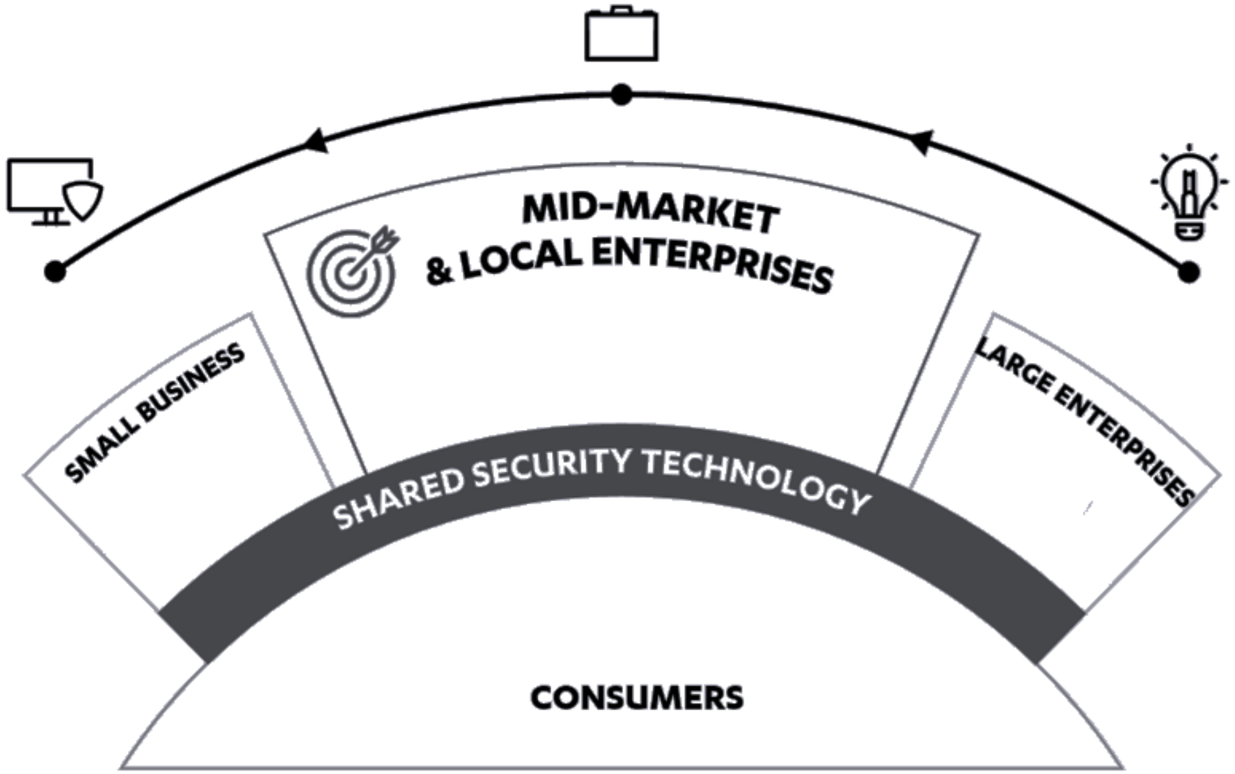
Formerly
F-Secure Business

F-Secure Business is now **WithSecure**

Protecting businesses in 100+ countries

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



We are targeting the corporate mid-market and local enterprises

„Next-gen“ for 10+ years

2006 – DeepGuard 1.0

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

2008 – DeepGuard 2.0

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

2010 – DeepGuard 3.0

Expanded use of metadata. DeepGuard now uses prevalence data.

2011 – DeepGuard 4.0

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

2013 – DeepGuard 5.0

DeepGuard now prevents exploits in commonly targeted applications.

2017 – DeepGuard 6.0

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

2019 – Security Cloud

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

Best protection on all fronts – verified by independent industry evaluations

Gartner peerinsights customers' choice 2020

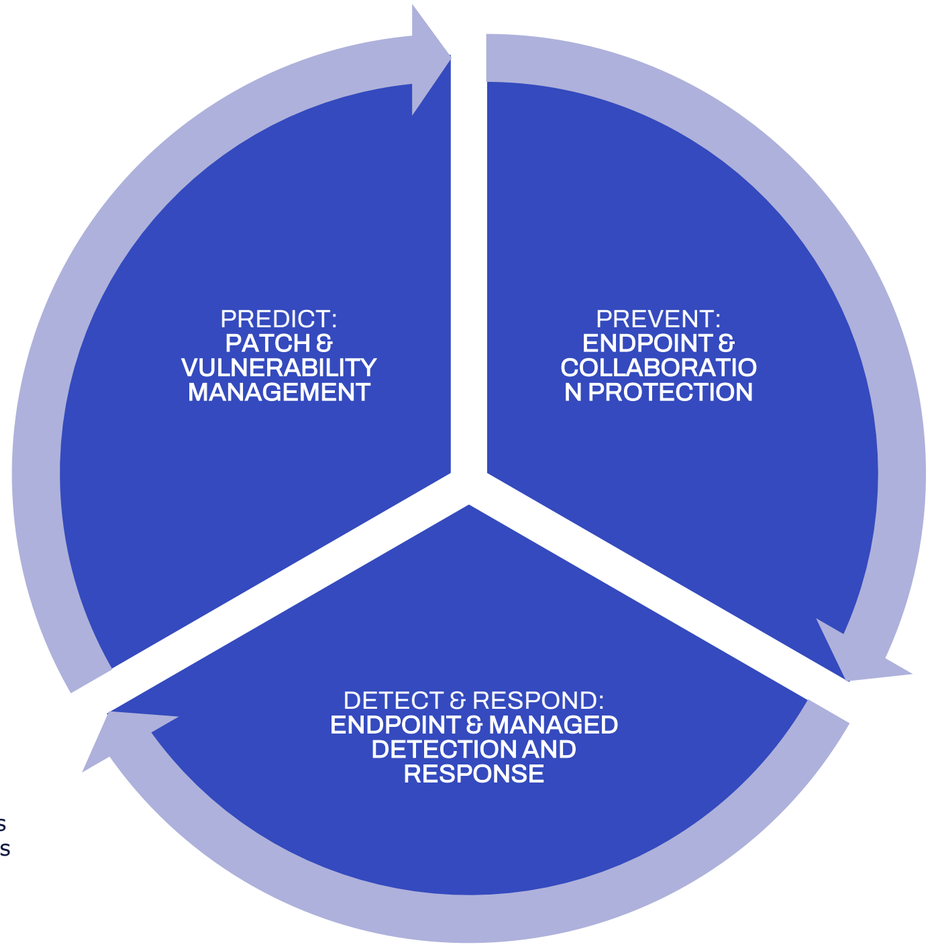
WithSecure™ named a 2020 Gartner Peer Insights Customers' Choice for Vulnerability Assessment

PCI Security Standards Council
APPROVED SCANNING VENDOR

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

MITRE ENGENUITY | ATT&CK® Evaluations

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



7 **Annual *Best Protection* awards**

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION MACOS

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

PC PCMAG.COM EDITORS' CHOICE

WithSecure™ Elements is PC Mag Editors' Choice 2022

SC 2021 awards EUROPE WINNER

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

AV comparatives Certified EPR 2021 Strategic Leader

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

LABYRINTH

WITH secure

Best prot… independ…

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

Rasmus Saxén

Researcher, WithSecure

…ction

APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT

APPROVED CORPORATE ENDPOINT PROTECTION MACOS

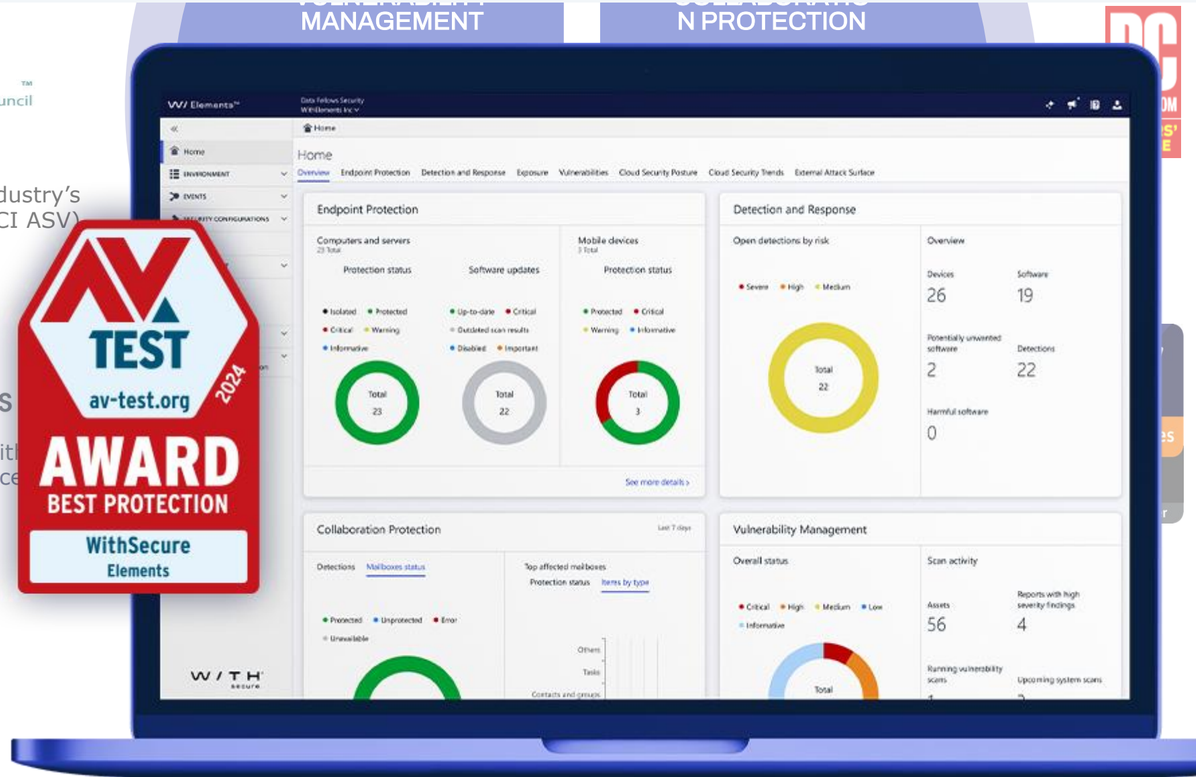
WithSecure™ named a 202… Customers' Choice for V…

