Formerly
F-Secure Business

F-Secure Business is now **WithSecure**

Protecting businesses in 100+ countries

A1 ICT Distribucija

WITH secure

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

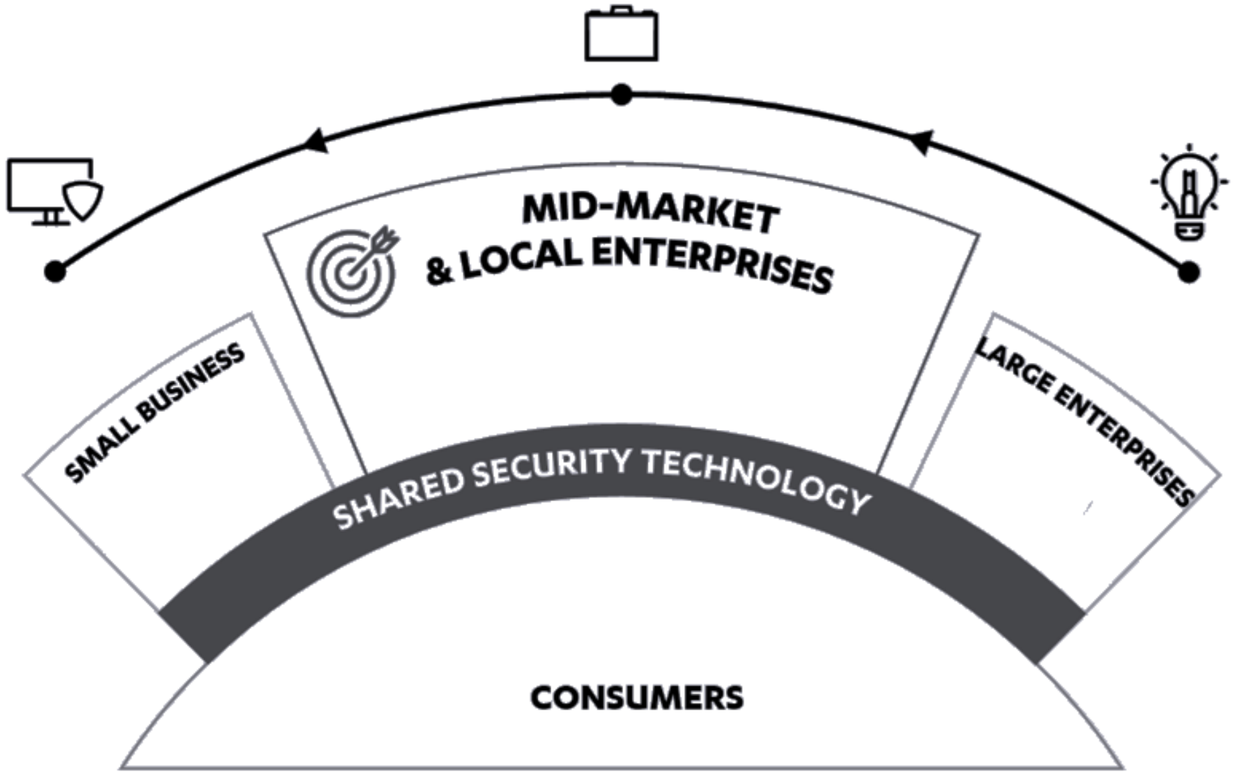
35
Years of history

€143m
Revenue 2023

Listed
On the NASDAQ OMX Helsinki Ltd

WITH secure™ A1

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



We are targeting the corporate mid-market and local enterprises

A1 ICT Distribucija

WITH secure

„Next-gen“ for 20+ 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

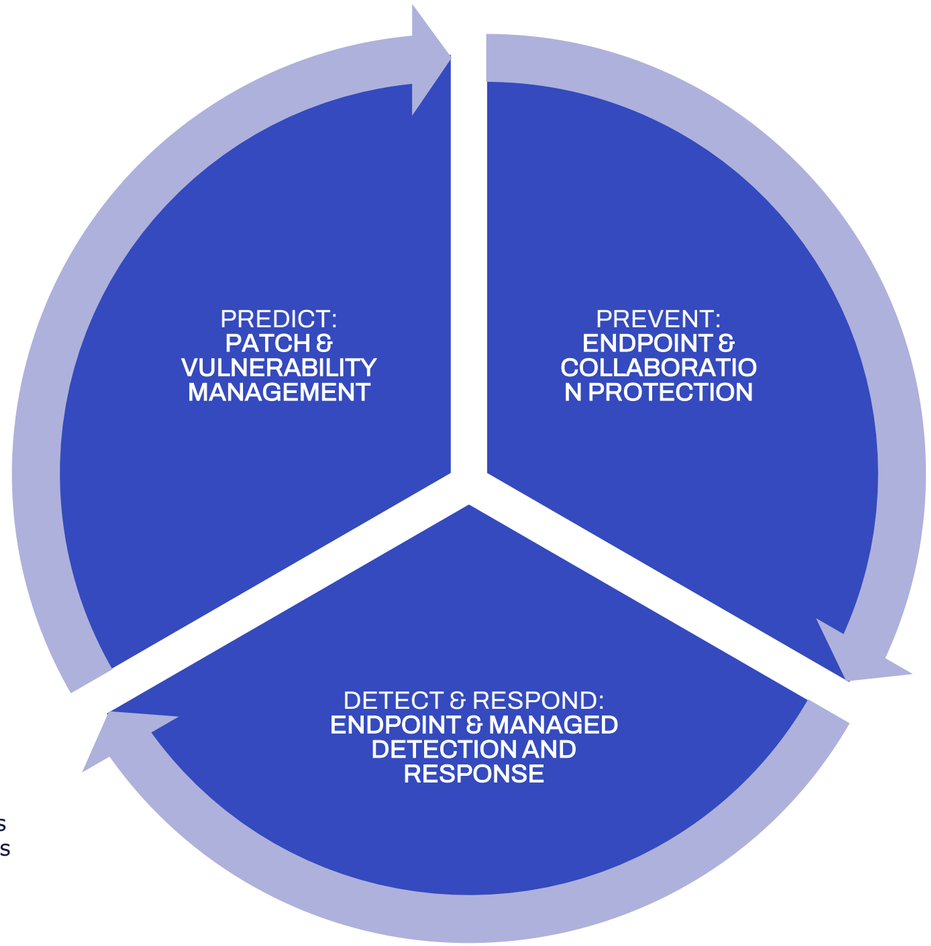
DeepGuard connected to F-Secure Security Cloud for new cloud-based analysis modes.

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



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 prot
independ

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

Rasmus Saxén

Researcher, WithSecure

WithSecure™ named a 202
Customers' Choice for V

ction

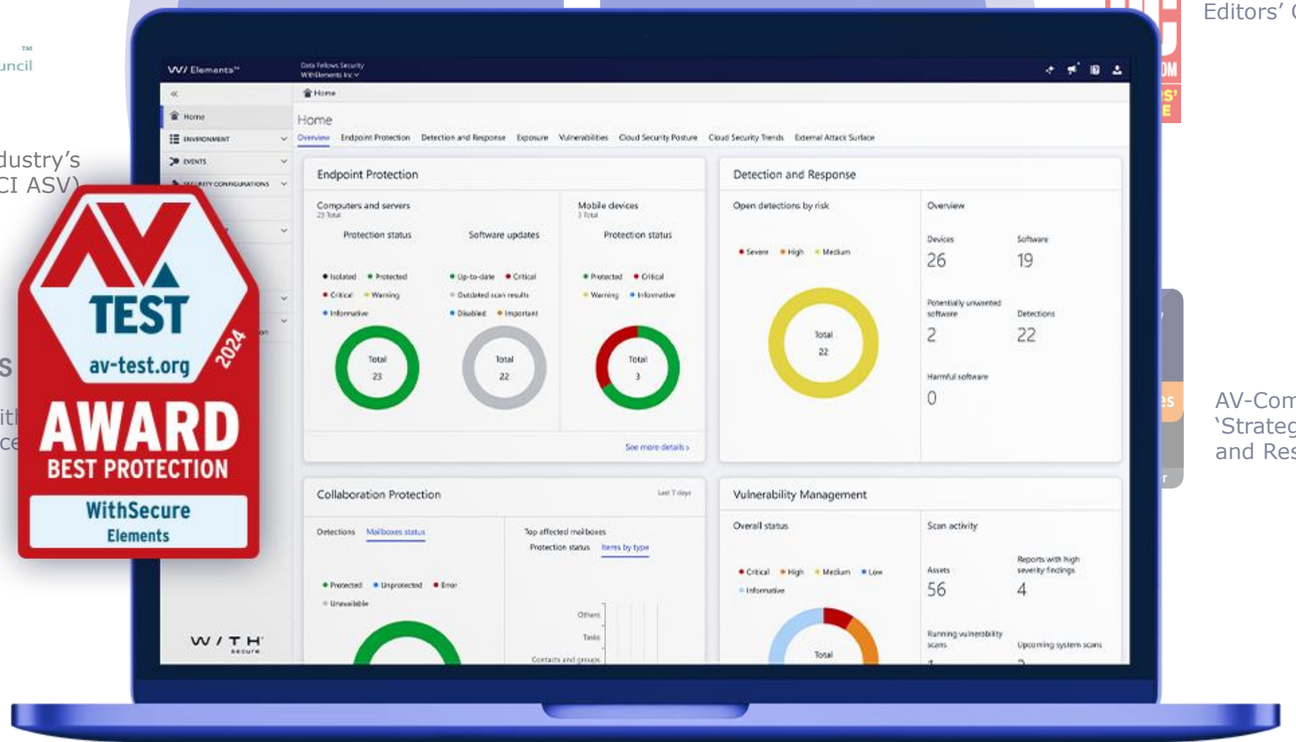
APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT

APPROVED CORPORATE ENDPOINT PROTECTION MACOS

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

MANAGEMENT

N PROTECTION



WithSecure™ Elements is PC Mag Editors' Choice 2022

PCI Security Standards Council

APPROVED SCANNING VENDOR

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

SC 2021 awards EUROPE WINNER

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

MITRE ENGENUITY | ATT&CK® Evaluations

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

AV-TEST av-test.org 2024 AWARD BEST PROTECTION WithSecure Elements

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

A1 ICT Distribucija

WITH secure

A1

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!

