Unified AI in XDR

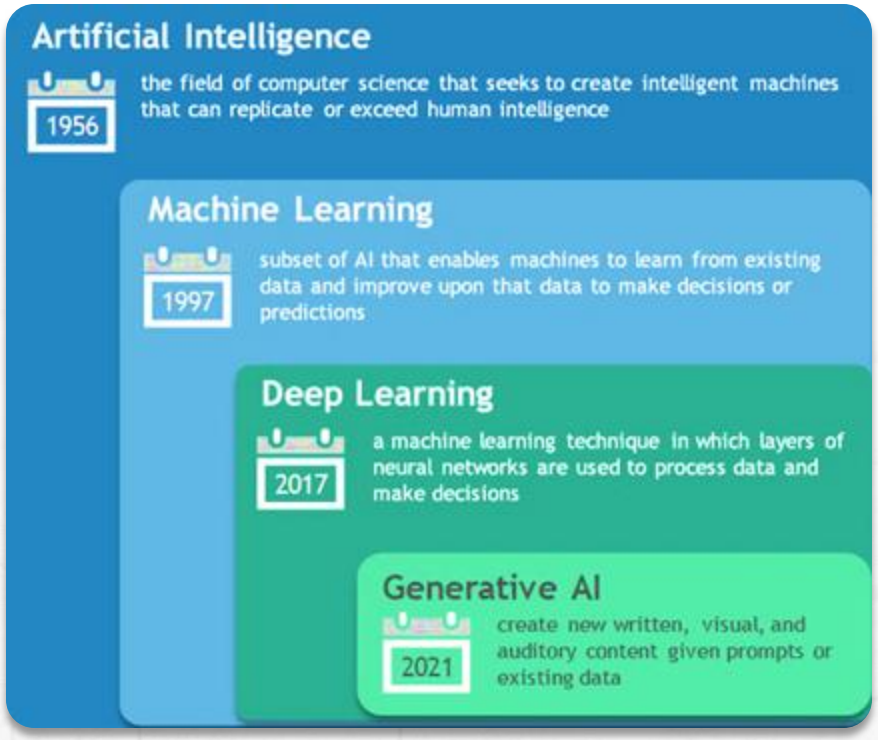
A Single Source of Cyber Truth

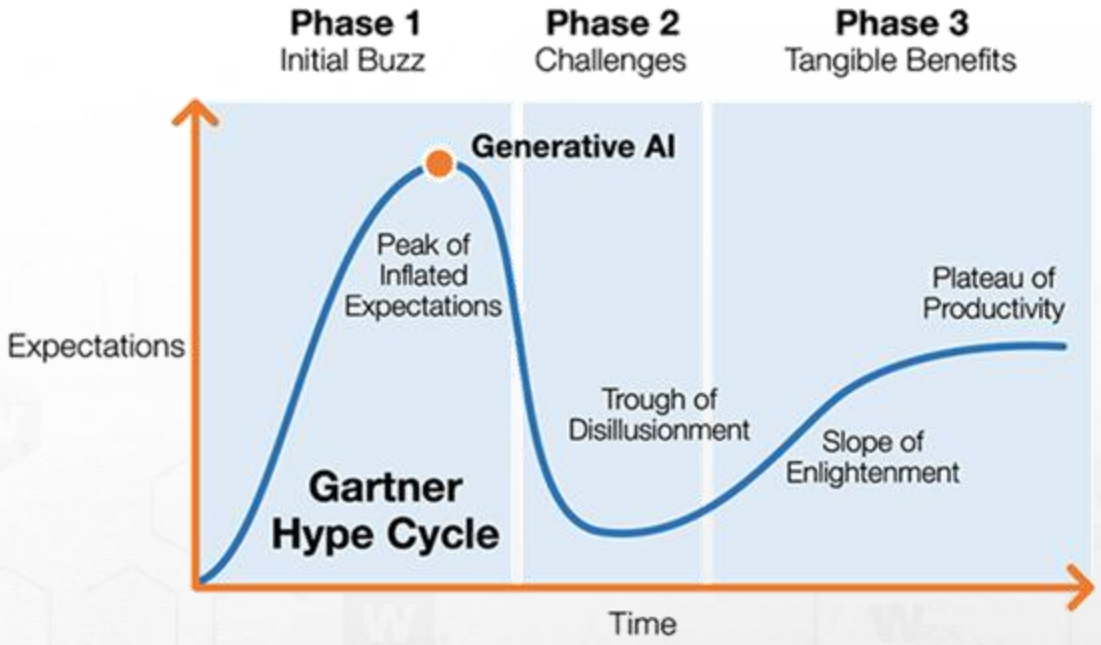
Jonas Spieckermann

Manager Sales Engineering
Central Europe

Real Security
for the Real World

Evolution of Artificial Intelligence





ChatGPT has over 200 million weekly active users

Efficient & Effective

Spy vs. Spy: Mad Magazine

90%

of security pros believe AI benefits security teams as much or more than threat actors

Spy vs. Spy: Mad Magazine

"**AI lowers the barrier for novice cyber criminals**, hackers-for-hire and hacktivists to carry out **effective** access and information gathering operations.

This enhanced access will likely contribute to the **global ransomware threat over the next two years**."

UK National Cyber Security Centre

Common Uses of AI in Cyber Attacks Today

- **Deepfakes** – AI-generated deepfake audio and video make social engineering attacks more convincing, tricking victims into transferring funds or revealing sensitive information.
- **Phishing Attacks** – AI crafts personalized phishing messages by analyzing social media profiles, past interactions, and email histories for highly convincing scams.
- **Password Cracking** – AI replaces brute-force methods by detecting password patterns, enabling hackers to generate highly probable guesses and even bypass two-factor authentication.
- **Data Mining** – Machine learning enables cybercriminals to rapidly sift through vast amounts of public and private data to uncover sensitive information.