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

PCI Security Standards Council

APPROVED SCANNING VENDOR

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



WithSecure™ Elements is PC Mag Editors' Choice 2022

SC 2021 awards EUROPE WINNER

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

MITRE ENGENUITY | ATT&CK® Evaluations

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

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

A1 ICT Distribucija

abacus computing

A1

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

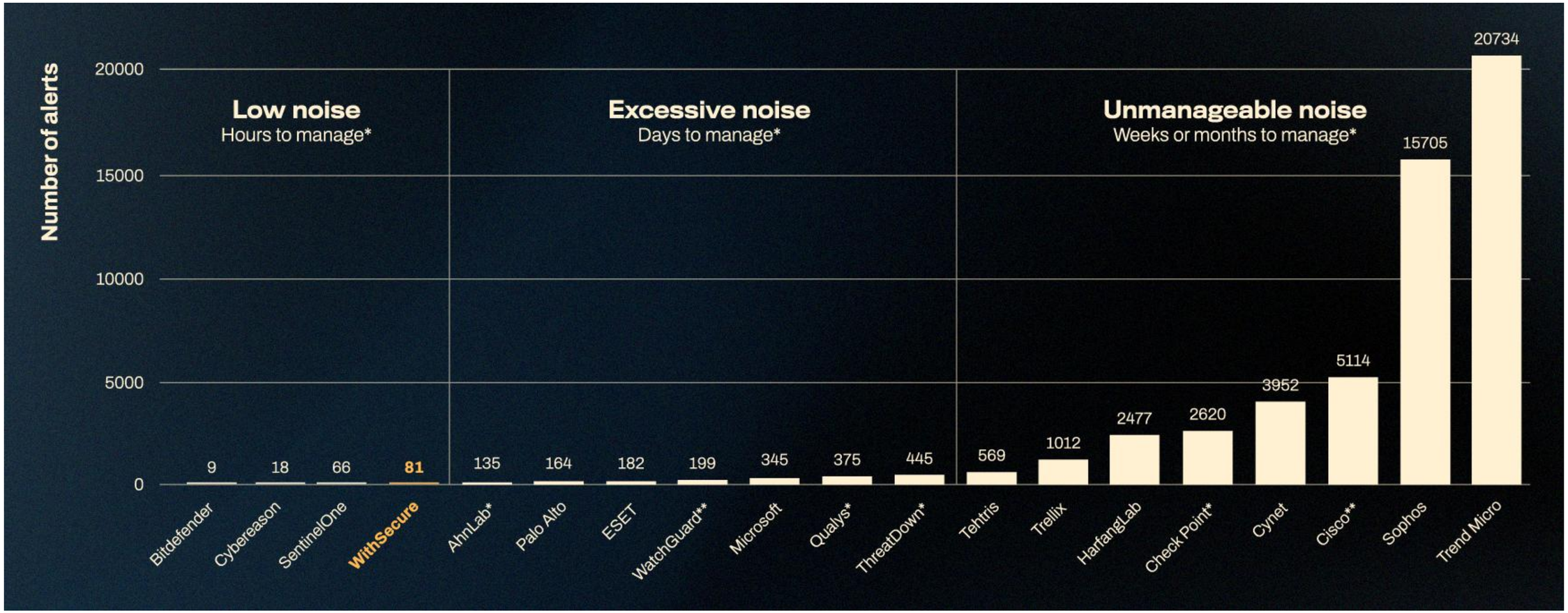
- WithSecure is once again identified as one of the leading **15** vendors in the Gartner Magic Quadrant for Endpoint Protection Platforms
- WithSecure is one of only four **European** cyber security vendors included in the report
- WithSecure **significantly improved** its position compared to the previous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

WithSecure is a good fit for small and midsize businesses

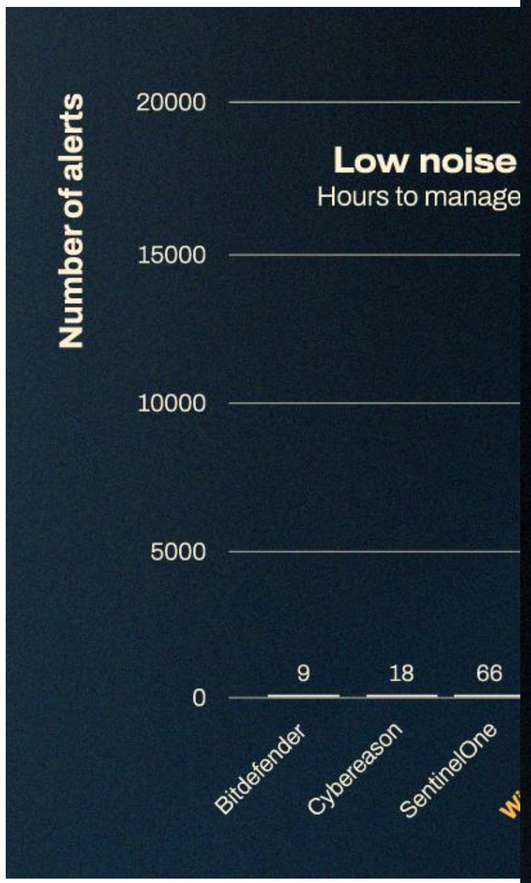
WithSecure's strengths:

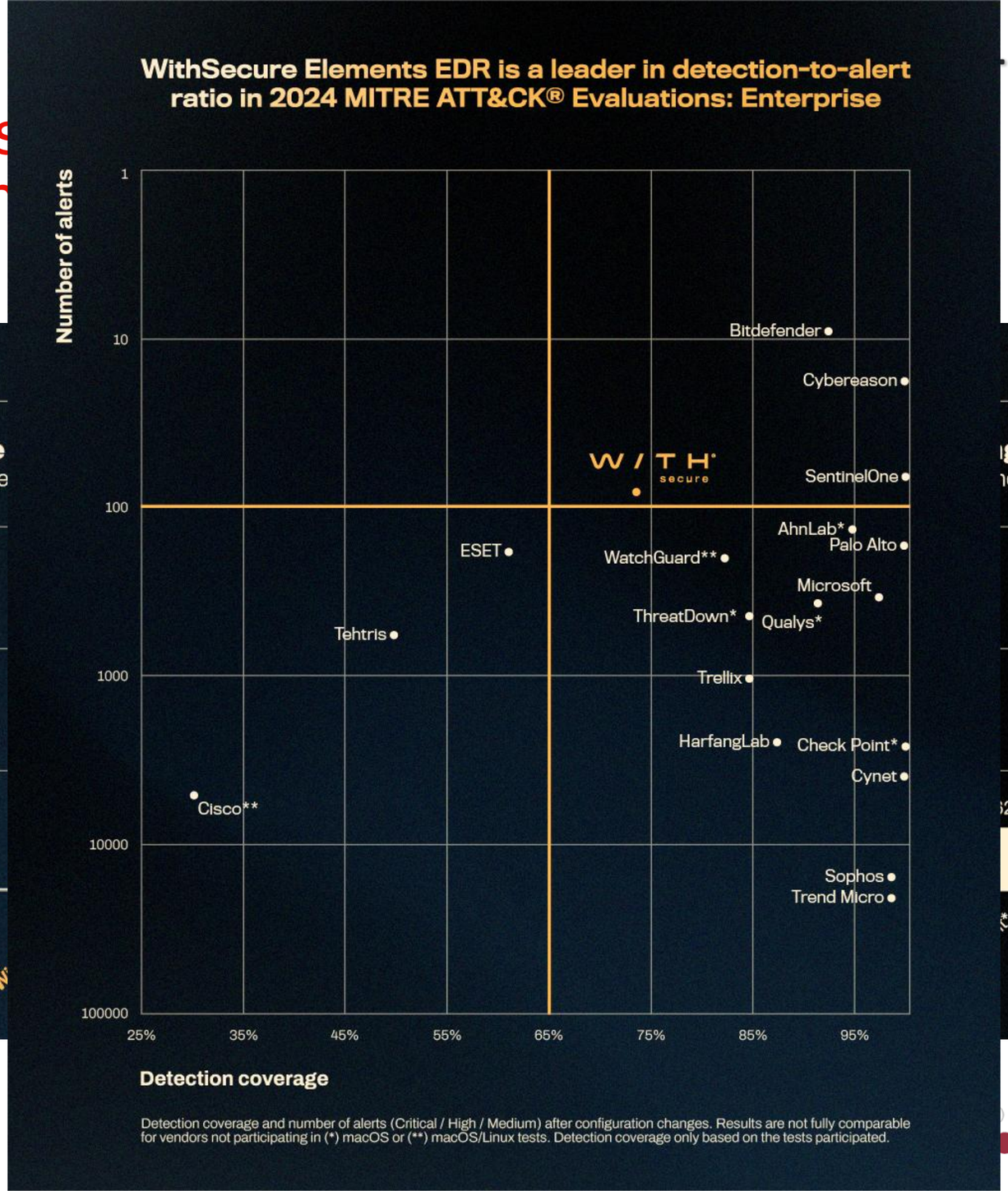
- **Attuned to the needs of the midmarket**, while Gartner is primarily targeting enterprises
- **Affordable and generally lower than average pricing** compared to other vendors in the report
- Customers generally rate the **support they receive from WithSecure** as good

