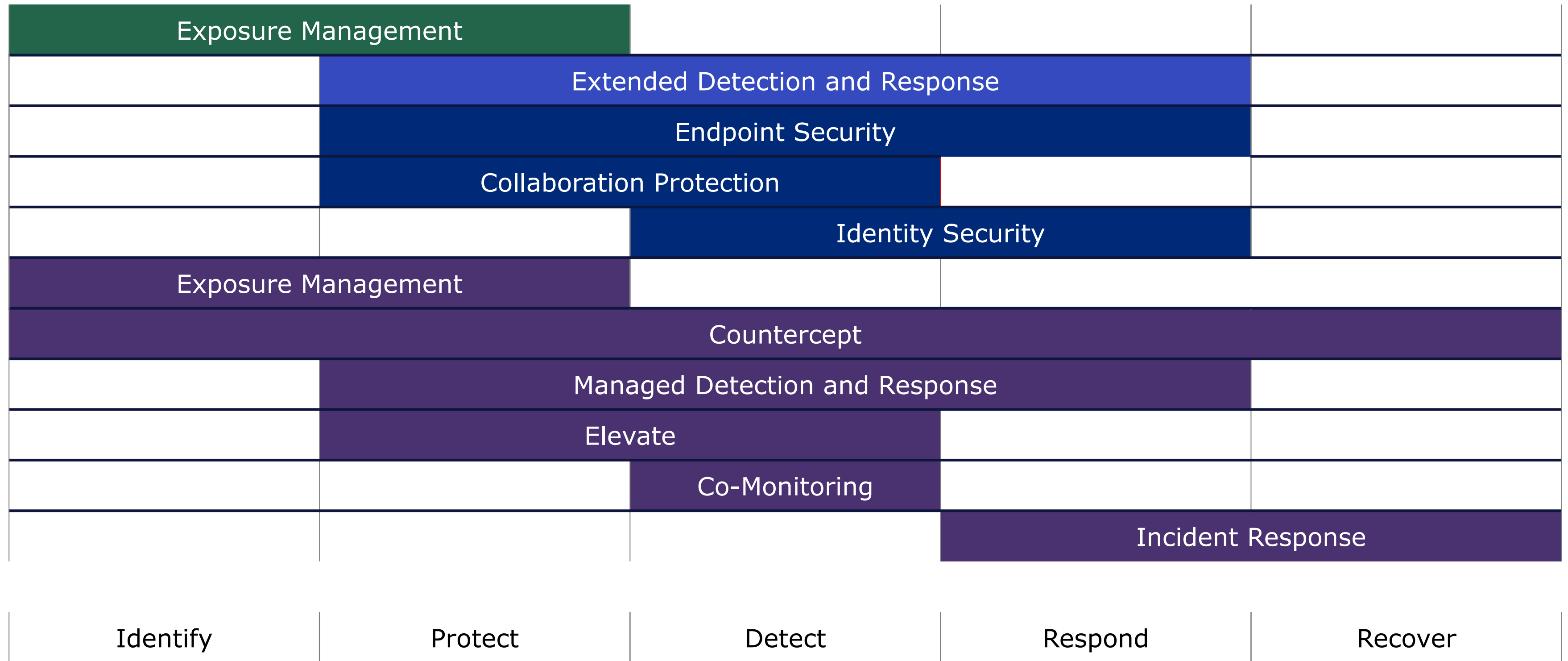
Co-Security Services

WithSecure™ Elements

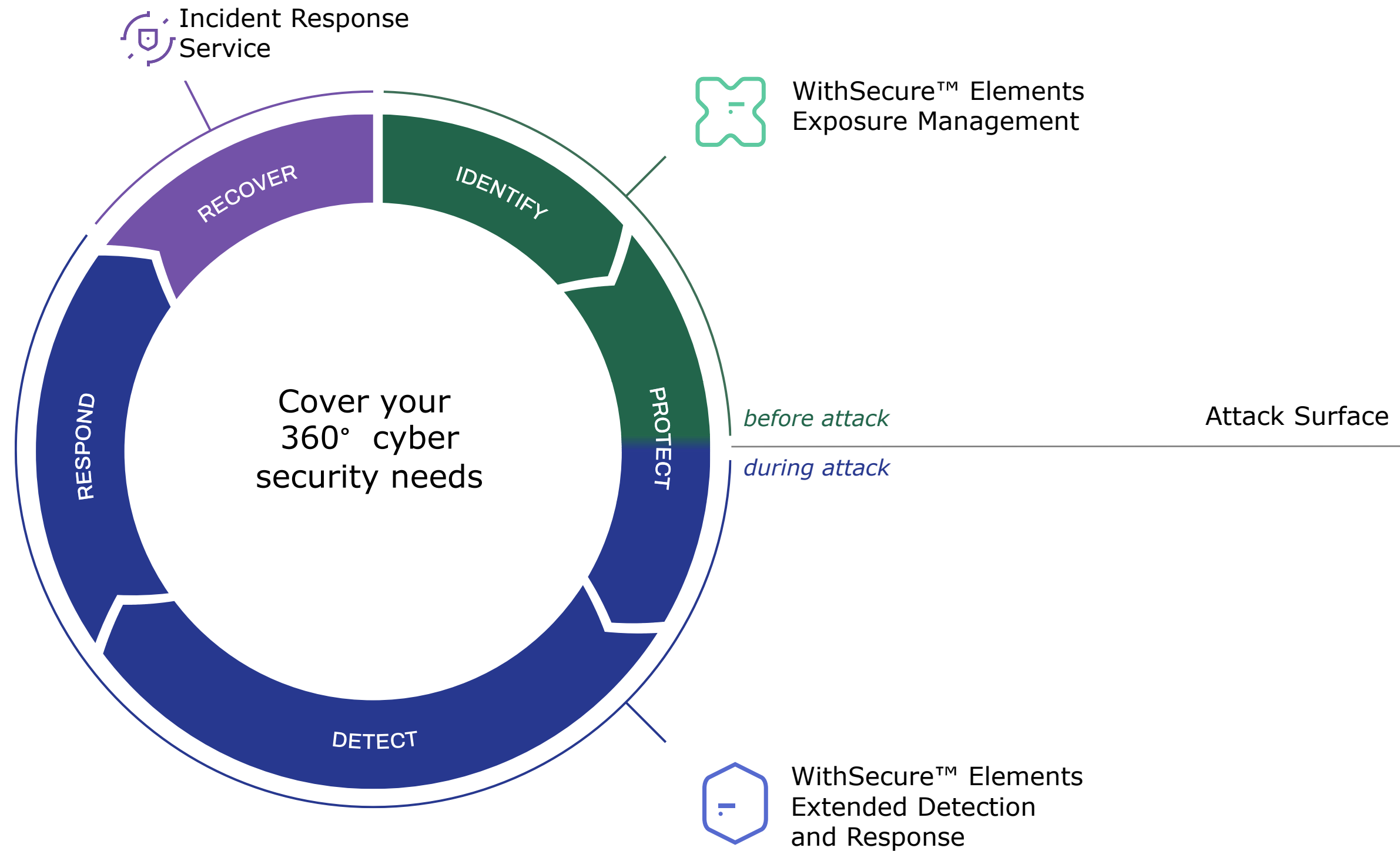
Proactive and Modular. Made for Co-Security.



WithSecure™ Elements Cloud - NIST



WithSecure™ Elements Cloud - NIST



WithSecure Elements Endpoint Protection

EPP for Windows, Linux, Mac, Android, iOS

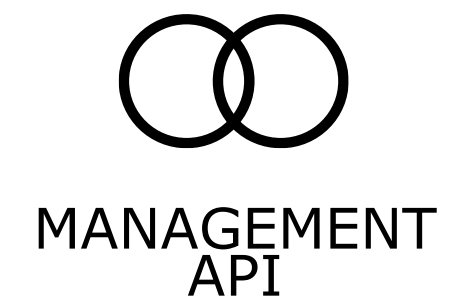
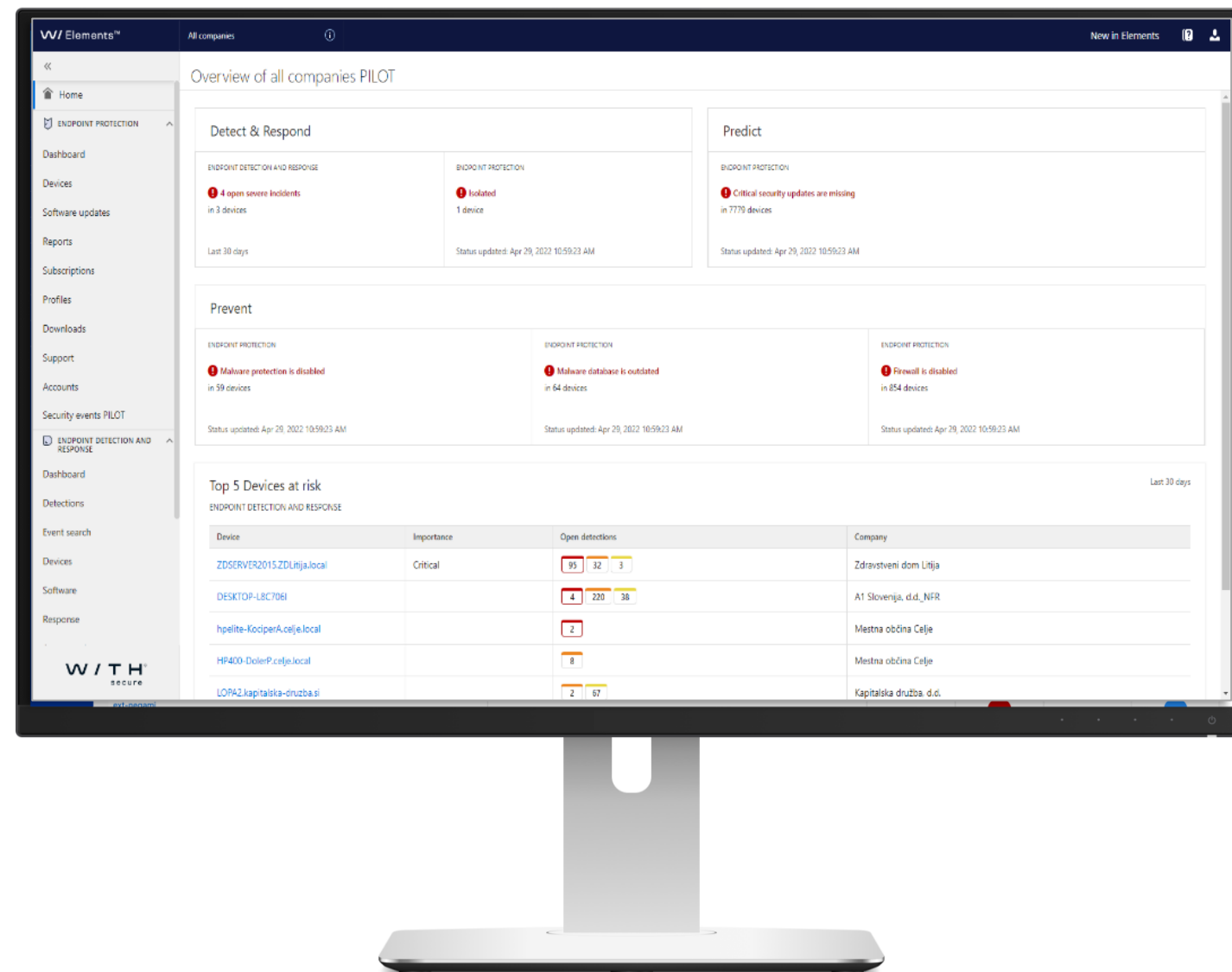
Elements Security center