A1 ICT Distribucija

Gartner

WITH secure

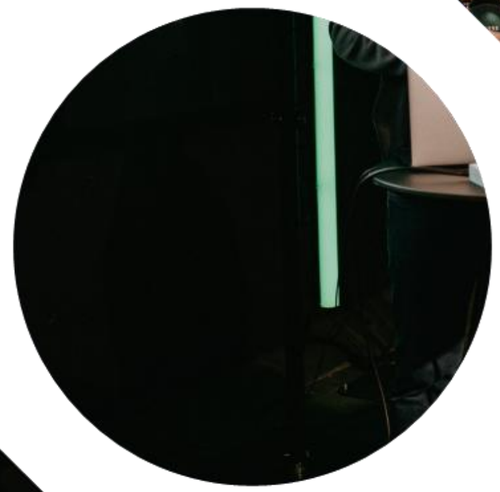
A1

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



A1 ICT Distribucija

Gartner

WITH secure

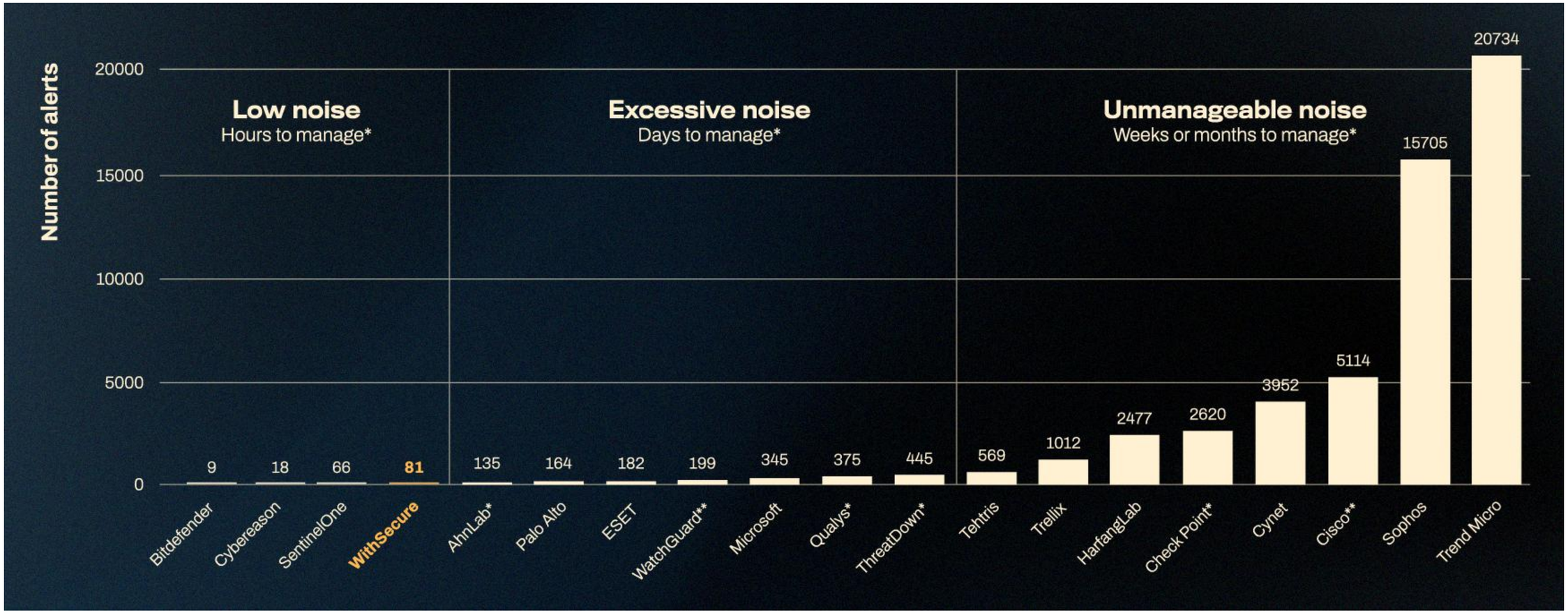
A1

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



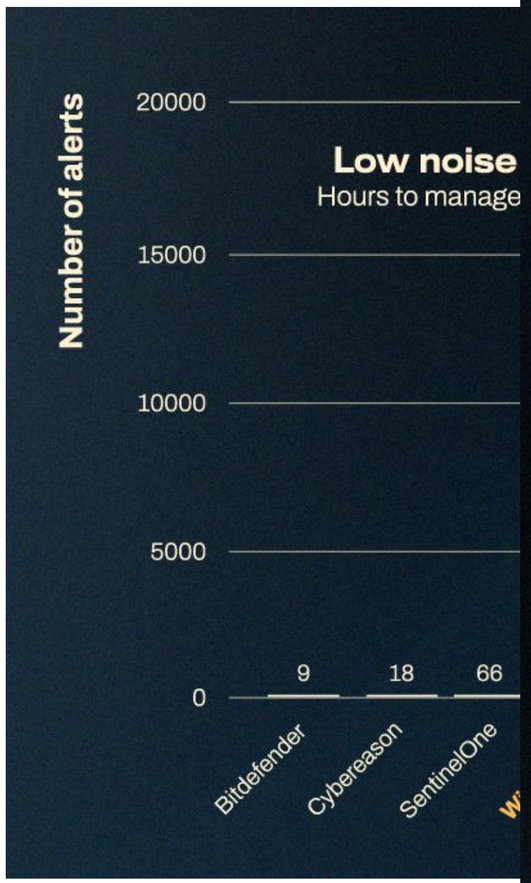
A1 ICT Distribucija

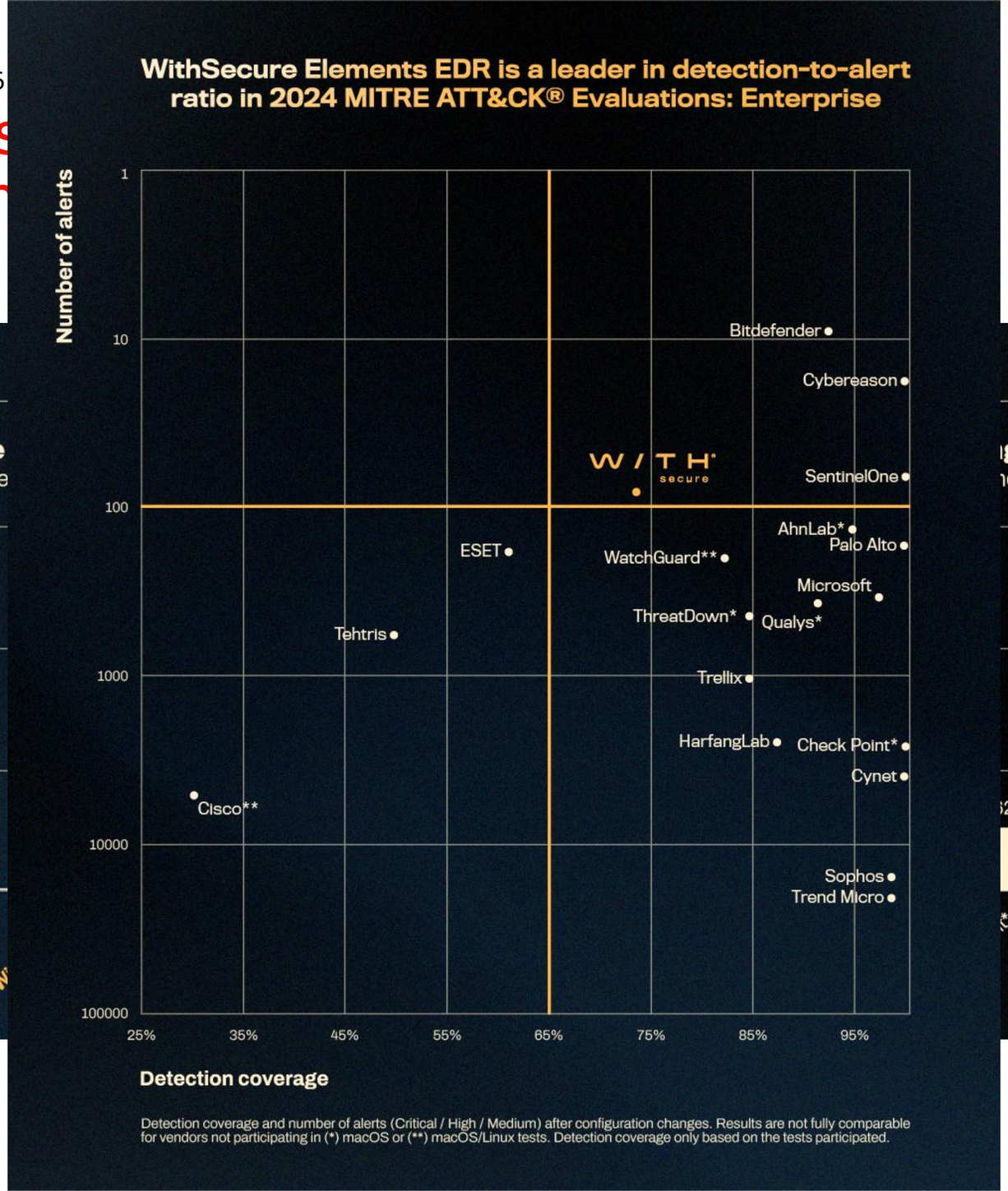
MITRE | ATT&CK®

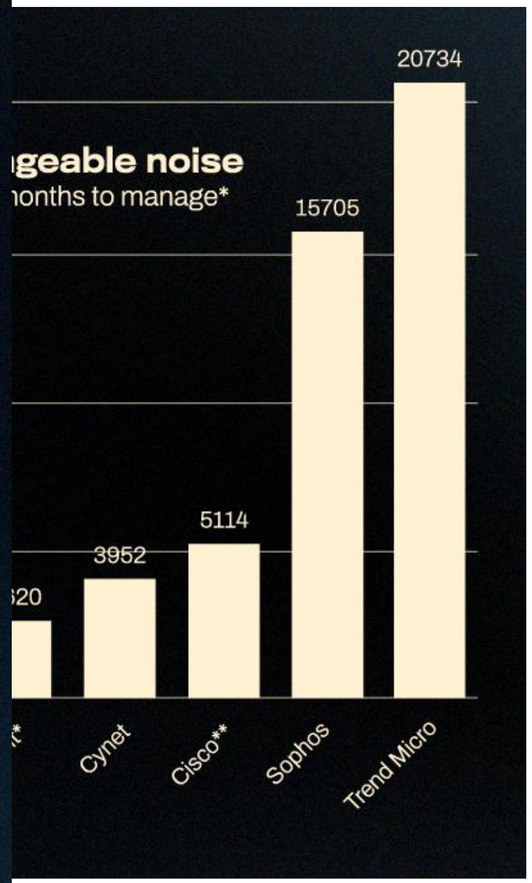
WITH secure

A1

WithSecure sets
alert ratio for th







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.