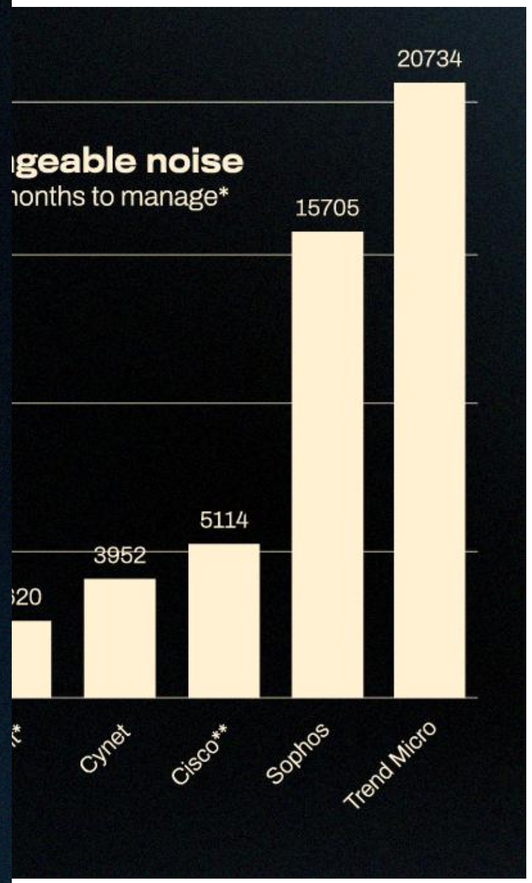
WithSecure sets new standards in detection-to-alert ratio for the mid-market



WithSecure sets
alert ratio for th







A1 ICT Distribucija

WithSecure **Elements™**

Proactive and Modular – Made for Co-Security

WithSecure™ Elements

Right security outcomes with optimal blend of technologies and services

Simple and efficient security management with AI-powered Elements Cloud

Prepare for tomorrow, strengthen your digital security today


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

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

Extended Detection and Response

Co-Security Services

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

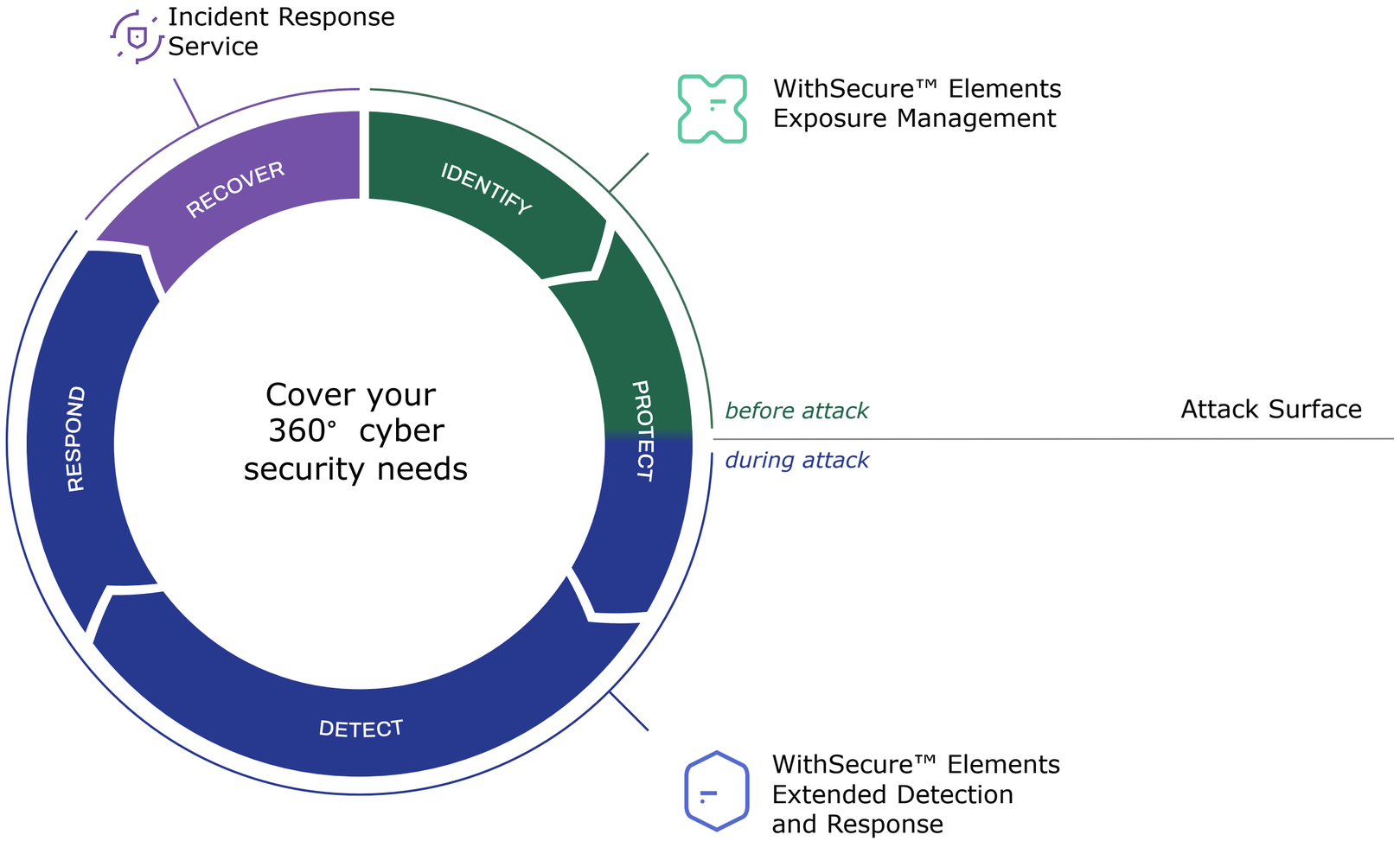
- Endpoint Security
- Identity Security
- Collaboration Protection

Co-Security Services

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

WithSecure™ Support Services

WithSecure™ Elements Cloud - NIST



LABYRINTH

WITH secure

WithSecure Elements Endpoint Protection

EPP for Windows, Linux, Mac, Android, iOS

A1 ICT Distribucija

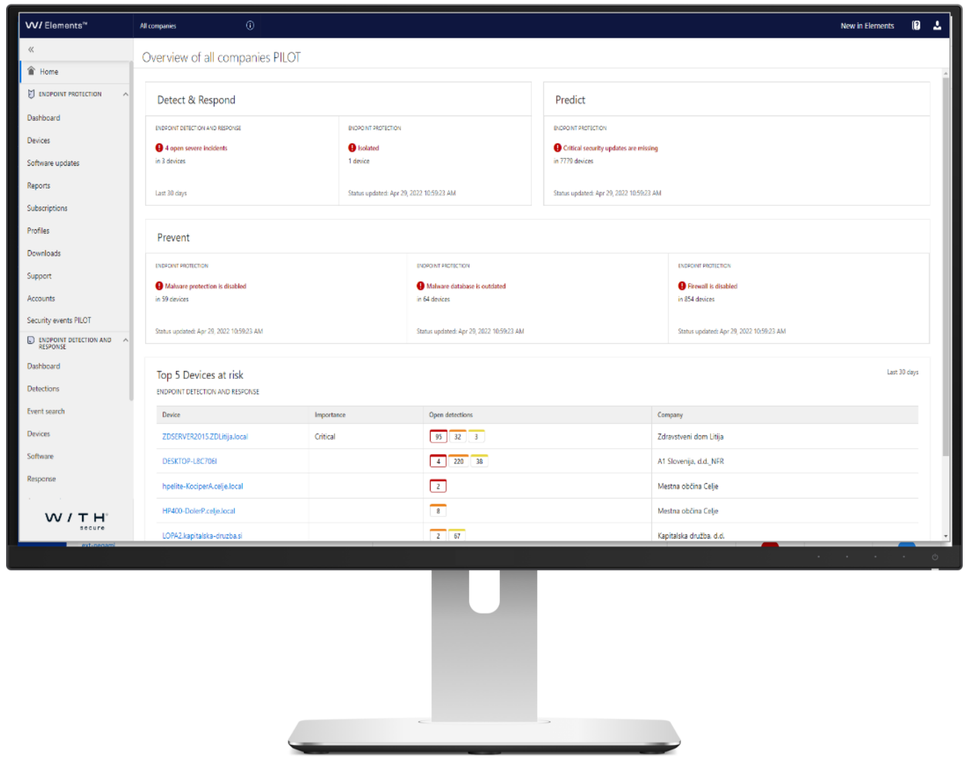
A1

Elements Security center

ESC PORTAL

- New portal for seamlessly managing all WithSecure 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

