NTT ITMAP | ASIA WatchGuard

PHÒNG CHỐNG RANSOMWARE VỚI CÔNG NGHỆ WATCHGUARD XDR & ENDPOINT SECURITY

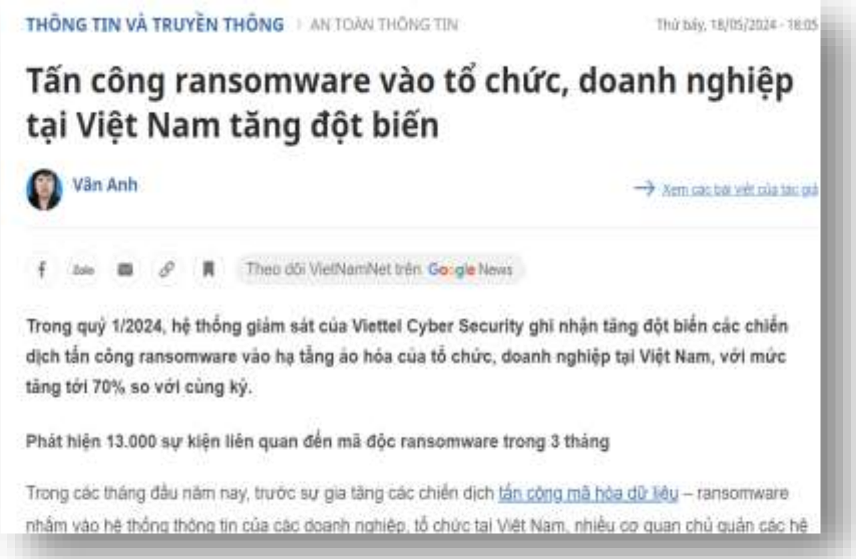
BỐI CẢNH RANSOMWARE ĐANG GIA TĂNG

Hậu quả nghiêm trọng, bao gồm:

- **Mất dữ liệu:** Dữ liệu bị mã hóa và không thể truy cập được, gây ảnh hưởng nghiêm trọng đến hoạt động kinh doanh.
- **Gián đoạn hoạt động:** Doanh nghiệp có thể buộc phải ngừng hoạt động trong thời gian dài để giải mã dữ liệu, dẫn đến thiệt hại về tài chính và uy tín.
- **Thiệt hại về tài chính:** Nạn nhân phải trả tiền chuộc cho kẻ tấn công, gây ra gánh nặng tài chính lớn.
- **Mất uy tín:** Việc bị tấn công ransomware có thể làm hỏng danh tiếng của tổ chức và khiến khách hàng mất niềm tin.

Quan điểm cá nhân:

“Các chuyên gia IT/an ninh mạng ngày nay càng phải giỏi và nhanh hơn để giữ cho hạ tầng CNTT của các doanh nghiệp không bị tấn công hoặc càng ít vấn đề càng tốt”



THÔNG TIN VÀ TRUYỀN THÔNG | AN TOÀN THÔNG TIN　　Thứ bảy, 18/05/2024 - 18:05

Tấn công ransomware vào tổ chức, doanh nghiệp tại Việt Nam tăng đột biến

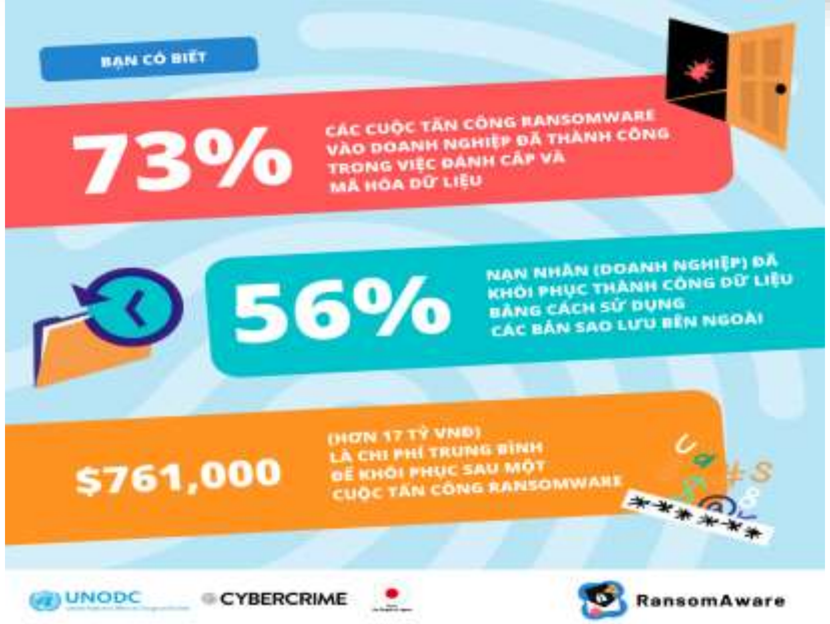
Vân Anh　　→ Xem các bài viết của tác giả

Theo dõi VietNamNet trên Google News

Trong quý 1/2024, hệ thống giám sát của Viettel Cyber Security ghi nhận tăng đột biến các chiến dịch tấn công ransomware vào hạ tầng ảo hóa của tổ chức, doanh nghiệp tại Việt Nam, với mức tăng tới 70% so với cùng kỳ.

Phát hiện 13.000 sự kiện liên quan đến mã độc ransomware trong 3 tháng

Trong các tháng đầu năm nay, trước sự gia tăng các chiến dịch tấn công mã hóa dữ liệu – ransomware nhắm vào hệ thống thông tin của các doanh nghiệp, tổ chức tại Việt Nam, nhiều cơ quan chủ quản các hệ

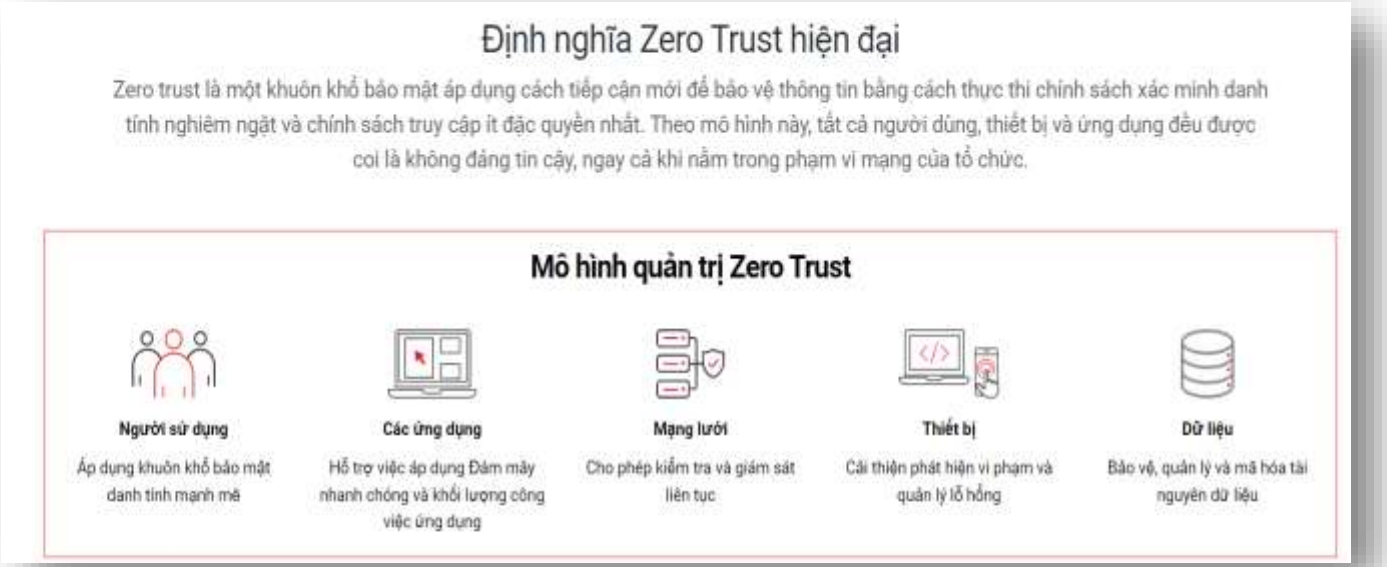

BẠN CÓ BIẾT
73%
CÁC CUỘC TẤN CÔNG RANSOMWARE VÀO DOANH NGHIỆP ĐÃ THÀNH CÔNG TRONG VIỆC ĐÁNH CẮP VÀ MÃ HÓA DỮ LIỆU
56%
NẠN NHÂN (DOANH NGHIỆP) ĐÃ KHÔI PHỤC THÀNH CÔNG DỮ LIỆU BẰNG CÁCH SỬ DỤNG CÁC BẢN SAO LƯU BÊN NGOÀI
$761,000
(HƠN 17 TỶ VND) LÀ CHI PHÍ TRUNG BÌNH ĐỂ KHÔI PHỤC SAU MỘT CUỘC TẤN CÔNG RANSOMWARE
UNODC
CYBERCRIME
RansomAware

CẦN TIẾP CẬN ĐẾN
GIẢI PHÁP CÔNG NGHỆ
PHÒNG CHỐNG RANSOMWARE TIÊN TIẾN

ZERO TRUST FRAMEWORK
MÔ HÌNH BẢO MẬT TIÊN TIẾN

Thuật ngữ "zero trust" lần đầu tiên được đặt ra bởi **John Kindervag** là một kiến trúc sư bảo mật.
Trong một bài báo được xuất bản vào năm 2010, Kindervag giải thích cách các mô hình an ninh mạng truyền thống không cung cấp sự bảo vệ đầy đủ vì tất cả chúng đều yêu cầu một yếu tố tin cậy.

“không tin tưởng ai, bất kể họ là ai hoặc đến từ đâu”



Định nghĩa Zero Trust hiện đại

Zero trust là một khuôn khổ bảo mật áp dụng cách tiếp cận mới để bảo vệ thông tin bằng cách thực thi chính sách xác minh danh tính nghiêm ngặt và chính sách truy cập ít đặc quyền nhất. Theo mô hình này, tất cả người dùng, thiết bị và ứng dụng đều được coi là không đáng tin cậy, ngay cả khi nằm trong phạm vi mạng của tổ chức.

Mô hình quản trị Zero Trust

Người sử dụng
Áp dụng khuôn khổ bảo mật danh tính mạnh mẽ

Các ứng dụng
Hỗ trợ việc áp dụng Đám mây nhanh chóng và khối lượng công việc ứng dụng

Mạng lưới
Cho phép kiểm tra và giám sát liên tục

Thiết bị
Cải thiện phát hiện vi phạm và quản lý lỗ hổng

Dữ liệu
Bảo vệ, quản lý và mã hóa tài nguyên dữ liệu

https://www.watchguard.com/wgrd-solutions/security-trends/zero-trust/understanding-zero-trust

WatchGuard EDR

WatchGuard's Endpoint Security products boast a secret advantage that sets them apart and redefines threat detection

Daniel Phuan
Senior Principal Consultant

WatchGuard Endpoint Security in numbers

Global. Experienced. Trusted.

