The Role of MDR in Identity, Cloud, Endpoint, and Network

Closing Gaps and Stopping Threats Across the Entire Attack Chain

Jonas Spieckermann

Manager Sales Engineering Central Europe

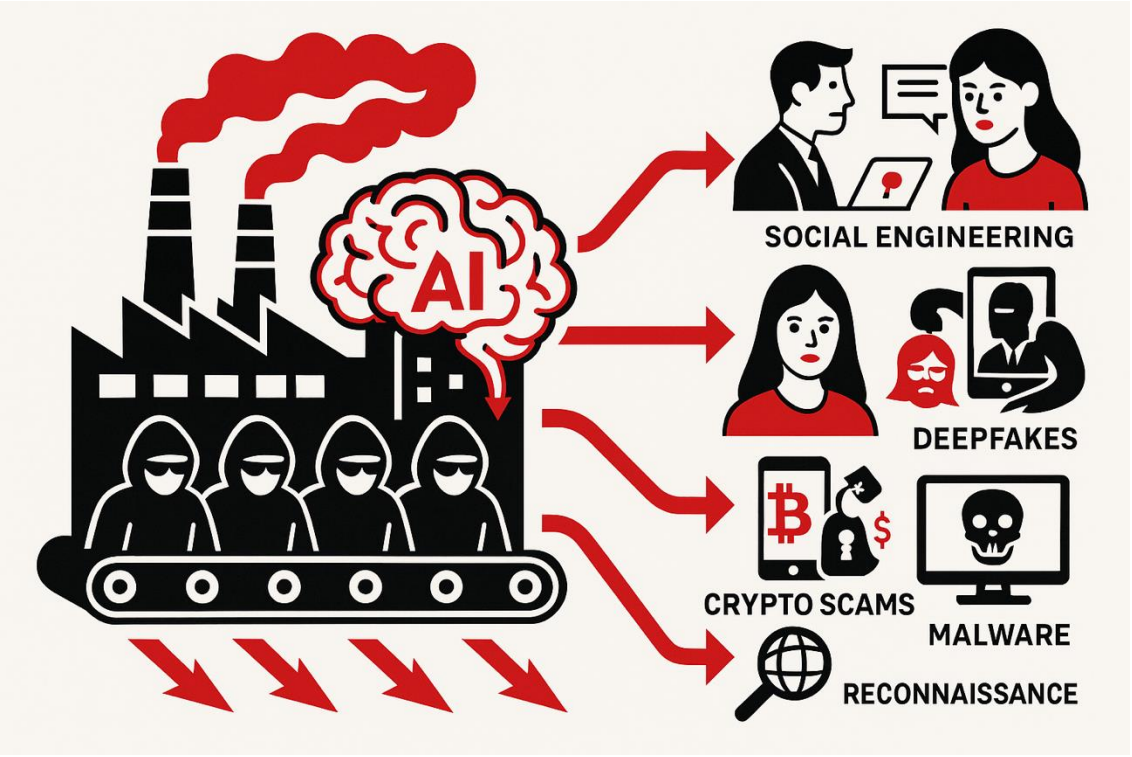
Real Security for the Real World

Why Is MDR Crucial Now

Hybrid IT is here to stay

- Ubiquitous access has increased our attack surface
- Organizations will maintain legacy and Cloud/SaaS native for the foreseeable future

AI catalyzing cyberattacks



- **Better:** Deepfakes and Social Engineering to Crypto Scams
- **Faster:** Automation of Everything from Reconnaissance, Zero-Day Exploits and Malware
- **Stronger:** Business Email Compromise Increasing Click Rates to 50%

Evolving AI in the SOC

Basic Machine Learning ’05

Rise of Ransomware Gangs ‘17

AI Arms Race ’20 GPT born

2005 – Smarter Antivirus
Early machine learning makes antivirus smarter.

2010 – Stuxnet Wake-Up Call
Nation-state attacks prompt behavior-based detection.

2014 – DARPA Cyber Challenge
AI competes to detect and patch vulnerabilities.

2016 – AI in Endpoint Security
Predictive EDR launched by major AV vendors

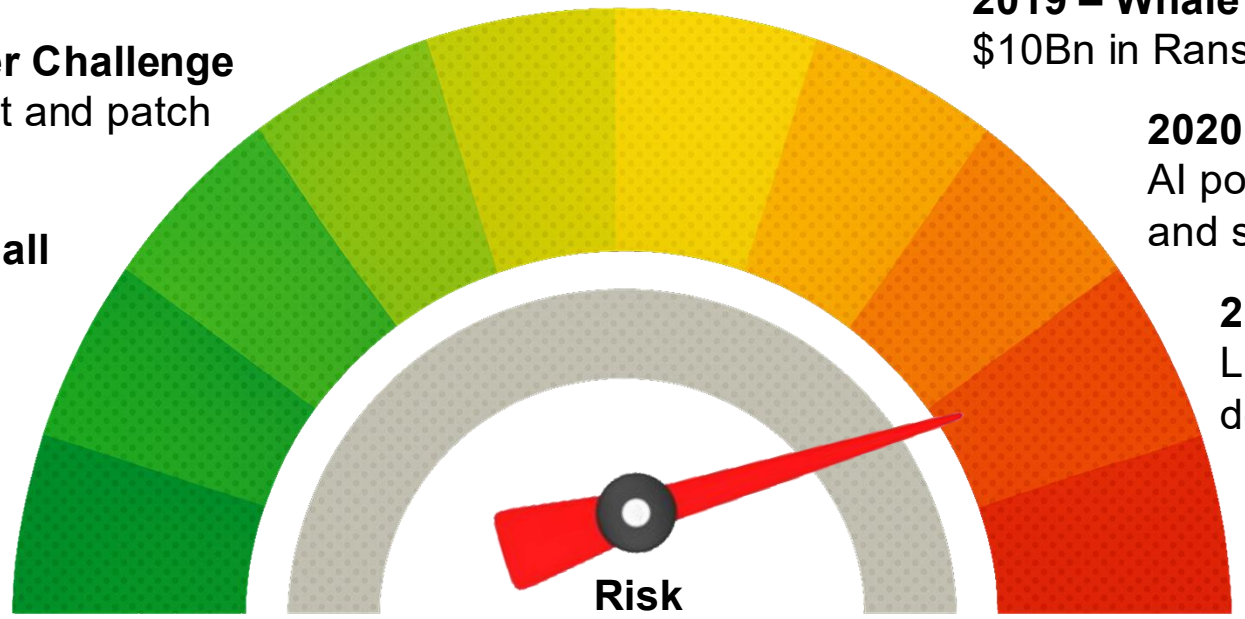
2017 – Automation of SOC
Using ML Across the Stack