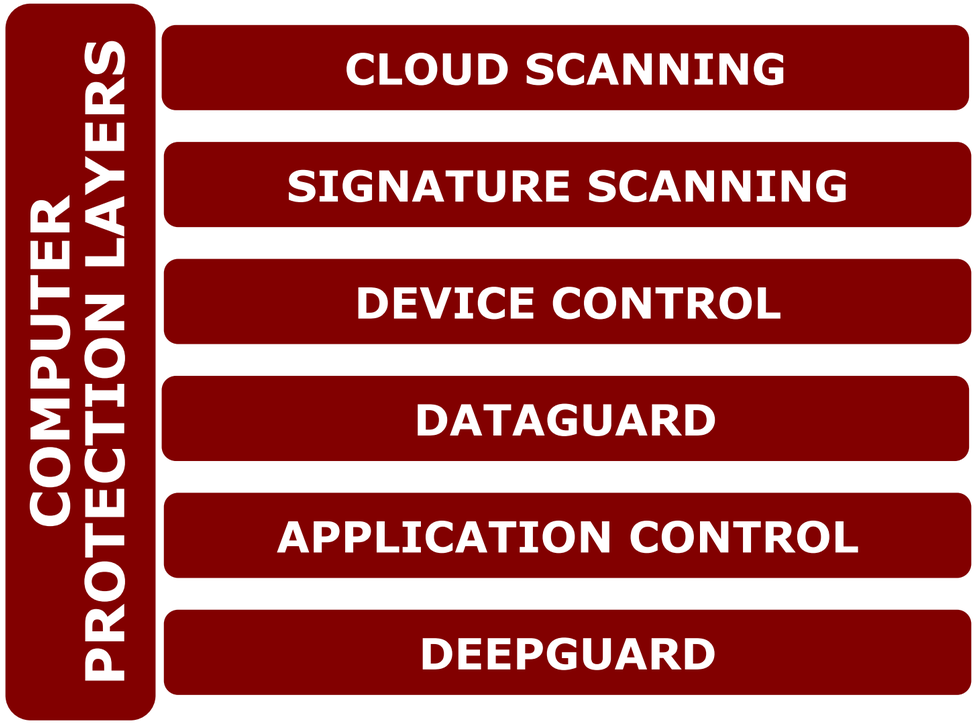
A1 ICT Distribucija

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

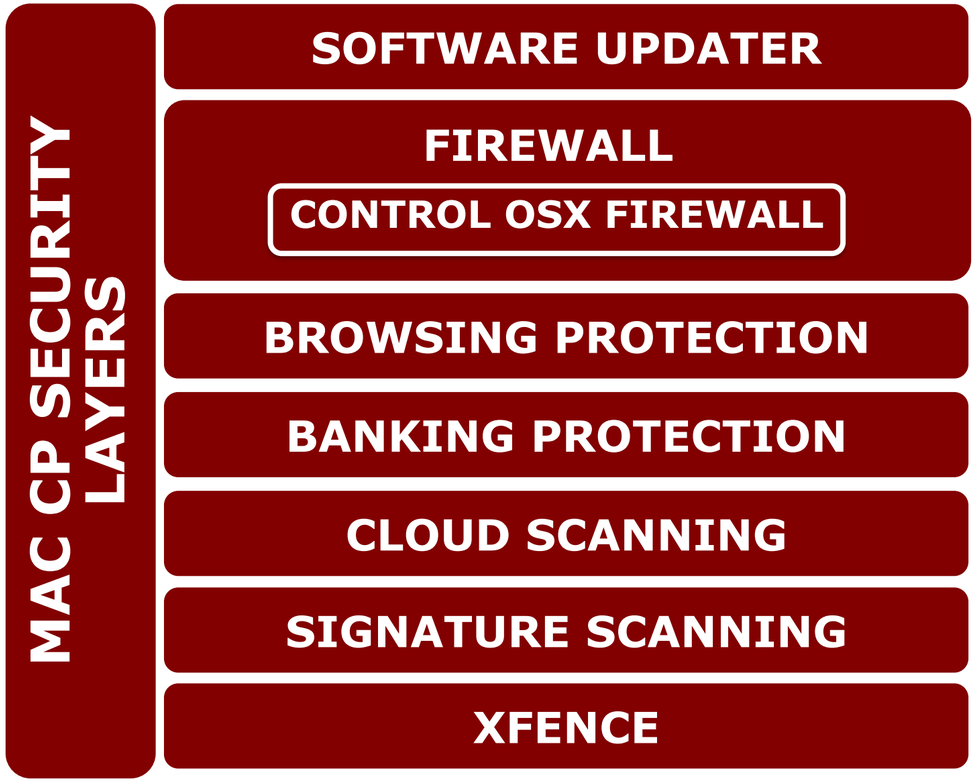
Elements EPP for Computers - PC

- 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

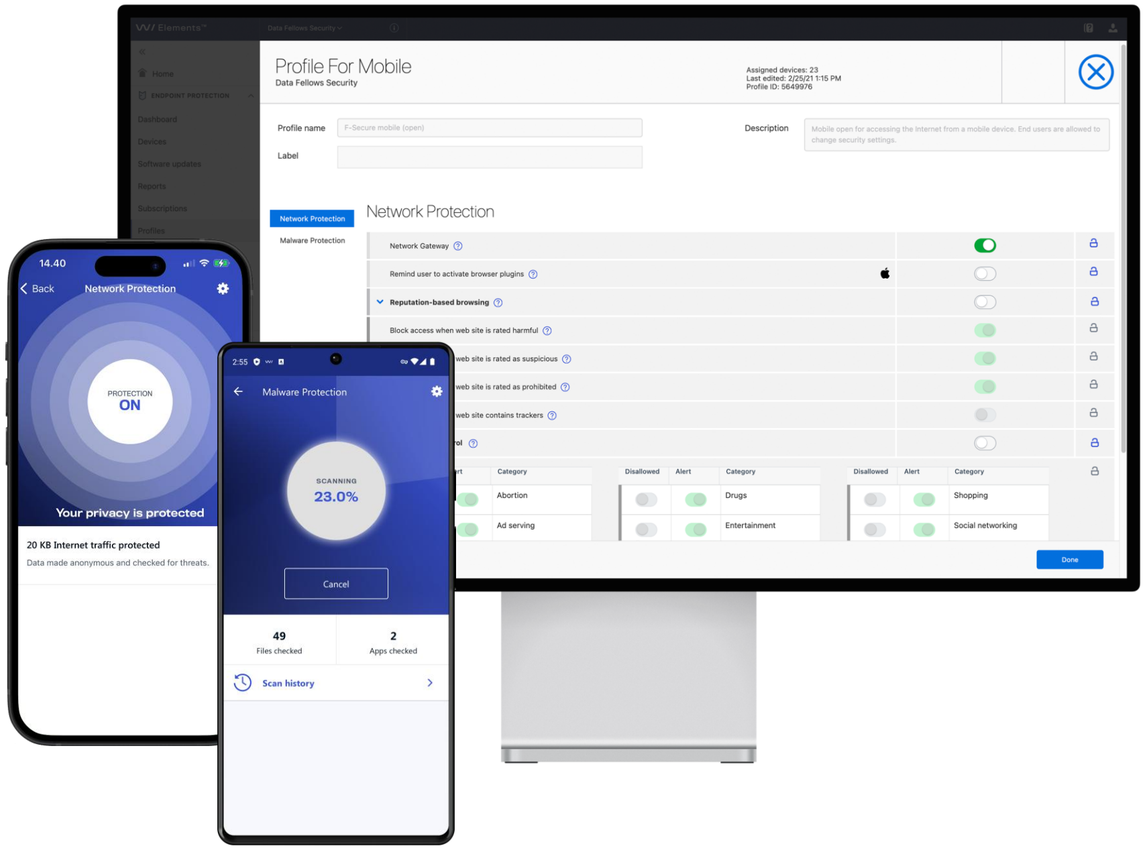
DEEPGUARD 6

APPLICATION CONTROL*

DATAGUARD*

* = PREMIUM FEATURE

Elements for Mobile



NETWORK PROTECTION

SECURITY CLOUD

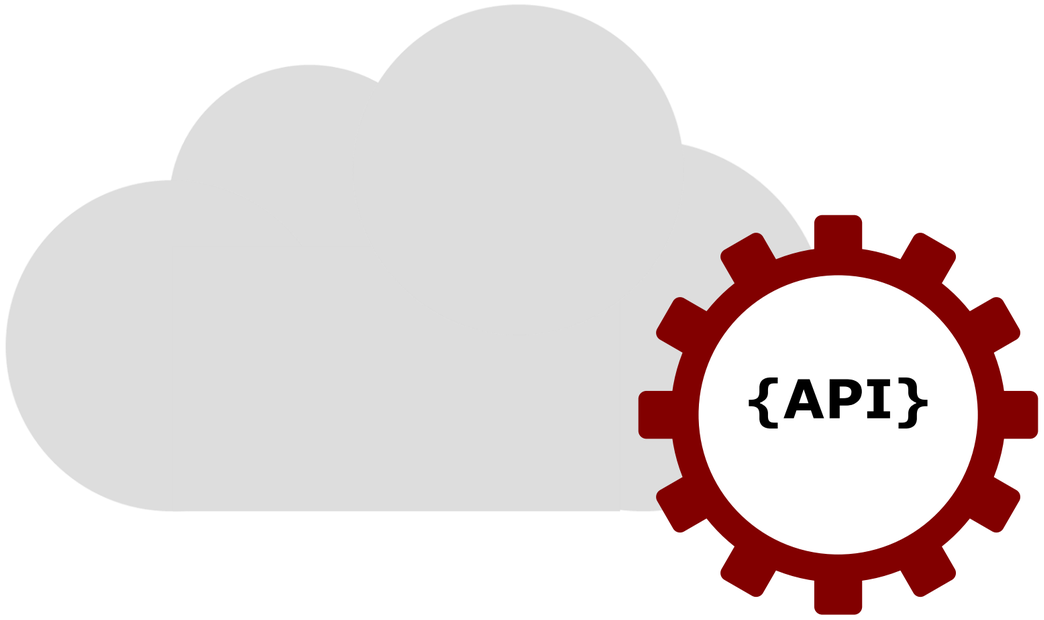
APPLICATION PROTECTION

BROWSING PROTECTION

TRACKING PROTECTION

MDM SUPPORT

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

LABYRINTH

WITH secure