ESC PORTAL

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

The ESC portal



Elements EPP clients

Windows PCs and MACs

- Elements EPP for Computers
 - Windows
 - Mac

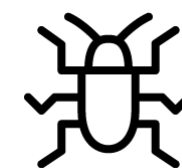
Mobile Devices

- Elements EPP for Mobiles
 - iOS
 - Android

Servers

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

Elements EPP for Computers



MULTI-ENGINE ANTI-MALWARE



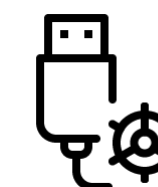
MANAGED FIREWALL



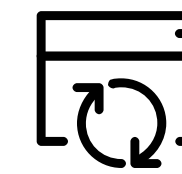
THREAT INTELLIGENCE



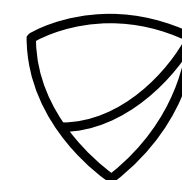
ADVANCED WEB PROTECTION



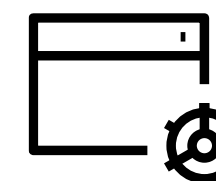
DEVICE CONTROL



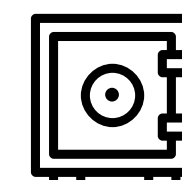
PATCH MANAGEMENT



DEEPGUARD



APPLICATION CONTROL*



DATAGUARD*

* = PREMIUM FEATURE

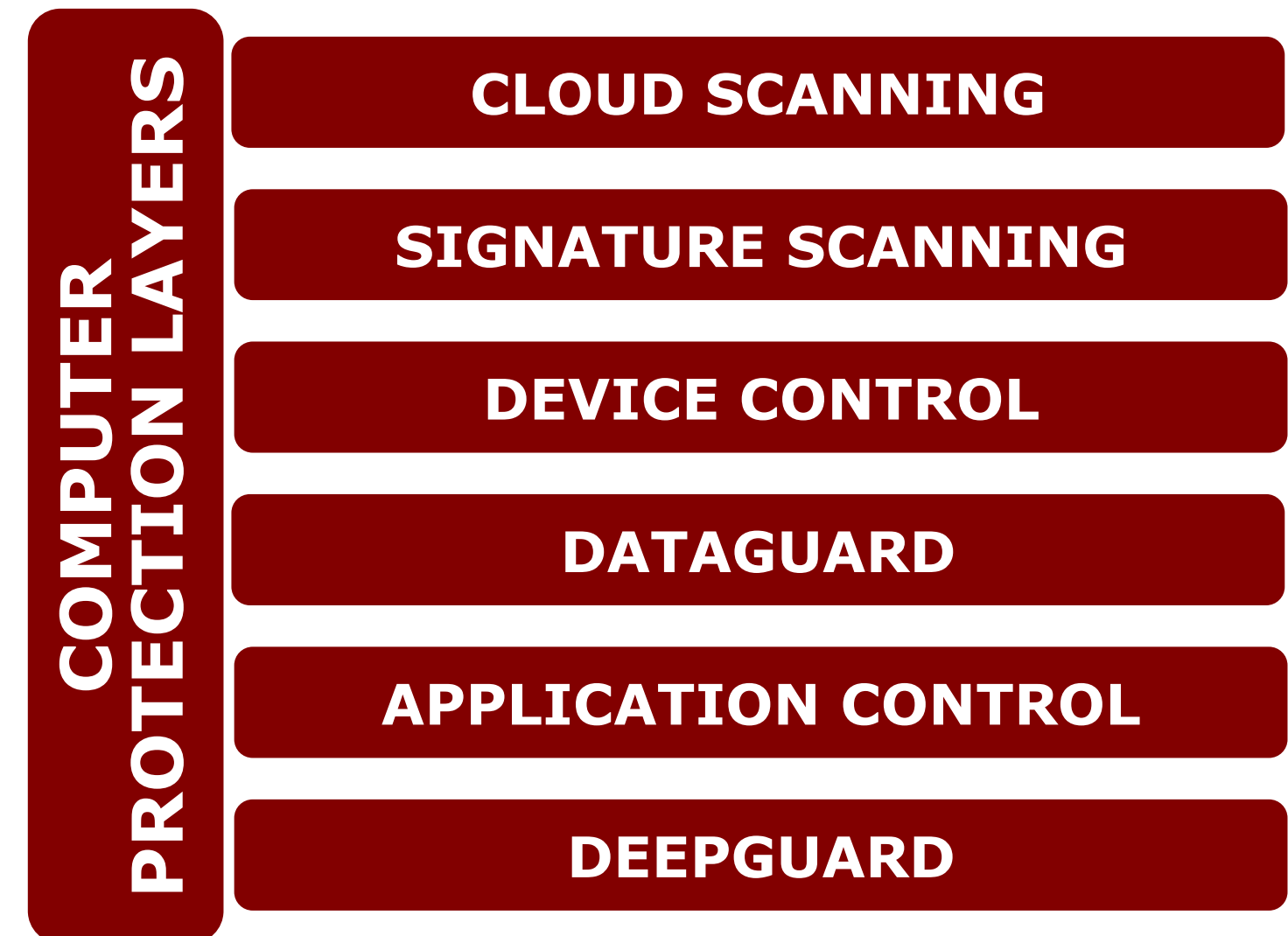
Elements EPP for Computers - PC

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



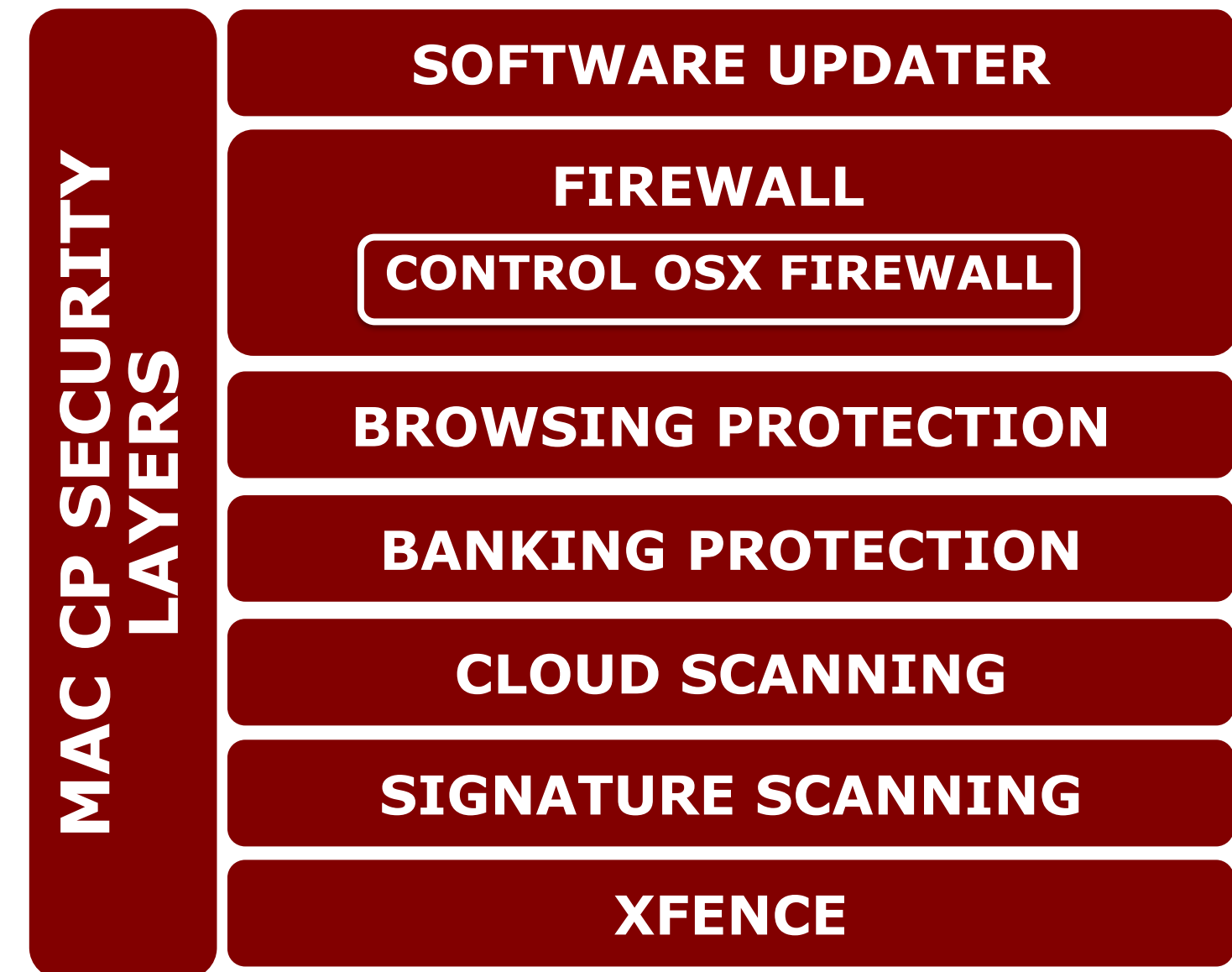
Elements EPP for Computers - PC

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

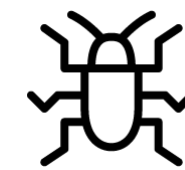


Elements EPP for Computers - Mac

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



Elements for Servers



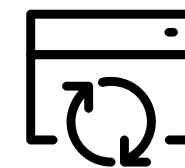
MULTI-ENGINE
ANTI-MALWARE



CENTRALLY
MANAGED
FIREWALL



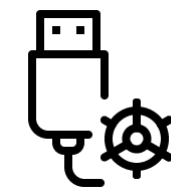
THREAT
INTELLIGENCE



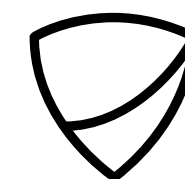
PATCH
MANAGEMENT



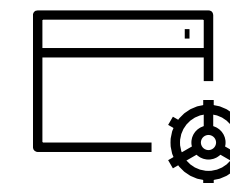
ADVANCED WEB
PROTECTION



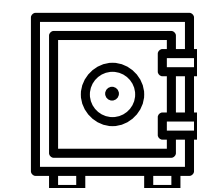
DEVICE
CONTROL



DEEPCUARD 6



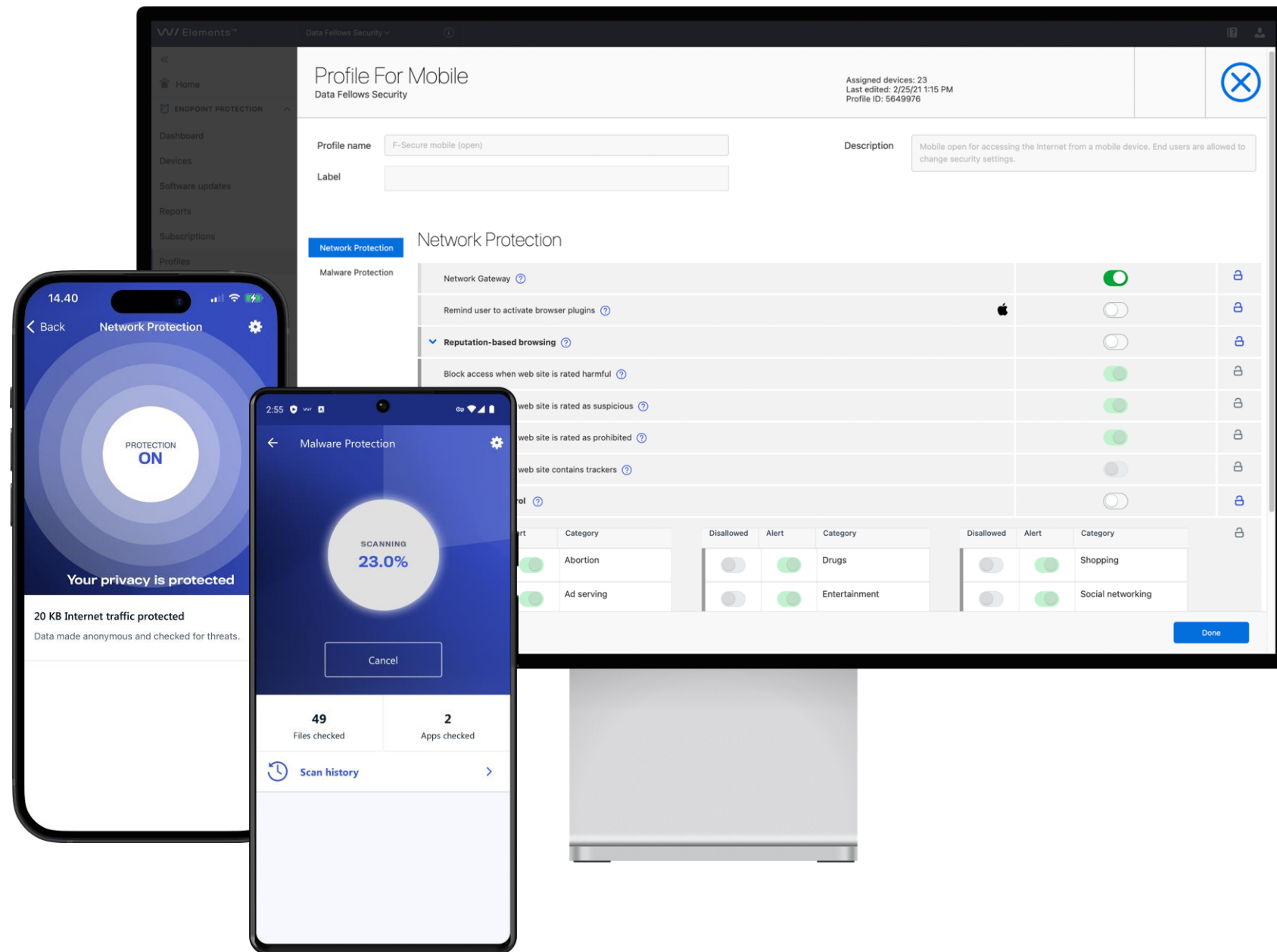
APPLICATION
CONTROL*



DATAGUARD*

* = PREMIUM FEATURE

Elements for Mobile



Elements EPP API

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



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

Solution packages

Features

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

NOTE: Features may differ with operating systems

WithSecure Elements Endpoint Detection & Response

EDR for Windows, Linux, Mac

How Is The Security Landscape Changing?

EVERY COMPANY IS A TARGET

All companies are targets when criminals go for the easiest victims

RANSOMWARE WITH BITCOIN

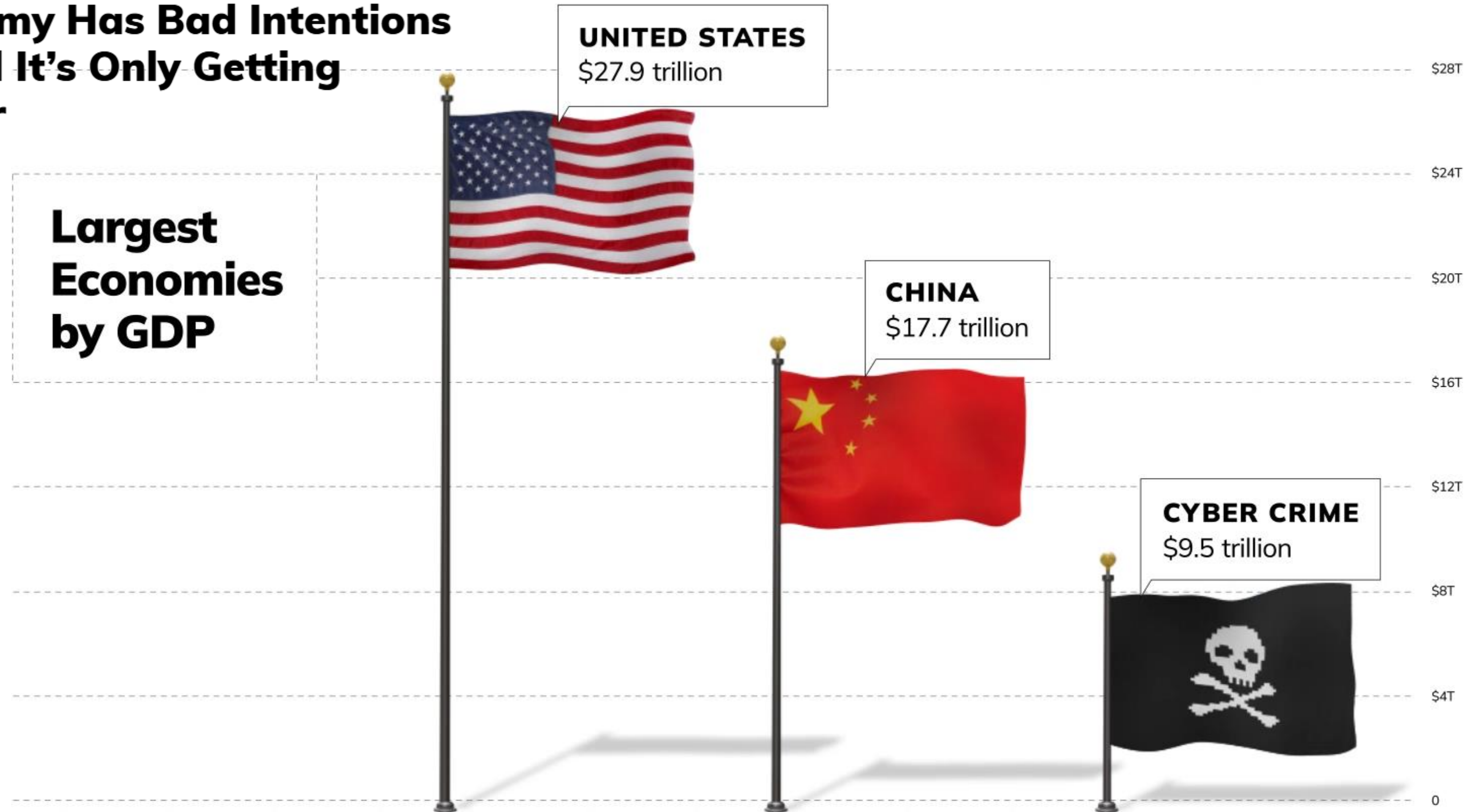
With Bitcoin, criminals can easily receive money without getting caught

NO MORE EASILY DETECTED METHODS

Criminals are now using fileless attacks and normal operating system tools

Endpoint Protection remains the foundation for securing your environment

The World's Third-Largest Economy Has Bad Intentions — and It's Only Getting Bigger