2019 – Whale Hunting
$10Bn in Ransomware damage

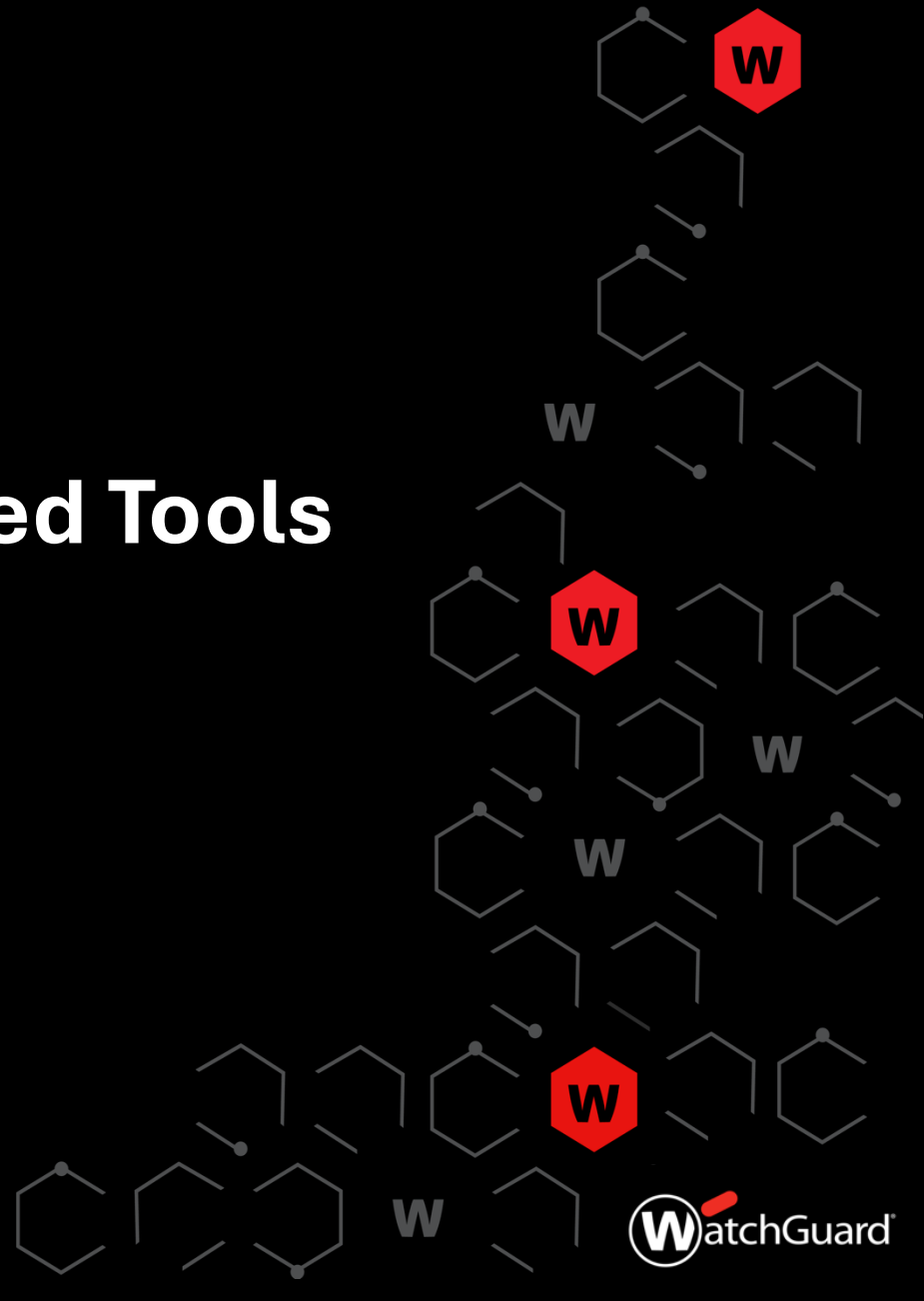
2020 – Deepfake Attacks Rise
AI powers phishing, impersonation, and social engineering.

2025 – Generative AI in Hacking
LLMs used by both attackers and defenders at scale.

2027 – Agentic Hacking
Fully autonomous attack campaigns

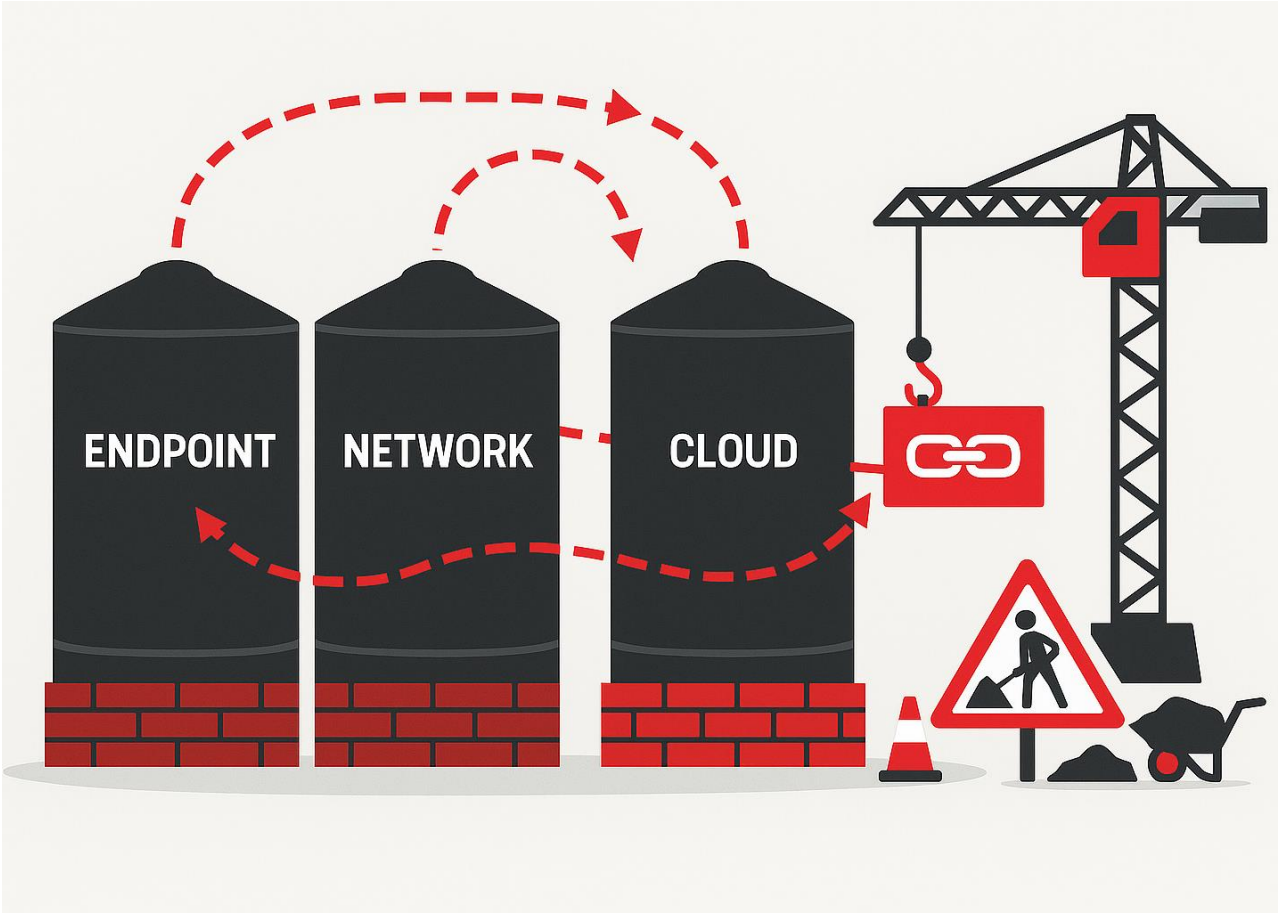


Common Pitfalls of Siloed Tools



The problem with silos

- In the past URL filtering, IPS, and firewalling required teams to look in three separate places to find network attacks.
- Today, teams don’t have unified telemetry, policy, and automation to power their SOC and try to stitch things together with a SIEM.
- Limited visibility across attack surfaces.
- Disjointed alerts and high false positives.
- Delayed detection and inconsistent response.
- No ability to unify policy and layer on AI for copilots or strong automation.