WithSecure Elements Endpoint Detection & Response

EDR for Windows, Linux, Mac

A1 ICT Distribucija

A1

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

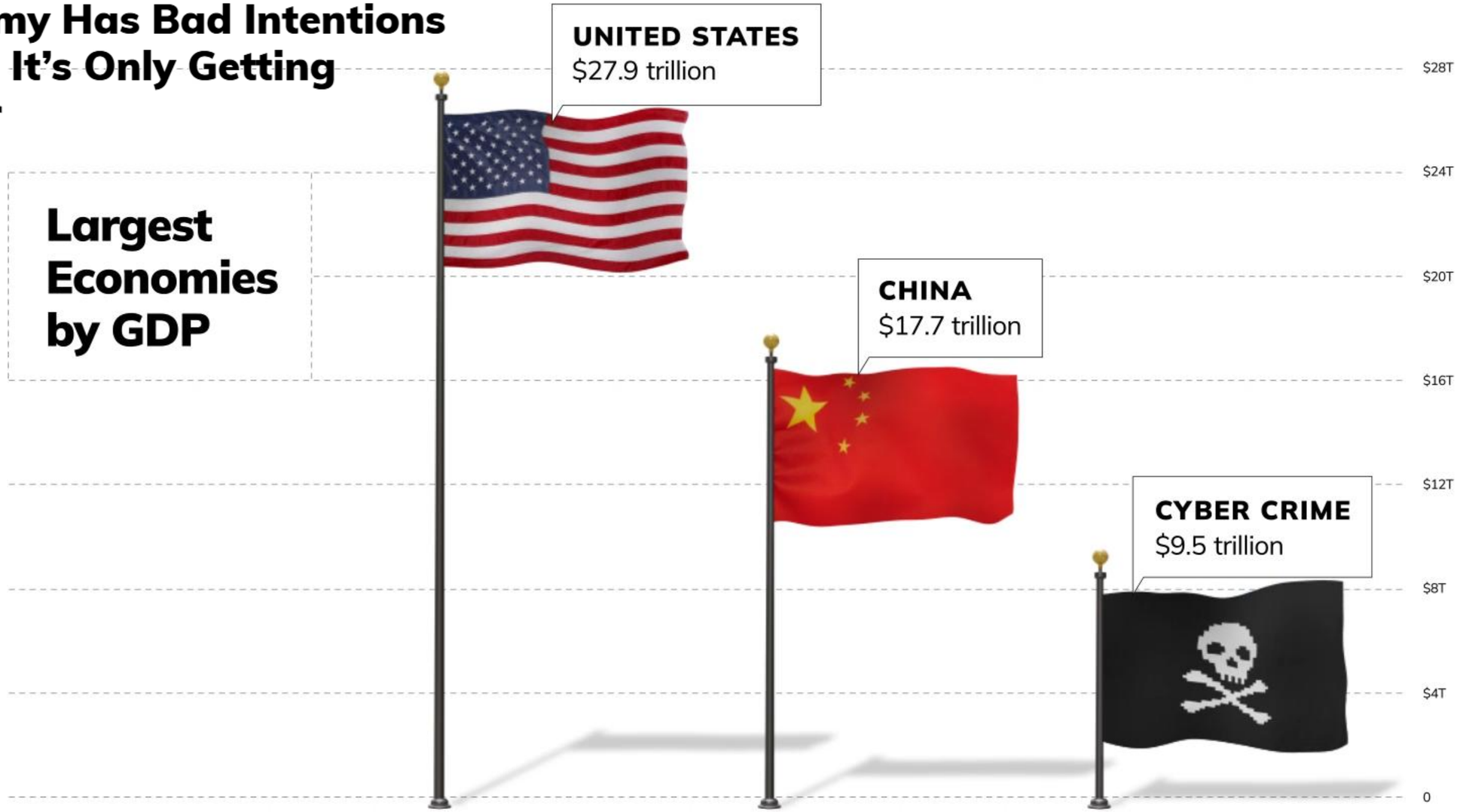
With Bitcoin, criminals can easily receive money without getting caught

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

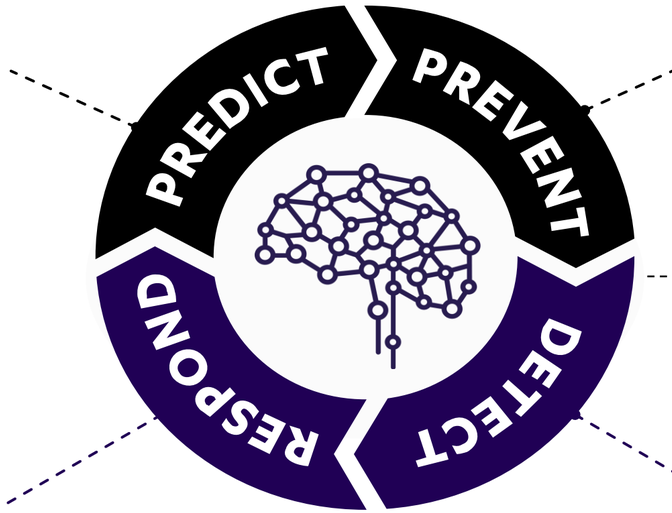
Vir: https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger

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

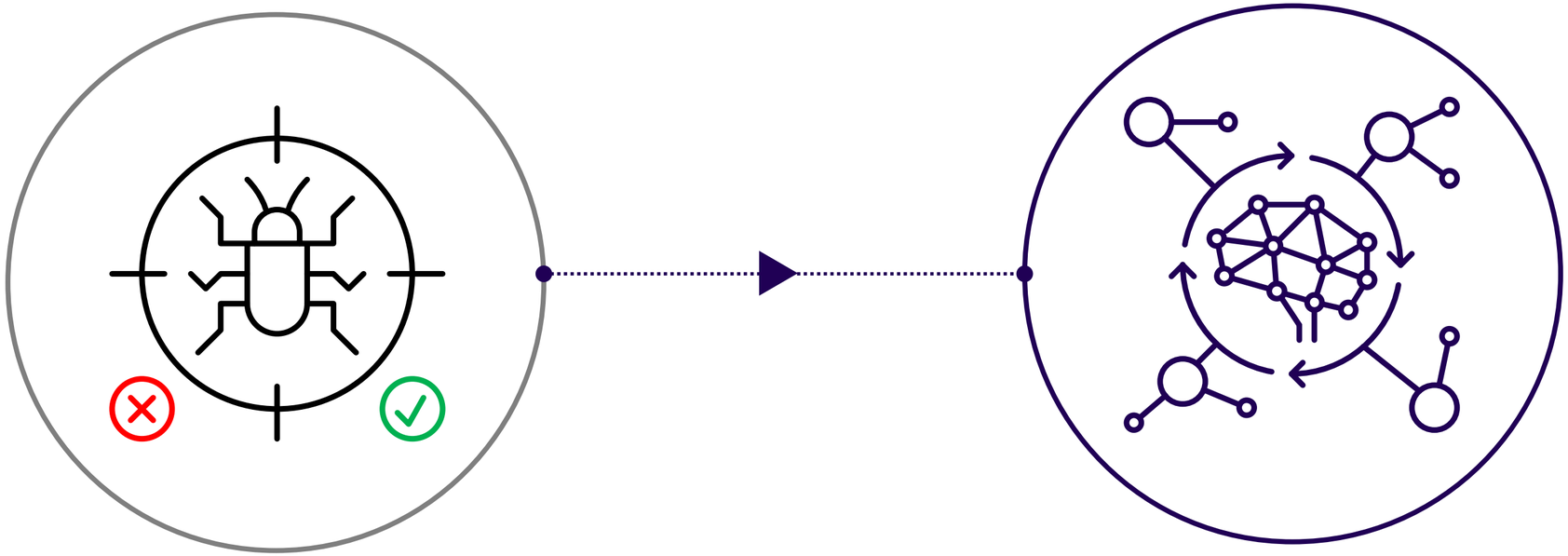
Recognize incidents and threats, isolate and contain them

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.