The **Zero-Trust Application Service**, empowered by advanced AI technologies, classifies **over 5 million new binaries every week**

Unmatched security. **AI-based technology**, working hand in hand with our team of **cybersecurity experts**, guarantees a **100% application classification** rate

3 out of 1,000 unknown applications, blocked by the Zero-Trust Application Service are classified as **new malware**

WatchGuard protects **+4 million endpoints**

ABOUT

Founded in **1996**

Operations in **7** countries; direct presence in **21**

1,200 Employees

250K+ Customers

100+ Distributors
16,000+ Active Partners

WatchGuard

Cybersecurity Landscape

Cybersecurity Landscape

Insider Threats

Security Risks Are Rising

CYBER ATTACK

54% of companies have experienced a third-party DATA BREACH in the past year

CVE-ID

RANSOMWARE

Vulnerabilities

Cost of Downtime

Business Challenges

44%

Of organizations lack sufficient visibility into endpoint activities

74%

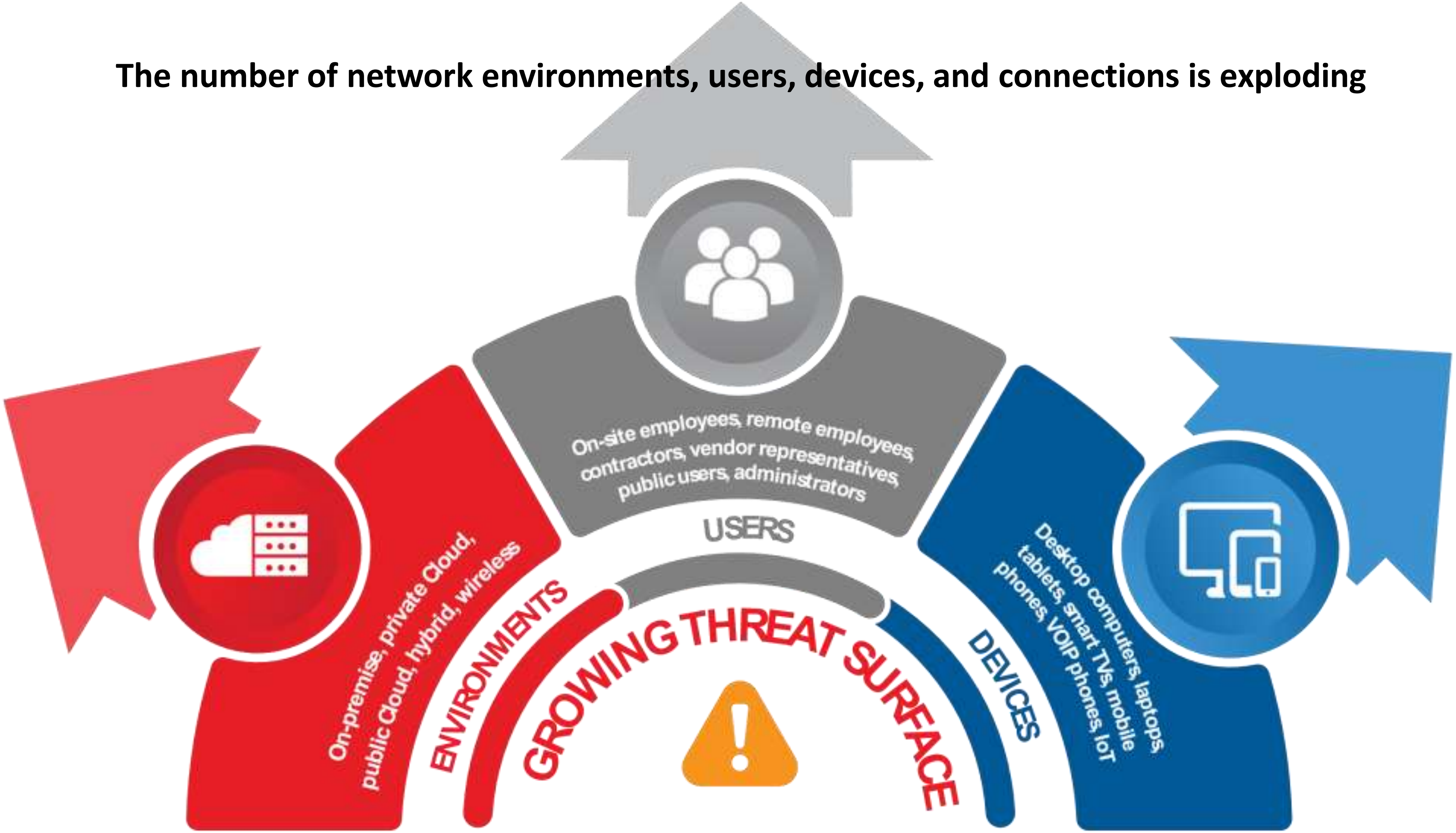
Of all breaches include the human element

60%

Of victims were breached due to an unpatched known vulnerability where the patch was not applied

An Expanding, Highly Complex Threat Surface

The number of network environments, users, devices, and connections is exploding


On-site employees, remote employees, contractors, vendor representatives, public users, administrators
USERS
On-premise, private Cloud, public Cloud, hybrid, wireless
ENVIRONMENTS
Desktop computers, laptops, tablets, smart TVs, mobile phones, VOIP phones, IoT
DEVICES
GROWING THREAT SURFACE

62% of midmarket organizations report their **IT environments are more complex now than two years ago**.

Why Endpoint Security?

Relating Endpoint Security and Home Security

Locks

Blocks access to protect the valuables inside. Locks can be picked or bypassed, and the homeowner would not immediately become aware of the intrusion.

Sensors

Cameras, motion sensors, lights and alarms alert on the presence of potential intruders. They can also be a deterrent. However, actions are delayed if the homeowner does not see the alert immediately and there are false alarms.

Monitoring

Security professionals install security technology and monitor 24/7 to evaluate real threats from false alarms and take immediate action to address home intrusions by dispatching security guards and/or police.

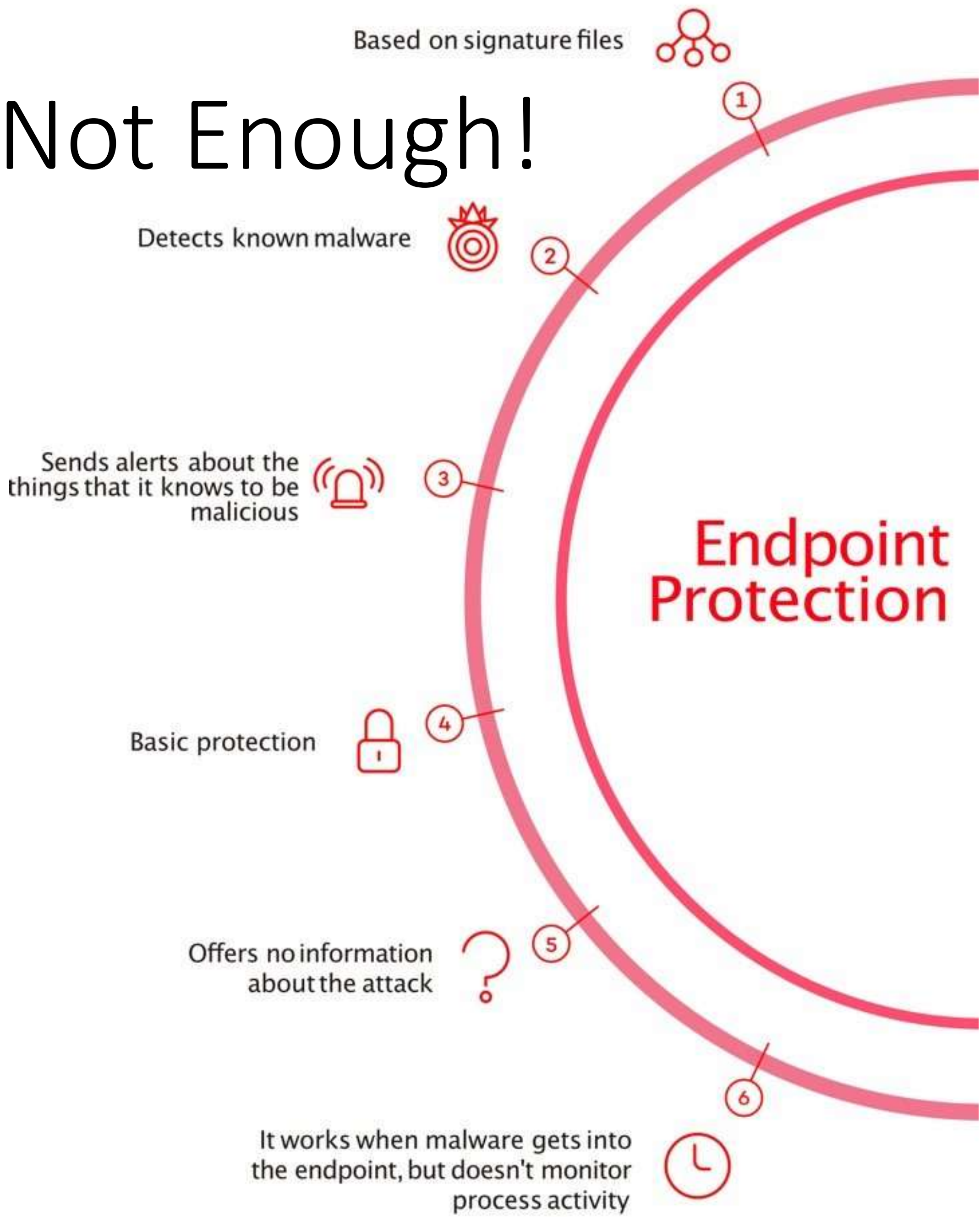
Can you use sensors without locks? Would you?

Traditional AV Protection is Not Enough!

- Baseline protection for all endpoints based on legacy methodologies
- No protection for unknown threats, fileless attacks, or in-memory exploits
- No proactive detections