Unified Managed Detection and Response

Comprehensive Managed Detection & Response (MDR) services built for organizations using WatchGuard security products.

Built on the unified threat visibility from WatchGuard firewalls, endpoint protection, identity, and network security tools

Combines signals across identity, endpoint, cloud, and network

AI-driven correlation and prioritization. Not possible with disparate data sources that aren't prepped

24/7 human-led SOC for investigation and guided response that can affect response, policy, and advisory from a single source of truth.

Product-Specific Defenses

AuthPoint: Protecting more than Identities

- Protects: SaaS Products and Corporate Access

- Conditional Access Policies Avoids:
- Detects MFA fatigue, credential stuffing, and unusual login patterns.
- Flags unusual geography, and device mismatches.
- Logon App secures local users with MFA.

- Helps the SOC
- Detect: Enrich logs from the network or cloud missing context for users. Fewer false positives in determining if an action was carried out by a user.
- Respond: By revoking access to 3rd-party apps like Slack that otherwise would have a control point.

Endpoint Threats – Advanced EDR

- Protects: Endpoints and Identities
- Control of Local Workloads Avoids:
- Ransomware, privilege escalation, and fileless attacks
- Unwanted software including shadow IT apps and fake IT tools deployed by attackers
- Theft of cookies giving access to cloud apps like Office365

- Helps SOC:
- Performs kill process, isolate host, and threat scans
- Mapped to MITRE ATT&CK for consistent analyst triage

Cloud Threats – Microsoft, Amazon, and Google

- Protects: Office apps, cloud-hosted software and data
- Control of Cloud Workloads Avoids:
- Exfiltration of data such as customer records, documents, and sensitive employee data.
- Deletion or destruction of backups, software systems cause operational issues.
- Identities and APIs to 3rd-party apps or customers.

- Helps SOC:
- Gain visibility into create, read, update and deletion of cloud hosted documents and applications to inform of malicious users.
- Audit configurations for posture and see block attacks targeting the clouds.
- Detects IAM abuse, S3 mis-configs, and OAuth token misuse.
- Correlates with CloudTrail, Azure AD, and 365 logs
- Supports credential lockdown and cloud session termination in Microsoft.

Firewalling: Host, Local, Edge, SASE

- Protects: All Networks (Zero Trust)
- Control: Application and content in traffic everywhere
- Helps the SOC:
  - Identifies lateral movement, C2 callbacks, and DNS tunneling
  - Detects rogue APs and malware-laced IoT devices
  - Firebox + FireCloud + Host Firewall (EDR) + NDR block traffic and isolate affected segments/hosts/applications across all access scenarios

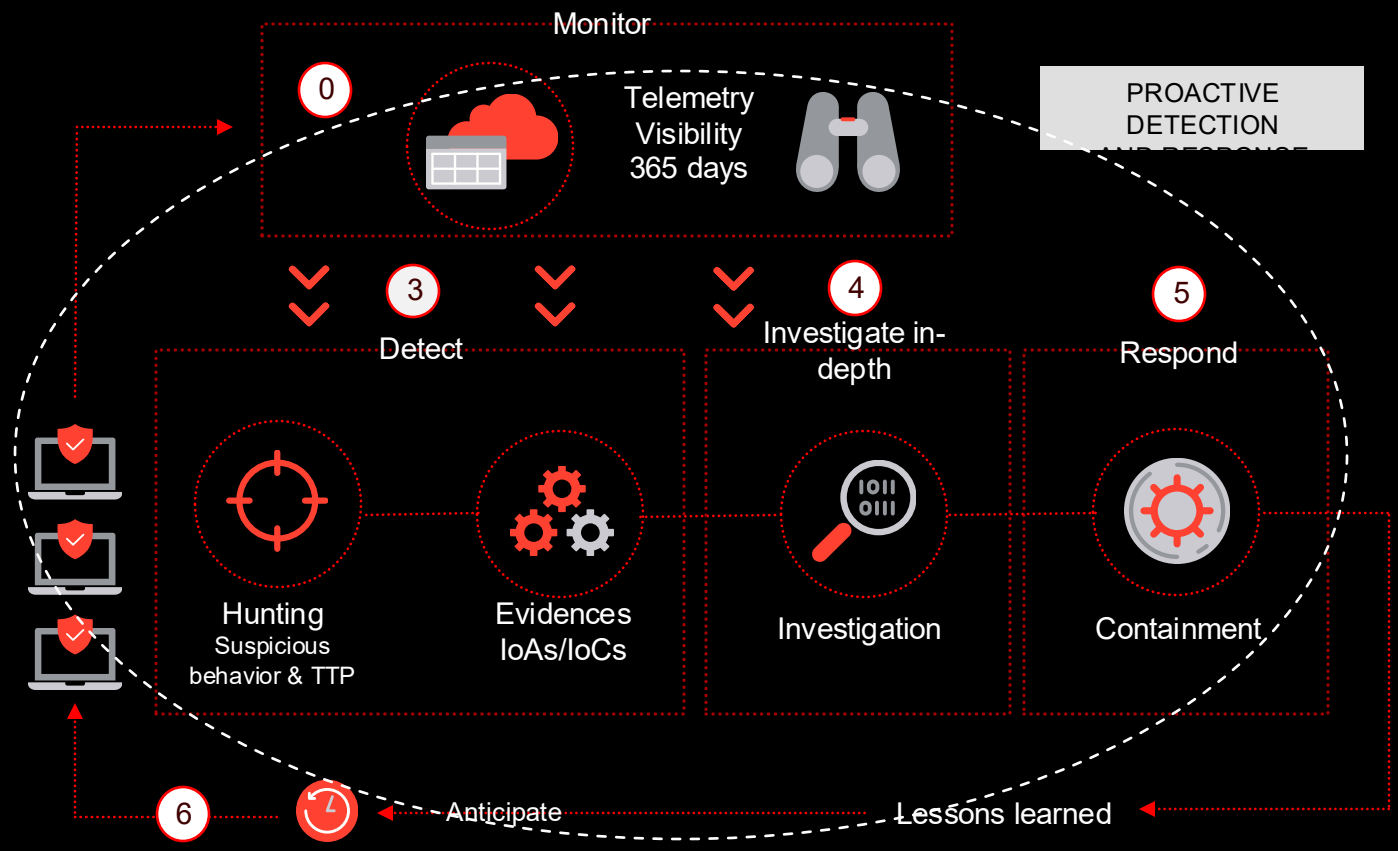
Unified SOC
AI and Human Expertise

WatchGuard Orion **Empowering your SOC**

A multi-tenant threat hunting, and incident response Cloud-native platform for SOCs, that leverages security analytics, machine learning and automation to proactively and efficiently uncover and responding unknown, sophisticated threats, that have passed other security controls.