Source: 2025 Cost of Data Breach Study by Ponemon Institute indicated the days to identify the data breach at 181 (mean time to to contain +60)

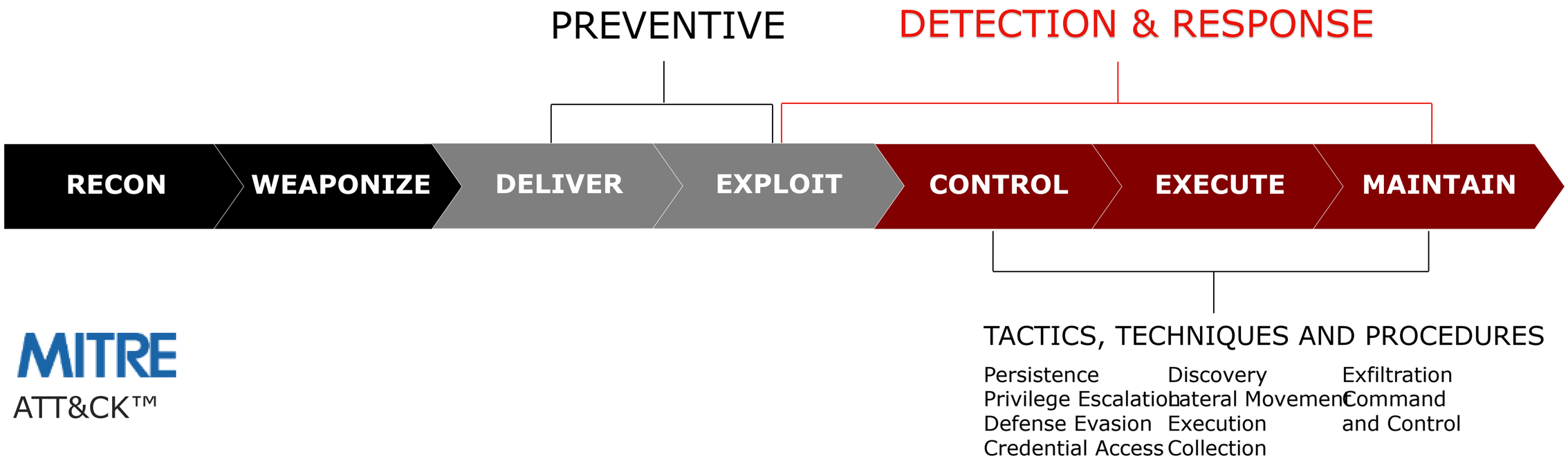
Call For A Paradigm Shift



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



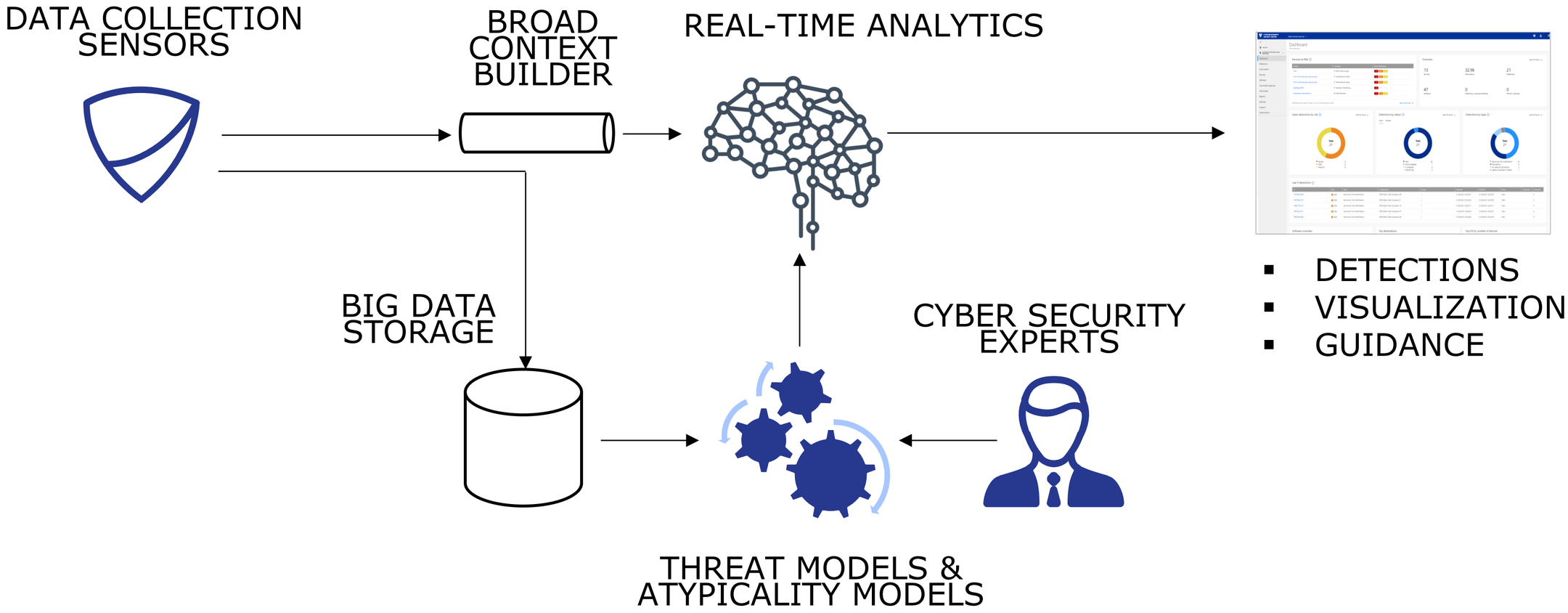
MITRE ATT&CK™

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

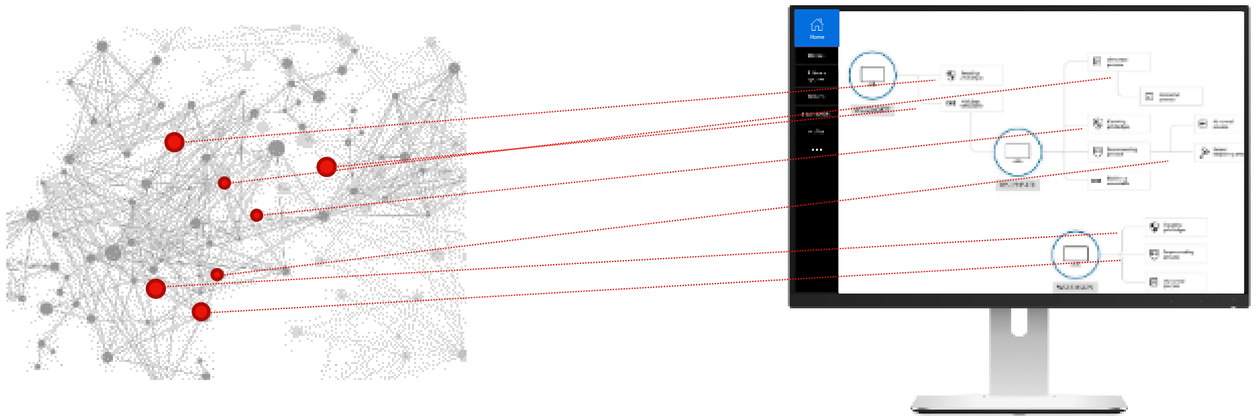
AI And Machine Learning At the Heart of the Solution



Why Broad Context Detection?

YES

NO

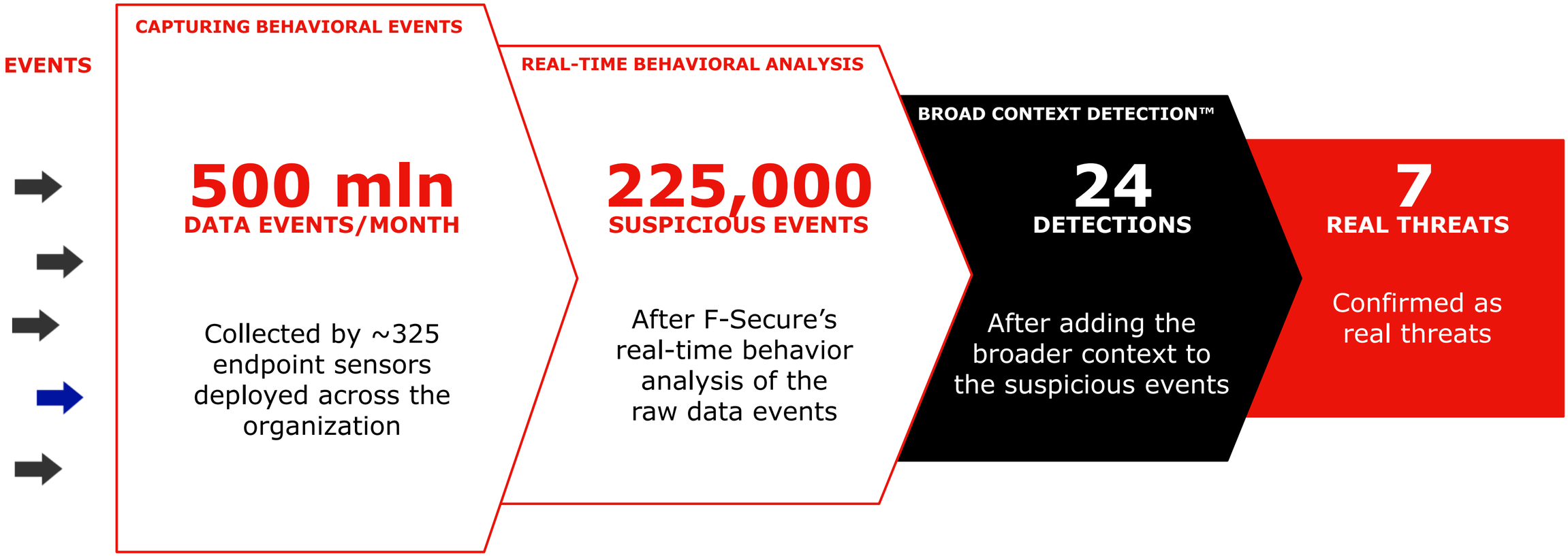


From single-shot, point detections
and binary (ON/OFF) responses
common for endpoint protection platforms.