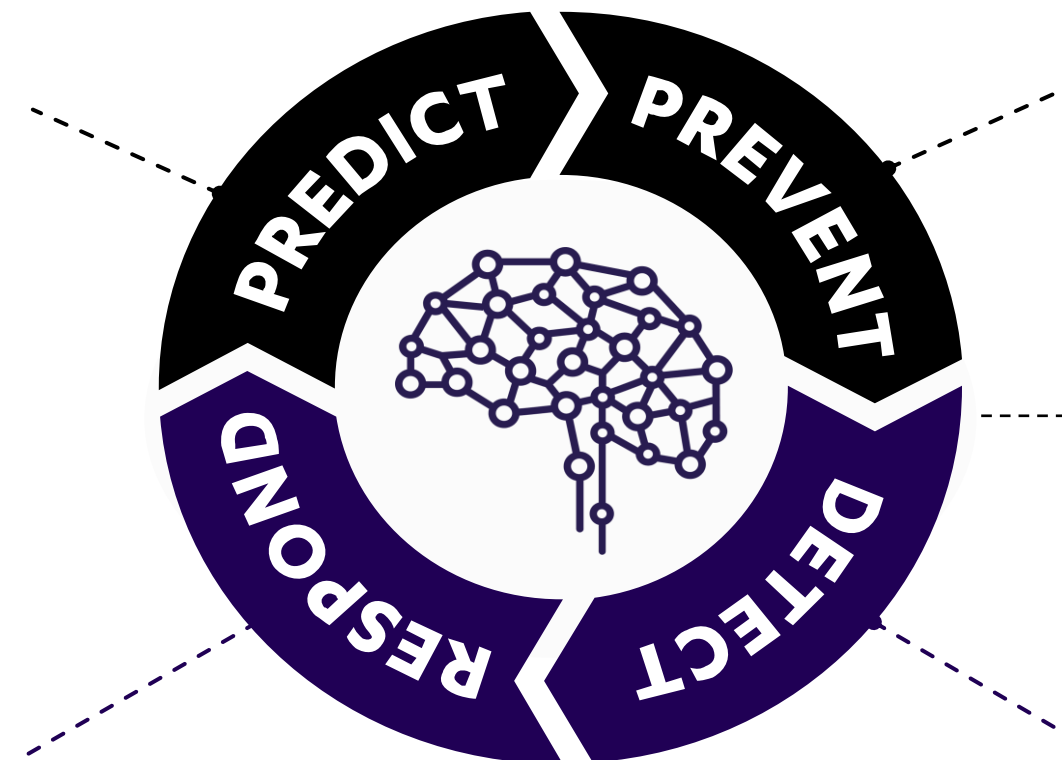


Source: IMF, Bloomberg, Cybersecurity Ventures

Cyber Security Must Be A Process

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

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



Minimize attack surface,
patch vulnerabilities and
prevent incidents

Pre-Compromise
Post-Compromise

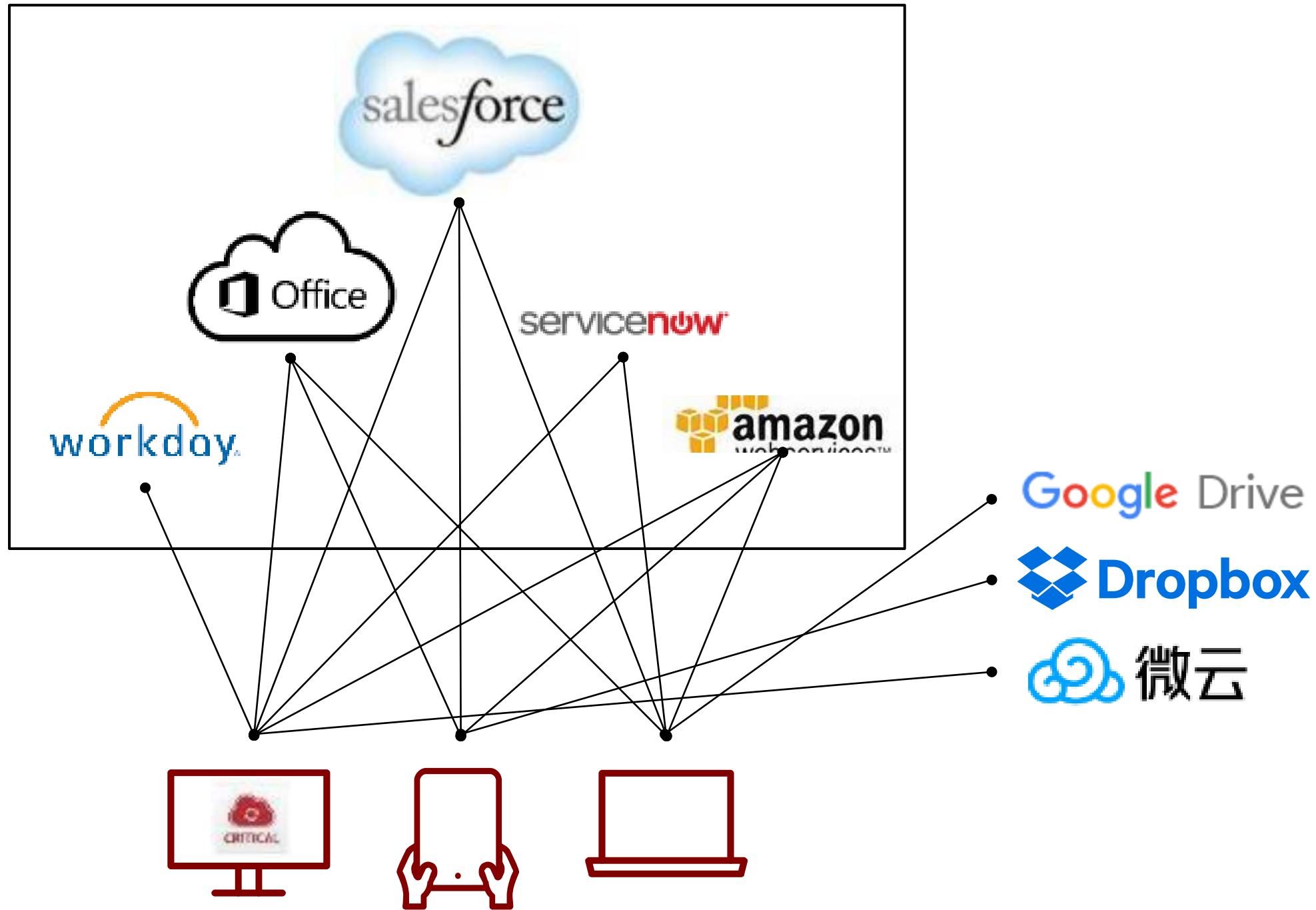
React to breaches,
mitigate the damage,
analyze and learn

Recognize incidents and
threats, isolate and contain
them

Preventing vs. Detecting

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

Modern IT Infrastructure Increases Exposure To Threats



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

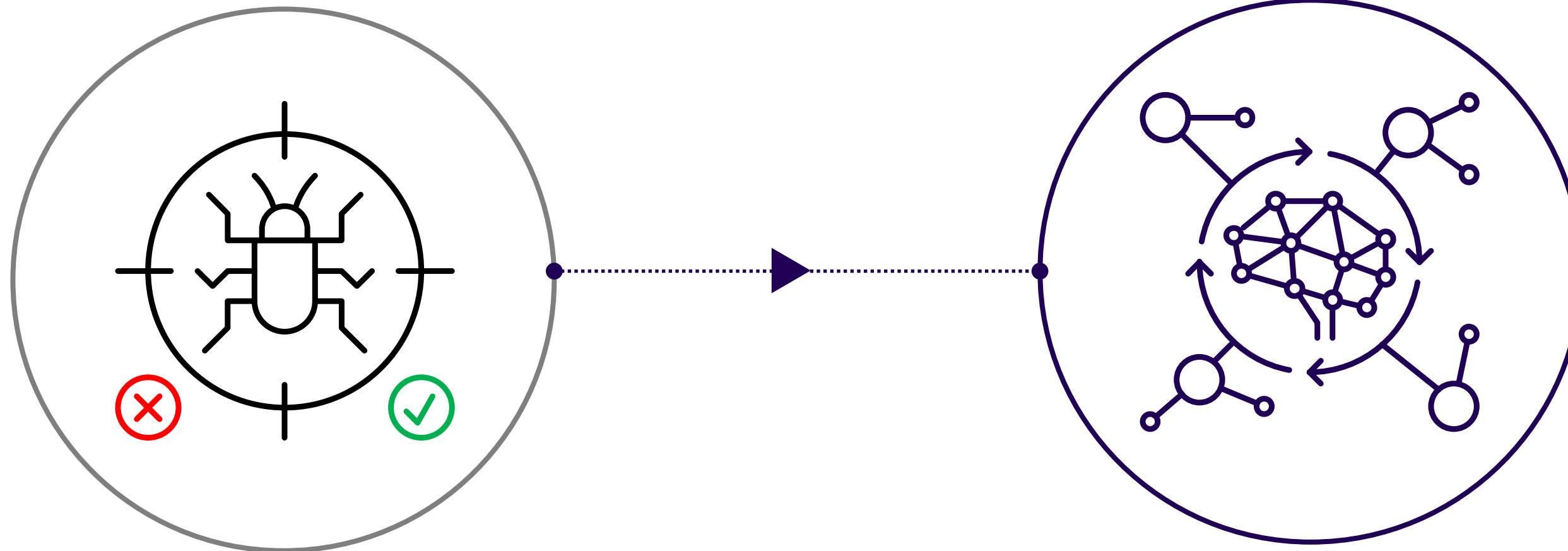


A1

**ON AVERAGE IT TAKES
100+ DAYS
TO DETECT A BREACH**

Source: 2024 Cost of Data Breach Study by Ponemon Institute indicated the days to identify the data breach at 194 (mean time to contain +64)