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

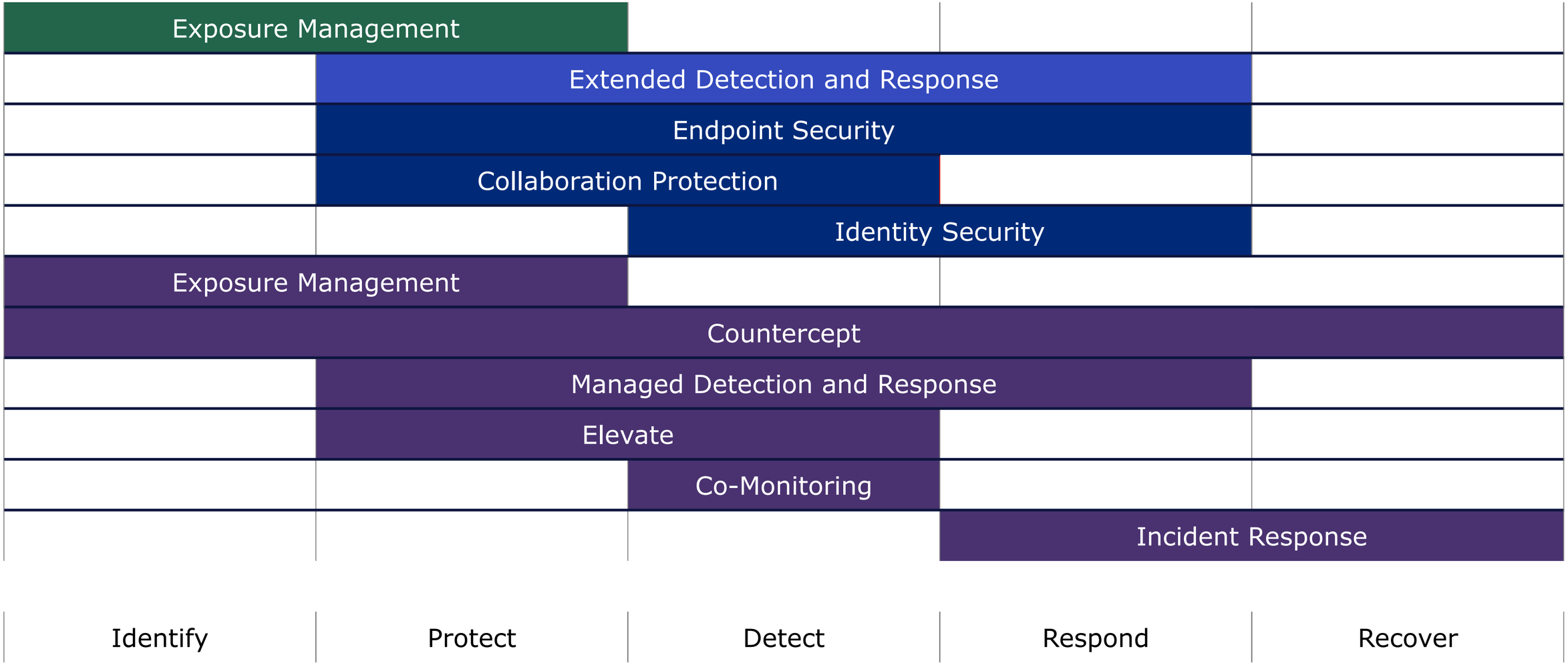
- Endpoint Security
- Identity Security
- Collaboration Protection

Co-Security Services

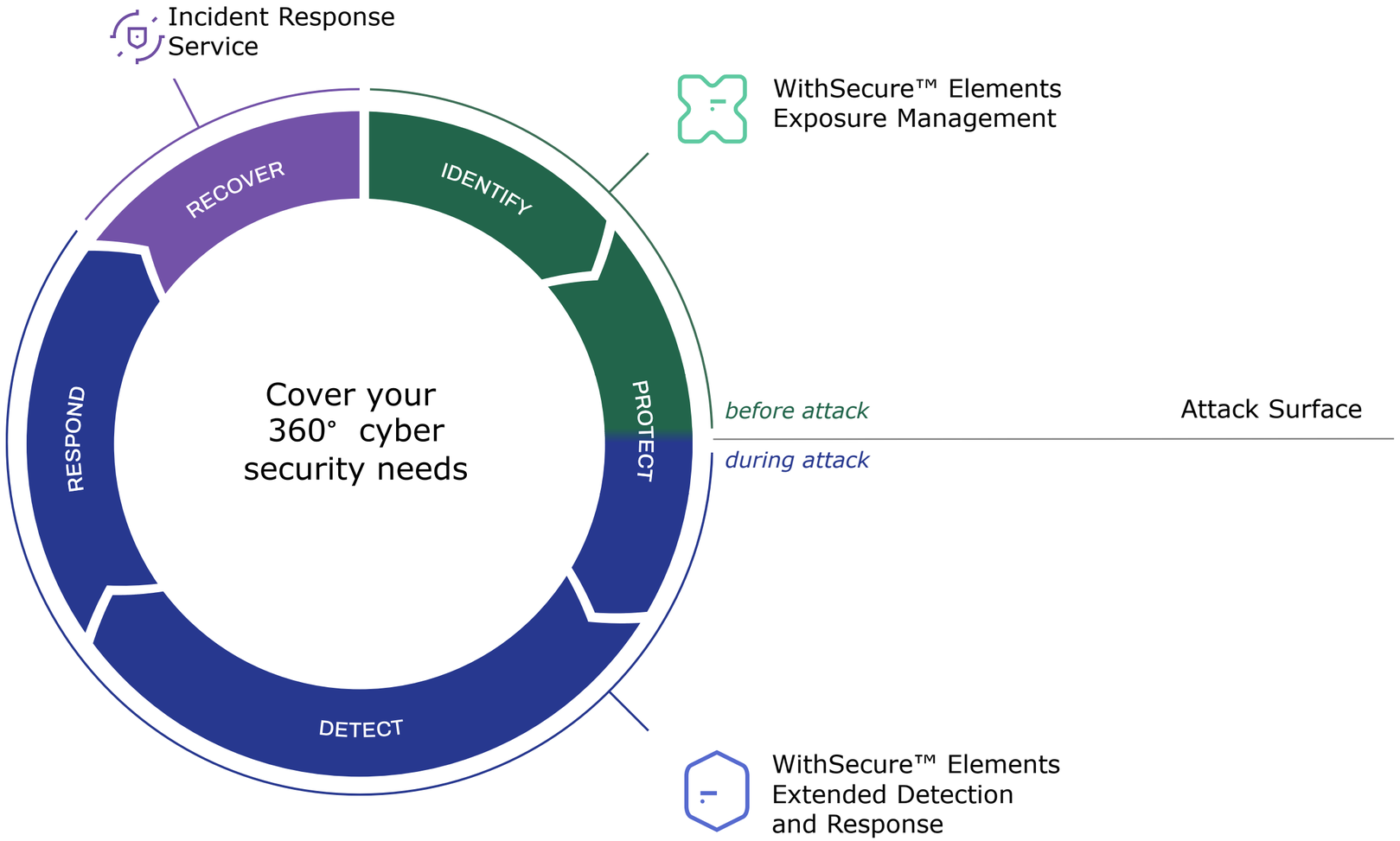
- Elevate
- Co-Monitoring
- Managed Detection and Response
- Incident Response
- Exposure Management
- Countercept