- **Attack Automation** – AI-powered bots scan thousands of networks for vulnerabilities, automate exploitations, and even optimize ransomware attacks.

https://www.sharp.co.uk/news-and-events/blog/how-ai-is-being-used-for-cyber-attacks

AI Impact on Cyber Actors

	Highly capable	Capable	Less-skilled
Common Profile	State threat actors	State actors, commercial companies selling to states, organized cyber crime groups	Hackers-for-hire, opportunistic cyber criminals, hacktivists
Skills & Resources	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Implications	Best placed to harness AI's potential in advanced cyber operations	Most capability uplift in reconnaissance, social engineering and exfiltration.	Lower barrier to entry to effective and scalable access operations
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift
Tools (malware, exploits)	Uplift	Minimal uplift	Moderate uplift
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift

Push Tools & Capabilities Downstream

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Ghost Ransomware Group

FBI and CISA warns about China's Ghost ransomware group targeting businesses and critical infrastructure worldwide

February 24, 2025

Profile

Ghost is one of the world's most dangerous groups and has been indiscriminately targeting networks containing vulnerabilities in more than 70 countries worldwide since early 2021.

Target Selection

Focuses on small businesses, critical infrastructure, government networks, schools, healthcare, and manufacturing. Exploits outdated software and firmware vulnerabilities.