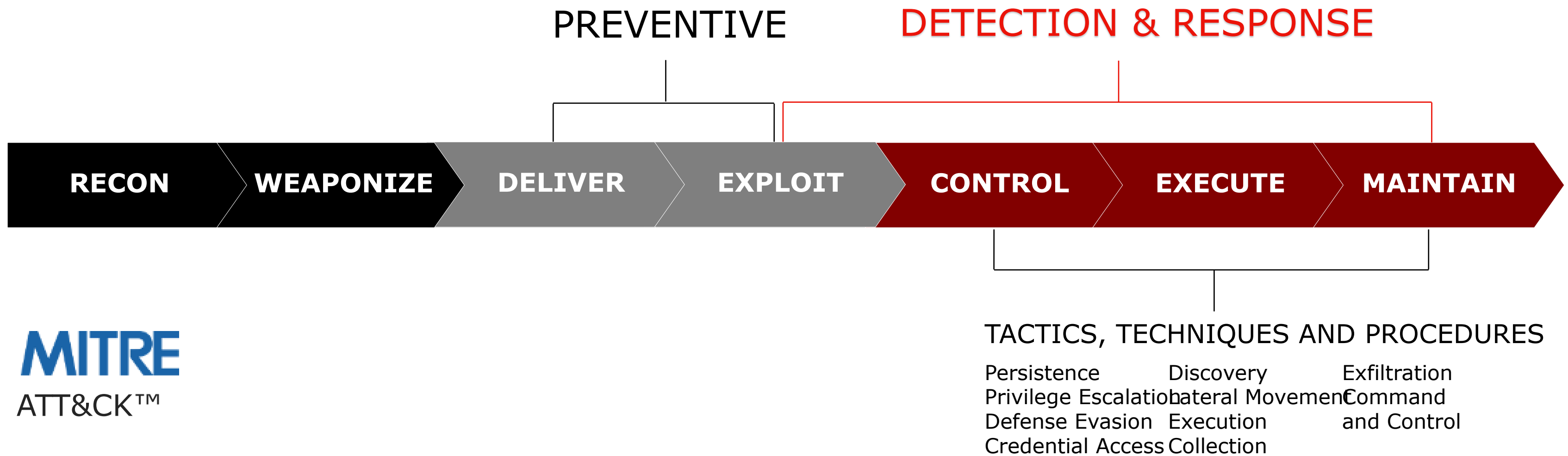
Call For A Paradigm Shift



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

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

Answering The Paradigm Shift

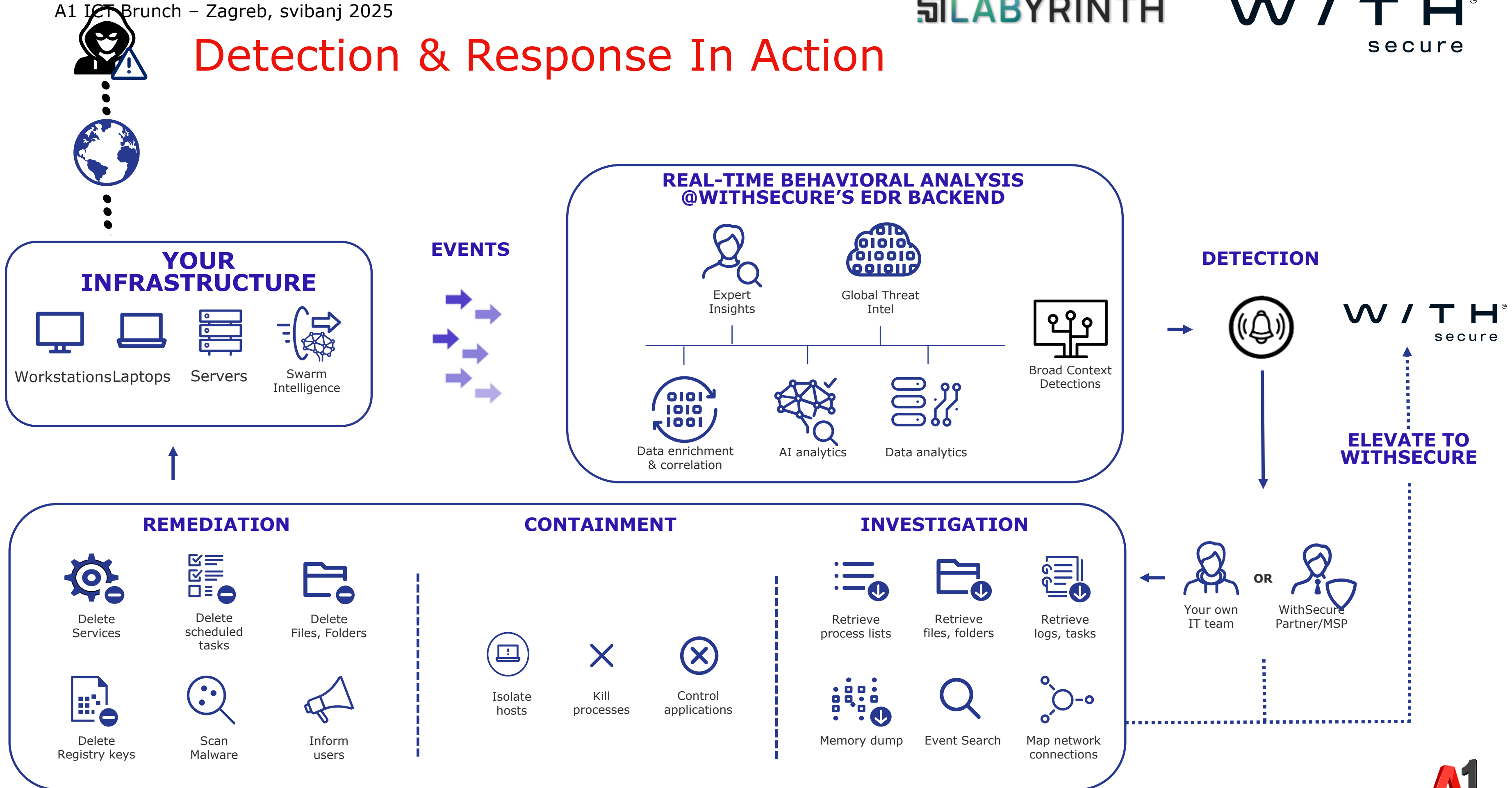


MITRE
ATT&CK™

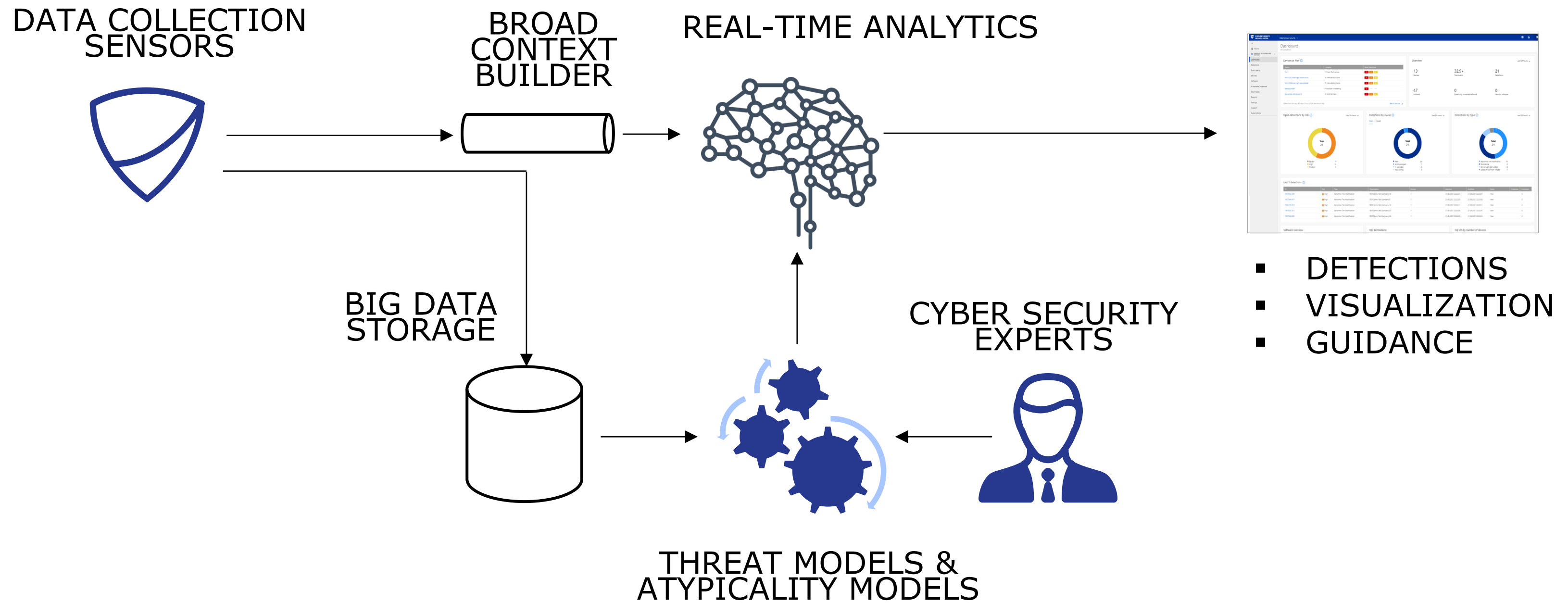
Solution packages

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

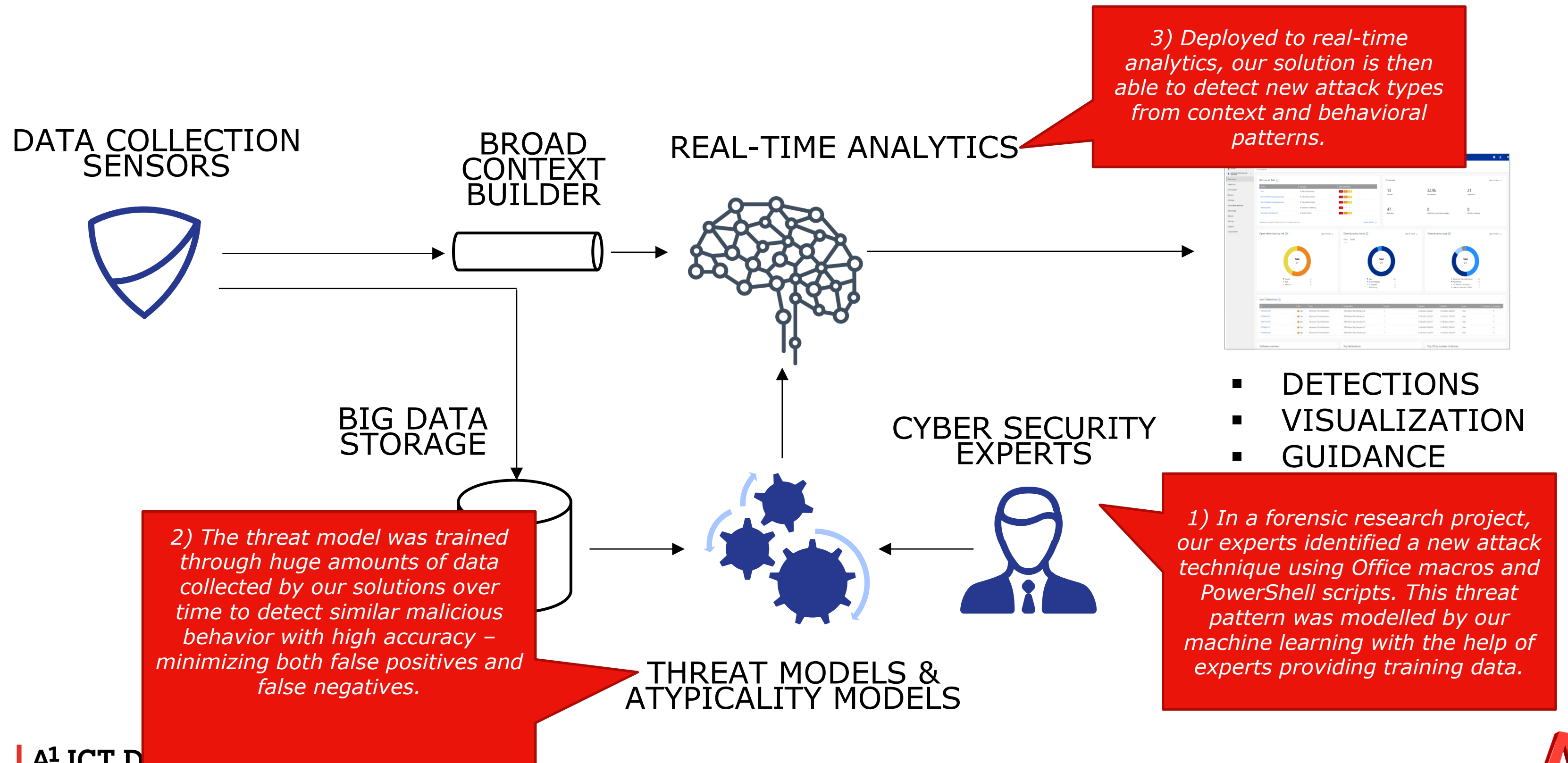
Detection & Response In Action



AI And Machine Learning At the Heart of the Solution

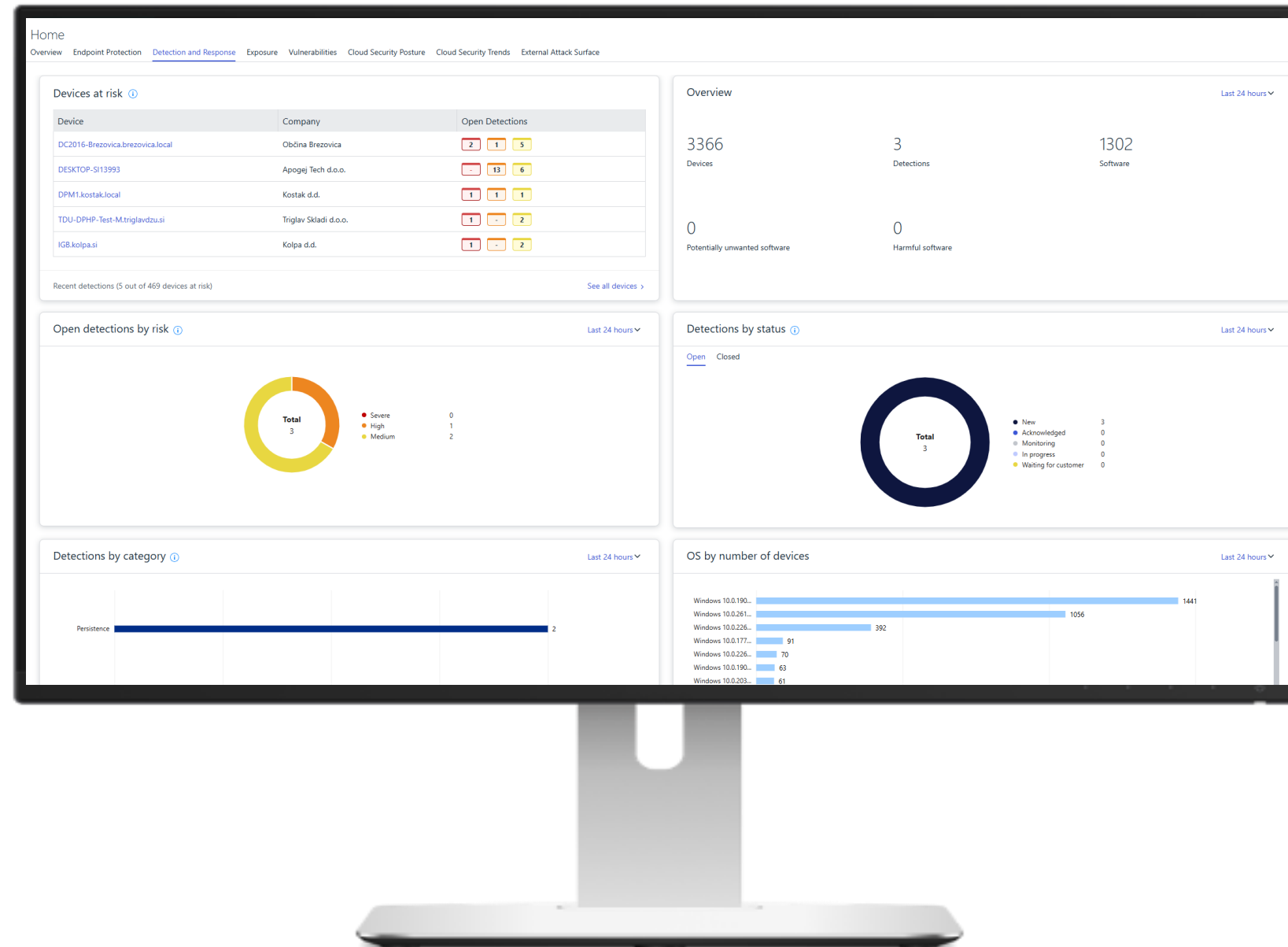


Threat Model Training In Action



WithSecure Endpoint Detection & Response

KEY FEATURES





BROAD CONTEXT
DETECTION™


INCIDENT
MANAGEMENT


GUIDANCE
TO RESPOND


APPLICATION
INVENTORY


CENTRALIZED
MANAGEMENT


HOST
ISOLATION

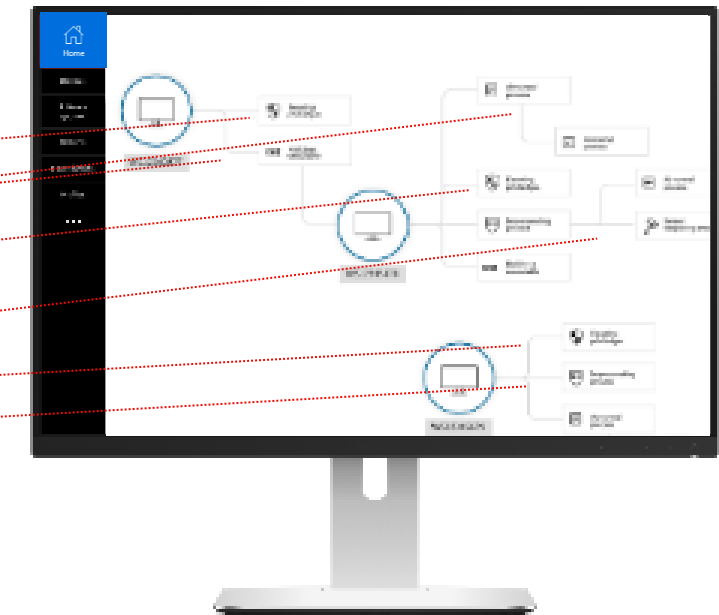
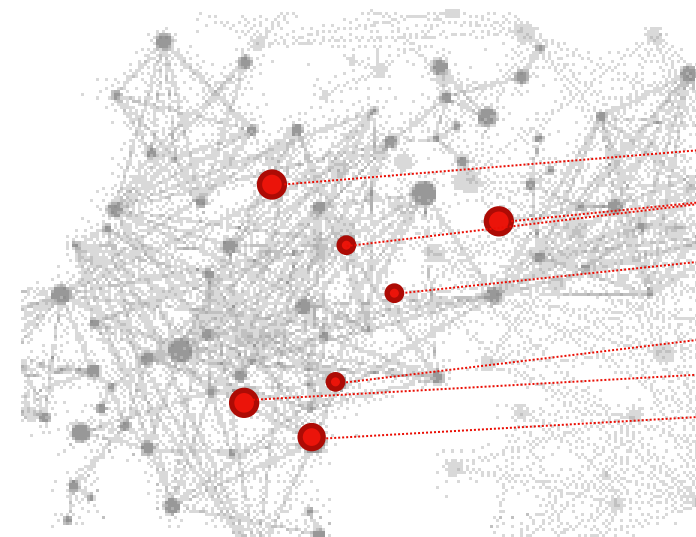

ELEVATE TO
WITHSECURE


AUTOMATED
RESPONSE

Why Broad Context Detection?

YES

NO

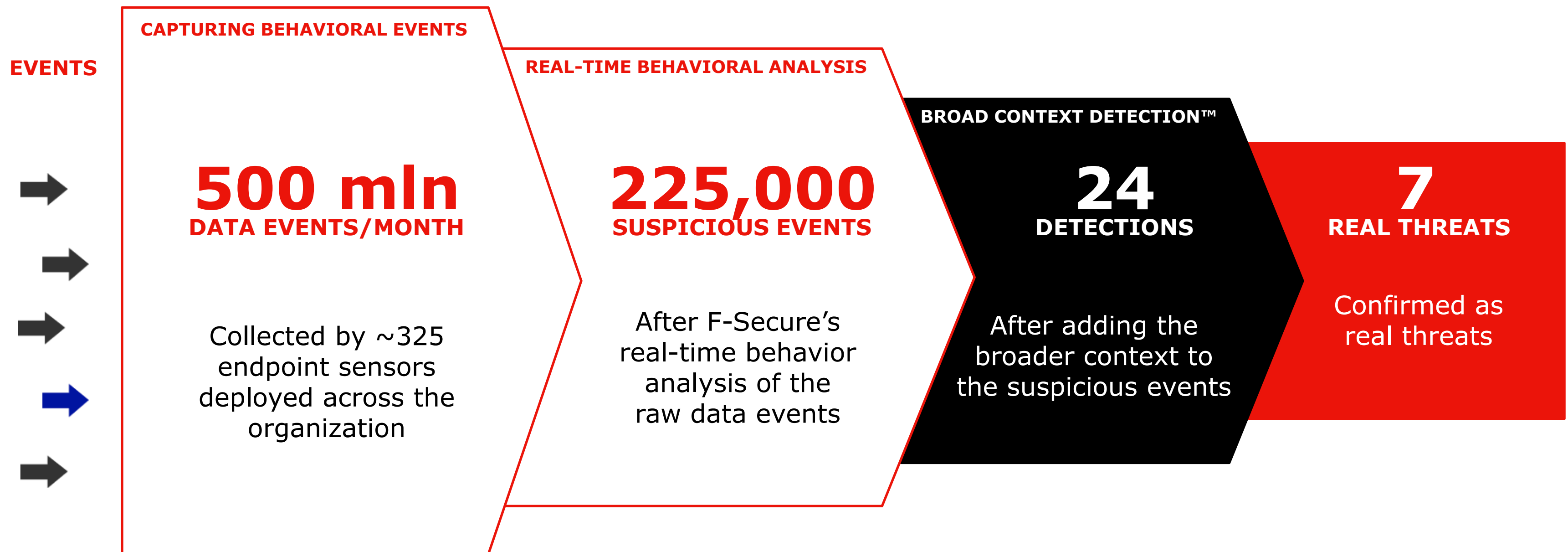


From single-shot, **point detections** and binary (ON/OFF) responses common for endpoint protection platforms.