Unlike other solutions, WatchGuard Orion centralizes:

- Pre-built and customer analytics
- Real-time and 365-day retrospective visibility for effective hunting and full root cause analysis
- A broad range of tools to deeply investigate and respond. All embedded in the single lightweight agent.
- Repeatable and extensible in-depth investigations and playbooks with the native integration of Jupyter Notebooks

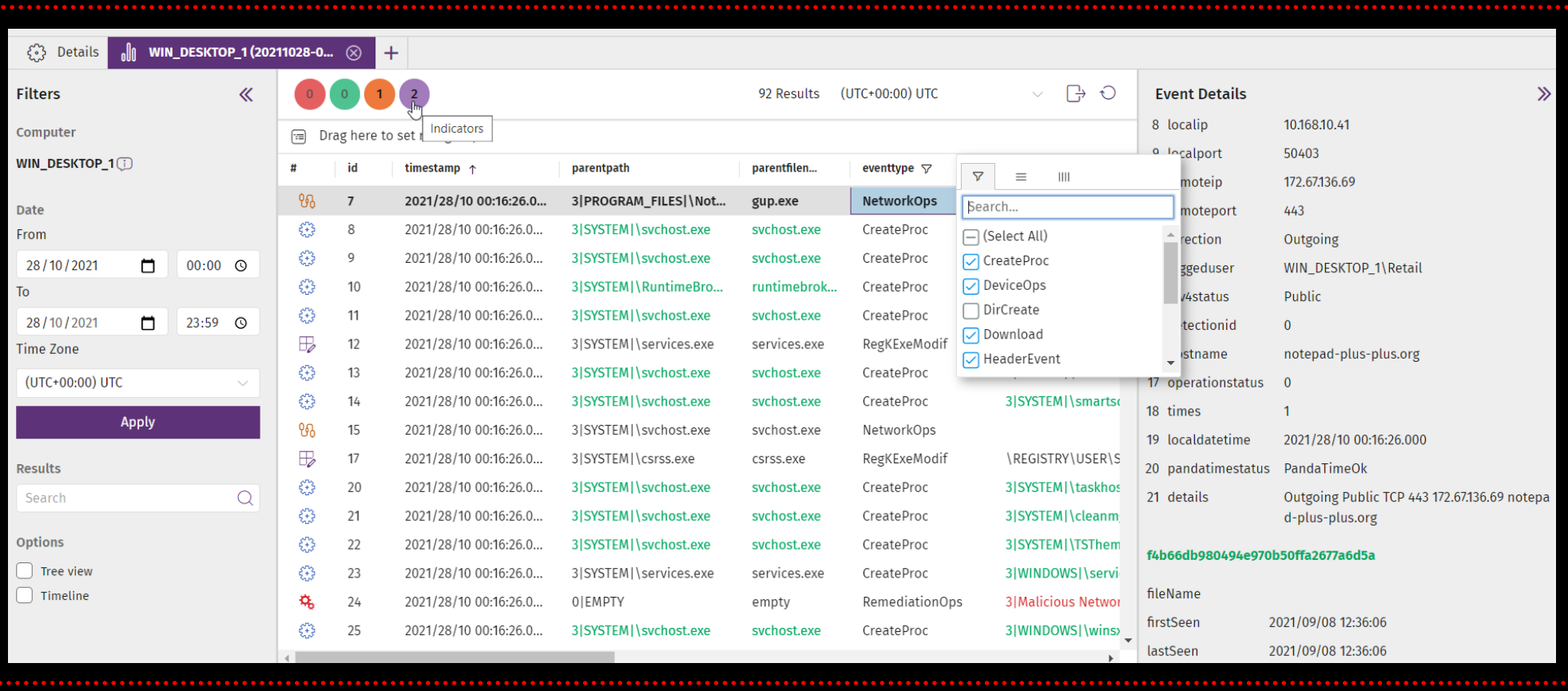


Threat Life Cycle Management (TLCM) – Hunt, Detect, Investigate, Respond and Anticipate

WatchGuard

Deep Investigation in WatchGuard Orion

The investigation console allows in-depth investigation on specific computers and dates. This resource offers all the necessary tools for an analyst to inspect the processes run on a computer in detail