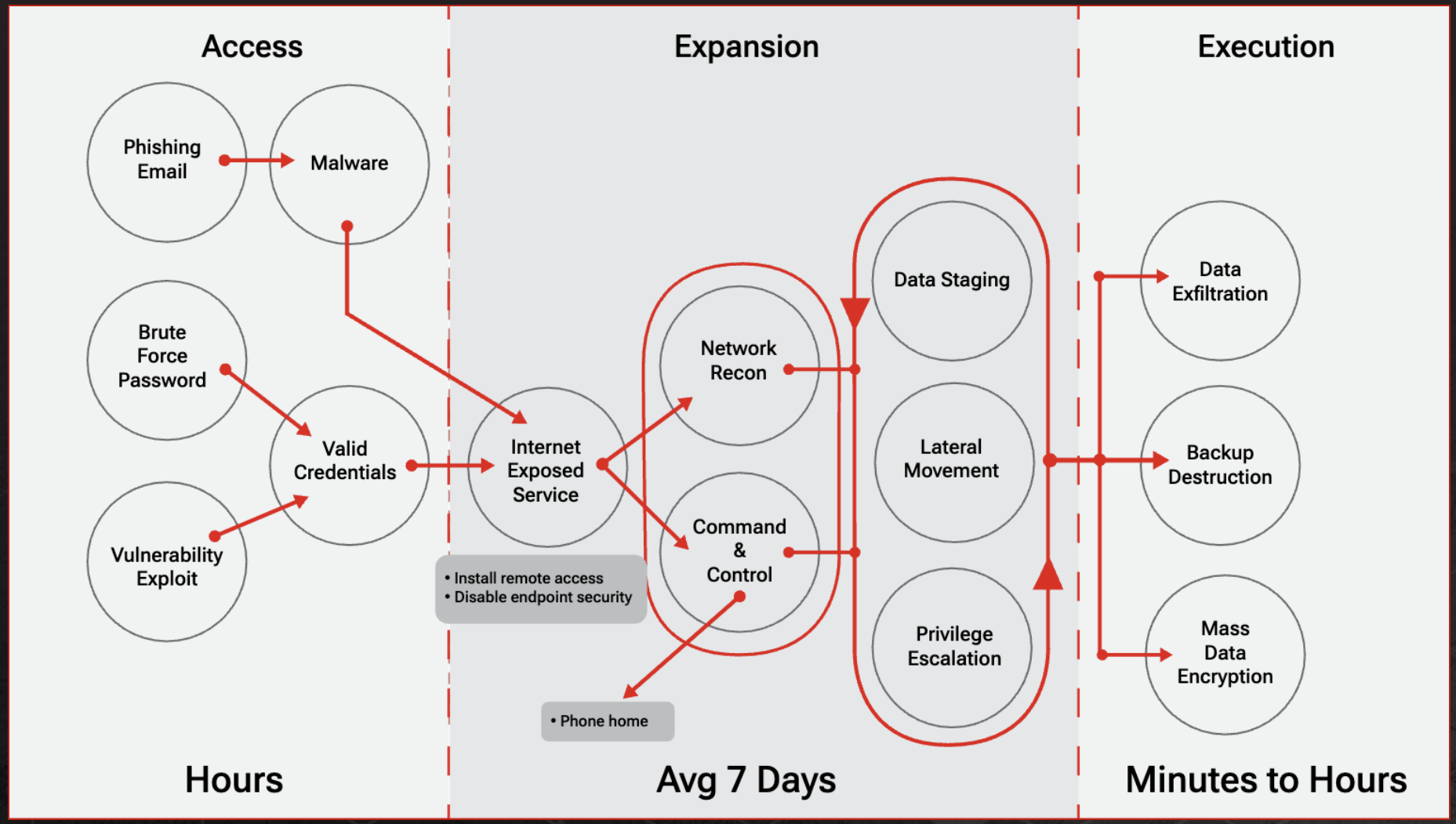
Details

- Gains entry by exploiting public-facing vulnerabilities in common applications like Microsoft SharePoint
- Uses Cobalt Strike Beacon to escalate privileges
- Deploys ransomware within hours or days of initial access
- Uses legitimate email services to communicate ransom demands
- Typically steals only limited amounts of data
- Regularly changes ransomware payloads, file extensions, and ransom note details.
- Moves on to new targets if faced with secure, well-protected networks

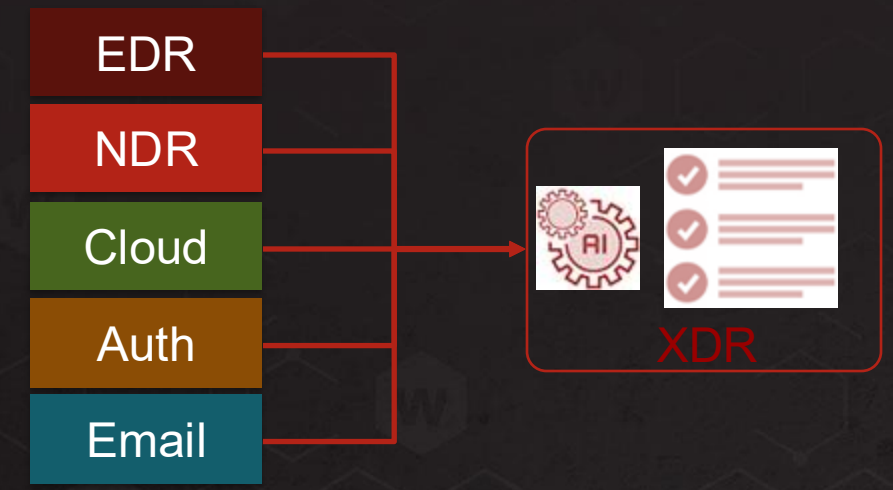
"...attackers will soon be able to specify desired outcomes, as opposed to needing to manually control every step. From there, agents will carry out — on a continuous, never-sleeping basis — the required steps to make those outcomes a reality."