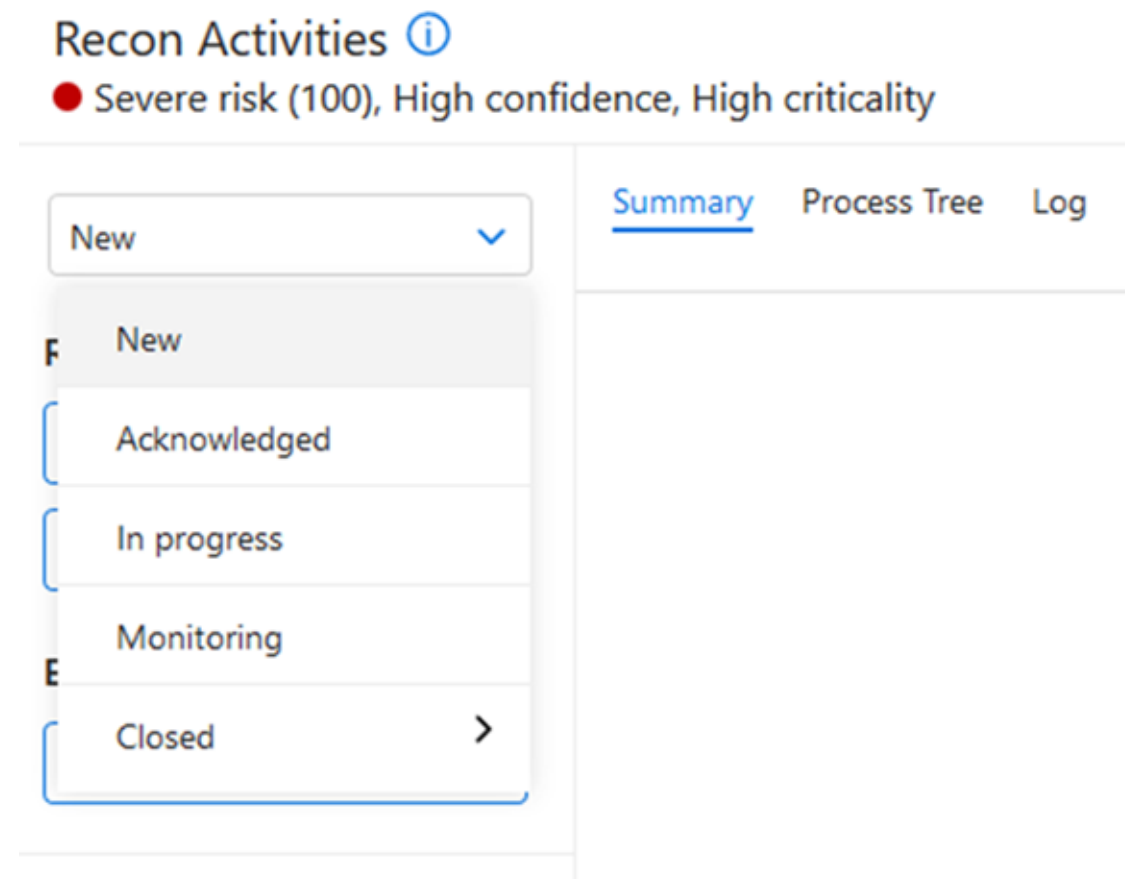
To **context-based detections** including risk levels, affected host criticality, and prevailing threat landscape.

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

Broad Context Detection In Action



Incident Management



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

Response Actions

INVESTIGATIVE ACTIONS

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

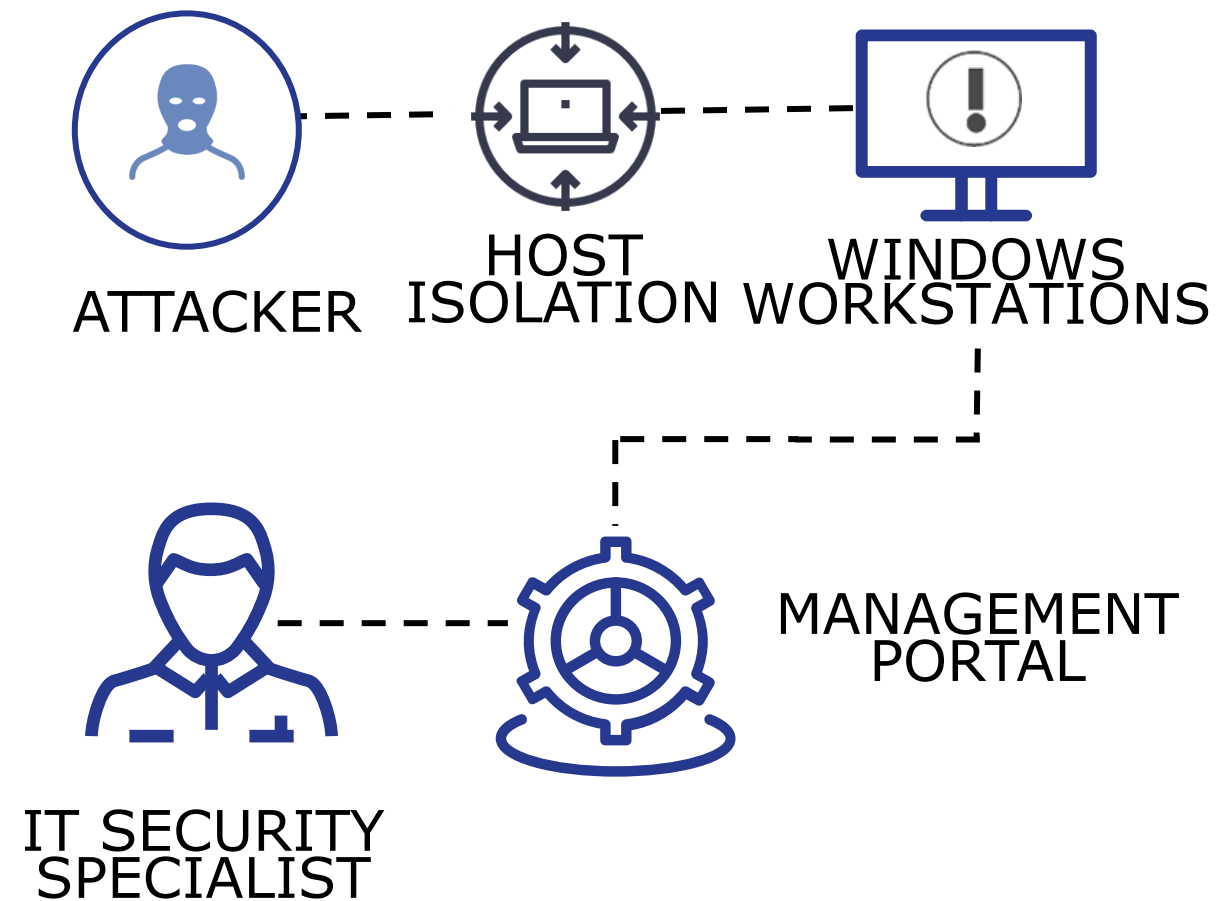
CONTAINMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

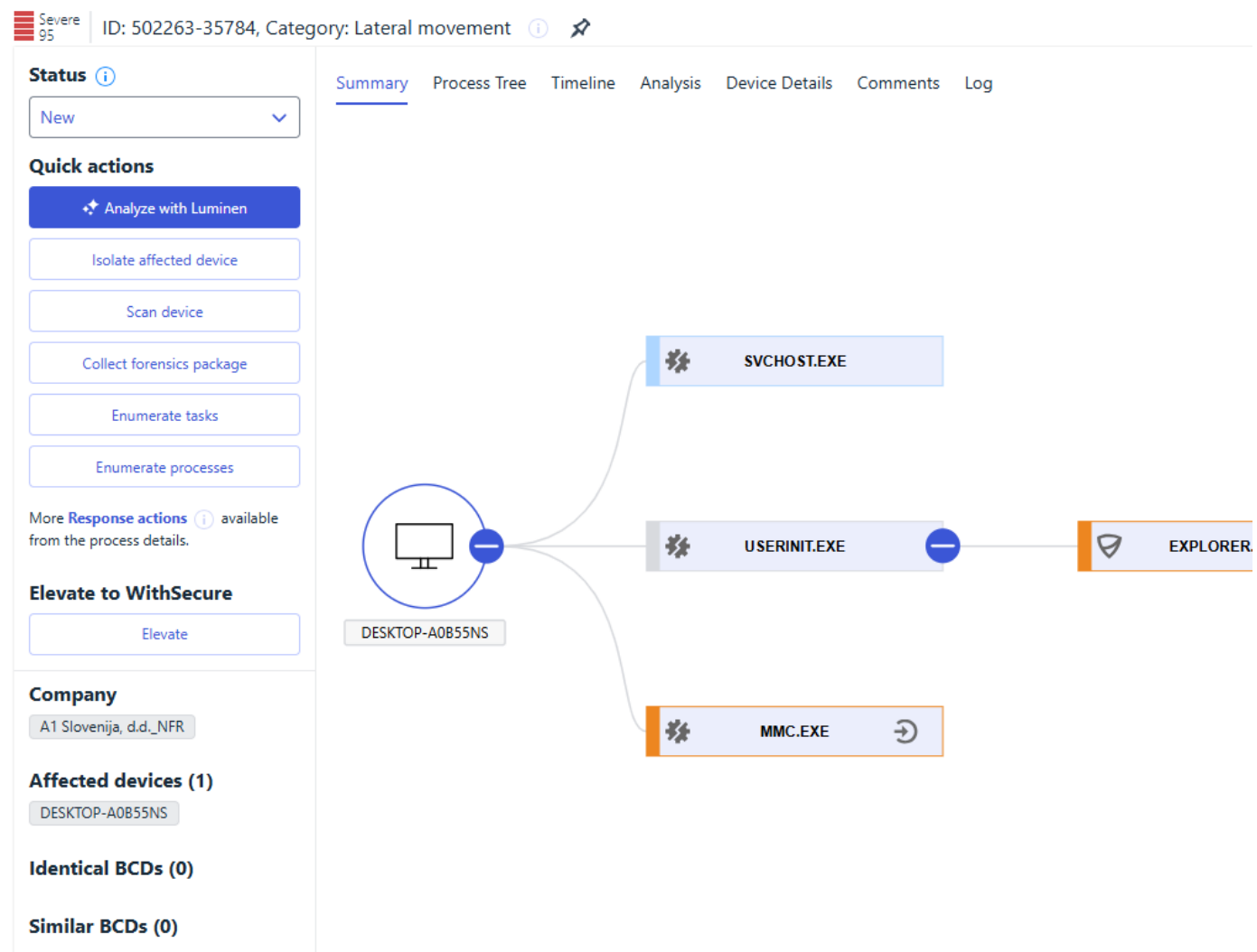
- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

Host Isolation



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

Guidance To Respond



⊕ Recommends **response actions** like informing users or **isolating hosts**

⊕ Get help on tough investigations from F-Secure experts with **Elevate to WithSecure**

⊕ **Machine learning** means EDR constantly improves its recommendations and detects **less false positives**

Automated Response

Automated response

Add rule

<input checked="" type="checkbox"/>	Name	Company	Action	Criteria	Schedule
<input checked="" type="checkbox"/>	Host isolat...	FS EDR	Isolate hosts	Risk level: Severe, h...	Continuous
<input checked="" type="checkbox"/>	Host isolat...	FS EDR Security Tes...	Isolate hosts	Risk level: Severe	Continuous
<input checked="" type="checkbox"/>	Host isolat...	FS EDR, FS EDR ...	Isolate hosts	Risk level: Severe	Continuous
<input checked="" type="checkbox"/>	Host isolat...	FS EDR, FS EDR ...	Isolate hosts	Risk level: Severe a...	Continuous

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

Elevate To WithSecure



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

Investigate with an Integrated Assistant

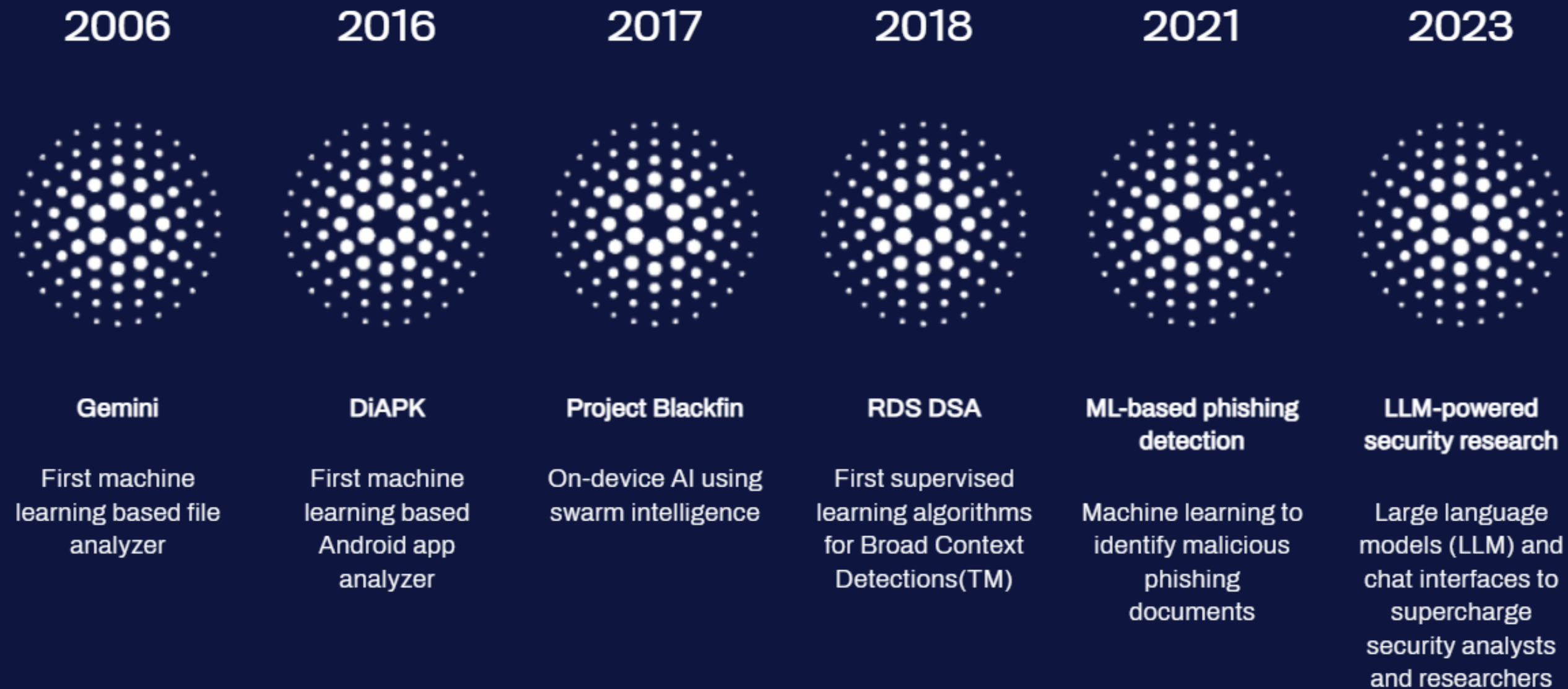
Prompt Down Hackers with Luminen™ GenAI

- 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.