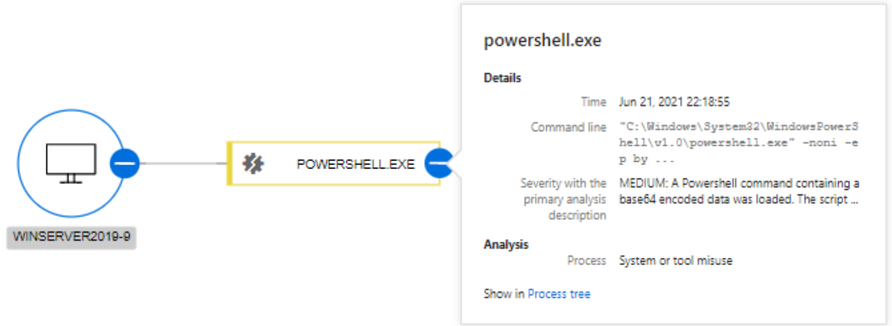
To context-based detections
including risk levels, affected host criticality,
and prevailing threat landscape.

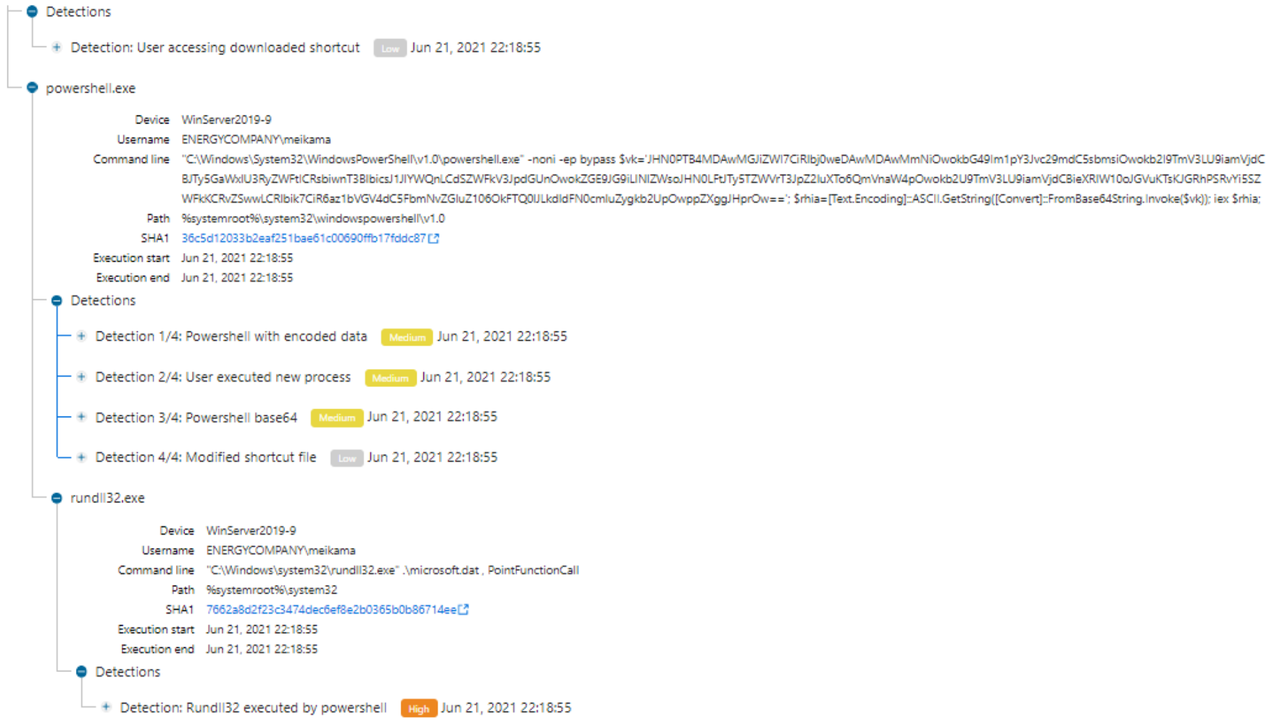
Presents only relevant detections with actionable visualization for risk-based and multi-faceted response.

Broad Context Detection In Action

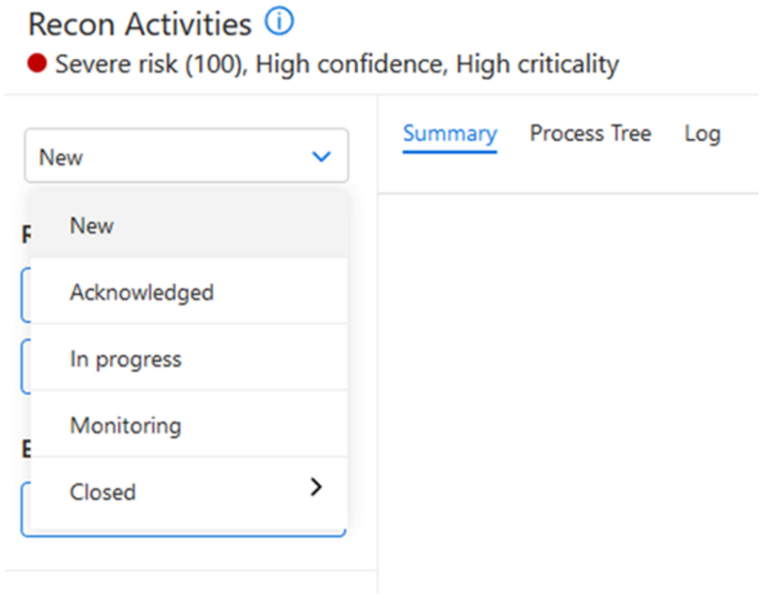


Broad Context Detection





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

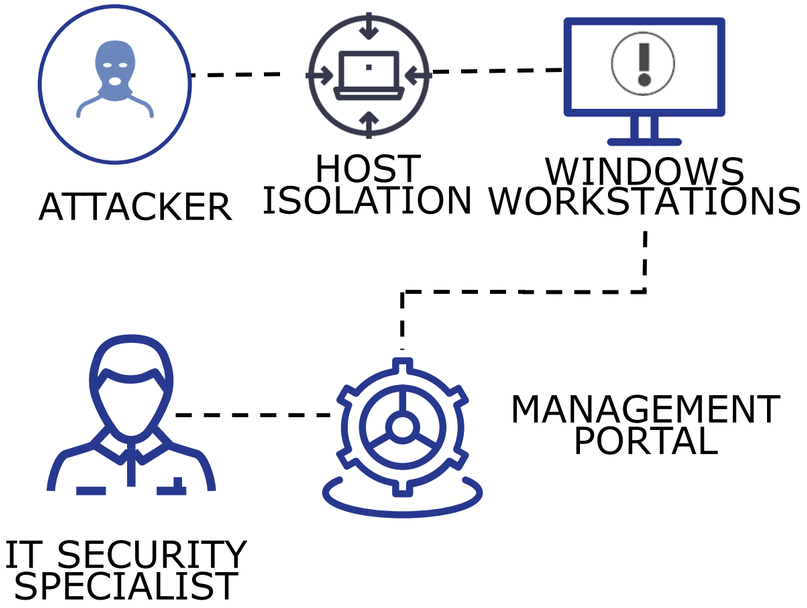
CONTAIMENT ACTIONS

- Kill processes
- Kill threads

REMEDIATION ACTIONS

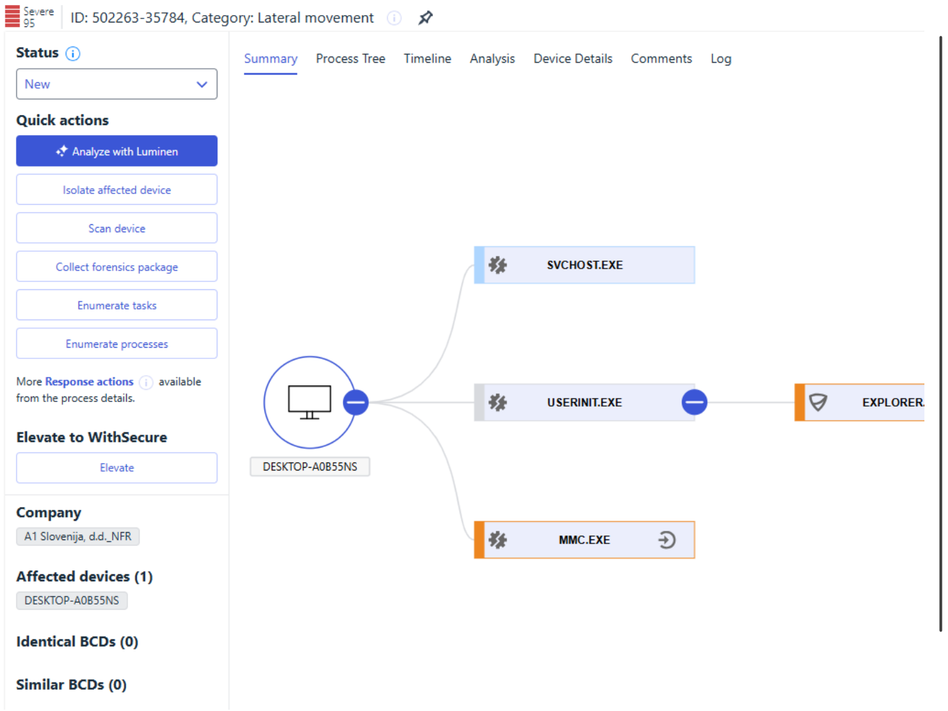
- Delete files
- Delete registry
- Delete services
- Delete scheduled tasks