WithSecure™ Support Services

WithSecure™ Elements Cloud - NIST



WithSecure™ Elements Cloud - NIST



A1 ICT Distribucija

WITH secure

WithSecure Elements Endpoint Protection

EPP for Windows, Linux, Mac, Android, iOS

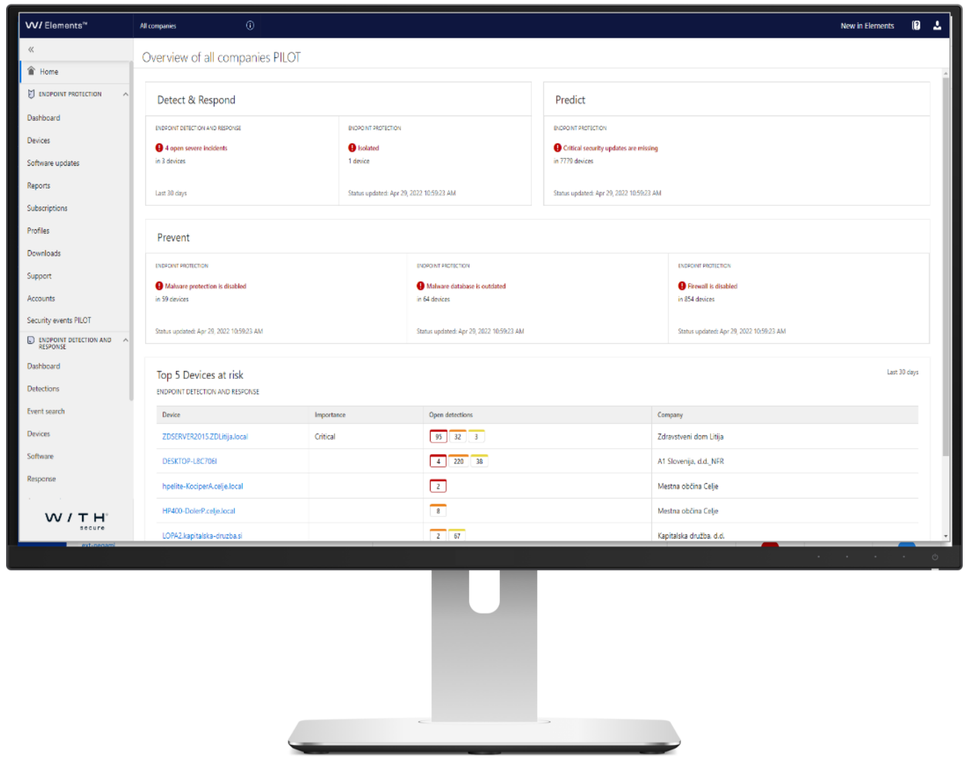
A1 ICT Distribucija

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



CENTRAL DEPLOYMENT

INCIDENT MANAGEMENT

SECURITY MONITORING

GRAPHICAL REPORTING

PATCH MANAGEMENT

MANAGEMENT HIERARCHY

AUTOMATIC SECURITY UPDATES

MANAGEMENT API

MANAGED FIREWALL

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

W / T H secure

Elements for Servers

MULTI-ENGINE ANTI-MALWARE

CENTRALLY MANAGED FIREWALL

THREAT INTELLIGENCE

PATCH MANAGEMENT

ADVANCED WEB PROTECTION

DEVICE CONTROL

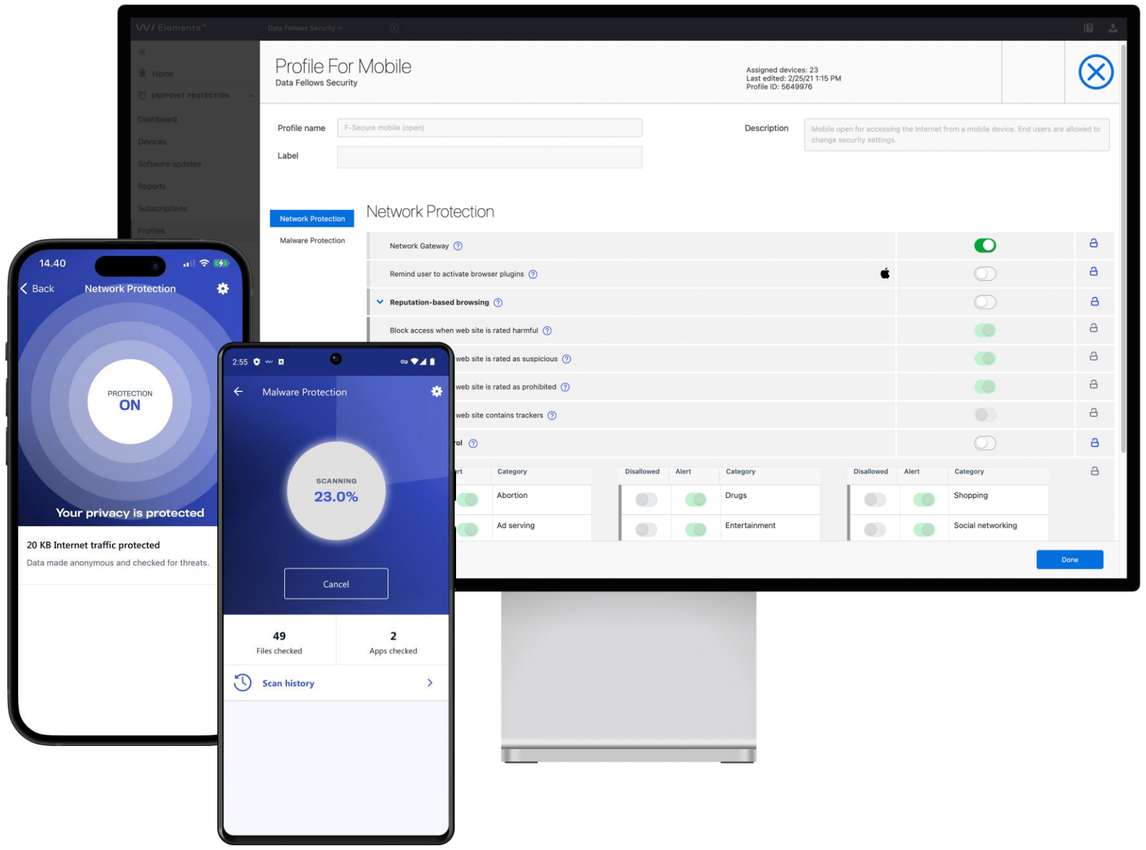
DEEPGUARD 6

APPLICATION CONTROL*

DATAGUARD*

* = PREMIUM FEATURE

Elements for Mobile



NETWORK PROTECTION

SECURITY CLOUD

APPLICATION PROTECTION

BROWSING PROTECTION

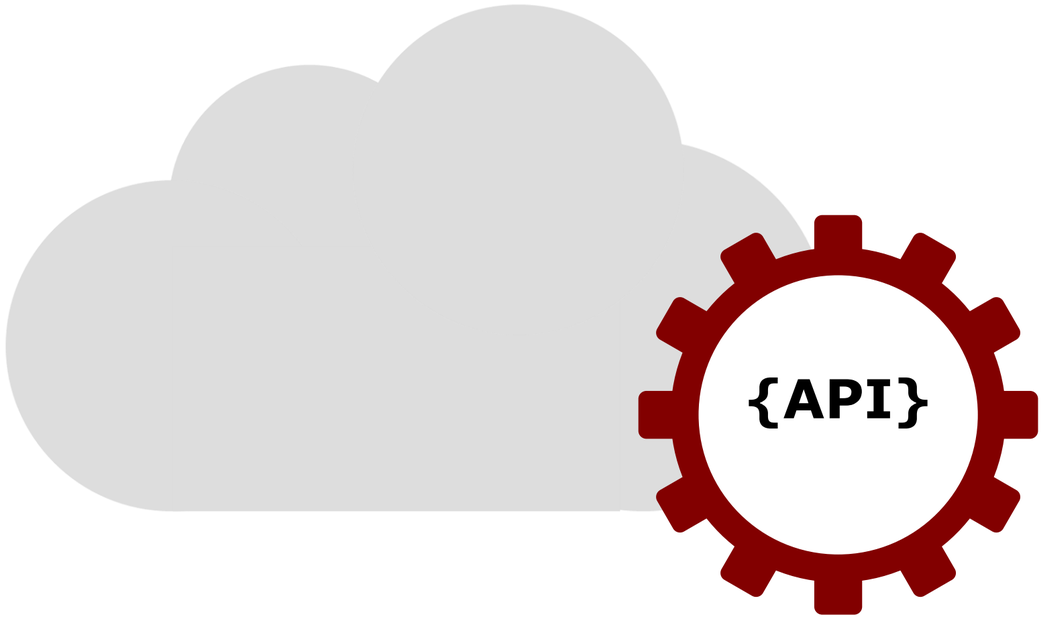
TRACKING PROTECTION

MDM SUPPORT

A1 ICT Distribucija

WITH secure

Elements EPP API



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

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

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

A1 ICT Distribucija

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

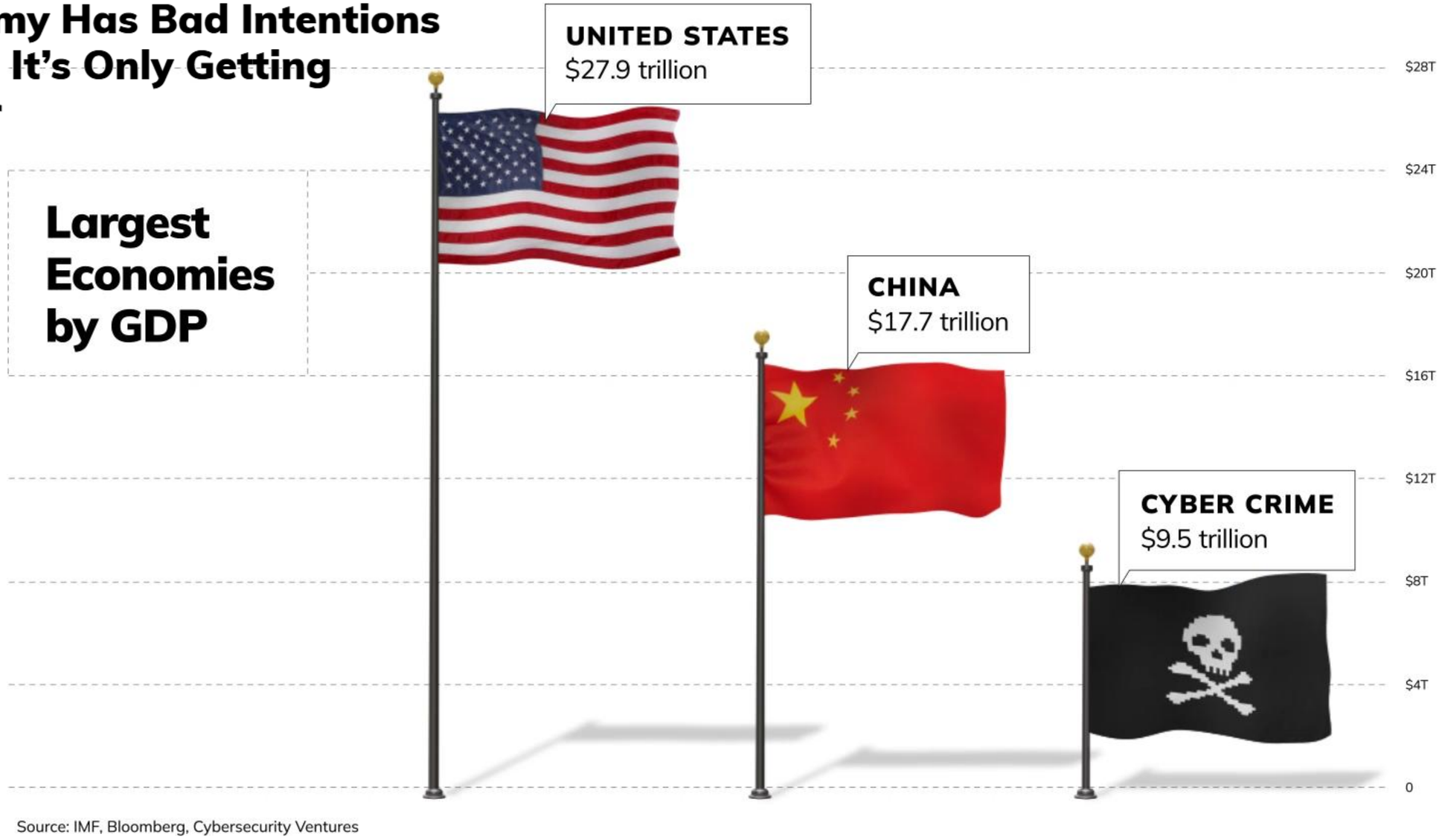
With Bitcoin, criminals can easily receive money without getting caught

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



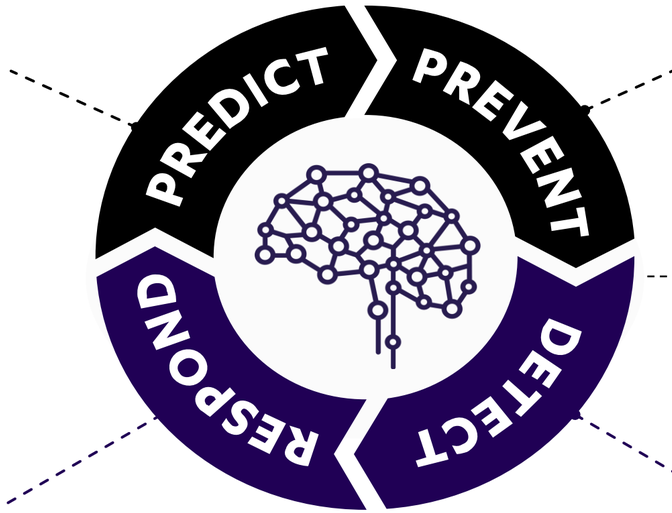
Vir: https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger