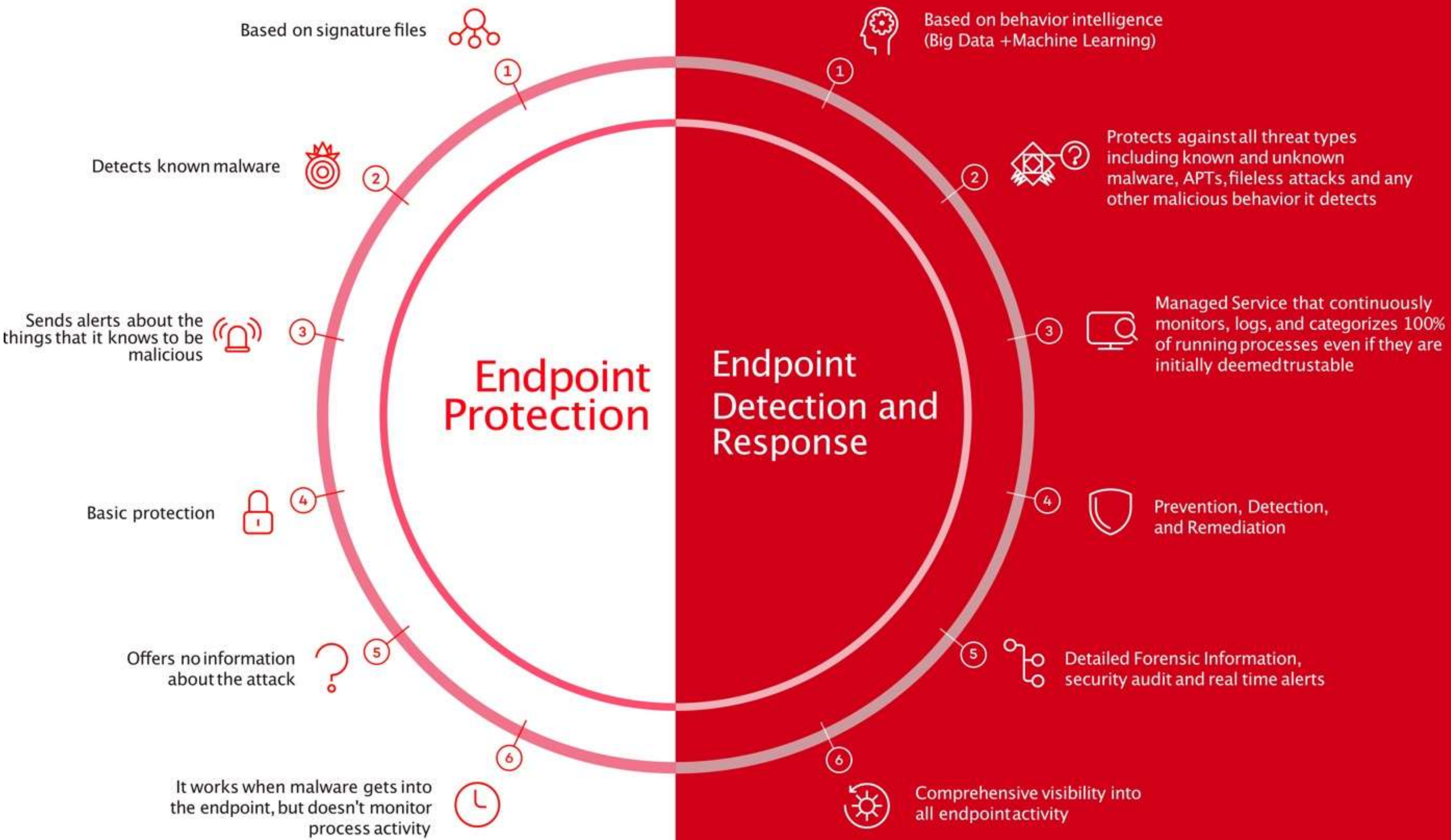
Evolving threat landscape

- Continually growing number of threats
- Increasing sophistication of threats



Endpoint Protection

1. Based on signature files
2. Detects known malware
3. Sends alerts about the things that it knows to be malicious
4. Basic protection
5. Offers no information about the attack
6. It works when malware gets into the endpoint, but doesn't monitor process activity



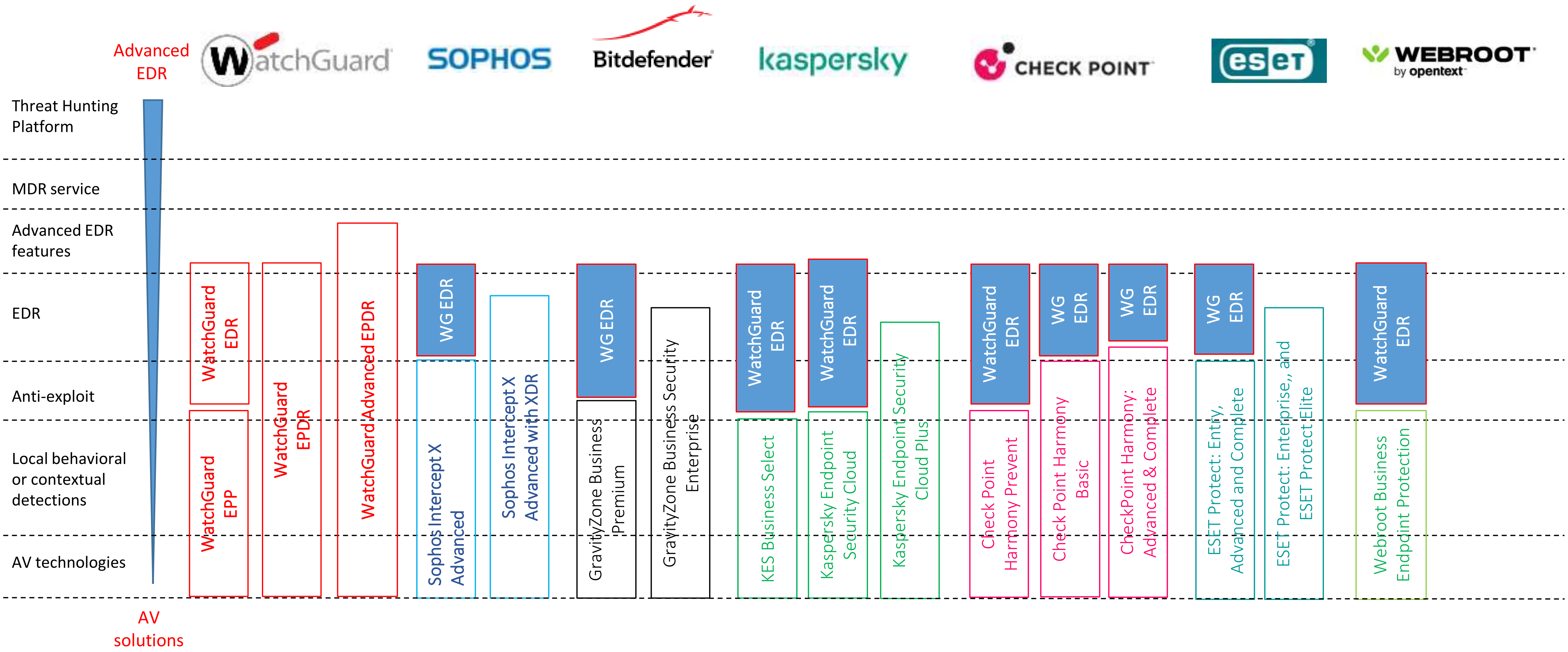
Endpoint Protection

1. Based on signature files
2. Detects known malware
3. Sends alerts about the things that it knows to be malicious
4. Basic protection
5. Offers no information about the attack
6. It works when malware gets into the endpoint, but doesn't monitor process activity

Endpoint Detection and Response

1. Based on behavior intelligence (Big Data +Machine Learning)
2. Protects against all threat types including known and unknown malware, APTs, fileless attacks and any other malicious behavior it detects
3. Managed Service that continuously monitors, logs, and categorizes 100% of running processes even if they are initially deemed trustable
4. Prevention, Detection, and Remediation
5. Detailed Forensic Information, security audit and real time alerts
6. Comprehensive visibility into all endpoint activity

WatchGuard EDR, On Top of Existing Solutions for Complete Protection


Advanced EDR
WatchGuard
SOPHOS
Bitdefender
kaspersky
CHECK POINT
eset
WEBROOT by opentext
Threat Hunting Platform
MDR service
Advanced EDR features
EDR
Anti-exploit
Local behavioral or contextual detections
AV technologies
AV solutions
WatchGuard EDR
WatchGuard EPP
WatchGuard EPDR
WatchGuard Advanced EPDR
WG EDR
Sophos Intercept X Advanced
Sophos Intercept X Advanced with XDR
WG EDR
GravityZone Business Premium
GravityZone Business Security Enterprise
WatchGuard EDR
KES Business Select
WatchGuard EDR
Kaspersky Endpoint Security Cloud
Kaspersky Endpoint Security Cloud Plus
WatchGuard EDR
Check Point Harmony Prevent
WG EDR
Check Point Harmony Basic
WG EDR
CheckPoint Harmony: Advanced & Complete
WG EDR
ESET Protect: Entry, Advanced and Complete
ESET Protect: Enterprise,, and ESET Protect Elite
WatchGuard EDR
Webroot Business Endpoint Protection

Why WatchGuard EDR?

The Endpoint Is the Epicenter of Today's Cybersecurity Attacks

Deploying an evolved endpoint security solution such as **WatchGuard EDR** offers a preventive zero-day approach.

Good, Better, Best:

- Antivirus or traditional endpoint protection is a necessary, base security layer
- Adding an EDR (Endpoint Detection and Response) solution complements existing antivirus endpoint protection, introducing advanced security capabilities
- A combination of AV + EDR gives your clients an integrated Antivirus + EDR product, creating a comprehensive solution for complete security

WatchGuard EDR Is Compatible with Third-Party AV-like Solutions

Our backend shows that we run alongside other products

- % of WG Endpoint Security deployments with other AVs/EDRs:
  - 12.60% representing nearly 500K devices!
- Main products we are coexisting with are listed below:

Sophos	Bitdefender
Kaspersky	Trend Micro
Malwarebytes	SentinelOne
Microsoft Defender	Broadcom (Symantec)
Trellix (McAfee)	Carbon Black
Cylance	…and more.

Exclusions for third-party products are not a requirement

Customer Objections

Q

We've been using our current antivirus for years without any issues. Our current system seems to be working fine. Why should we change something that works?

A

Traditional antivirus solutions are excellent at detecting known threats. However, they can miss advanced threats, like zero-day attacks and fileless malware that are present in today’s landscape of cyber threats. You don’t need to change anything; EDR complements your current protection.

Q

Why should I buy another endpoint security solution when you've provided the best endpoint security solution as a partner? Having two security systems seems redundant. Aren't they doing the same thing?

A

While it might seem that way, EDR and traditional antivirus serve different purposes. Antivirus is excellent for catching known threats using signature-based detection. EDR provides advanced behavioral analysis and continuous monitoring to detect and respond to unknown threats. Together, they offer a more comprehensive security solution, ensuring no threat goes unnoticed.

Q

Can the EDR handle the noise from constant alerts? Our current system generates too many alerts, making it hard to manage.

A

WatchGuard EDR significantly reduces alert noise with its AI-driven detection and Zero-Trust Application Service. It filters out irrelevant alerts and prioritizes genuine threats, allowing your team to focus on high-priority tasks. This streamlined approach improves efficiency and ensures faster response times, making your work easier and more effective.

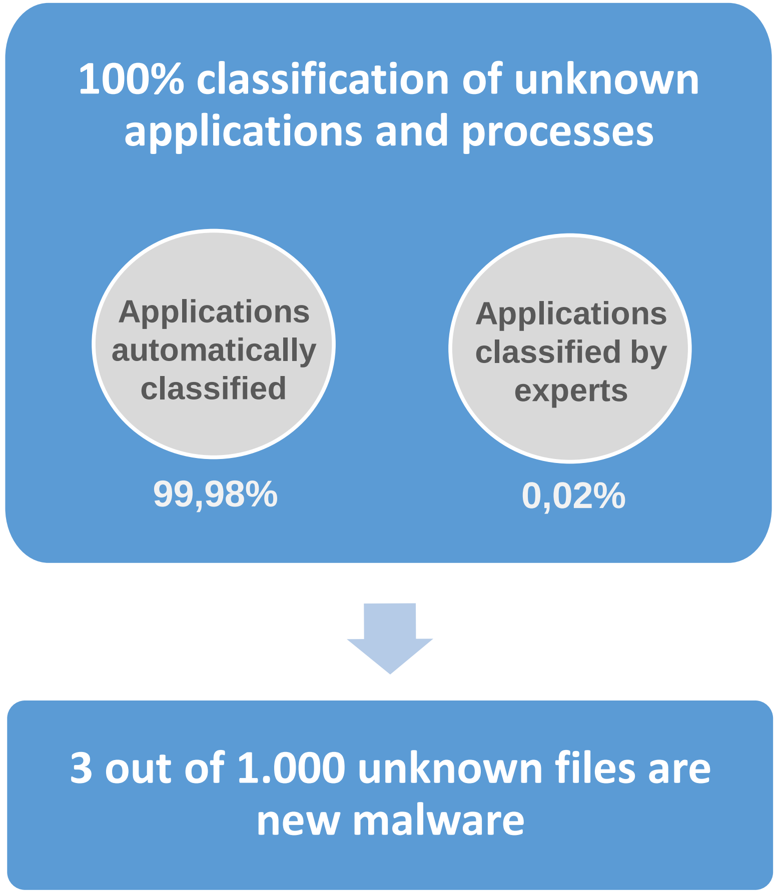
What Makes Our EDR Technology Unique

- **Innovative deny-by-default approach to endpoint security** – there is no other endpoint solution on the market with the Zero-Trust philosophy built in.