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
for Microsoft Entra ID



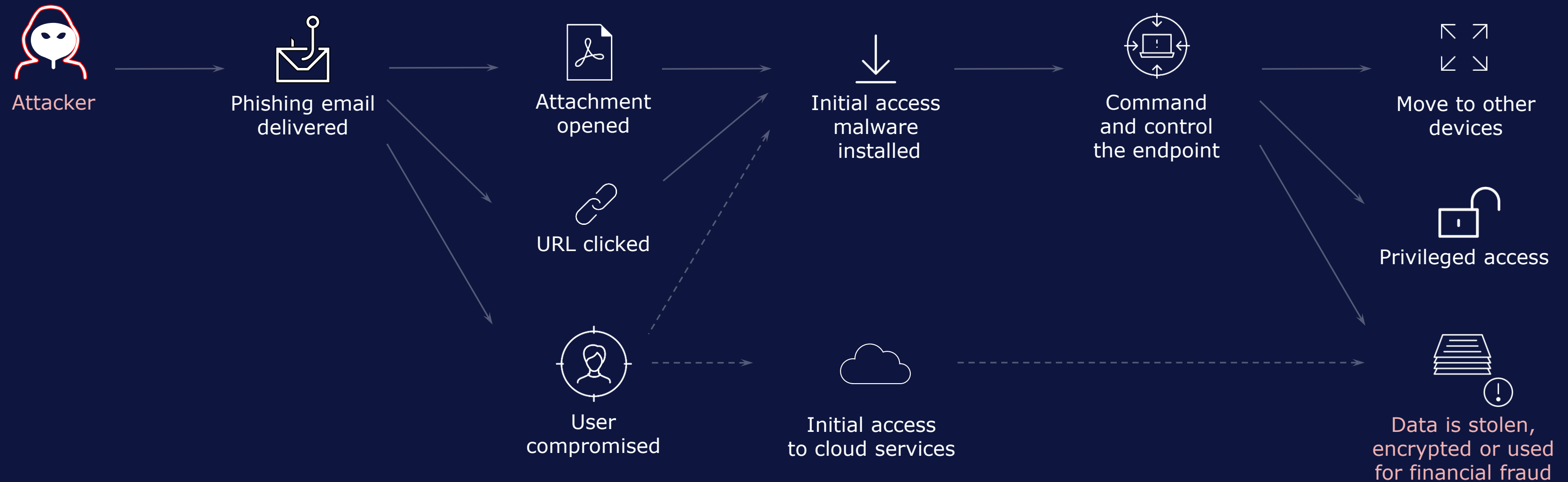
Collaboration Protection

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 protection scenarios



Attachment or URL blocked

Risky user session detected

Malware blocked

Malicious process detected, host isolated

 Ransomware prevented

W/ Elements™ | Extended Detection and Response

Preventive and reactive security

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**

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

WithSecure™ Elements XM vs XDR

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



LABYRINTH

W / I T H[®]
secure

Labyrinth Deception



Drugačiji pristup za praćenje mreže?



Tko je Labyrinth?

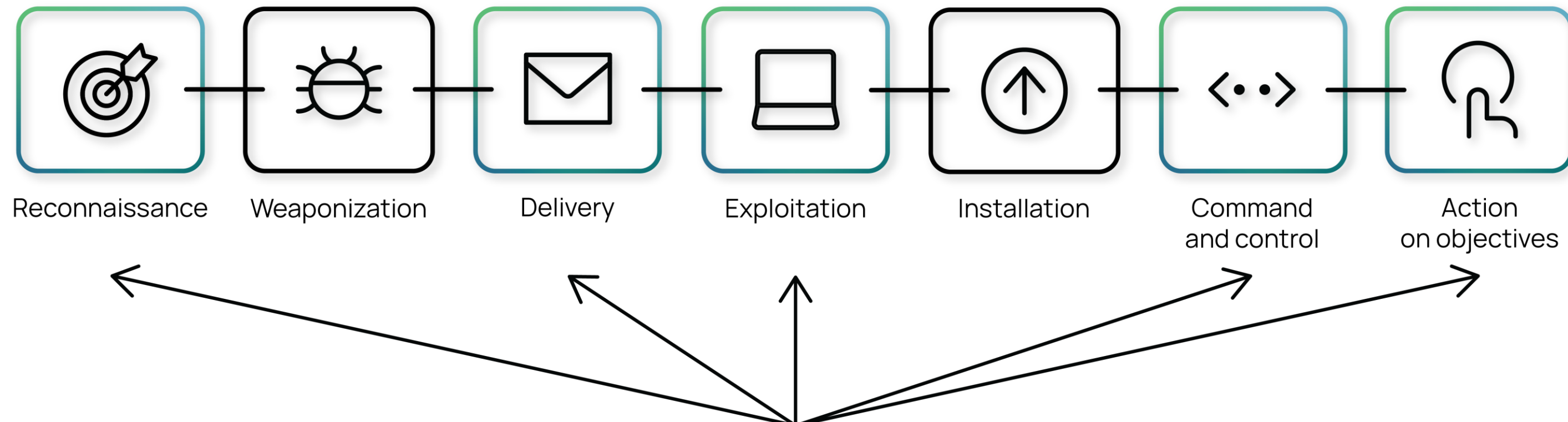
- **Osnovan u 2019.**
- HQ u Zabrze, Poljska
- Web stranica: www.labyrinth.tech
- LinkedIn profil: [link](#)
- YouTube kanal: [link](#)



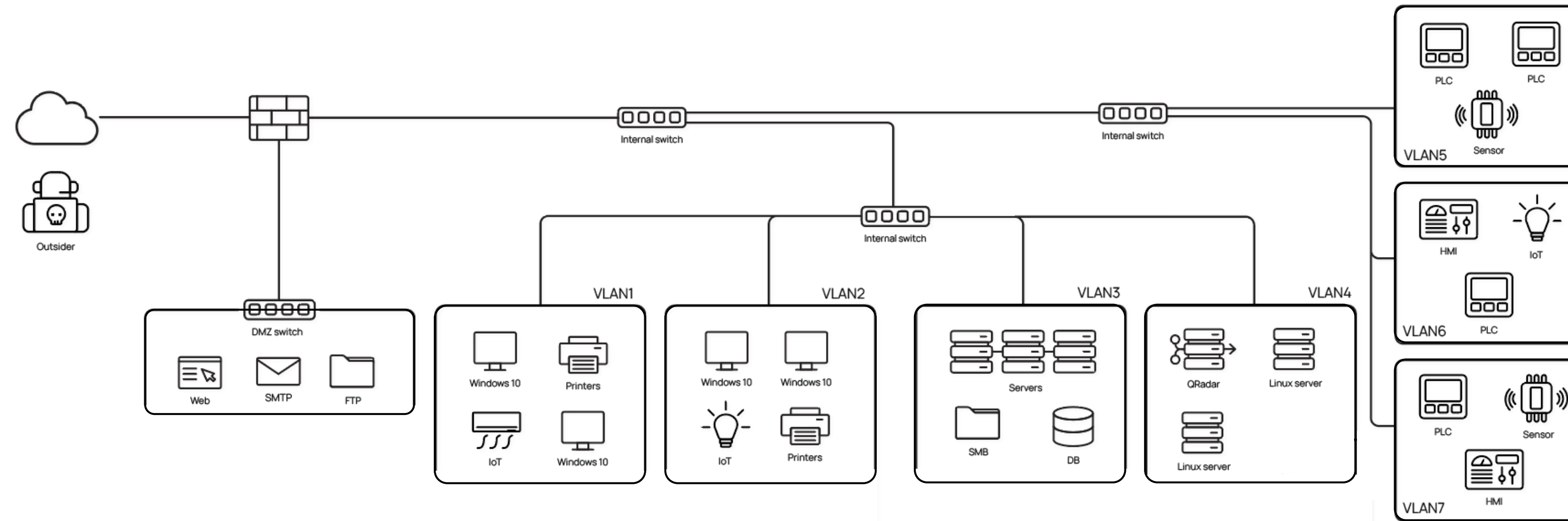
LABYRINTH

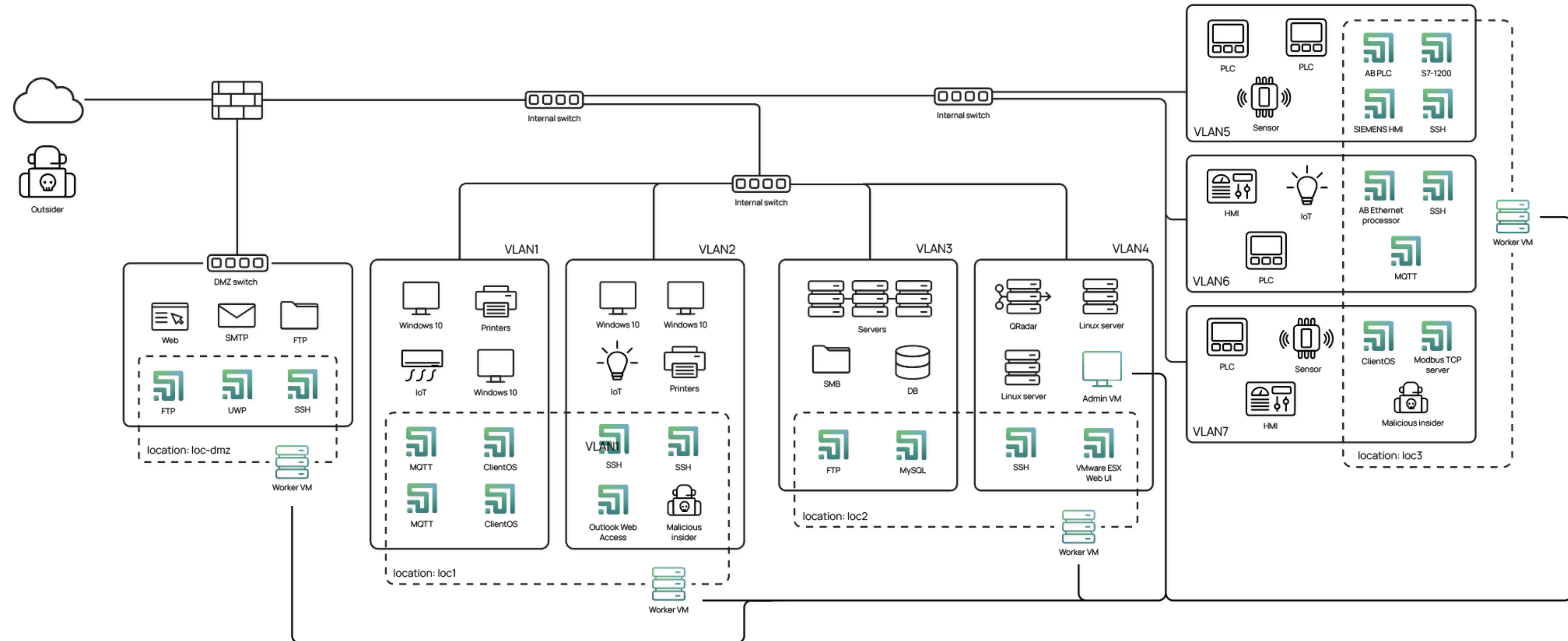
Kibernetički „kill-chain“

Labyrinth je najučinkovitiji u **ranom otkrivanju napada**



LABYRINTH



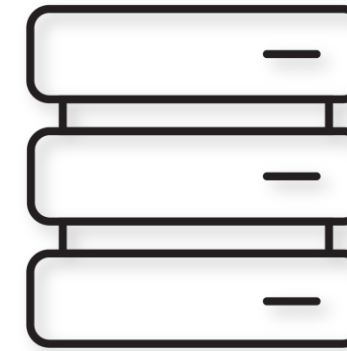


Gradniki platforme



Admin VM (Management Console)

All information collected at the Points is forwarded to the Management Console for incident analysis and response.



Worker VM

The Worker VM is the host that hosts all the Points in Labyrinth. It can operate in multiple VLANs simultaneously.



Point

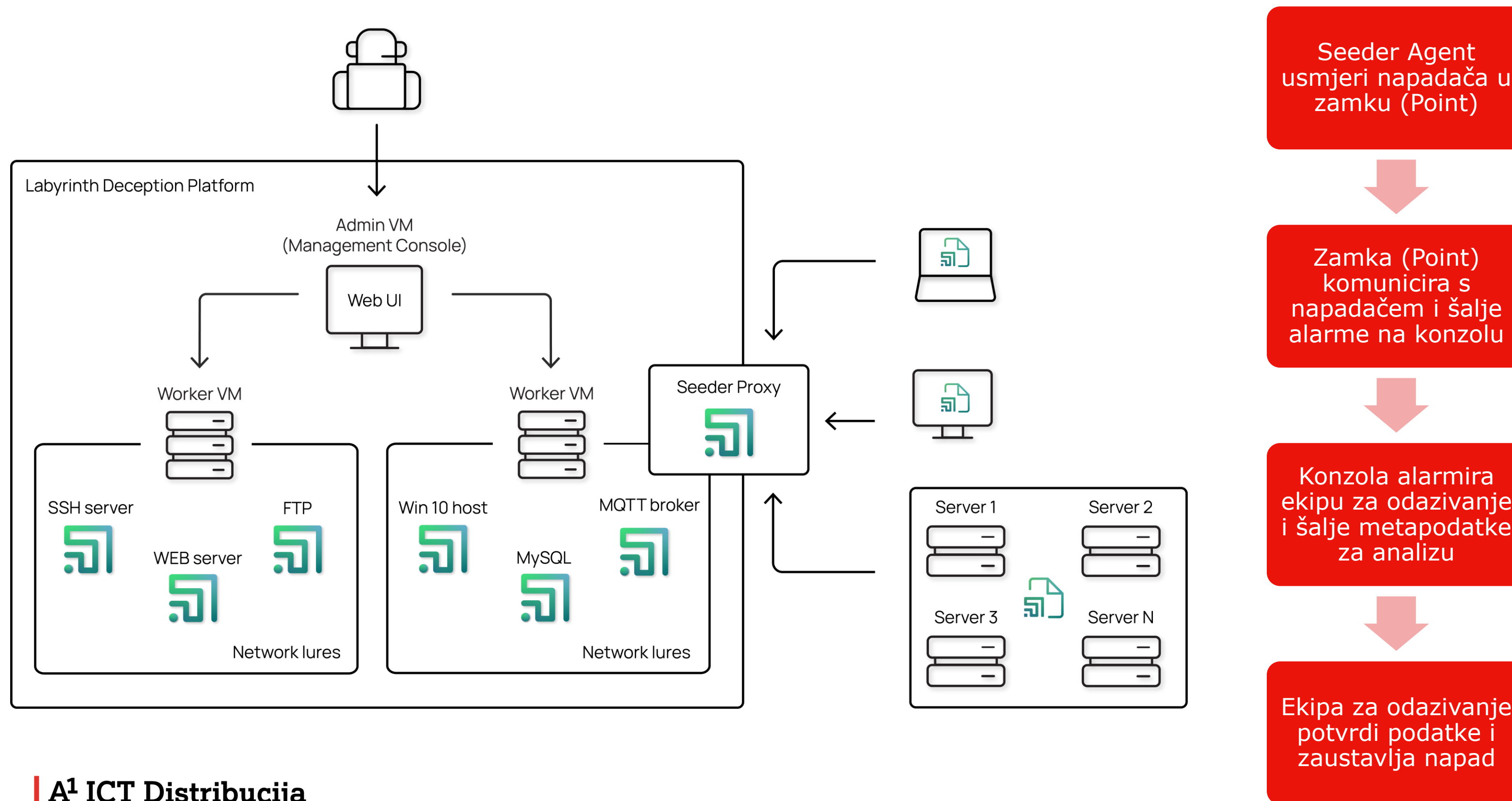
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.



Host with Seeder Agent

Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.