Daniel Miessler, Security Researcher, Founder of Unsupervised Learning

Typical Flow of Cyber Attacks



Extended Detection and Response: Essential Cybersecurity



- ❑ To many products
- ❑ No correlation
- ❑ Complexity
- ❑ Alert Fatigue

- ❑ Full correlation
- ❑ Risk scored incidents
- ❑ Single UI
- ❑ Automation
- ❑ Integrated remediation

XDR = Simple, affordable, effective

Why XDR Now?

1. **Eliminate Security Gaps & Blind Spots**
   Relying on patchwork of security tools that operate independently, leads to fragmented visibility and delayed threat response.

2. **Boost Operational Efficiency & Reduce Costs**
   With XDR, automation and AI handle complex threat analysis, reducing manual workloads and increasing efficiency.

3. **Offer Stronger Security to Happier Clients**
   Provide your clients with a proactive, AI-driven security solution that offers real-time detection and response.

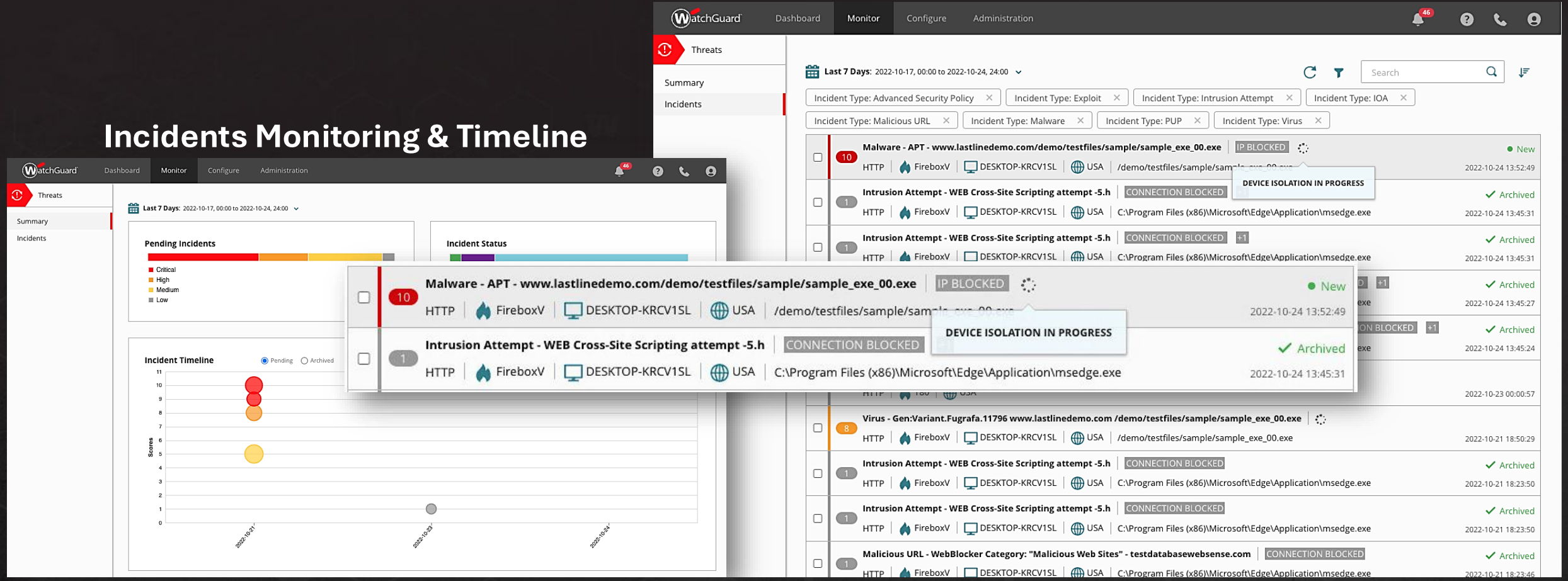
4. **Solve More Complex Security Problems**
   Cybersecurity is no longer just about staying safe. XDR can help your clients save on compliance, adhere to industry controls, apply for cyber insurance, and demonstrate security to their supply chain partners.