- Classifies all the UNKNOWNS; only allows goodware to execute.

- Extremely effective protection model.
  - Low level of unknowns due to the knowledge in our Collective Intelligence and the AI-powered classification technologies
  - **No burden for administrators** to classify UNKNOWNs, the Zero-Trust Application Service does it for them.
  - Continuously **classifying** processes that were already classified as goodware, to detect **supply chain attacks or silent attacks** that use goodware to perform malicious actions.

The Zero-Trust Application Service



100% classification of unknown applications and processes

Applications automatically classified

99,98%

Applications classified by experts

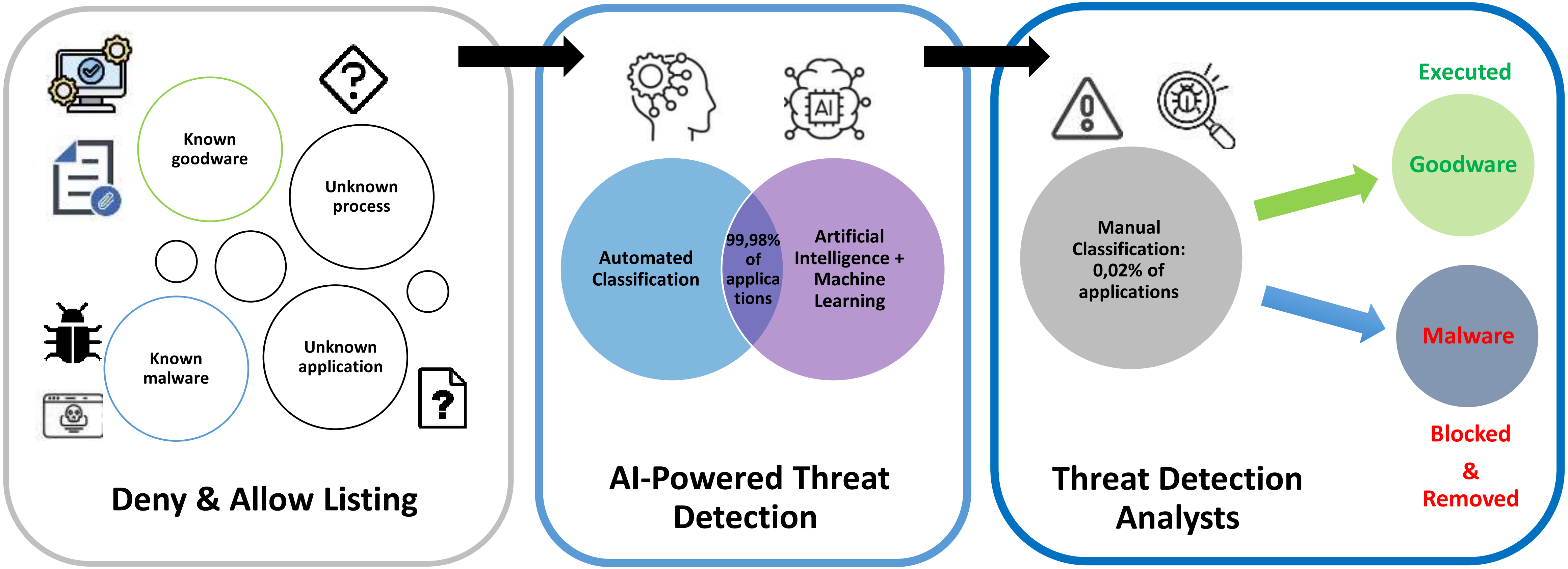
0,02%

3 out of 1.000 unknown files are new malware

The Zero-Trust Application Service:

Your Guard Against the Unknown

How the Zero-Trust Application Was Born



Known goodware

Unknown process

Known malware

Unknown application

Deny & Allow Listing

Automated Classification

99,98% of applications

Artificial Intelligence + Machine Learning

AI-Powered Threat Detection

Manual Classification: 0,02% of applications

Executed

Goodware

Malware

Blocked & Removed

Threat Detection Analysts

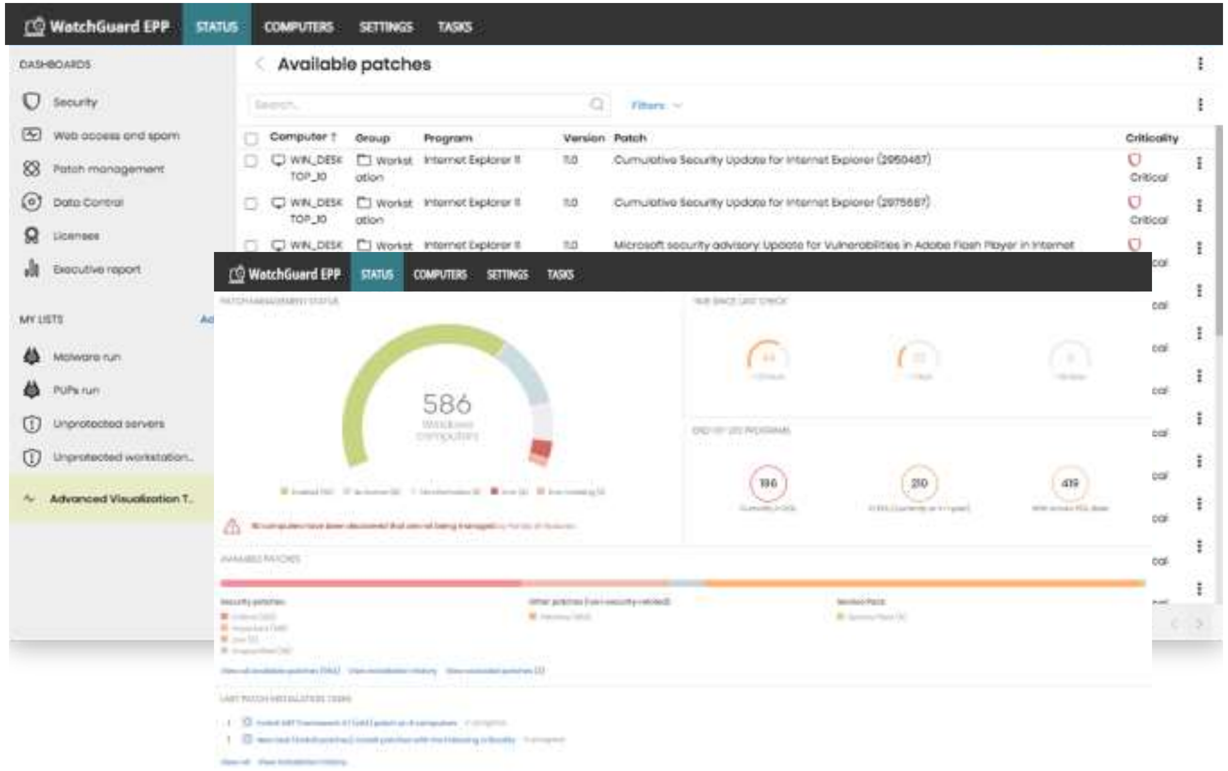
100% Classification

Add-on: WatchGuard Patch Management

Patch assessment and management for OS and 3rd-party applications

Patch Management is a module for managing vulnerabilities of the operating systems and third-party applications on Windows workstations and servers but also to:

- **Audit, monitor and prioritize** operating systems and application updates.
- **Prevent incidents**, systematically reducing the attack surface created by software vulnerabilities.
- **Contain and mitigate vulnerability exploitation attacks** with immediate updates.
- **Reduce operating costs**. It does not require the deployment of additional agents. Updates are launched remotely and provides complete, unattended visibility into all vulnerabilities, pending updates and EOL (End of Life) applications.



Computer ↑	Group	Program	Version	Patch	Criticality
WIN_DESKTOP_10	Workstation	Internet Explorer 11	11.0	Cumulative Security Update for Internet Explorer (2950467)	Critical
WIN_DESKTOP_10	Workstation	Internet Explorer 11	11.0	Cumulative Security Update for Internet Explorer (2975687)	Critical
WIN_DESK	Workst	Internet Explorer 11	11.0	Microsoft security advisory: Update for Vulnerabilities in Adobe Flash Player in Internet	

More than 80% of all successful cyberattacks exploited **known vulnerabilities**, where existing patches hadn’t been applied. **WannaCry** and **Petya** exploited vulnerabilities that had been known for months.

WatchGuard EPDR Delivers Superior Security

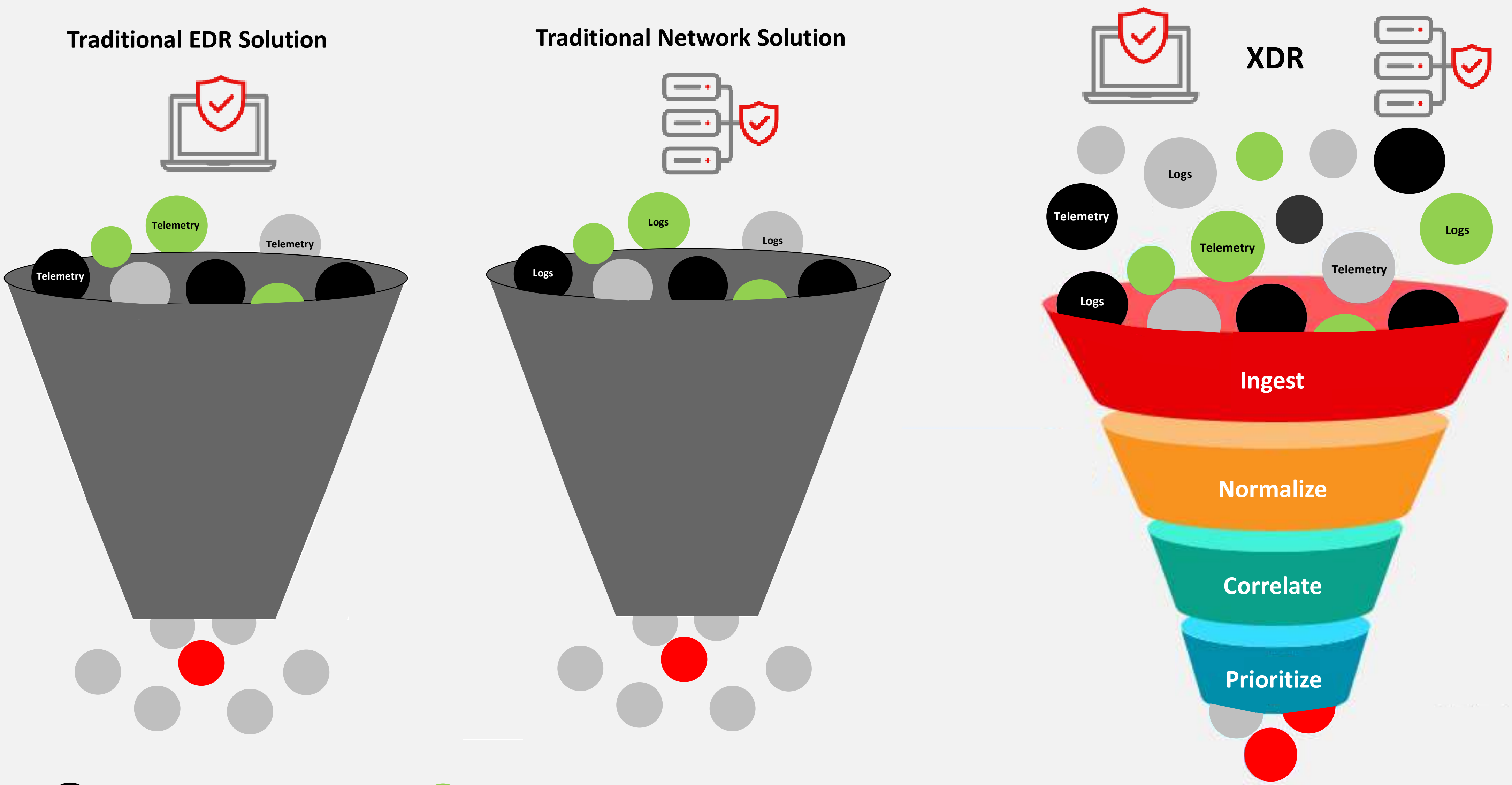
It goes beyond the traditional security with the Zero-Trust approach, the combined classification service, machine learning and threat hunting service.