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

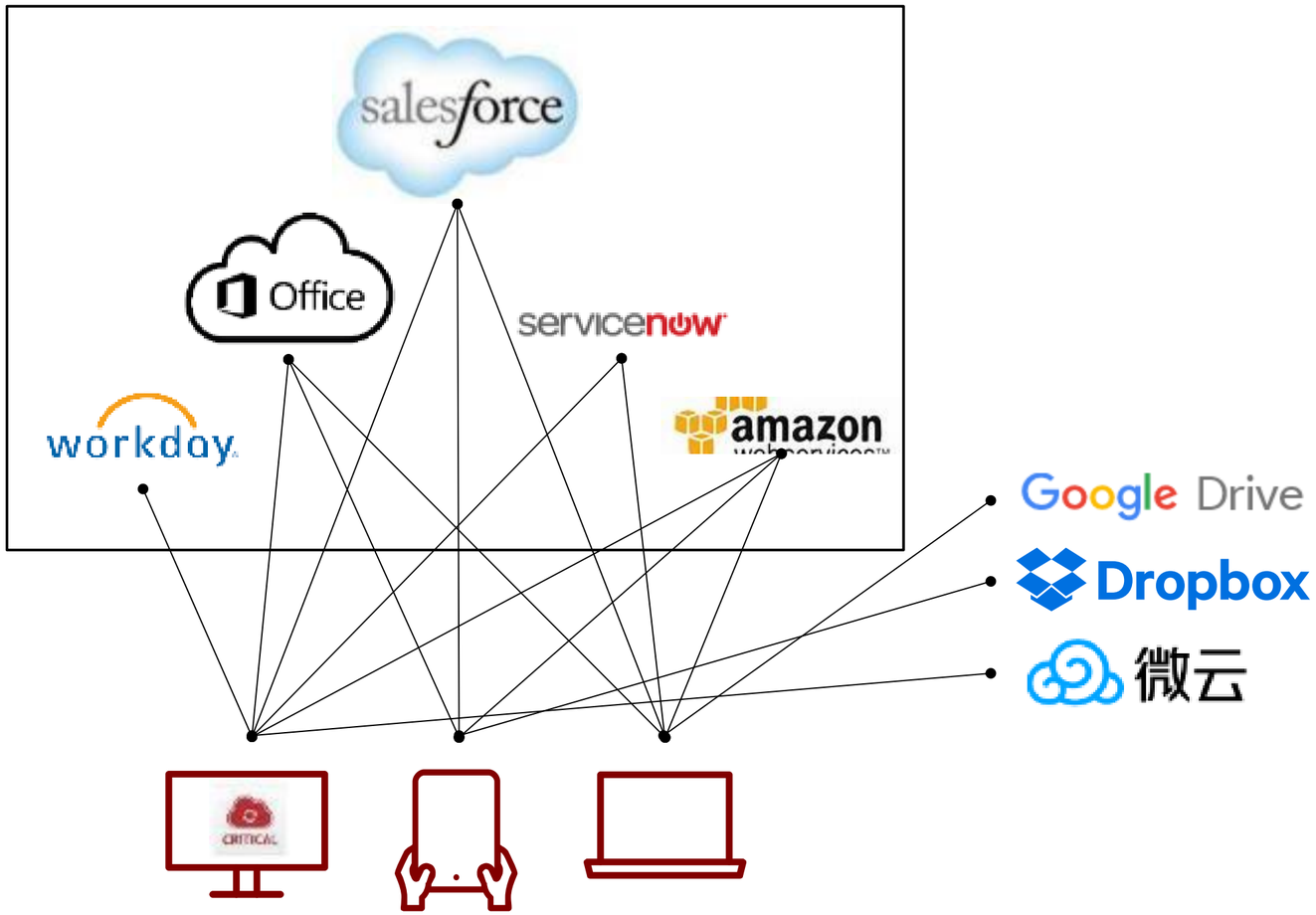
React to breaches, mitigate the damage, analyze and learn

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.

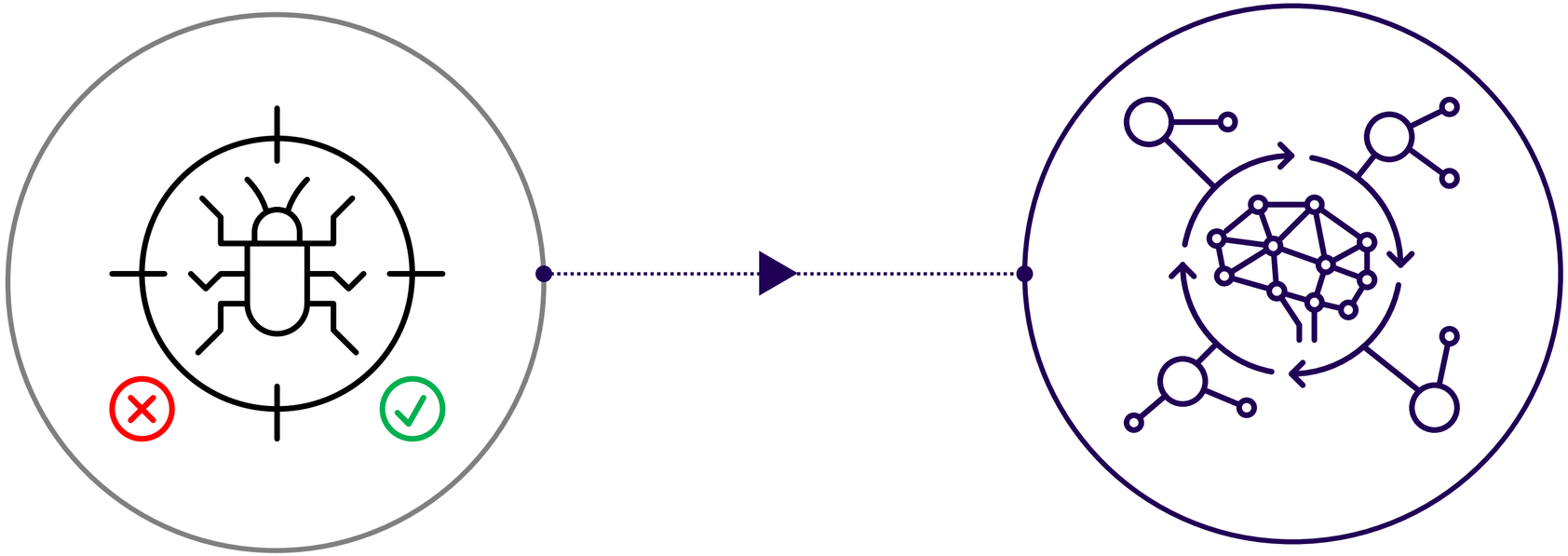
Modern IT Infrastucture Increases Exposure To Threats



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

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

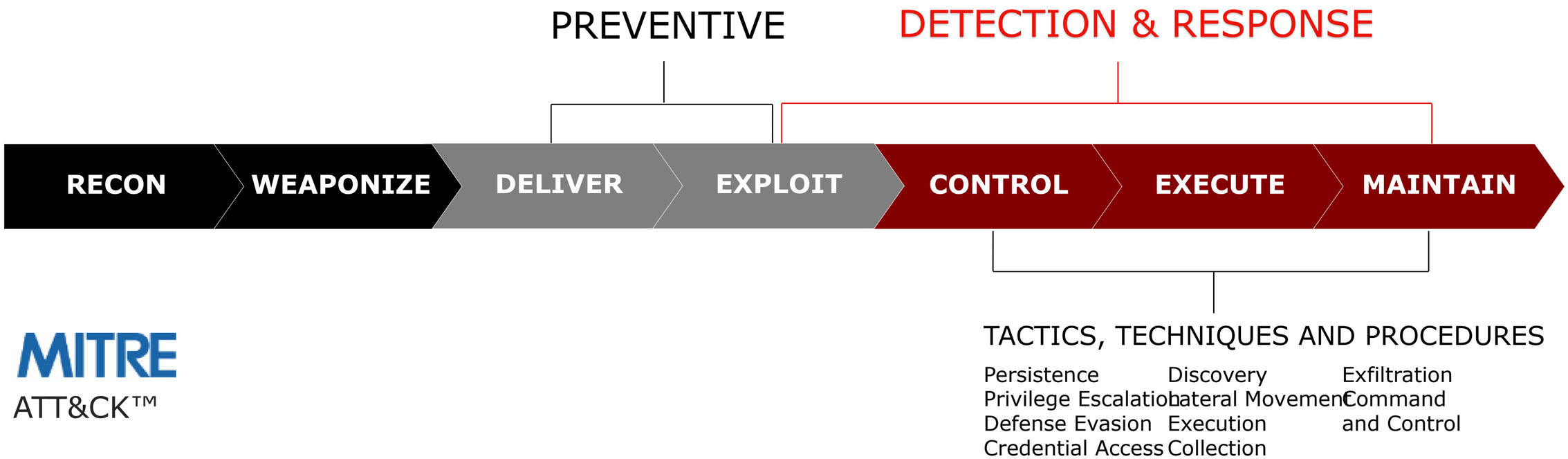
Call For A Paradigm Shift



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

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

Answering The Paradigm Shift



MITRE ATT&CK™

WITH secure

Solution packages

Features	EPP	EPP Premium	EPP Premium with EDR
Central deployment with silent updates	✓	✓	✓
Multi-engine anti-malware	✓	✓	✓
Heuristic & behavioural analysis with DeepGuard	✓	✓	✓
Integrated Patch Management	✓	✓	✓
SIEM/RMM support	✓	✓	✓
Device Control	✓	✓	✓
Centrally managed firewall	✓	✓	✓
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			✓