5. **Tap Into a High-Growth Market**
   XDR is one of the fastest-growing segments in cybersecurity, with a CAGR of nearly 40%. XDR is a prime opportunity for MSPs to increase revenue, enhance service offerings, and stay ahead of competitors.

WatchGuard ThreatSync in WatchGuard Cloud

Correlated telemetry provides context & defines incidents

Incidents Monitoring & Timeline



AI and XDR with WatchGuard

ThreatSync+ is an AI engine that monitors for anomalous behavior to automatically uncover early signs of misconfiguration, vulnerability, or a breach 24/7/365.

1. Multi-layered AI engine designed by DARPA
2. 100% cloud – no hardware!
3. Operates outside the network for full visibility
4. Intelligent detection and response capabilities across your entire threat surface

How it works

ThreatSync+ makes it easy for security teams to uncover evidence of threats as they progress across the cyber kill chain.

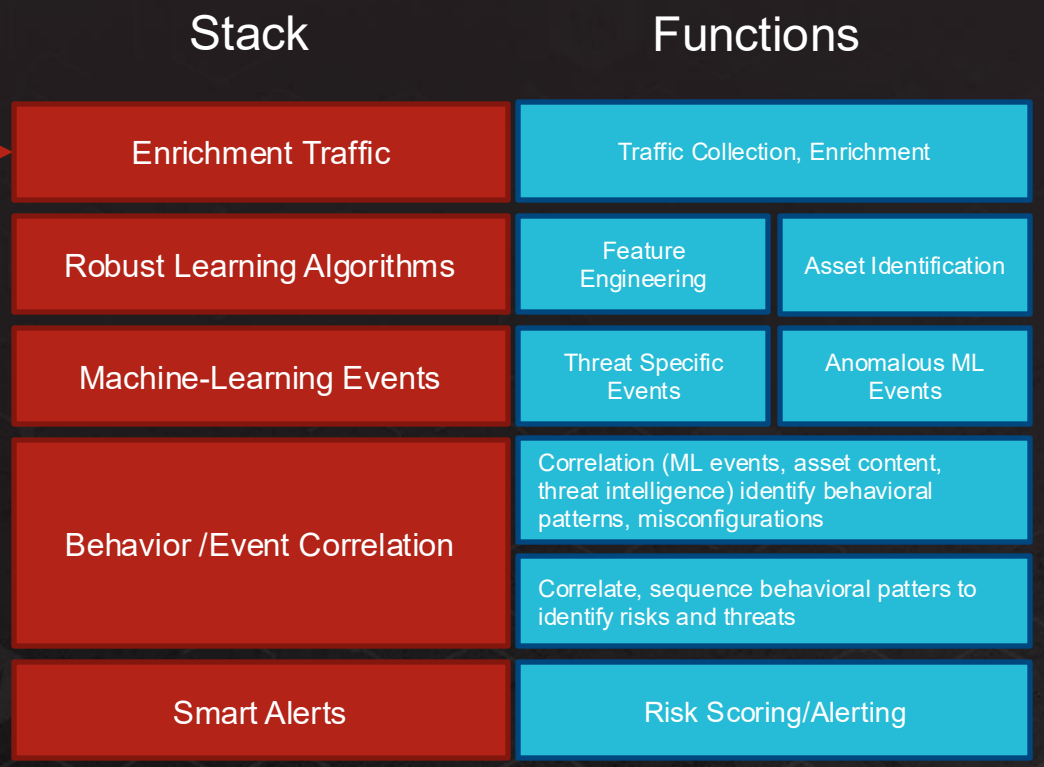
1. **Data Breadth**
   Multiple data sources to build context around the behaviors in your environment. ThreatSync+ collects telemetry from traffic logs, NetFlow, DHCP, VPN, Entr ID/ AD, and more.
2. **Intelligent Baselining**
   Undertakes an intensive learning process starting with a baseline of normal behaviors correlated to your network, users, services, and associated assets.
3. **Framework Mapping**
   Alerts are automatically mapped to a specific MITRE ATT&CK® type and provided with a link for more information, if available.
4. **Smart Alerts**
   Smart Alert details include several charts and maps and provide details about the behavior by time, historical activity, and timeline.
5. **Response Actions**
   ThreatSync enables automatic detection, and response to threats detected on the network, endpoint devices, or identity infrastructure.