Zero-day, ransomware, crypto-jacking and advanced targeted attack are not a challenge anymore for any SMB, mid-size company or large enterprise.

- On top of its EPP capabilities against known & zero day malware
- Advanced protection against never-seen before threats
- Proactive defense against emerging and APT threats
- Built on new and evolving ML and Deep Learning models
- Automatic detailed forensic analysis
- Immediate protection against all threat, known and unknown
- True "Zero-Trust" Model:
  - **Zero-Trust Application Service**: 100% classification of applications
  - **Threat Hunting Service**: detecting hackers and insiders

WatchGuard XDR

How Does XDR Work?



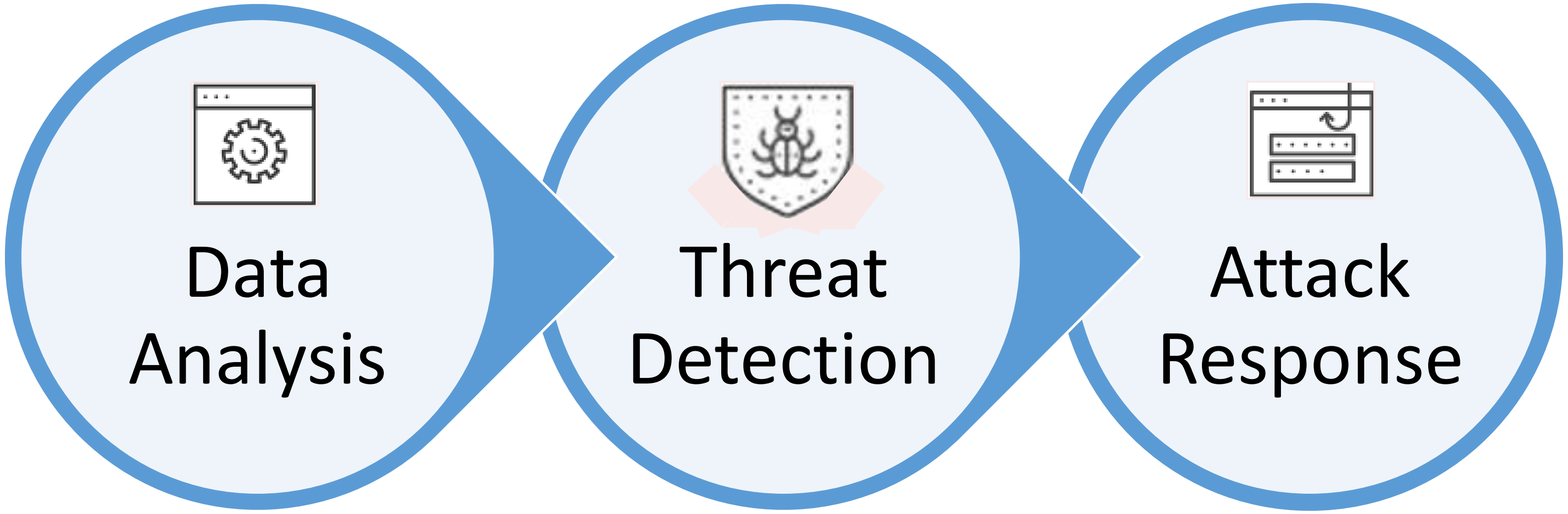
● Known bad data

● Known good data

● Unknown data

● High confident detection

What is XDR used for?



Data Analysis

Threat Detection

Attack Response

Data aggregation and context correlation

Examine alerts and report critical ones

Remove detected threat and apply security policies

Why is XDR Important?

1 - Prioritized View

XDR correlates and combines activity data at different security levels, enabling a prioritized view of threats.

2 – Security Consolidation

Integrating XDR into workstations, devices, servers, and networks leads to a more effective and unified threat viewpoint.

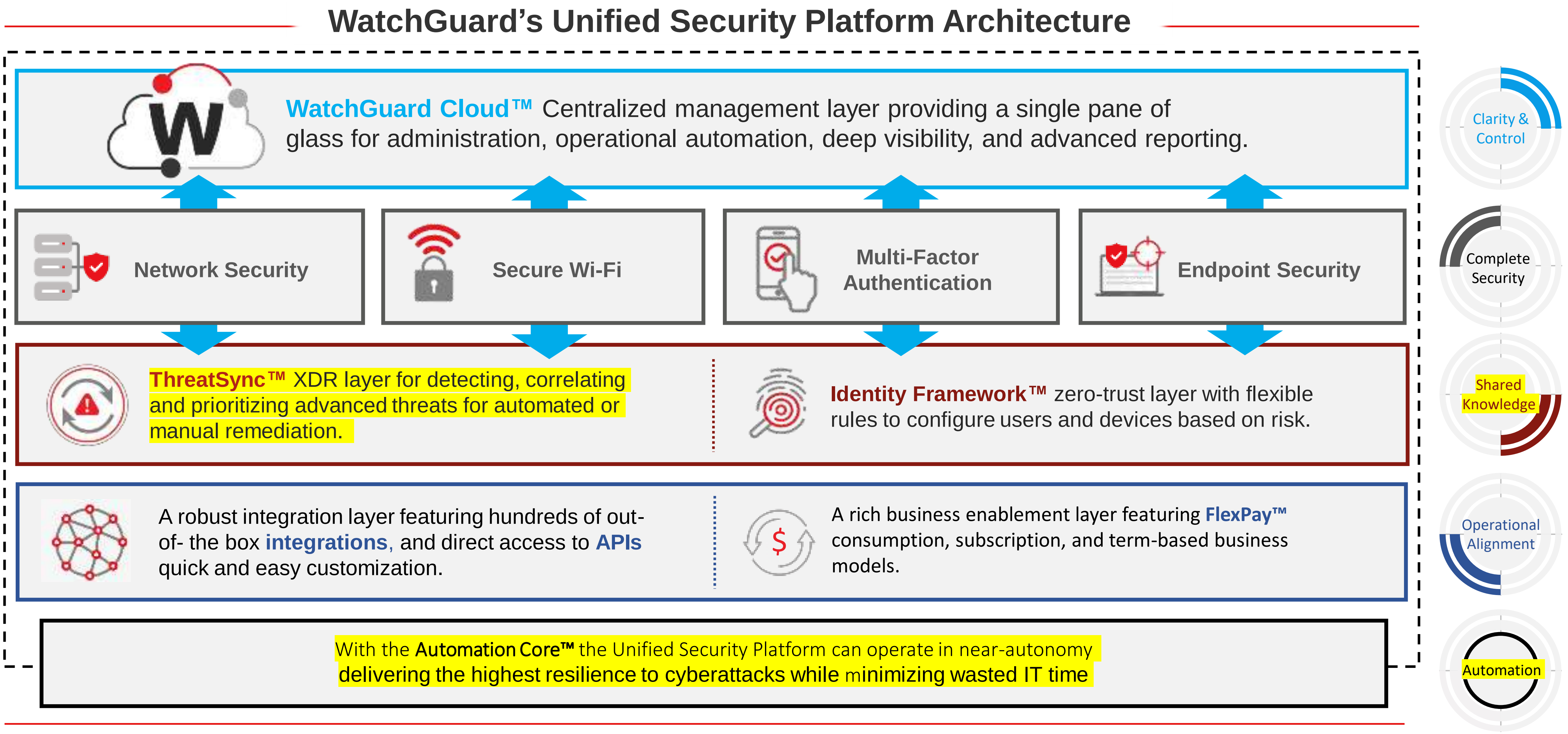
3 - Contextual View

Many individual events as a whole can be indicators of an incident. XDR enables more insightful data and cross-domain contextualization to detect earlier.

4 – Stop Attacks Faster

XDR provides better protection for your business through earlier detection and faster response.

XDR Is a Key Element of Shared Knowledge and Automation



WatchGuard's Unified Security Platform Architecture

WatchGuard Cloud™ Centralized management layer providing a single pane of glass for administration, operational automation, deep visibility, and advanced reporting.

Network Security

Secure Wi-Fi

Multi-Factor Authentication

Endpoint Security

ThreatSync™ XDR layer for detecting, correlating and prioritizing advanced threats for automated or manual remediation.

Identity Framework™ zero-trust layer with flexible rules to configure users and devices based on risk.

A robust integration layer featuring hundreds of out-of- the box **integrations**, and direct access to **APIs** quick and easy customization.

A rich business enablement layer featuring **FlexPay™** consumption, subscription, and term-based business models.

With the **Automation Core™** the Unified Security Platform can operate in near-autonomy delivering the highest resilience to cyberattacks while minimizing wasted IT time

WatchGuard ThreatSync Is the Right Answer

Simple to Use

We prioritize XDR features for a skills-deprived market with an intuitive interface and automation for MSPs.

Other companies have complex XDR set-up and configuration steps requiring specialized knowledge.

1

Comprehensive

New XDR capabilities fuel our Unified Security Platform with broad technology including identity security.

Other companies misleadingly market an XDR product with only endpoint capabilities and lack identity security and MSP features.

2

No Added Costs

XDR is a key tenet of security and should be available to every customer. ThreatSync is a platform capability – add products and grow your XDR with no additional costs.

Other companies charge an additional XDR license to expose detection and response features.

3

“Another benefit of XDR products is that they can provide what traditionally have been complex security operations capabilities and make them more accessible to security teams that do not have the resources for more custom-made point solutions.”

Gartner Innovation Insight for Extended Detection and Response, Refreshed April 8, 2021

ThreatSync in Action!