NOTE: Features may differ with operating systems

Detection & Response In Action

YOUR INFRASTRUCTURE

Workstations Laptops Servers Swarm Intelligence

EVENTS

REAL-TIME BEHAVIORAL ANALYSIS @WITHSECURE'S EDR BACKEND

Expert Insights

Global Threat Intel

Broad Context Detections

Data enrichment & correlation

AI analytics

Data analytics

DETECTION

ELEVATE TO WITHSECURE

Your own IT team

OR

WithSecure Partner/MSP

REMEDIATION

Delete Services

Delete scheduled tasks

Delete Files, Folders

Delete Registry keys

Scan Malware

Inform users

CONTAINMENT

Isolate hosts

Kill processes

Control applications

INVESTIGATION

Retrieve process lists

Retrieve files, folders

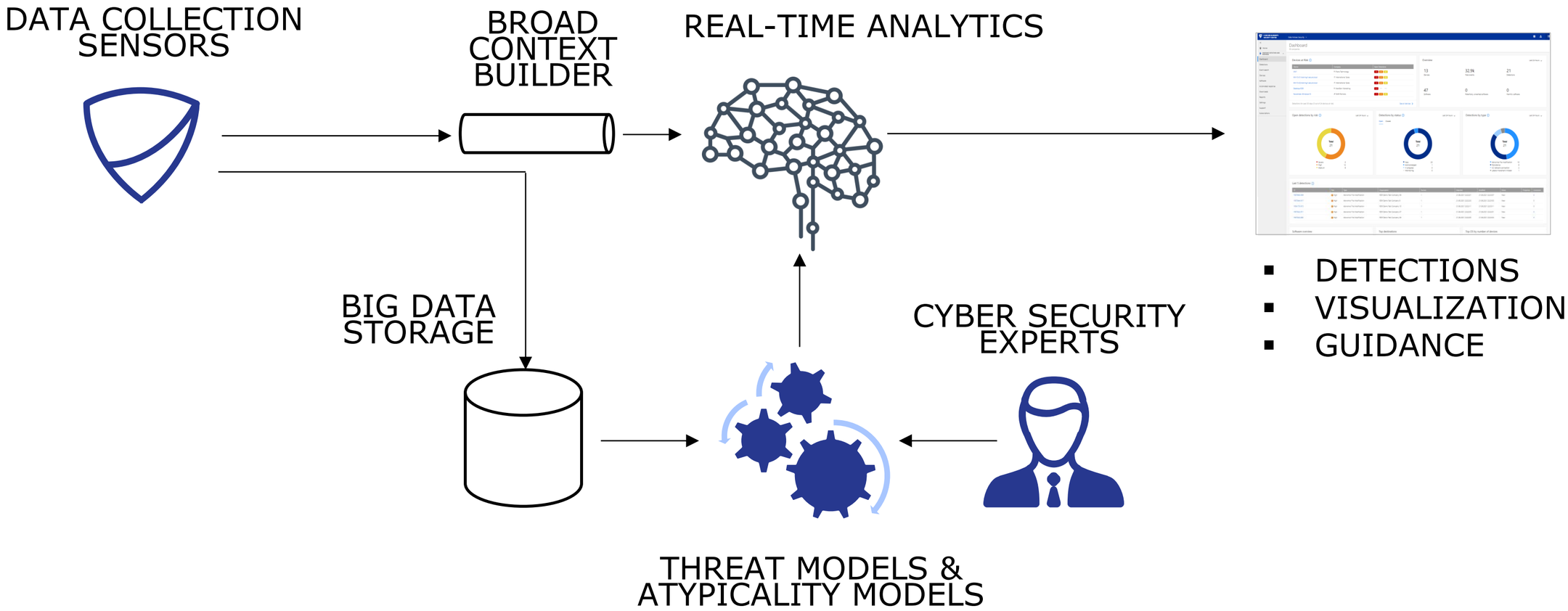
Retrieve logs, tasks

Memory dump

Event Search

Map network connections

AI And Machine Learning
At the Heart of the Solution



- DETECTIONS
- VISUALIZATION
- GUIDANCE

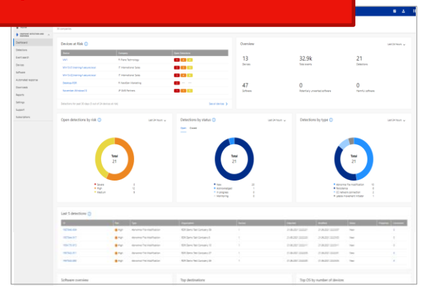
Threat Model Training In Action

DATA COLLECTION SENSORS

BROAD CONTEXT BUILDER

REAL-TIME ANALYTICS

3) Deployed to real-time analytics, our solution is then able to detect new attack types from context and behavioral patterns.



- DETECTIONS
- VISUALIZATION
- GUIDANCE

BIG DATA STORAGE

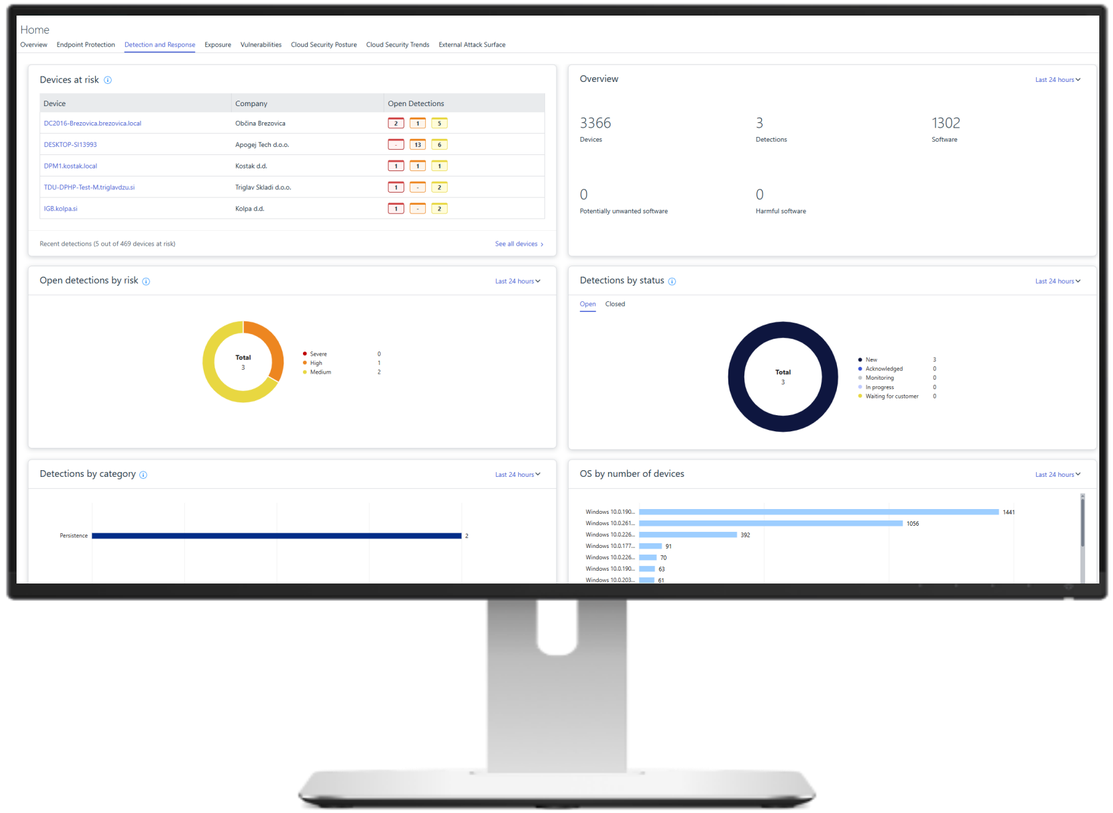
CYBER SECURITY EXPERTS

2) The threat model was trained through huge amounts of data collected by our solutions over time to detect similar malicious behavior with high accuracy – minimizing both false positives and false negatives.

THREAT MODELS & ATYPICALITY MODELS

1) In a forensic research project, our experts identified a new attack technique using Office macros and PowerShell scripts. This threat pattern was modelled by our machine learning with the help of experts providing training data.

WithSecure Endpoint Detection & Response



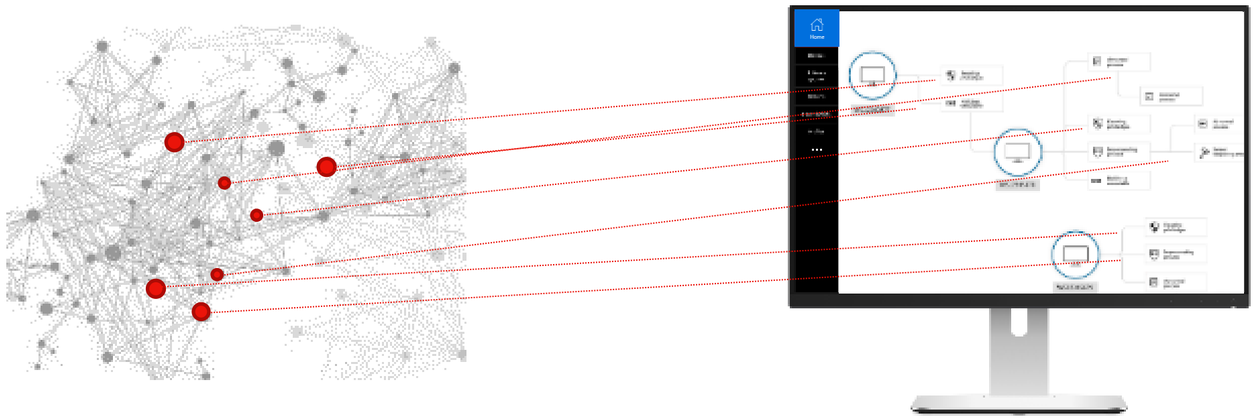
KEY FEATURES

- 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

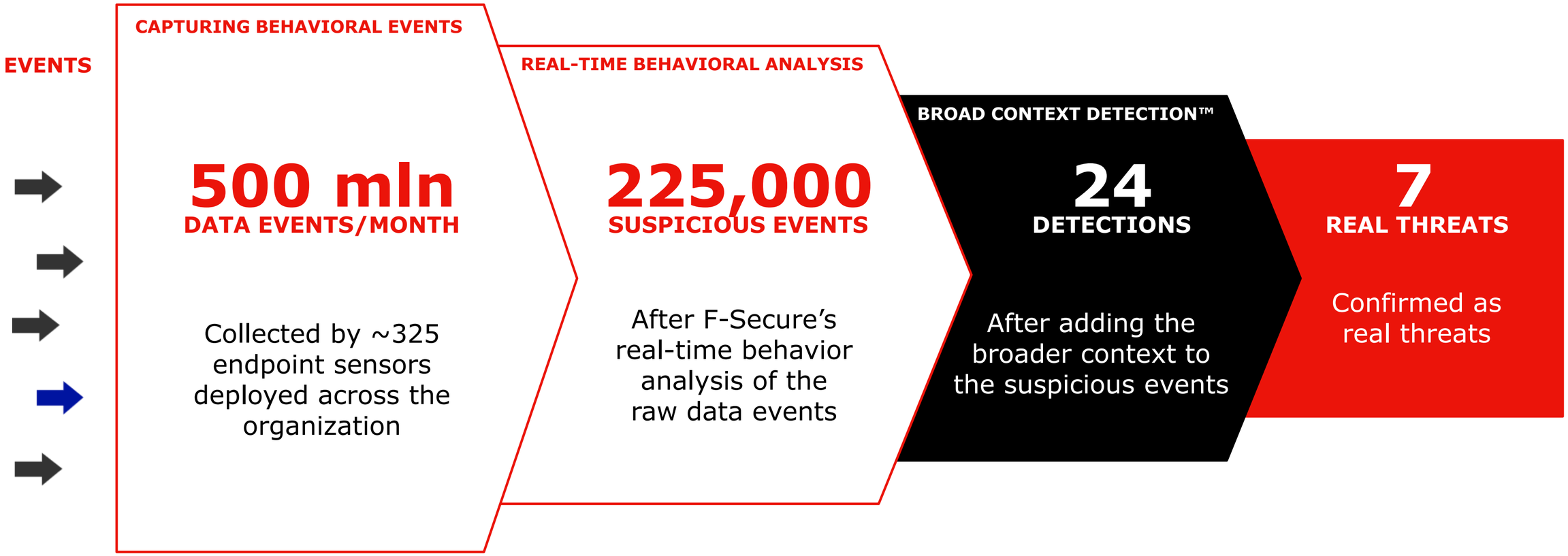


From single-shot, point detections
and binary (ON/OFF) responses
common for endpoint protection platforms.

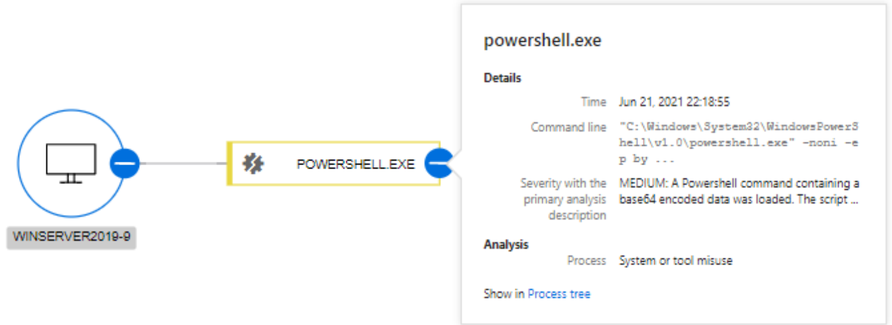
To context-based detections
including risk levels, affected host criticality,
and prevailing threat landscape.