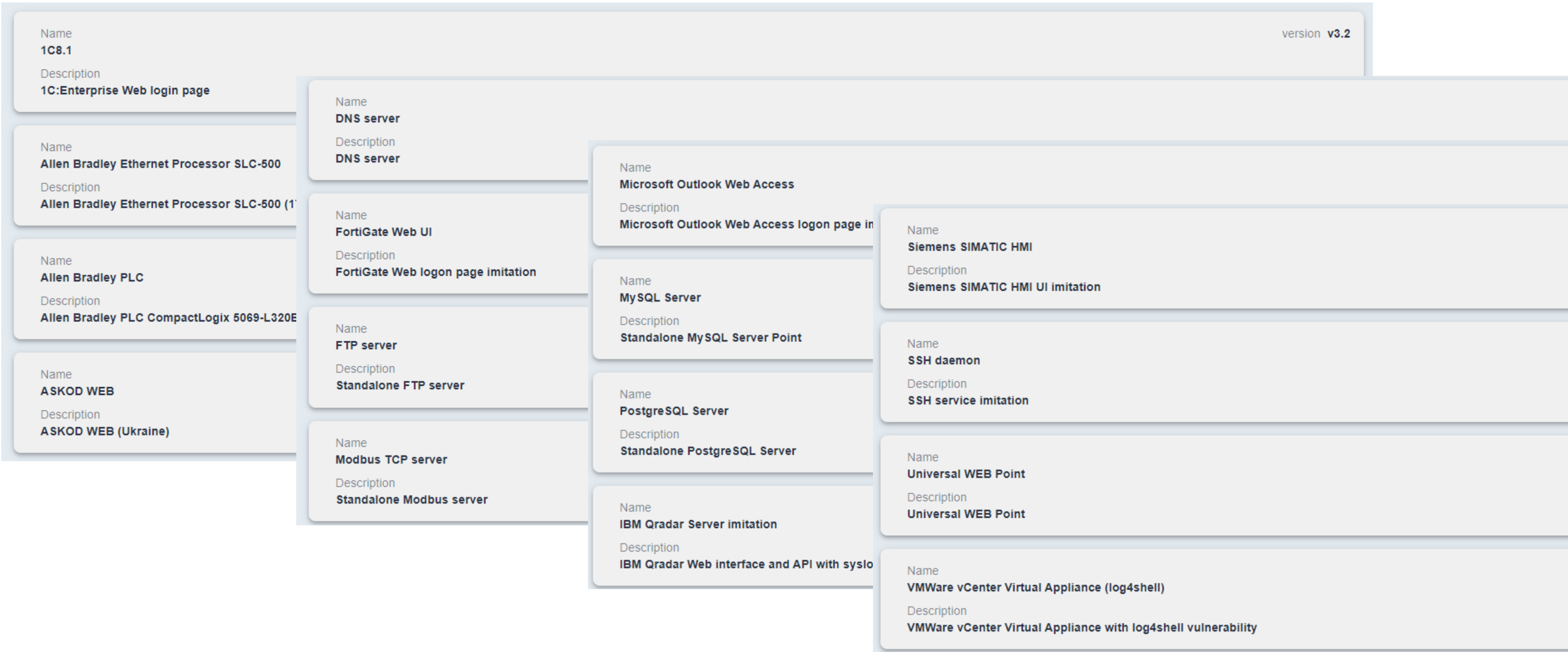
Arhitektura rješenja



Podržane platforme



Deception Point Type Bases

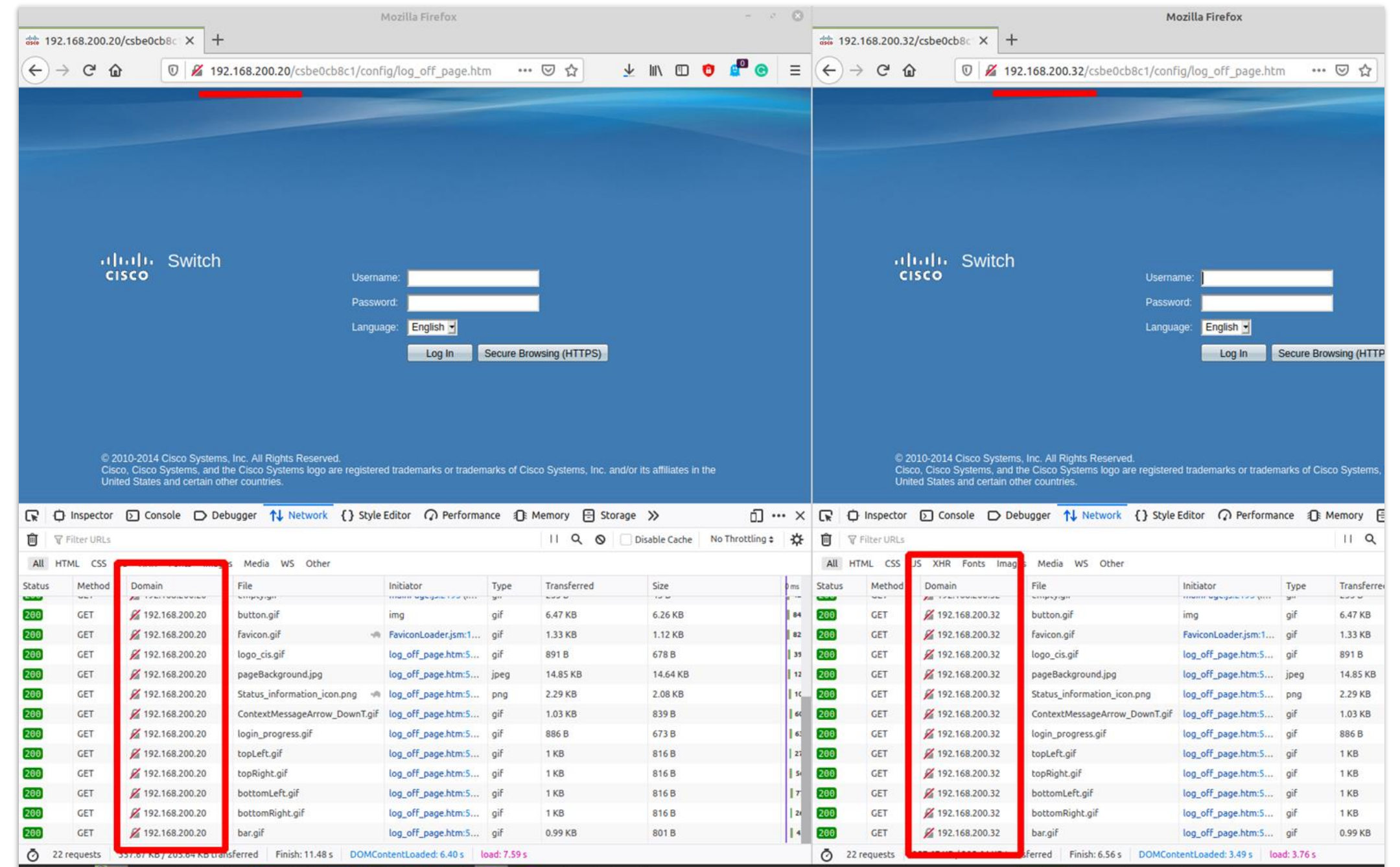


Universal Web Point

The screenshot shows a security dashboard interface. At the top, there is a navigation bar with a dropdown menu set to 'corporate', a shield icon, and a notification bell with '99+'. Below this, a 'Latest alerts' panel is displayed, showing two identical alert entries. Each alert is titled 'Potentially dangerous HTTP method (POST, PUT or DELETE)' and occurred on '2023-04-05'. The first alert is at 17:11:46 and the second at 17:13:22. Both alerts have a source IP of '172.16.254.129'. The first alert's details are: Point ID 'universalweb-c0463b85', Honeynet 'honeynet01', Location 'labdev', Point IP '172.16.72.122', and Point Type 'universalweb'. A red 'open' button is visible below the first alert. The second alert's details are partially obscured but show the same source IP and location. A 'VIEW ALL' link is at the bottom of the alerts panel. To the left of the alerts panel, a network diagram shows a central node with a tooltip. The tooltip contains the following information: Point Type 'universalweb', Hostname 'ophelia', IP Address '172.16.72.116', and status 'running'. The diagram shows several nodes connected by lines, with some nodes having red warning icons.

Universal Web Point

- „Kloniranje“ web aplikacije
- Dodan ranjivosti iz OWASP TOP10
- Radi kao proxy



Primjer alarma


<input type="checkbox"/>	Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason	
<input type="checkbox"/>	H	open	2024-05-16 11:08:58	sshd-3eae0458	10.10.10.1	sshd successful login detected	^

2024-05-16 11:08:58

Alert ID: **54b8ce4b-f9e7-4047-b731-3e02e1010c94**

Alert Reason: **sshd successful login detected**

Destination IP: **10.10.10.71**

 **Download PCAP**
21.31 KB

File Type: pcap
MD5: d0dfc9beff7552a0af6c142c5da6a885

Detajli alarma

DETAILS **EVENTS** ACTIVITY(0)

11:08:58	
2024-05-16 11:08:58	Hostname: - Username: testol1 Message: login attempt [testol1/robot] succeeded
2024-05-16 11:08:58	Hostname: - Message: SSH client hassh fingerprint: 55b7fab6f5d2b485a6773eee233e4a52
2024-05-16 11:08:58	Hostname: - Message: New connection: 10.10.10.1:12033 (10.10.10.71:22) [session: 8495d6e5e930]
2024-05-16 11:08:58	Hostname: - Message: Remote SSH version: SSH-2.0-OpenSSH_7.8 FreeBSD-20180909
2024-05-16 11:08:50	Transport: tcp Source IP: 10.10.10.1 Source Port: 12033 Destination IP: 10.10.10.71 Destination Port: 22 TCP Flags: SYN

Detajli alarma

DETAILS	EVENTS	ACTIVITY(0)
11:08:50	2024-05-16 11:08:58	2024-05-16 11:09:01 Hostname: - Message: CMD: ping 8.8.8.8
11:08:58	2024-05-16 11:08:58	2024-05-16 11:09:16 Hostname: - Message: CMD: sudo su
11:08:58	2024-05-16 11:08:58	2024-05-16 11:09:19 Hostname: - Message: CMD: cd /etc
11:08:58	2024-05-16 11:08:58	2024-05-16 11:09:26 Hostname: - Message: CMD: cat passwd
11:08:58	2024-05-16 11:08:58	2024-05-16 11:09:41 Hostname: - Message: CMD: ps

TCP Flags: **SYN**

Integracije



State	Name	Edit
	CrowdStrike	/
	Cuckoo Sandbox	/
	Fortigate	/
	Microsoft Teams Notifications	/
	IBM-Qradar	/
	Slack Notification	/
	SMTP Notification	/
	Splunk	/
	SIEM Integration (Syslog forwarder)	/
	TheHive	/

A1

LABYRINTH

W / T H[®]
secure

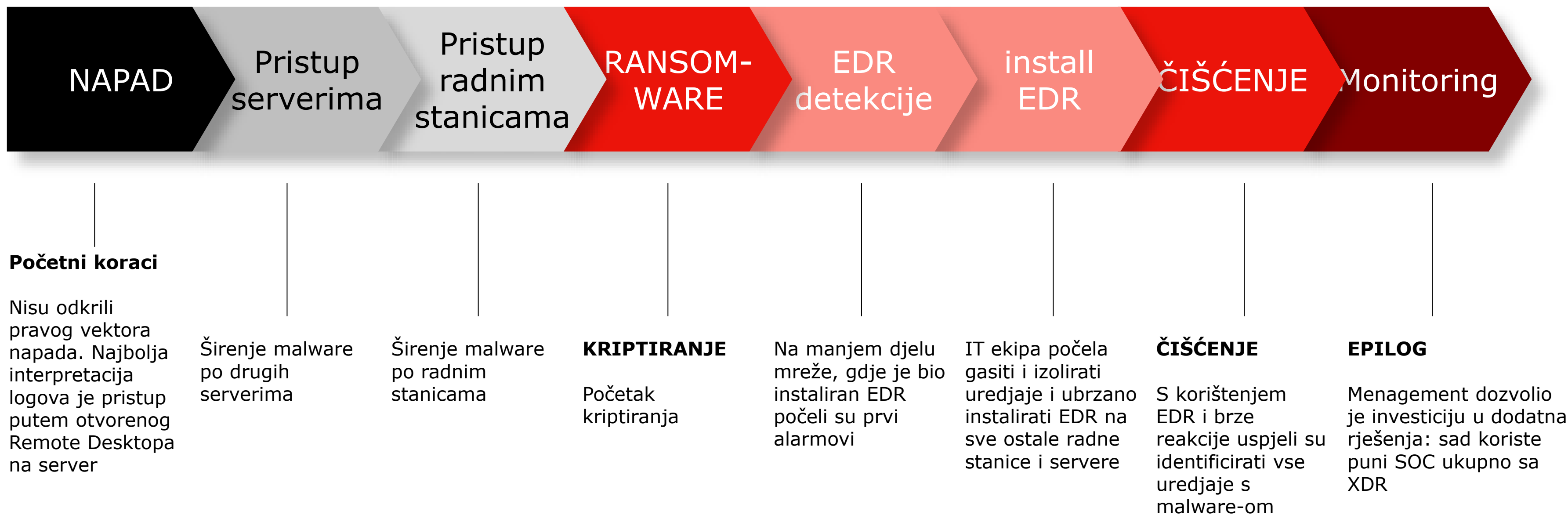
Kako se zapravo tvrtke brane?

Company M

- Proizvodna tvrtka
- 100+ zaposlenih
- Sigurnosna rješenja:
 - Firewall
 - Windows Defender
 - Zaštita emaila za M365
 - Backup s kritičnih servera
- Menagementu prioritet zadovoljstvo zaposlenih:
 - Dopuštene slabe lozinke
 - Malo ili bez ograničenja dostupa internim sistemima
 - Često korisnici imali admin prava
- Aktivno testirali EDR rješenje



Company M – incident



Company

Ne znamo koje alate i koji korisnici su bili kompromitirani.

Prvi indici o problemima tek kad se usporio server.



Nemamo podataka o početku, koje bi koristili za promjenu sigurnosnih pravila na svim rješenjima.