Uses Cases: Let’s see XDR in Action! (I)

Problem: Zero Day Advanced Persistent Threats (APTs) Detections

- Due to the near instant expectation for files to be downloaded over HTTP(S), today the firewall must allow unknown files to be downloaded while it submits the file for sandbox analysis.

Solution: XDR Solution Unmasks a Zero-Day APT

- **Detect** using behavioral analysis and machine learning, to identify anomalous behavior that may indicate a zero-day APT.
- **Prioritize** the potential zero-day APT, with a risk score based on the severity and potential impact of the threat.
- **Contain** the risk using containment actions, such as isolating affected endpoints, blocking malicious traffic, quarantine files or terminating suspicious processes of the zero-day APT.
- **Remediate** automatically using security policies to prevent future incidents.
- **Notify** security teams through an email alert that includes relevant details about the suspicious behavior and affected devices.

Uses Cases: Let’s see XDR in Action! (II)

Problem: Processes Making Malicious Connections

- There are many processes running on our computers that are not malicious but can make malicious connections, including browsers and email clients.

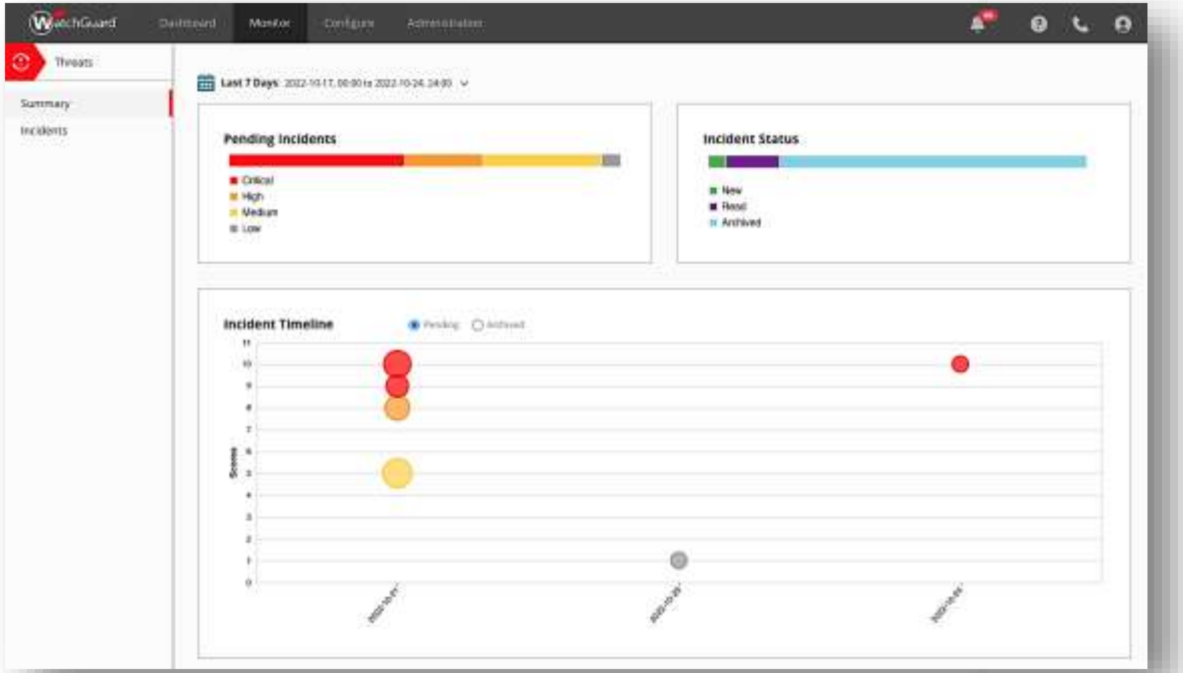
Solution: XDR Solution alerts Unusual Connection Behaviors

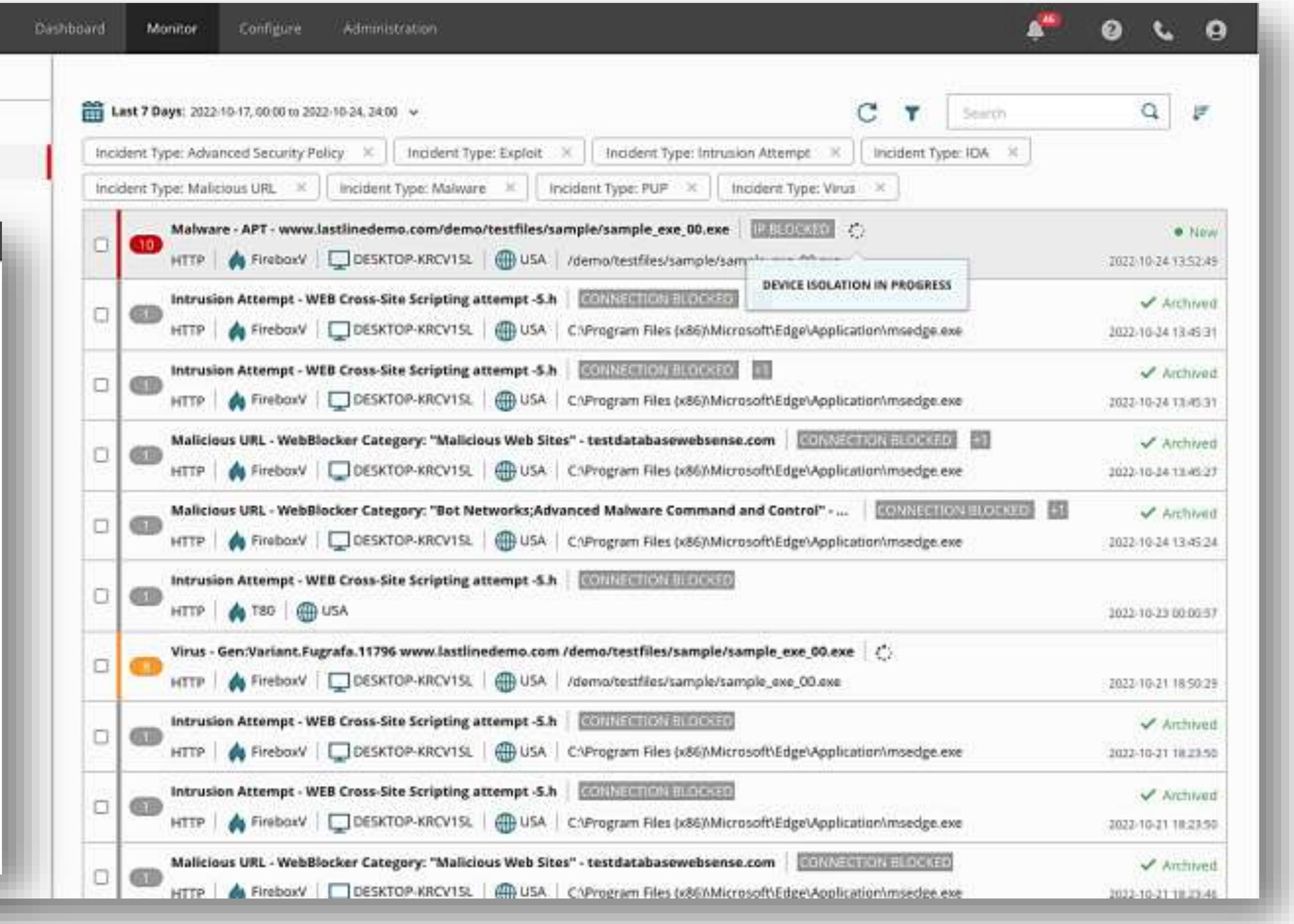
- **Detect** potentially malicious connections made by processes on endpoints.
- **Prioritize and Score the Risk** if the process making the potentially malicious connection is a known and trusted application like a browser or email client.
- **Respond** by blocking the connections at the firewall or terminate the process on endpoints to correlate them to individual applications running on endpoints.
- **Remediate** automatically using security policies to prevent future incidents.
- **Notify** security teams through an email alert that includes relevant details about the suspicious behavior and affected devices.

WatchGuard ThreatSync in WatchGuard Cloud

Incidents Monitoring and Timeline

Correlated telemetry provides context and defines incidents





Last 7 Days: 2022-10-17, 00:00 to 2022-10-24, 24:00

Incident Type: Advanced Security Policy ✕ | Incident Type: Exploit ✕ | Incident Type: Intrusion Attempt ✕ | Incident Type: IOA ✕ | Incident Type: Malicious URL ✕ | Incident Type: Malware ✕ | Incident Type: PUP ✕ | Incident Type: Virus ✕

□ 10 **Malware - APT - www.lastlinedemo.com/demo/testfiles/sample/sample_exe_00.exe** | IP BLOCKED ● New
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | /demo/testfiles/sample/sam... 2022-10-24 13:52:49

DEVICE ISOLATION IN PROGRESS

□ 1 **Intrusion Attempt - WEB Cross-Site Scripting attempt -5.h** | CONNECTION BLOCKED ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-24 13:45:31

□ 1 **Intrusion Attempt - WEB Cross-Site Scripting attempt -5.h** | CONNECTION BLOCKED +1 ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-24 13:45:31

□ 1 **Malicious URL - WebBlocker Category: "Malicious Web Sites" - testdatabasewebsense.com** | CONNECTION BLOCKED +1 ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-24 13:45:27

□ 1 **Malicious URL - WebBlocker Category: "Bot Networks;Advanced Malware Command and Control" - ...** | CONNECTION BLOCKED +1 ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-24 13:45:24

□ 1 **Intrusion Attempt - WEB Cross-Site Scripting attempt -5.h** | CONNECTION BLOCKED
HTTP | T80 | USA 2022-10-23 00:00:57

□ 8 **Virus - Gen:Variant.Fugrafa.11796 www.lastlinedemo.com /demo/testfiles/sample/sample_exe_00.exe**
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | /demo/testfiles/sample/sample_exe_00.exe 2022-10-21 18:50:29

□ 1 **Intrusion Attempt - WEB Cross-Site Scripting attempt -5.h** | CONNECTION BLOCKED ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-21 18:23:50