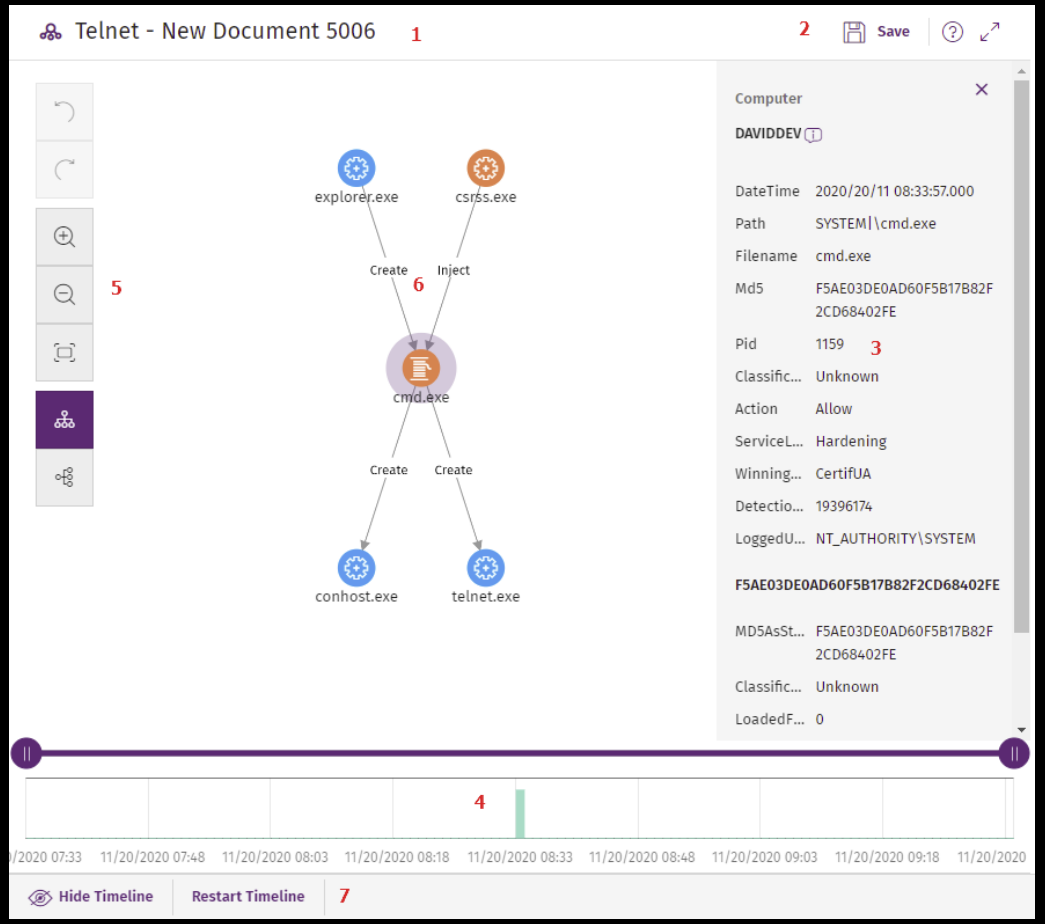


Investigation Graphs in WatchGuard Orion

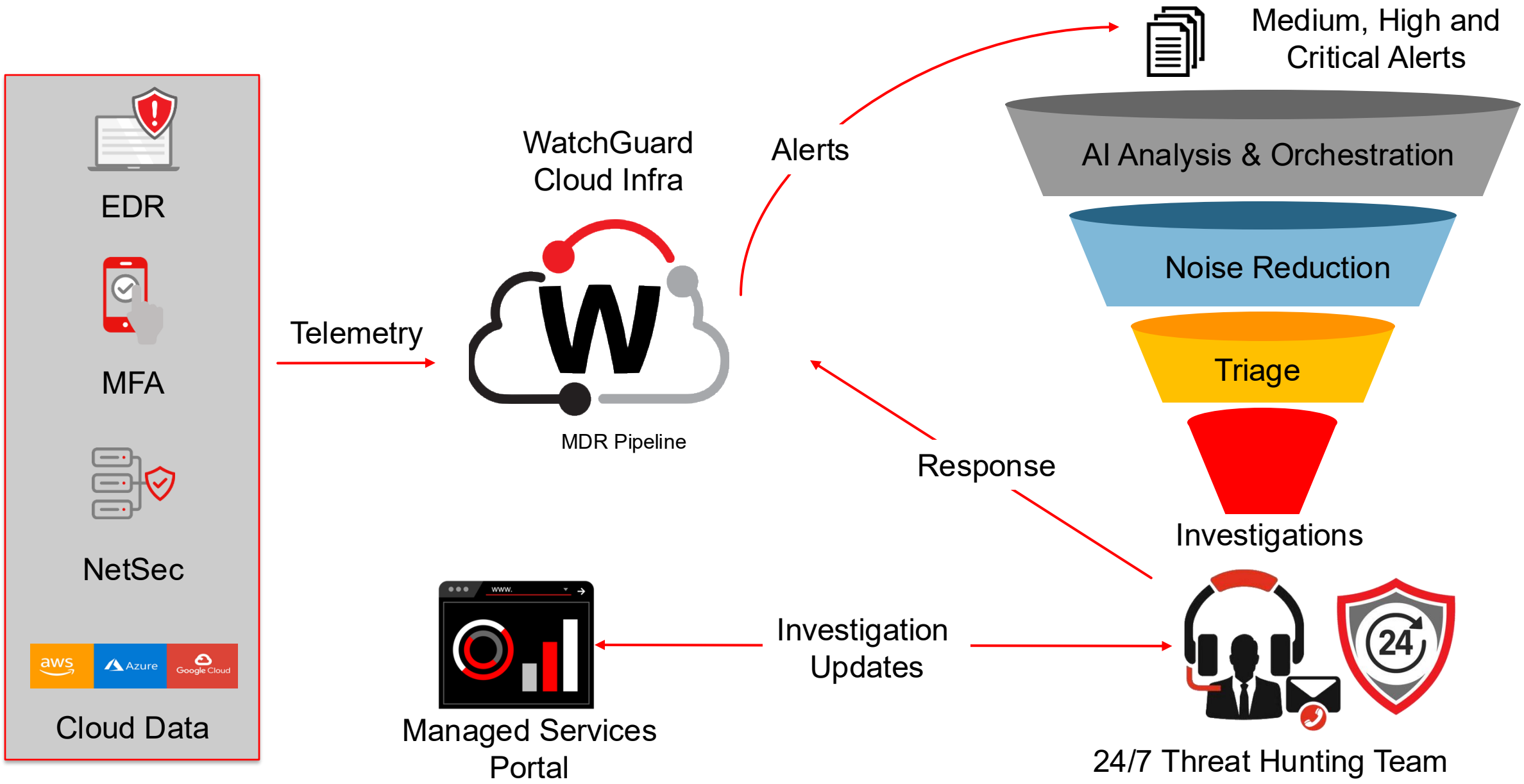
The investigation graph provides to the analysts:

- Visual context from a suspicious activity
- Entity relationships extracted from the enriched events in the data lake
- Connections across different signals
- Visual access to the telemetry extensible up to 365 days

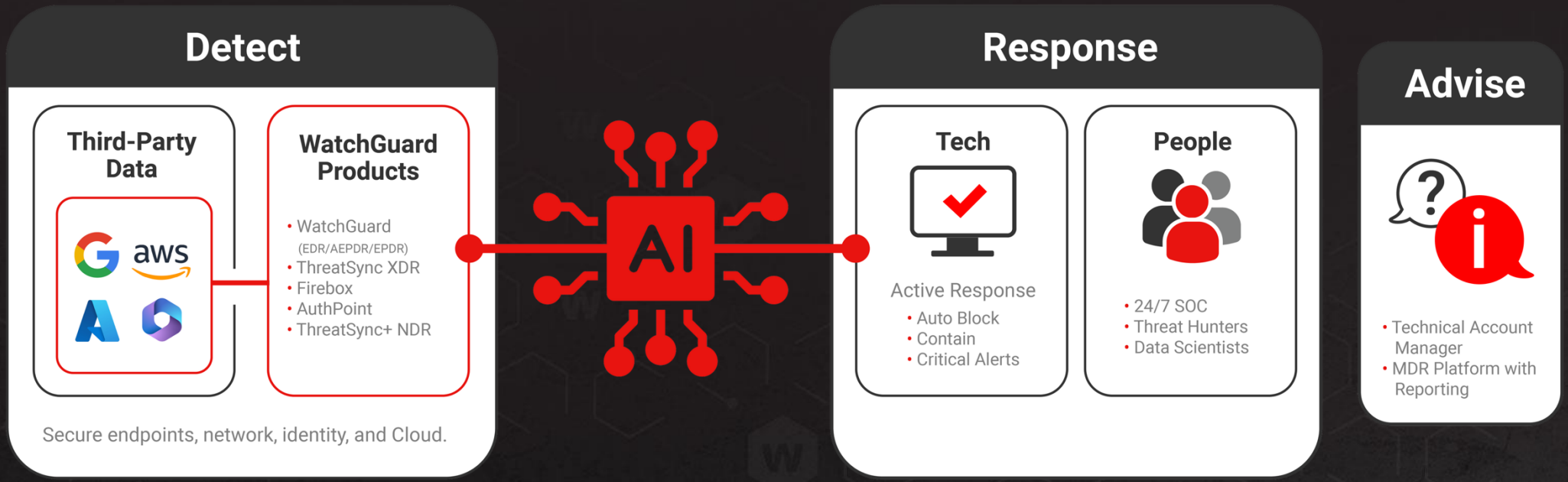
The information displayed on a graph is equivalent to the one displayed in the investigation console or in advanced queries, but arranged and presented in a clearer, easier-to-interpret way.