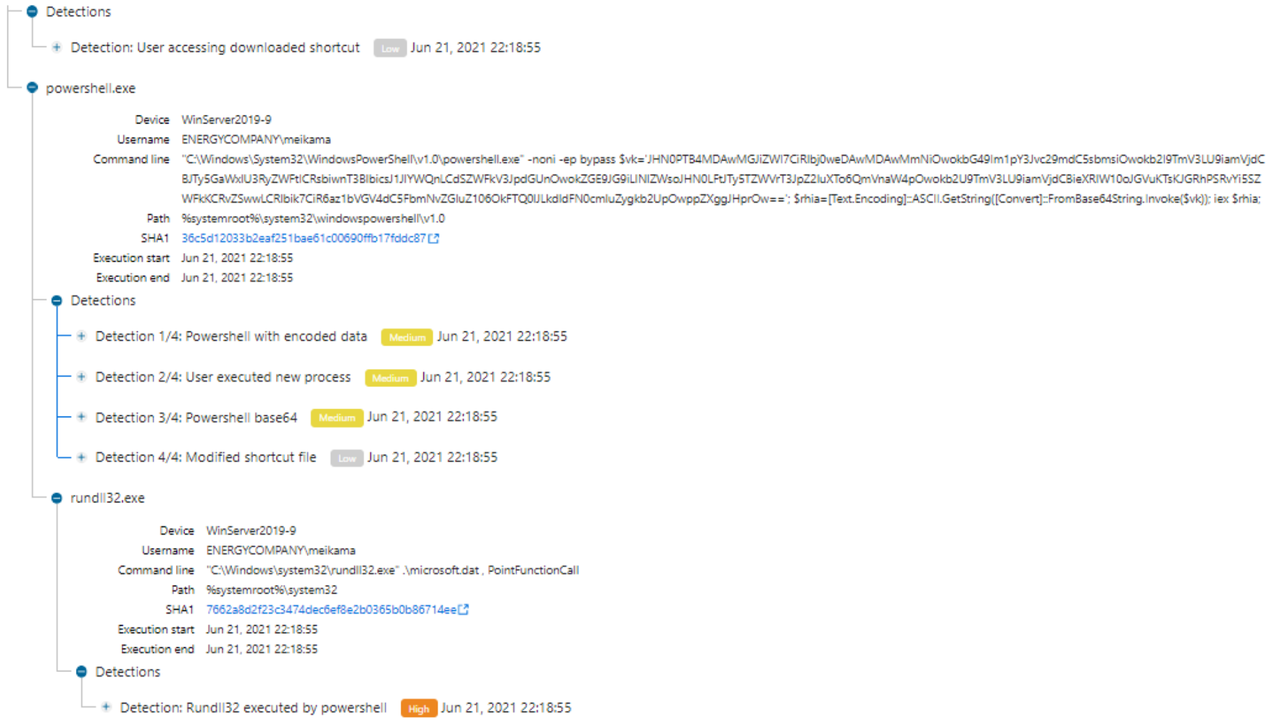
Presents only relevant detections with actionable visualization for risk-based and multi-faceted response.

Broad Context Detection In Action

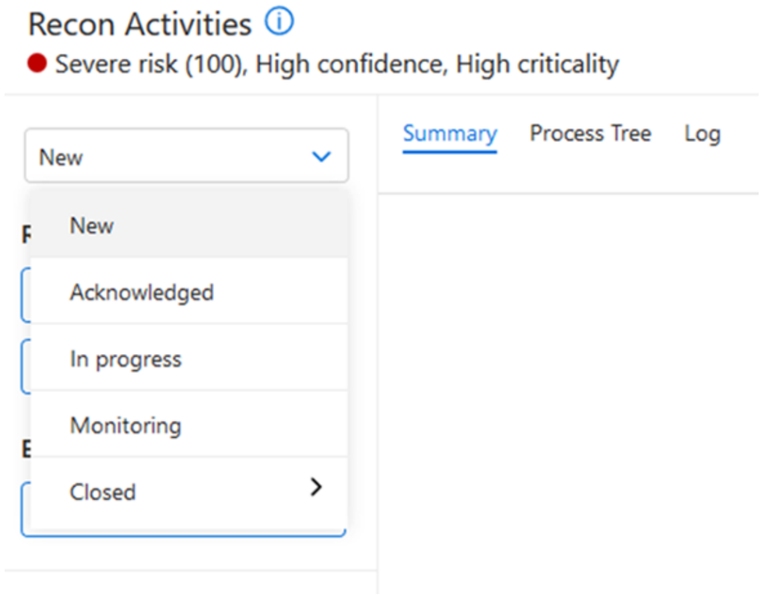


Broad Context Detection





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

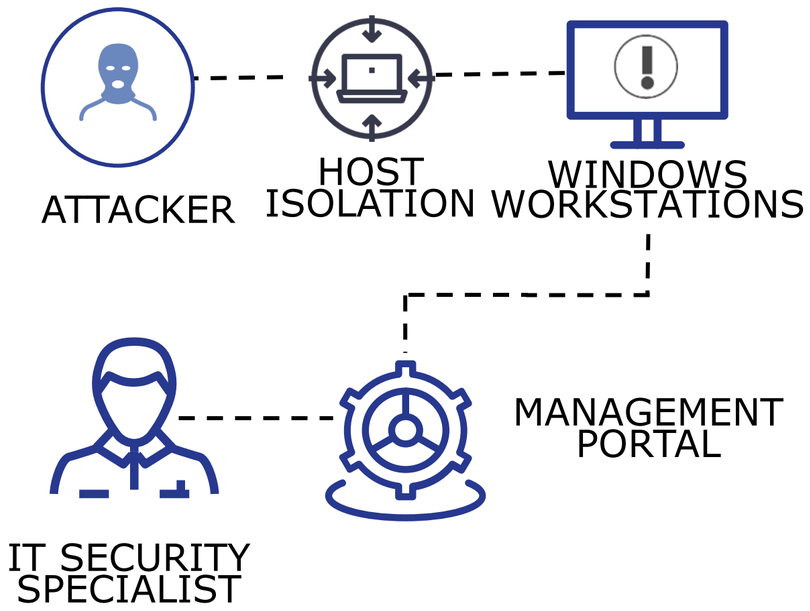
CONTAIMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

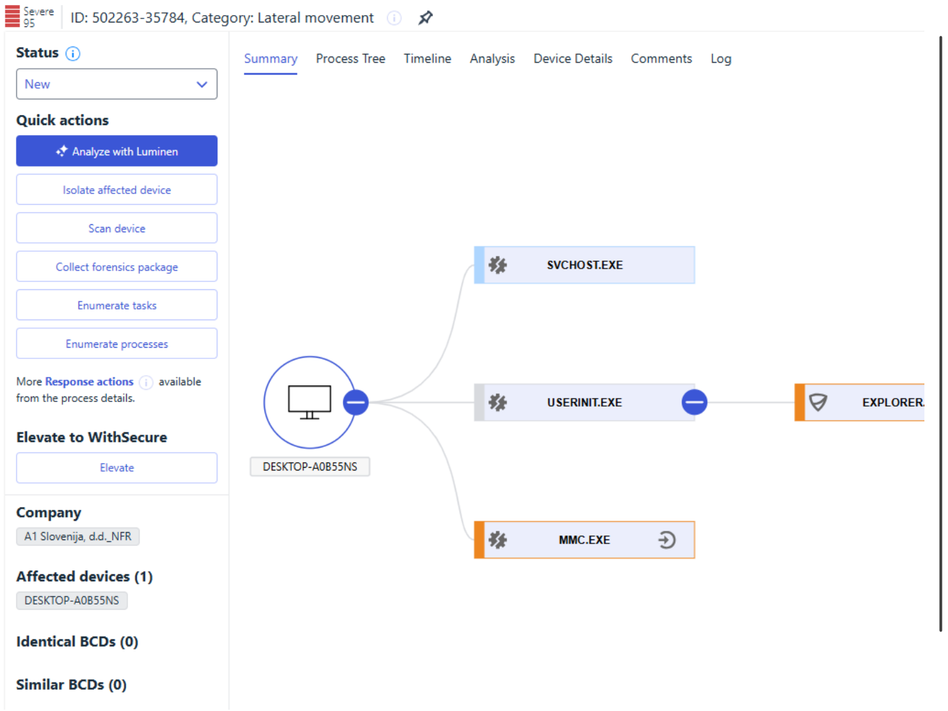
- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

Host Isolation



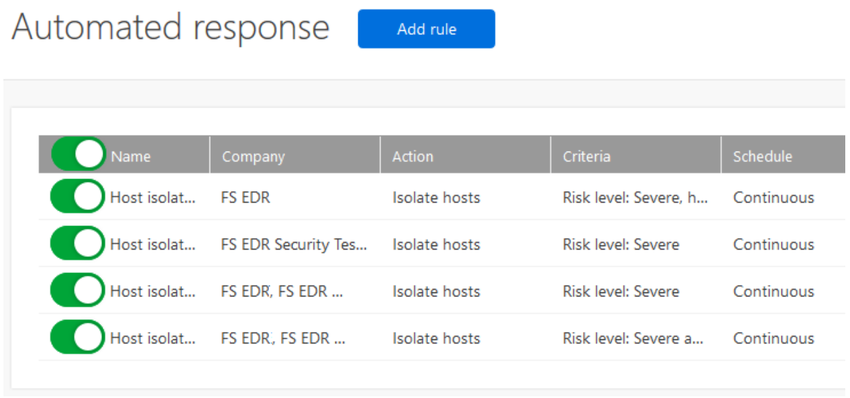
- Stops the attacker’s command & control connections by isolating selected hosts
- Displays a warning message on the isolated hosts about restricted network access
- Allows the isolated hosts to be managed remotely from the Elements Security Center Portal

Guidance To Respond



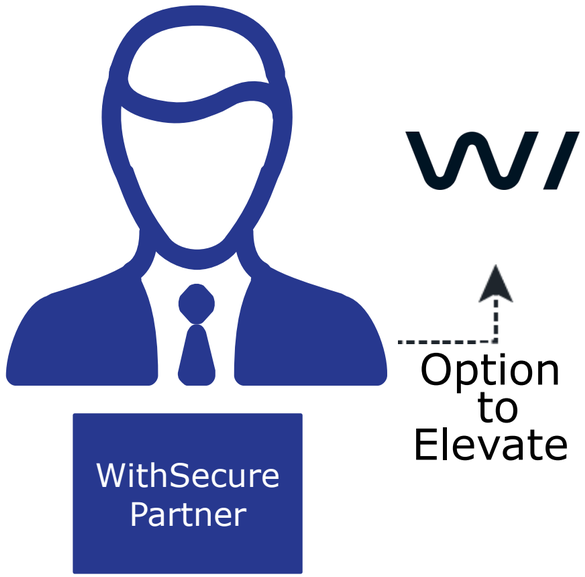
- Recommends response actions like informing users or isolating hosts
- Get help on tough investigations from F-Secure experts with Elevate to WithSecure
- Machine learning means EDR constantly improves its recommendations and detects less false positives

Automated Response



- 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.