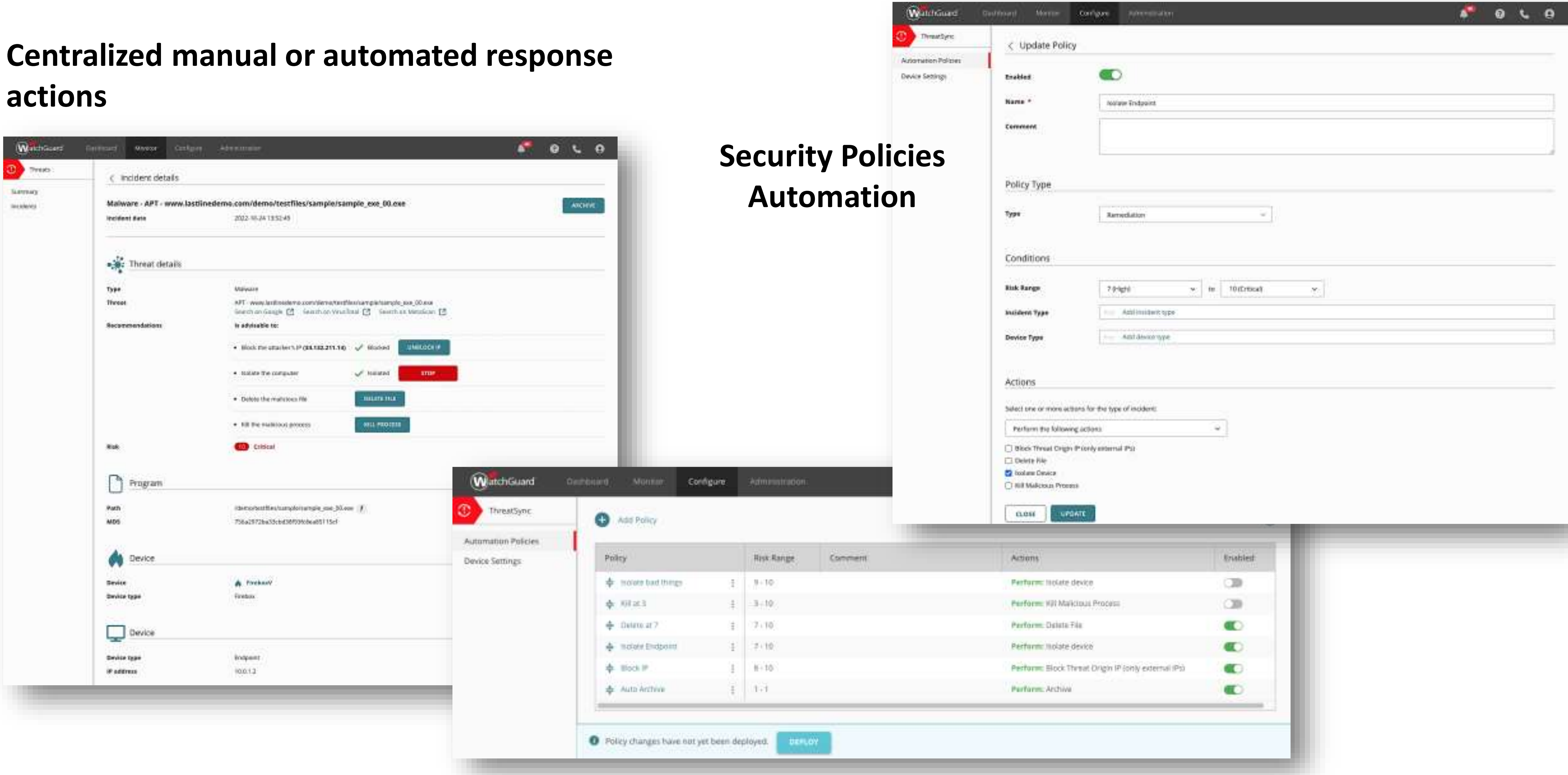
□ 1 **Intrusion Attempt - WEB Cross-Site Scripting attempt -5.h** | CONNECTION BLOCKED ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-21 18:23:50

□ 1 **Malicious URL - WebBlocker Category: "Malicious Web Sites" - testdatabasewebsense.com** | CONNECTION BLOCKED ✓ Archived
HTTP | FireboxV | DESKTOP-KRCV1SL | USA | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe 2022-10-21 18:23:46

WatchGuard ThreatSync in WatchGuard Cloud

Centralized manual or automated response actions

Security Policies Automation



Incident details

Malware - APT - www.lastlinedemo.com/demo/testfiles/sample/sample_exe_00.exe ARCHIVE

Incident date	2022-10-24 13:52:49

Threat details

Type	Malware
Threat	APT - www.lastlinedemo.com/demo/testfiles/sample/sample_exe_00.exe Search on Google · Search on VirusTotal · Search on MetaScan
Recommendations	**It is advisable to:**
	• Block the attacker's IP (**34.132.211.14**) ✓ Blocked UNBLOCK IP
	• Isolate the computer ✓ Isolated STOP
	• Delete the malicious file DELETE FILE
	• Kill the malicious process KILL PROCESS
Risk	10 Critical

Program

Path	/demo/testfiles/sample/sample_exe_30.exe
MD5	756a2572ba33cbd36f036bea85115cf

Device

Device	FireboxV
Device type	Firebox

Device

Device type	Endpoint
IP address	10.0.1.2

Add Policy

Policy	Risk Range	Comment	Actions	Enabled
Isolate bad things	9 - 10		**Perform:** Isolate device	○
Kill at 3	3 - 10		**Perform:** Kill Malicious Process	○
Delete at 7	7 - 10		**Perform:** Delete File	●
Isolate Endpoint	7 - 10		**Perform:** Isolate device	●
Block IP	8 - 10		**Perform:** Block Threat Origin IP (only external IPs)	●
Auto Archive	1 - 1		**Perform:** Archive	●

Policy changes have not yet been deployed. DEPLOY

Update Policy

Enabled	●
Name *	Isolate Endpoint
Comment	

Policy Type

Type	Remediation

Conditions

Risk Range	7 (High) to 10 (Critical)
Incident Type	Add incident type
Device Type	Add device type

Actions

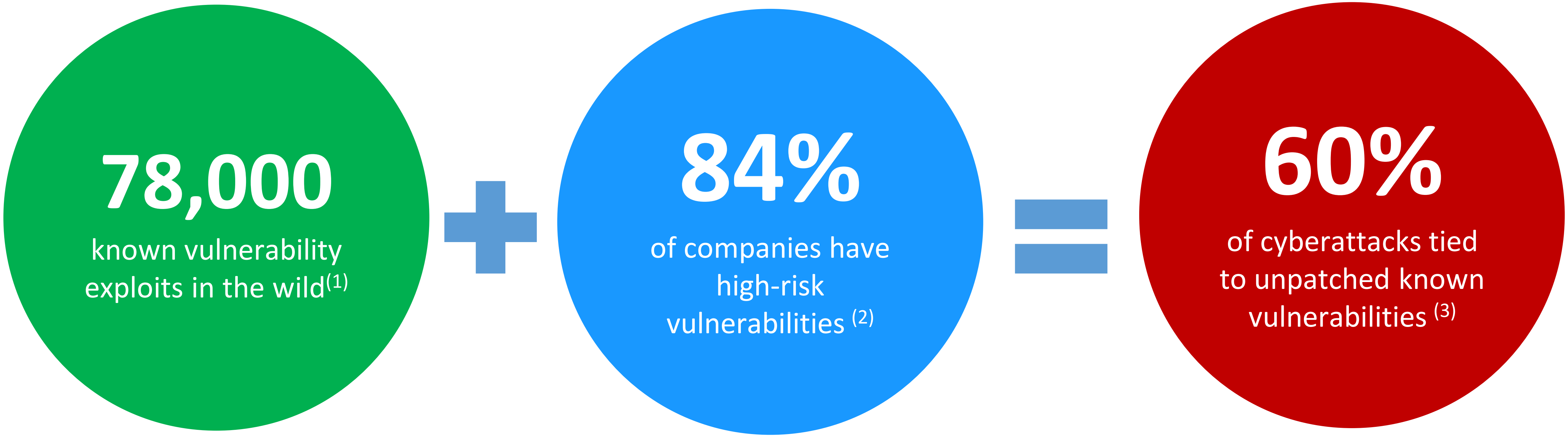
Select one or more actions for the type of incident:

Perform the following actions

- ☐ Block Threat Origin IP (only external IPs)
- ☐ Delete File
- ☑ Isolate Device
- ☐ Kill Malicious Process

CLOSE UPDATE

Did you know that …



78,000

known vulnerability exploits in the wild[1]

84%

of companies have high-risk vulnerabilities [2]

60%

of cyberattacks tied to unpatched known vulnerabilities [3]

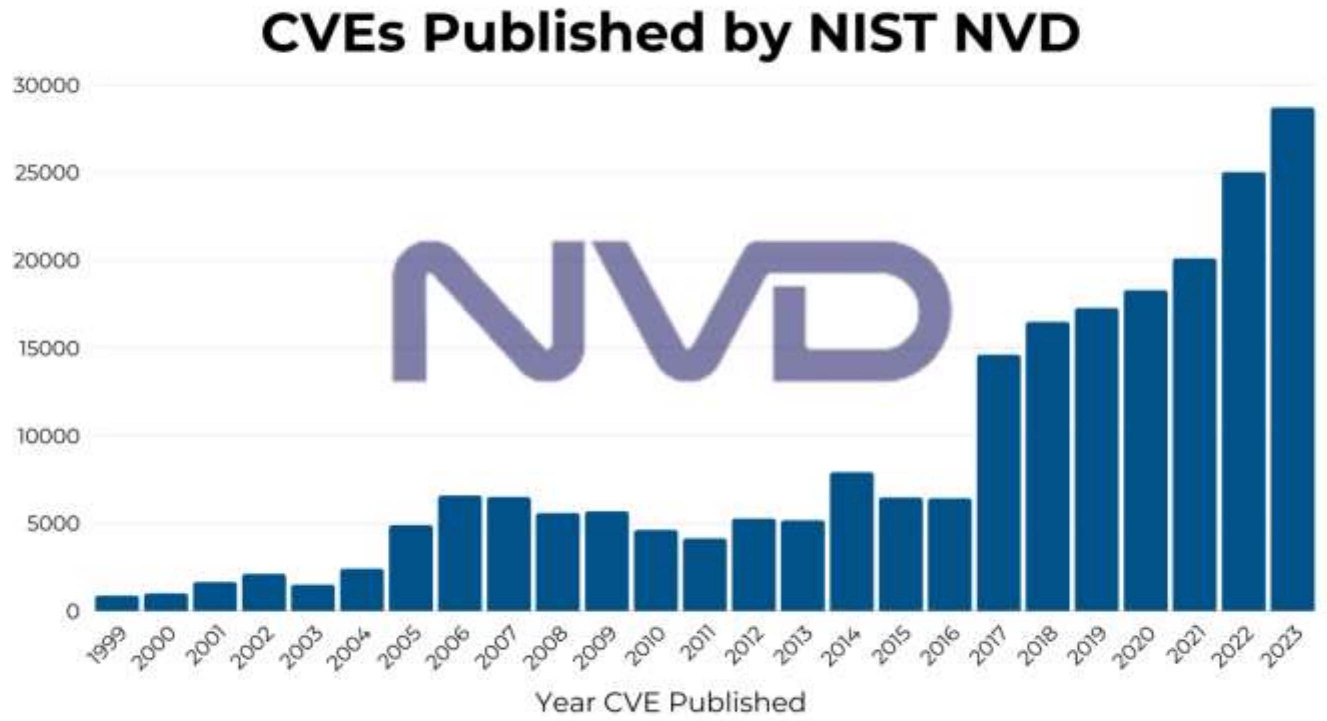
3 out of 4
of applications have at least one security flaw