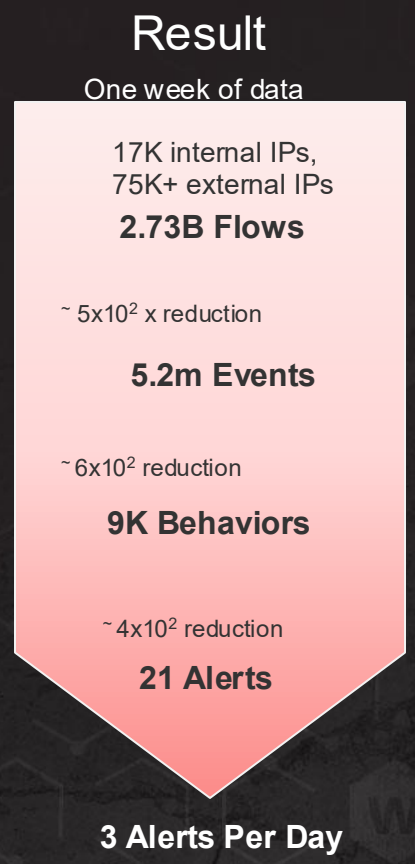
Unique Data Ingest into ThreatSync+ AI Engine

Results In Minimal Alerting and Maximum Detection Accuracy

Ingest Flow & Log Data

Firebox
Fire Cloud
Service Edge (SASE)
VPN
Office Firewall
Network Routers /Switches
Entra ID/Active Directory
SaaS Applications
Cloud Platforms