Širenje malware po drugih serverima

Širenje malware po radnim stanicama

KRIPTIRANJE
Početak kriptiranja

Na manjem djelu mreže, gdje je bio instaliran EDR počeli su prvi alarmovi

IT ekipa počela gasiti i izolirati uređaje i ubrzala instalirati EDR na sve ostale radne stanice i servere

Prvo su trebali imati velike probleme, kako bi promijenili to što su znali već prije.

reakcije uspjeli su identificirati vse uređaje s malware-om

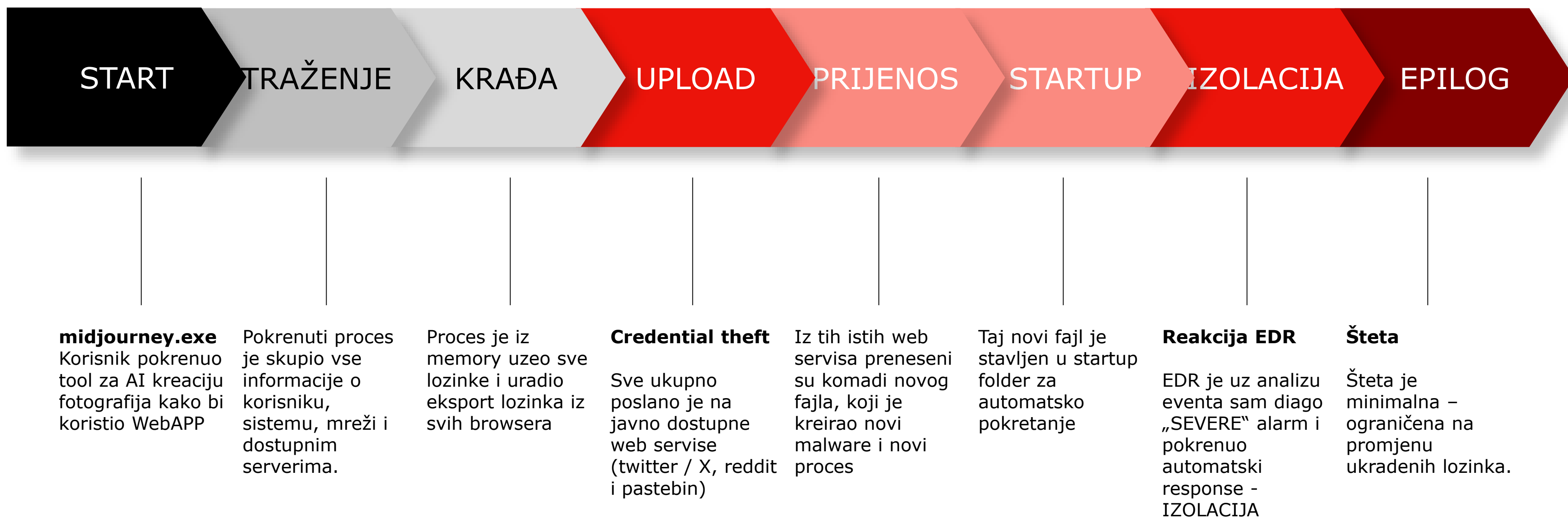
SILOG
management dozvolio investiciju u dodatna rješenja: sad koriste puni SOC ukupno sa XDR

Company K

- Usluge
- 200+ zaposlenih
- Sigurnosna rješenja:
 - Firewall
 - Zaštita emaila
 - Backup
 - Napredna zaštita radnih stanica s EDR
 - Kontrola mreže s postavljenim mamcima
 - Ograničena prava korisnika
 - Redoviti pen-testovi
 - Edukacija zaposlenih na području cyber security higijene
- Management podržava investicije u cyber security



Company K – incident



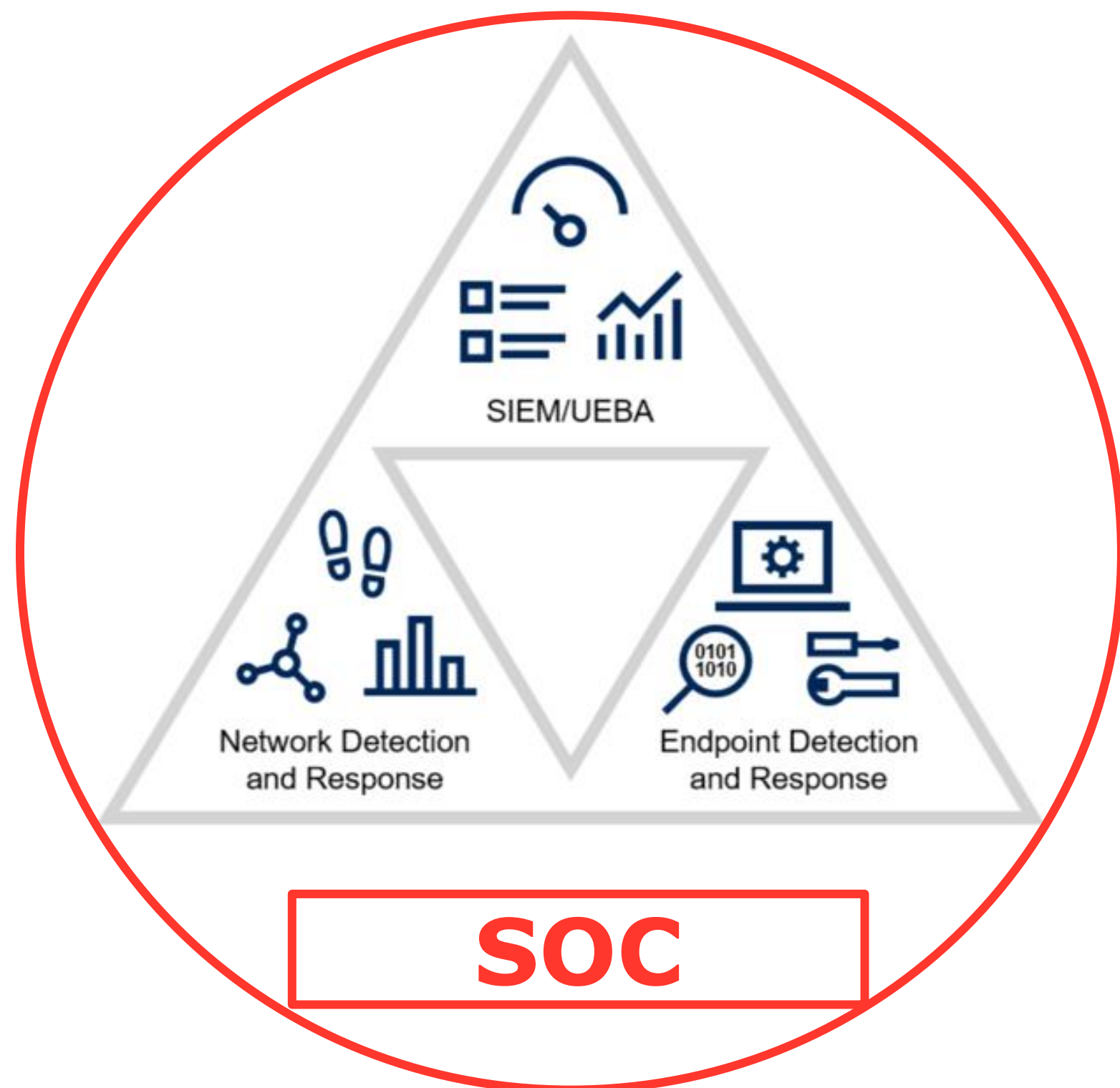
Usporedba incidenta



Usporedba incidenta



Ključ je u vidljivosti



Detekcije na mreži

Identifikacija sumnjivih mrežnih aktivnosti s monitoringom prometa za unutarnje i vanjske prijetnje

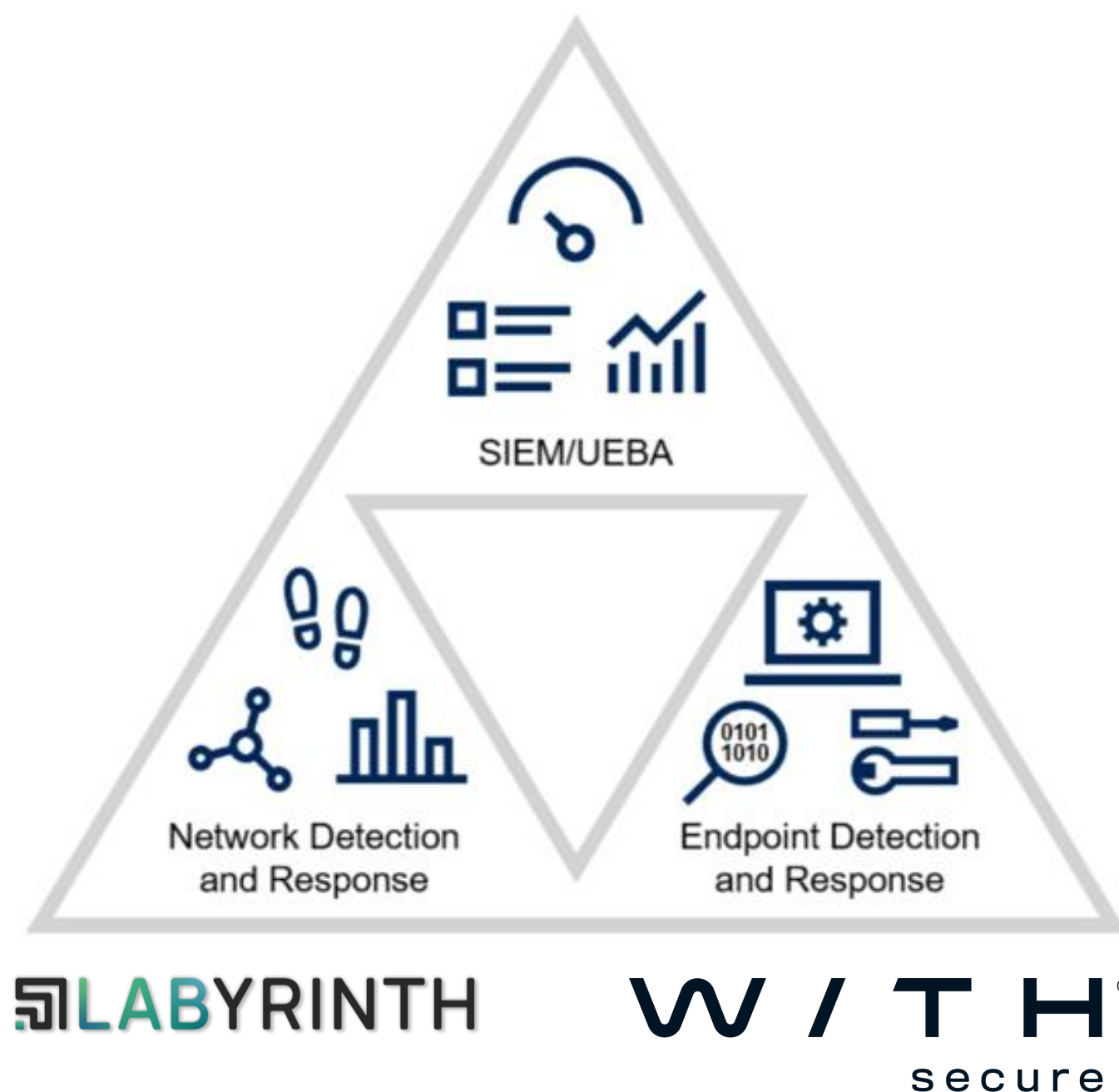
Detekcije na radnim stanicama i serverima

Praćenje pokretanja procesa i otvaranje fajlove, aktivacije mrežnih konekcija, aktivnosti u memoriji sistema

SIEM/UEBA:

Skupljanje, analiza i korelacija informacija i aktivnosti svih sistema (sigurnost, infrastruktura, korisnici)

Ključ je u vidljivosti



Detekcije na mreži

Identifikacija sumnjivih mrežnih aktivnosti s monitoringom prometa za unutarnje i vanjske prijetnje

Detekcije na radnim stanicama i serverima

Praćenje pokretanja procesa i otvaranje fajlove, aktivacije mrežnih konekcija, aktivnosti u memoriji sistema

SIEM/UEBA:

Skupljanje, analiza i korelacija informacija i aktivnosti svih sistema (sigurnost, infrastruktura, korisnici)

LABYRINTH

W / T H[®]
secure

DEMO

Europska rješenja za cybersecurity

Discover
cybersecurity
solutions from
Europe with
Cyberhive



Cyberhive EUROPE® offers a ui tool specialised to promote and cybersecurity solutions beyond your local borders. Increase your digital business resilience today, discover the Cyberhive Matrix and build towards a secure and stronger Europe!

[Explore solutions](#)



Učinkovita i jednostavna rješenja



Value Added Distributor

- **Partnerski program**
- Široka mreža partnera u Adria regiji
- **Prodajna i tehnička** podrška partnerima
- Organizacija **tehničkih** treninga
- Promocija brandova na eventima



Što slijedi?

- **Testirajte naša rješenja**
 - **Besplatan POC**
 - **Podrška i edukacija uz POC**
 - **Pomoć uz prodajne aktivnosti**
 - **Pomoć uz implementacije**
 - **Tehnički trening**

KONTAKTIRAJTE NAS:

- **Web stranica:** <https://varnostne-resitve.si>
- **Pišite nam na** ict-partners@A1.si



A1

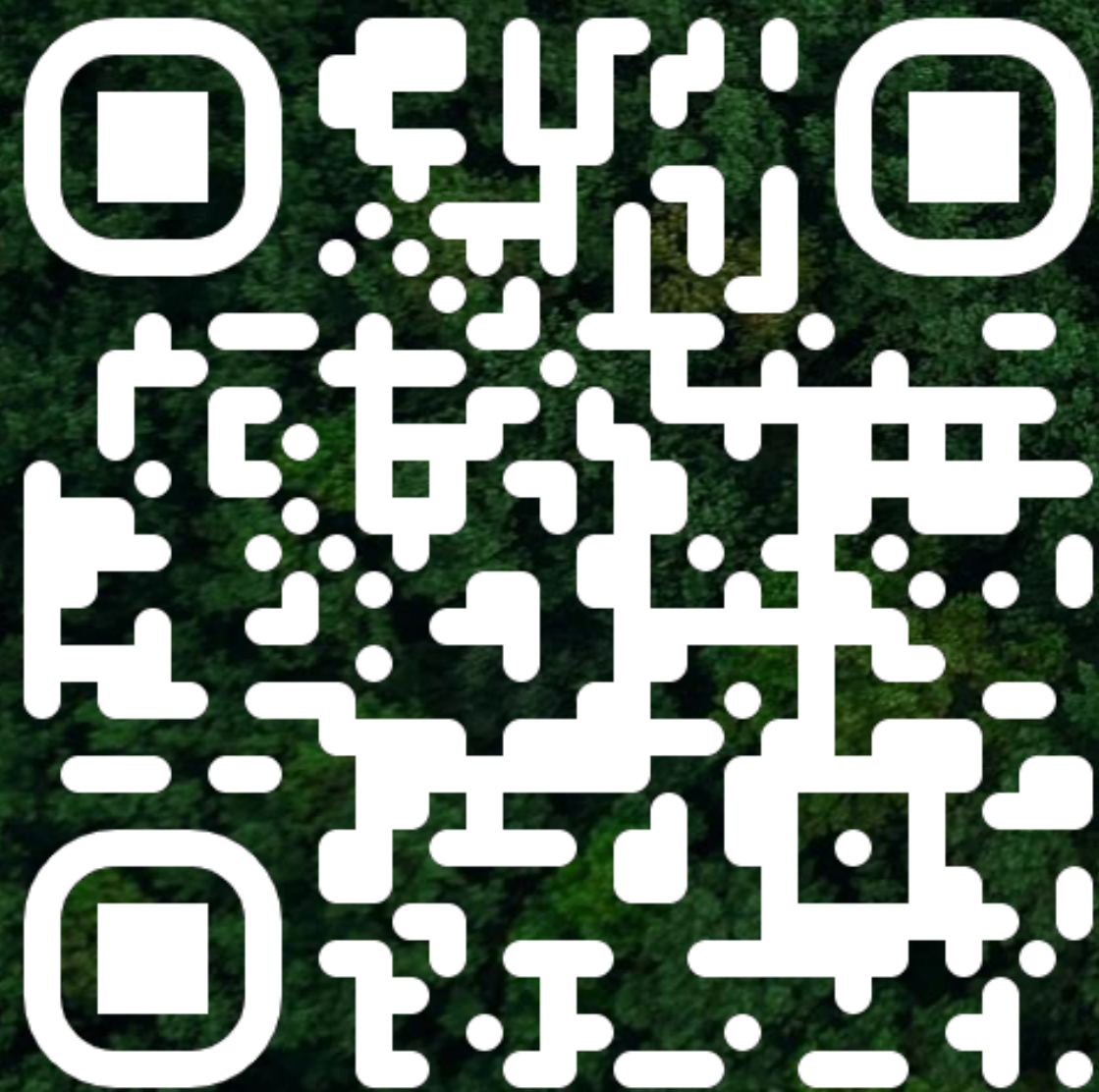
Pitanja?



A¹ ICT Distribucija

LABYRINTH

W / T H[™]
secure



HVALA NA POZORNOSTI!

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

ict-partners@A1.si