Host Isolation



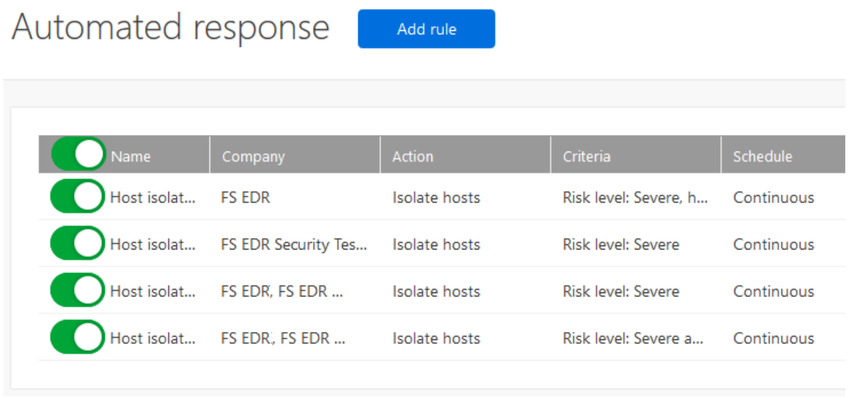
- Stops the attacker’s command & control connections by isolating selected hosts
- Displays a warning message on the isolated hosts about restricted network access
- Allows the isolated hosts to be managed remotely from the Elements Security Center Portal

Guidance To Respond



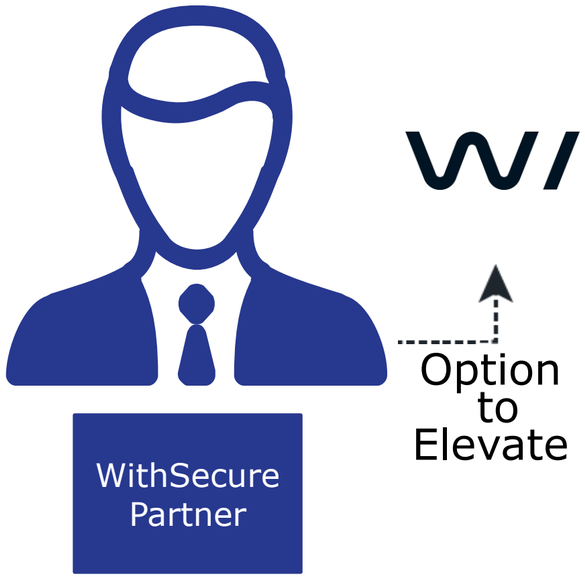
- Recommends response actions like informing users or isolating hosts
- Get help on tough investigations from F-Secure experts with Elevate to WithSecure
- Machine learning means EDR constantly improves its recommendations and detects less false positives

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
- WithSecure 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.

LABYRINTH

WITH secure

WithSecure Elements Extended Detection & Response

XDR for Windows, Linux, Mac and M365 cloud

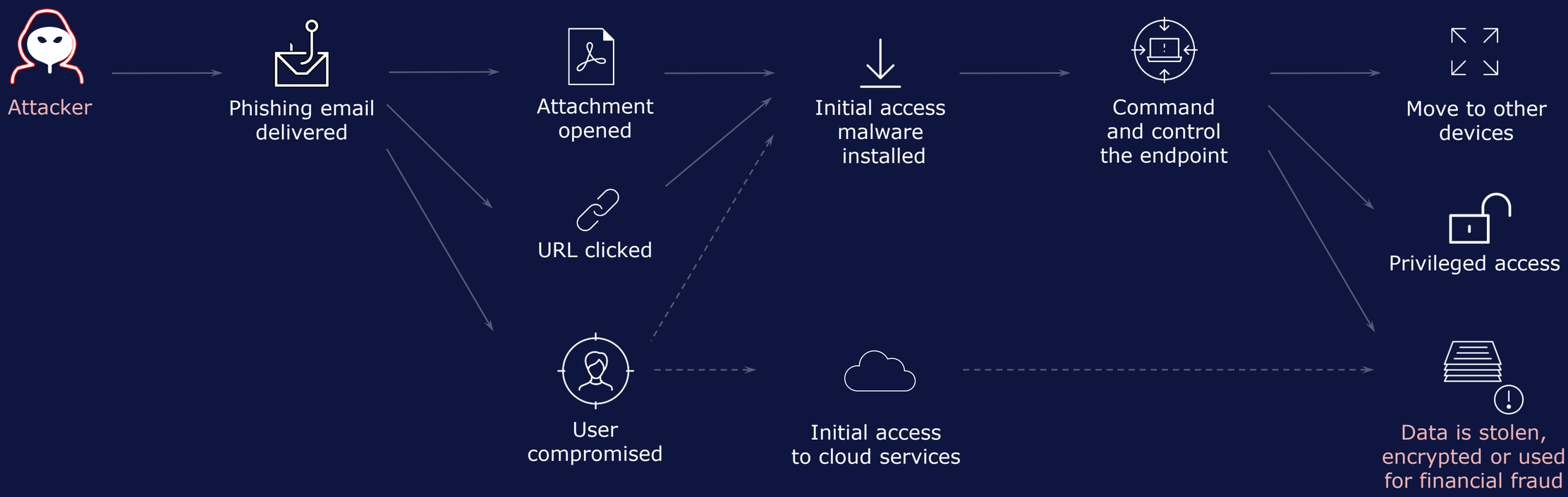
A1 ICT Distribucija

A1

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

LABYRINTH

WITH secure

WithSecure Elements Exposure Management

XM for Endpoints, Network, Users and Cloud

A1 ICT Distribucija

A1

Proactive security approach

Know what makes up your attack surface

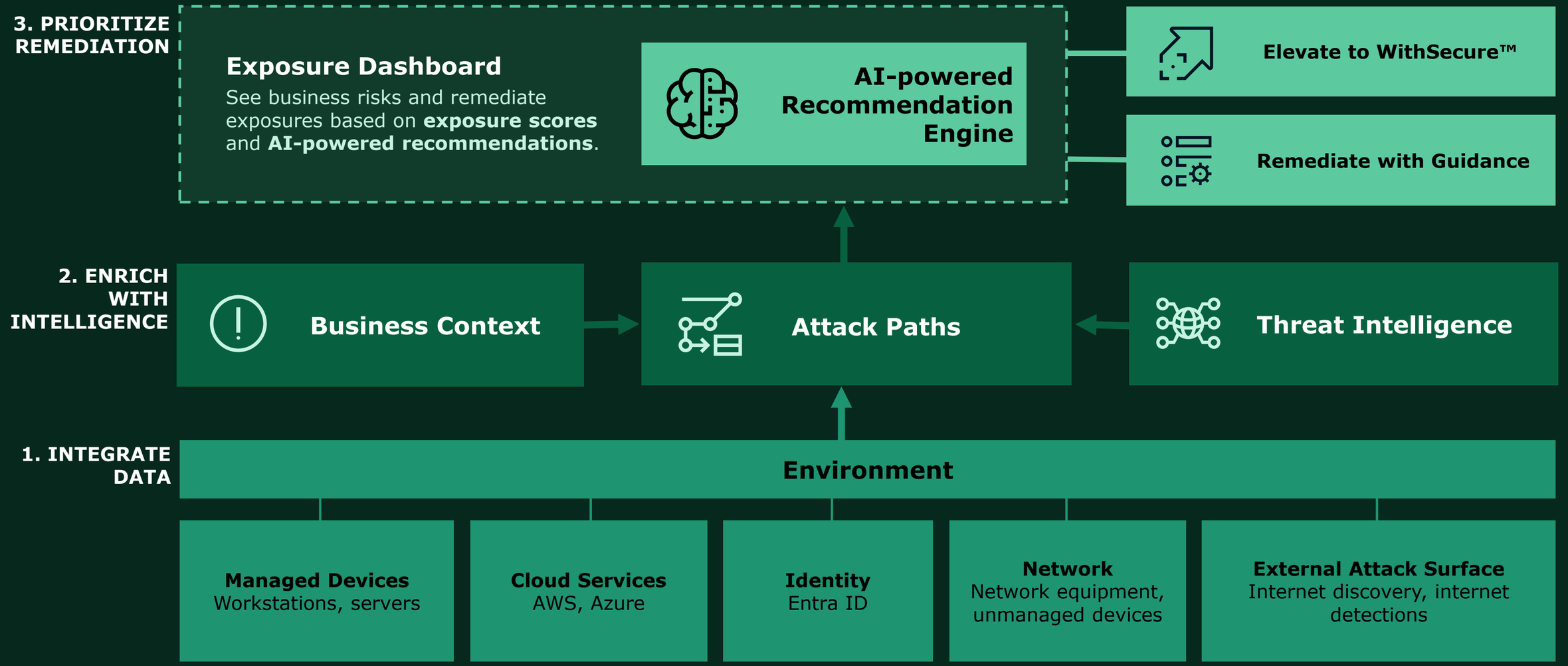
Know what to prioritize when remediating exposures

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

Pojmovi tehnologije WithSecure

- **Elements EPP** = **E**nd**p**oint **P**rotection = antivirusna zaštita, koja se instalira na radne stanice, servere i mobilne uređaje
  - Next-Generation zaštita sa ransomware zaštitom: DeepGuard, Rollback, DataGuard, Application Control
- **Elements EDR** = **E**ndpoint **D**etection & **R**esponse = aktivno traženje aktivnog cybersecurity napada prema ponašanju procesa – radi paralelno sa EPP
- **Elements XDR** = E**x**tended **D**etection & **R**esponse = proširenje kombinacije EPP+EDR u Microsoft365: Collaboration Protection (=antivirus za M365) + Identity Security (=EDR za M365 EntraID korisnike)
- **Elements XM** = E**x**posure **M**anagement = proaktivna zaštita, koja nam daje informacije o potencialnim ranjivostim u softveru, konfiguraciji, itd.