Putting it all together

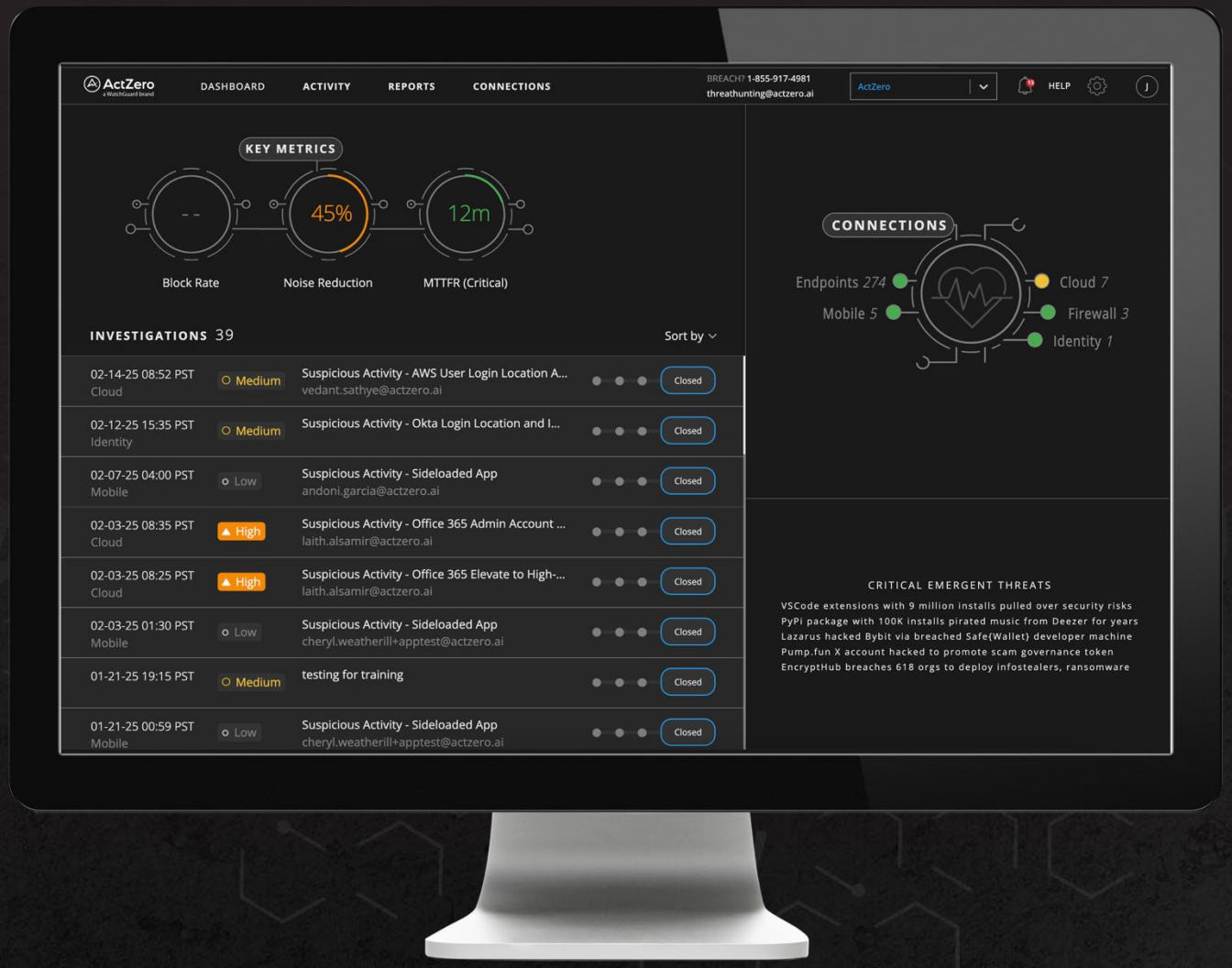


WatchGuard Total MDR

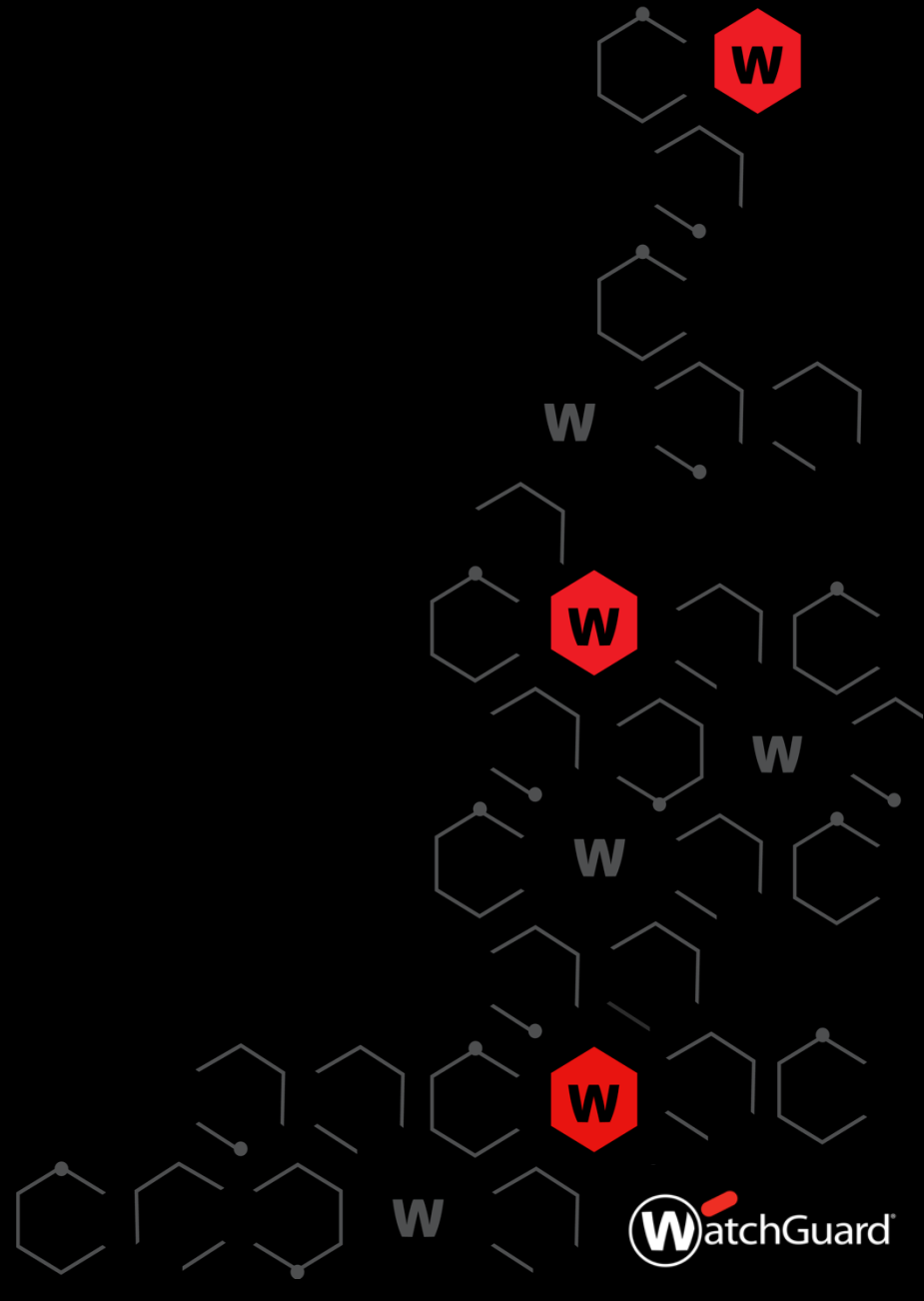


- **Endpoints:** WatchGuard EDR, EPDR
- **Firewall:** WatchGuard Firebox
- **Identity:** AuthPoint
- **Network:** ThreatSync+ NDR
- **Cloud:** Microsoft 365 / Azure, AWS CloudTrail, Google Workspace

MDR Portal

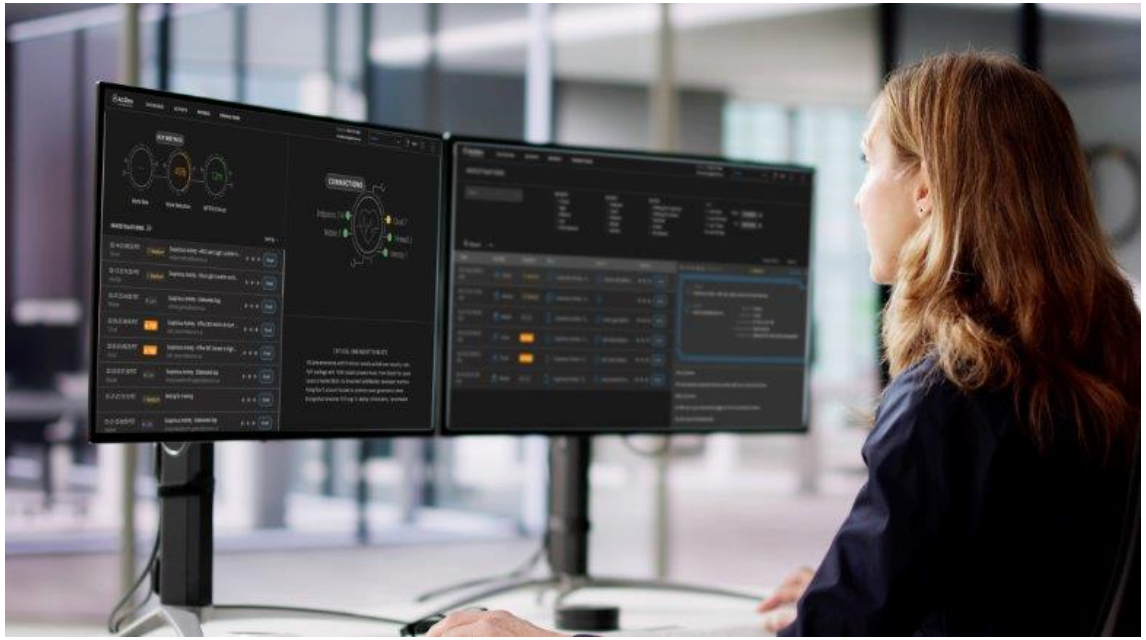

ActZero
DASHBOARD
ACTIVITY
REPORTS
CONNECTIONS
BREACH? 1-855-917-4981
threathunting@actzero.ai
ActZero
HELP
KEY METRICS
45%
12m
Block Rate
Noise Reduction
MTTFR (Critical)
CONNECTIONS
Endpoints 274
Mobile 5
Cloud 7
Firewall 3
Identity 1
INVESTIGATIONS 39
Sort by
02-14-25 08:52 PST
Cloud
Medium
Suspicious Activity - AWS User Login Location A...
vedant.sathye@actzero.ai
Closed
02-12-25 15:35 PST
Identity
Medium
Suspicious Activity - Okta Login Location and I...
Closed
02-07-25 04:00 PST
Mobile
Low
Suspicious Activity - Sideloaded App
andoni.garcia@actzero.ai
Closed
02-03-25 08:35 PST
Cloud
High
Suspicious Activity - Office 365 Admin Account ...
laith.alsamir@actzero.ai
Closed
02-03-25 08:25 PST
Cloud
High
Suspicious Activity - Office 365 Elevate to High-...
laith.alsamir@actzero.ai
Closed
02-03-25 01:30 PST
Mobile
Low
Suspicious Activity - Sideloaded App
cheryl.weatherill+apptest@actzero.ai
Closed
01-21-25 19:15 PST
Medium
testing for training
Closed
01-21-25 00:59 PST
Mobile
Low
Suspicious Activity - Sideloaded App
cheryl.weatherill+apptest@actzero.ai
Closed
CRITICAL EMERGENT THREATS
VSCode extensions with 9 million installs pulled over security risks
PyPi package with 100K installs pirated music from Deezer for years
Lazarus hacked Bybit via breached Safe{Wallet} developer machine
Pump.fun X account hacked to promote scam governance token
EncryptHub breaches 618 orgs to deploy infostealers, ransomware