2006

Gemini

First machine learning based file analyzer

2016

DiAPK

First machine learning based Android app analyzer

2017

Project Blackfin

On-device AI using swarm intelligence

2018

RDS DSA

First supervised learning algorithms for Broad Context Detections(TM)

2021

ML-based phishing detection

Machine learning to identify malicious phishing documents

2023

LLM-powered security research

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

WithSecure Elements Extended Detection & Response

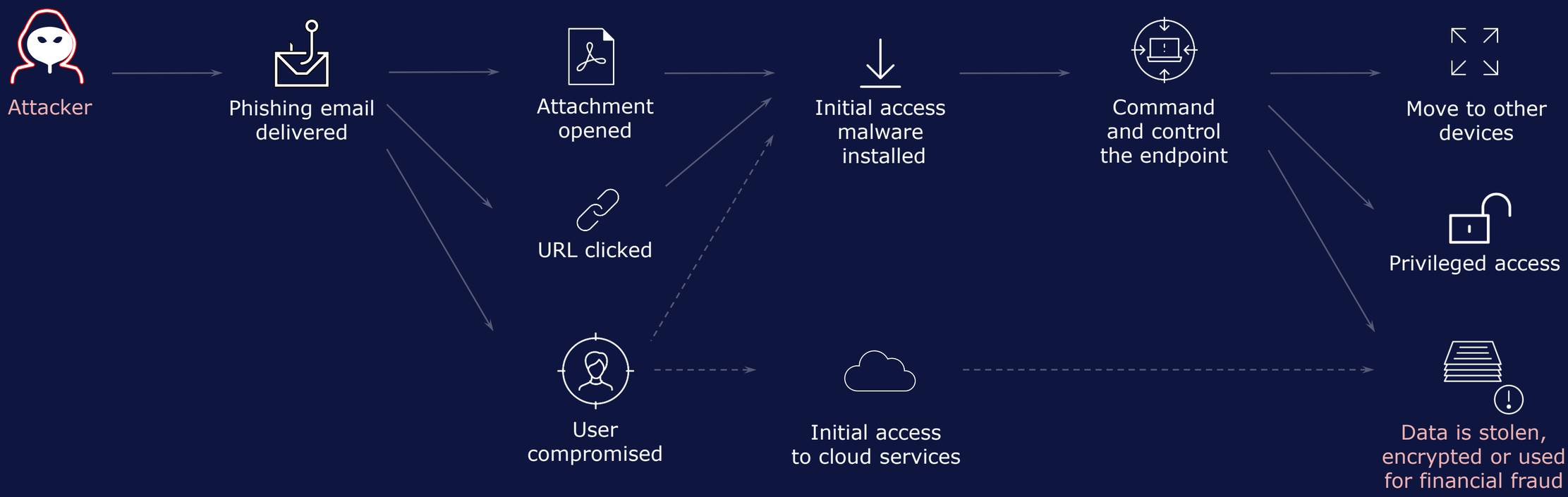
XDR for Windows, Linux, Mac and M365 cloud

A1 ICT Distribucija

WithSecure™ Elements Extended Detection and Response (XDR)

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

XDR protection scenarios



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

Elements™ | Extended Detection and Response

Preventive and reactive security

WITH secure

WithSecure Elements Exposure Management

XM for Endpoints, Network, Users and Cloud

A1 ICT Distribucija

Proactive security approach

Know what makes up your attack surface

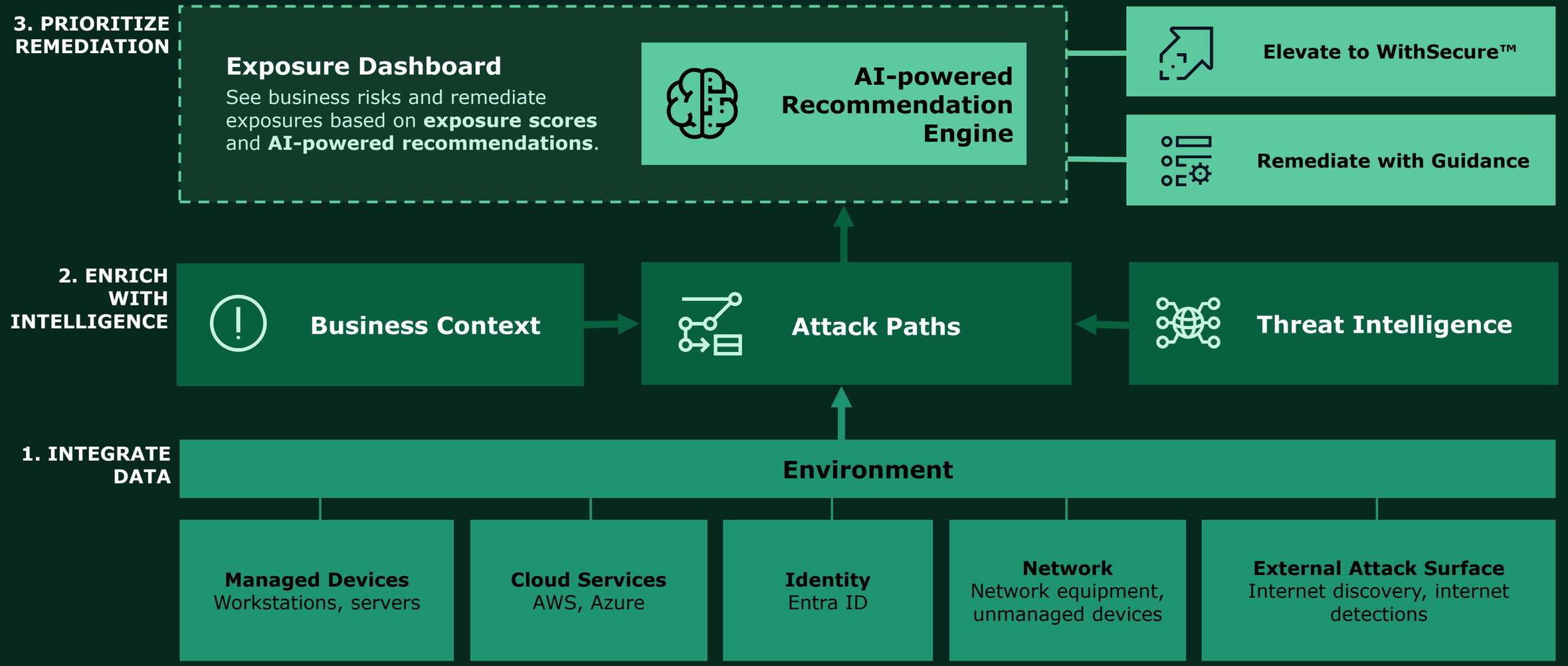
Know what to prioritize when remediating exposures

Have the right tools, people and means to remediate successfully

WITH secure

WithSecure™ Elements Exposure Management

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



WithSecure™ Elements XM vs XDR

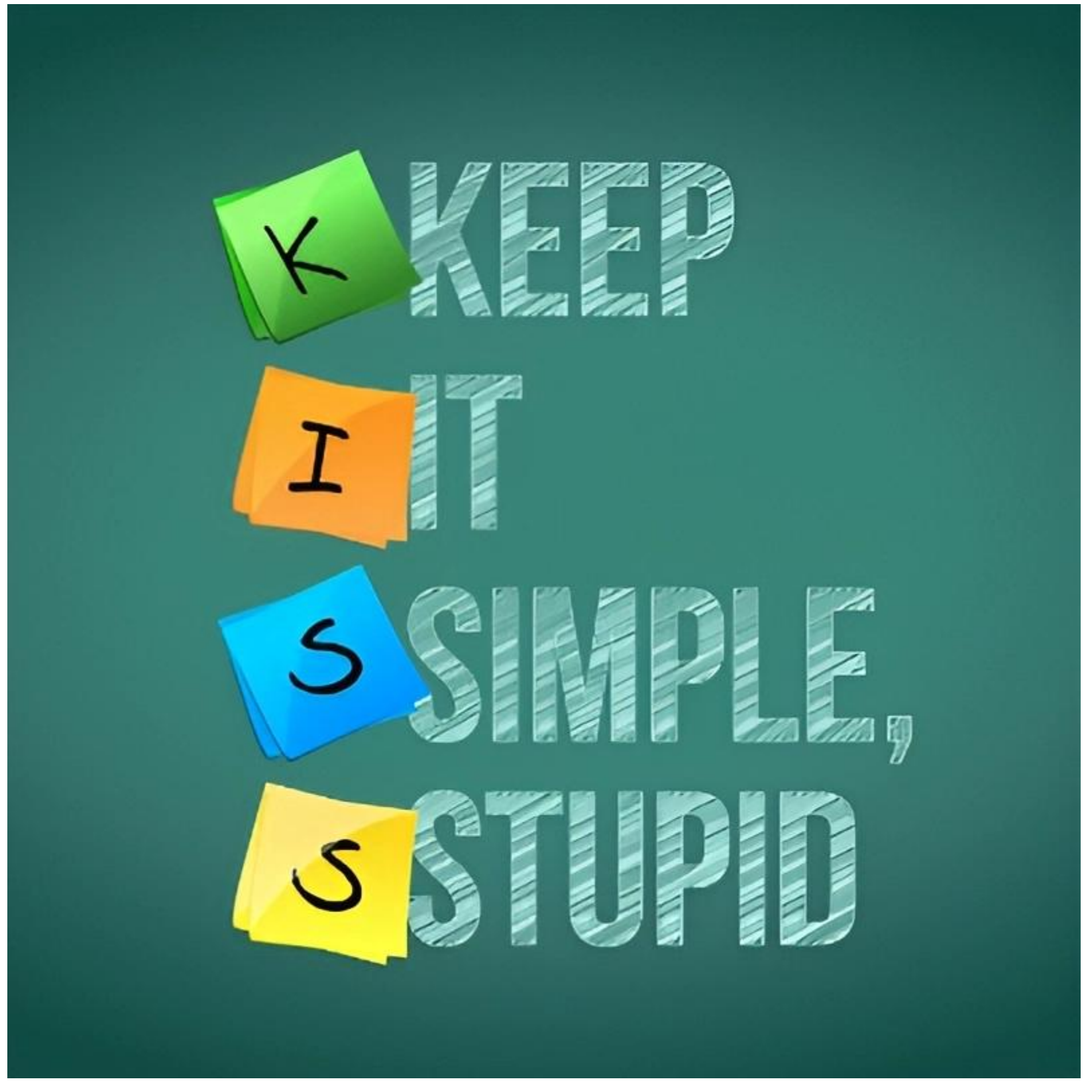
	Elements XM Continuous Proactive Security	**Elements XDR** Continuous Reactive Security
Focus Areas:	**Before attack:** "Locking down" your environment to be less attractive to attackers by understanding potential attack paths. Shrinking down the size of your attack surface.	**During attack:** The attacker 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.
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*

Environment

Europska rješenja za cybersecurity

WITH secure

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 riješenja**
  - **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**

WITH secure


LABYRINTH
wallix
secure
Pitanja?

HVALA NA POZORNOSTI!

https://varnostne-resitve.si/

ict-partners@A1.si

A1 ICT Distribucija