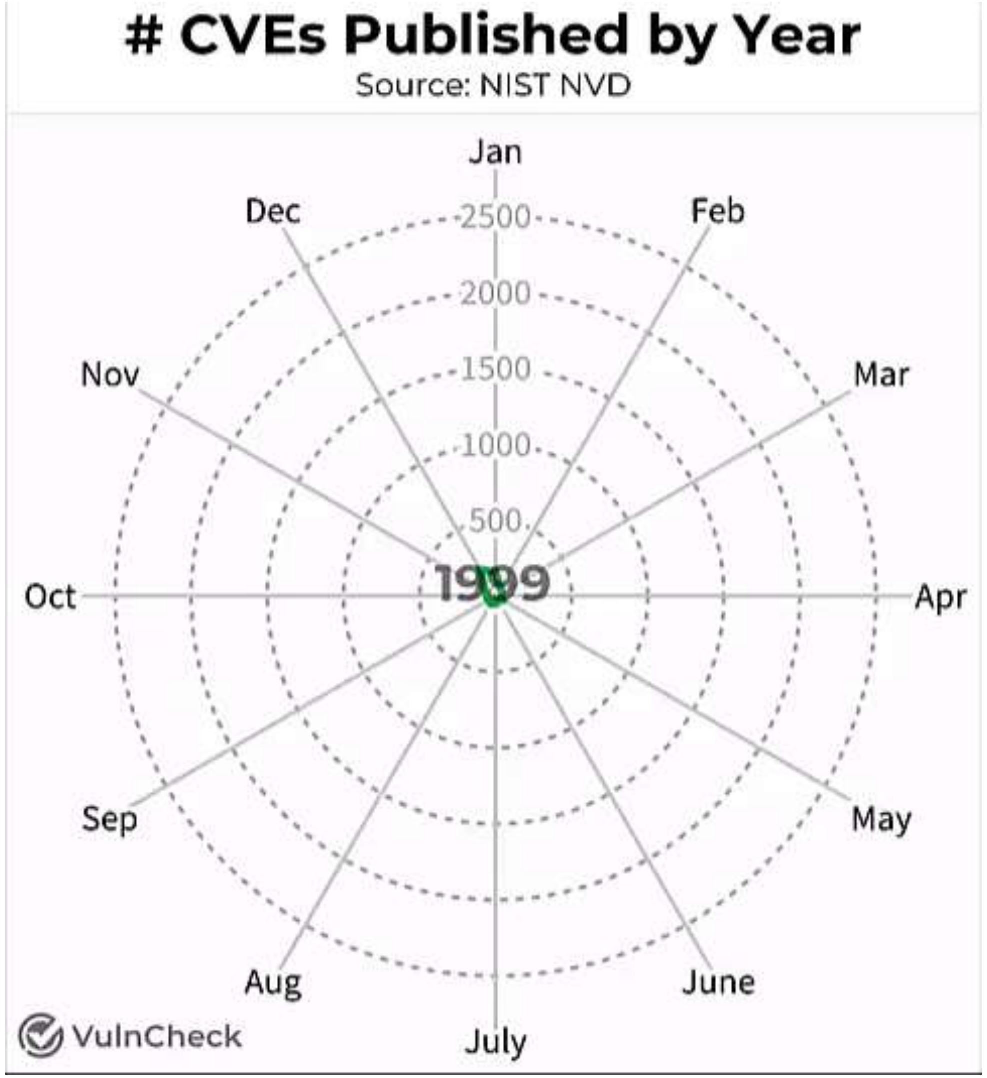
At least, 50%
have an available patch

These statistics point to a severe lack of vulnerability management

[1] IBM Security X-Force Threat Intelligence Index 2023
[2] https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-corporate-networks-2020/
[3] Ponemon Institute Vulnerability Survey

Why Patch Management





Compliance

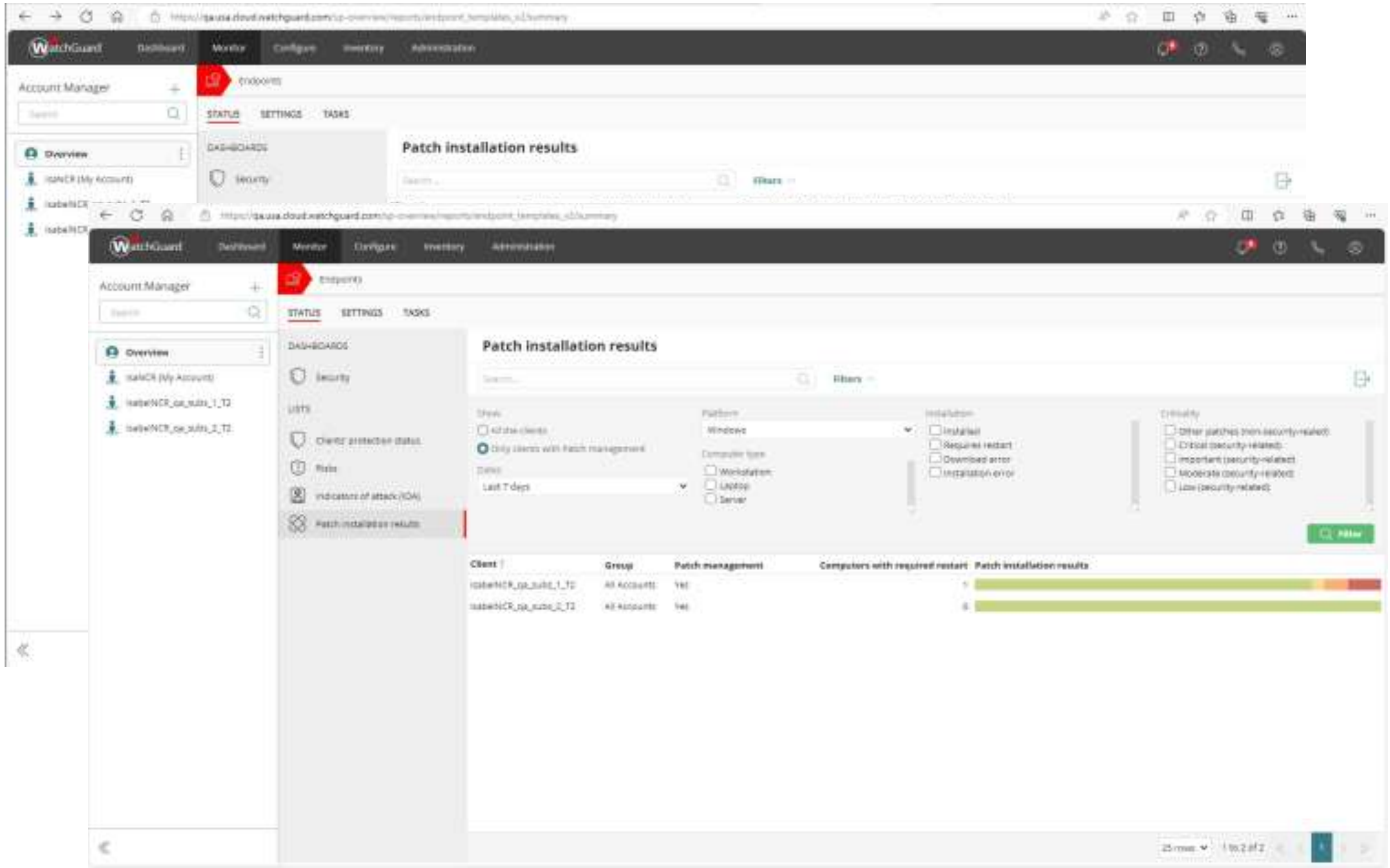
- All regulations emphasize vulnerability assessment and patch management

Regulation	Reference	
CIS	**7.5** **7.6**	Perform Automated **Vulnerability Scans** of Internal Enterprise Assets Perform Automated **Vulnerability Scans** of Externally-Exposed Enterprise Assets
PCI-DSS	**11.3** **11.4**	**External and internal vulnerabilities** are regularly identified, prioritized, and addressed. External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.
GDPR	**Security Measures**	Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.
NIST SP 800-171	**3.11.12**	**Scan for vulnerabilities** in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Service Providers Offering Patch- Management-as-a-Service (PMaaS)

Endpoint Manager (multi-client view):

- Patch Management allows scheduling tasks to install patches or do it on demand
- **New!** Visibility into patching installation status from the service provider
- **New!** Identify subscribers with patch installation tasks that generated errors and drill down to review them.
- **New!** Export option



Patch installation results

Show
□ All the clients
● Only clients with Patch management

Dates
Last 7 days

Platform
Windows

Computer type
□ Workstation
□ Laptop
□ Server

Installation
□ Installed
□ Requires restart
□ Download error
□ Installation error

Criticality
□ Other patches (non security-related)
□ Critical (security-related)
□ Important (security-related)
□ Moderate (security-related)
□ Low (security-related)

Client	Group	Patch management	Computers with required restart	Patch installation results
isabelNCR_qa_subs_1_T2	All Accounts	Yes	1	🟩🟧🟥
isabelNCR_qa_subs_2_T2	All Accounts	Yes	0	🟩

WatchGuard Patch Management

Scanning

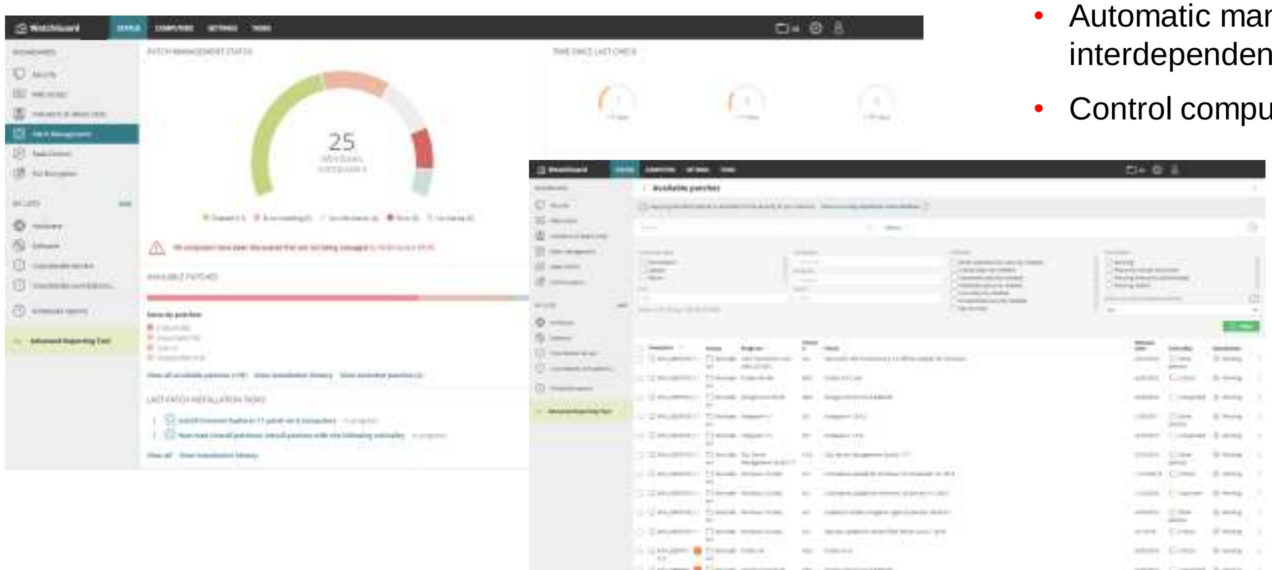
- Scan all computers from anywhere, at anytime.
- No need for additional deployments (single agent).

Assessment and planning

- Verification of impacted software component, priority of missing patch, etc.
- Gradual roll out of patches after testing, for standard and highly sensitive endpoints.
- Automatic updates with conditional rules and exceptions as needed.

WatchGuard Patch Management

Keeps systems and applications free from vulnerabilities at a minimal cost (reducing infrastructure, communication, and technical staff costs), without interrupting users' work.



Intelligence

- Update all versions of Windows.
- Update hundreds of third-party applications.
- Add the patch or software exclusions that you need.

Deployment

- Update hundreds or thousands of computers in real time.
- Automatic management of patch interdependencies.
- Control computer restarts.