Benefits

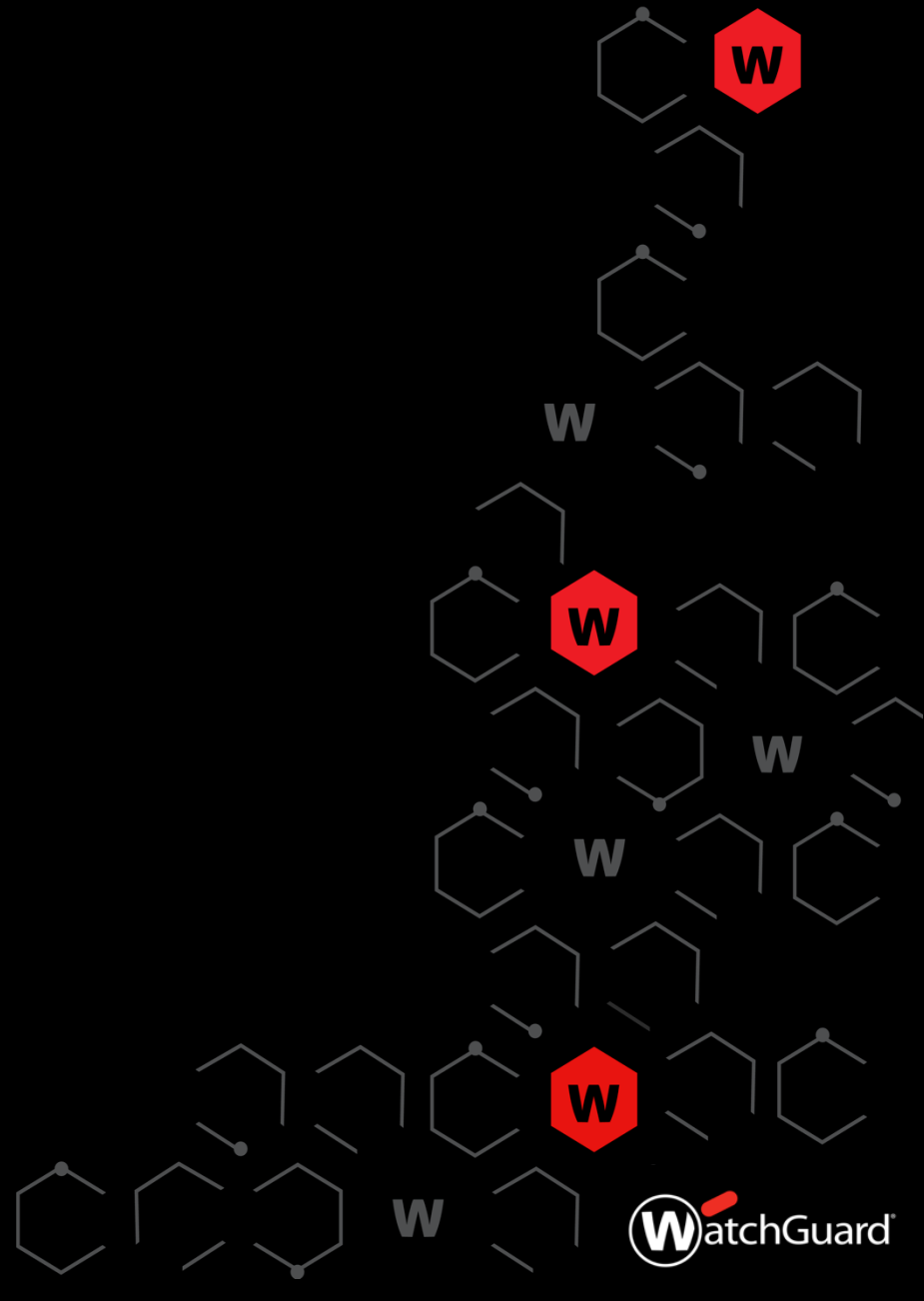


Key Benefits

- **Broader Coverage –** With the ability to detect attacks on the network and identify early stages on endpoint or cloud systems at critical moments, Total offers more coverage than simply linking systems together or leaving out critical components.
- **Faster Containment –** With full visibility and control across the WatchGuard security stack, threat hunters can find attackers and contain them faster than competitors.
- **More Proactive –** Teams learn from investigations and guidance how to design their policies and configurations to be more proactive

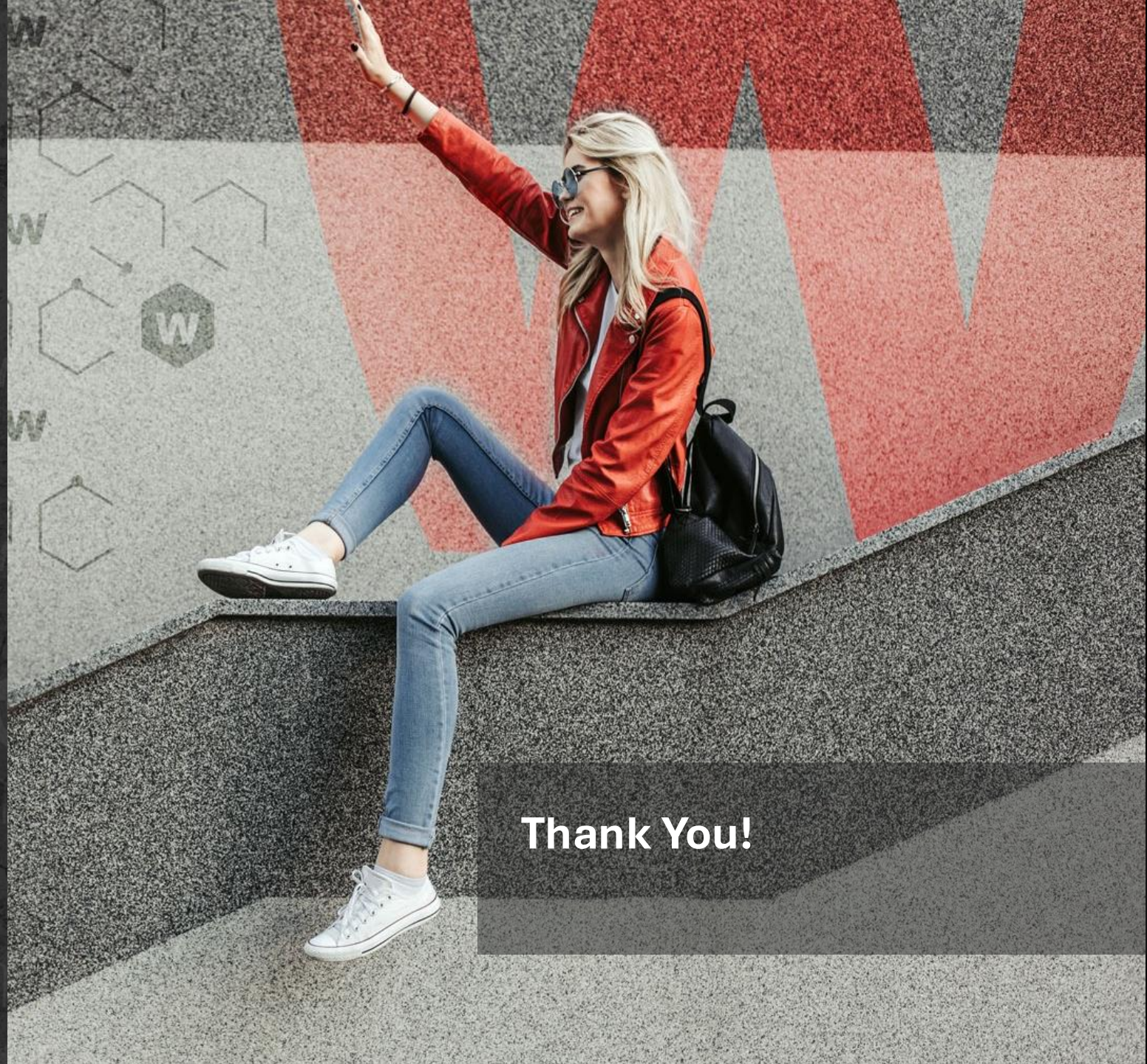


Live Demo



Real Security for the Real World

WatchGuard



Thank You!