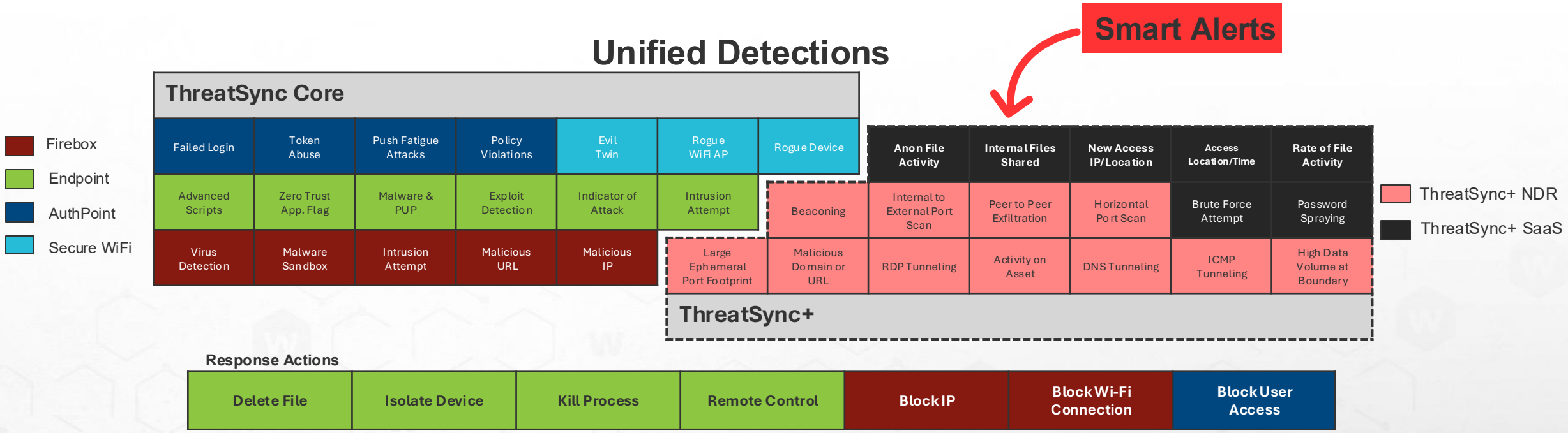




3 Alerts Per Day

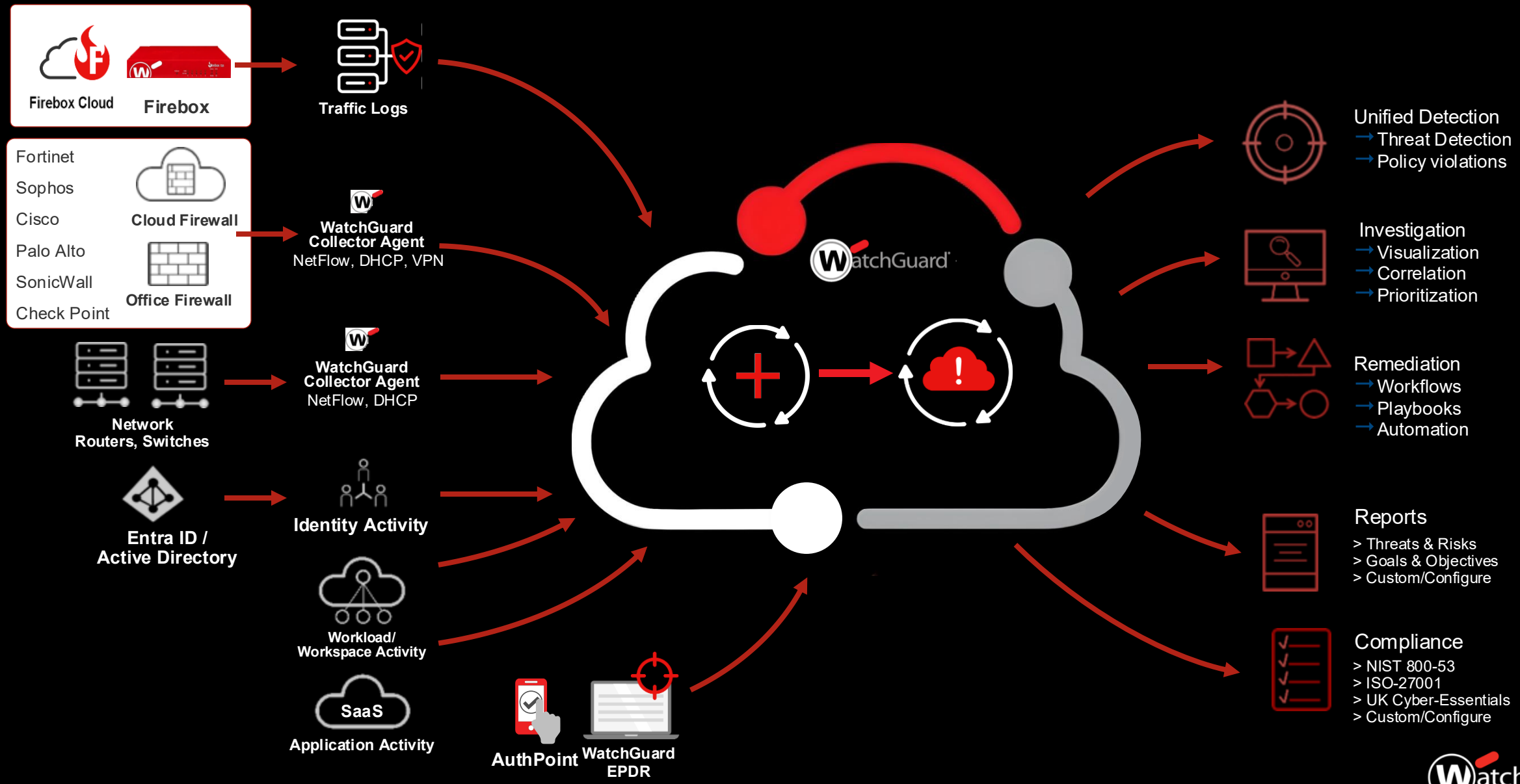
95 Layered AI models built by DARPA

ThreatSync+ *Supercharges* Unified Detection

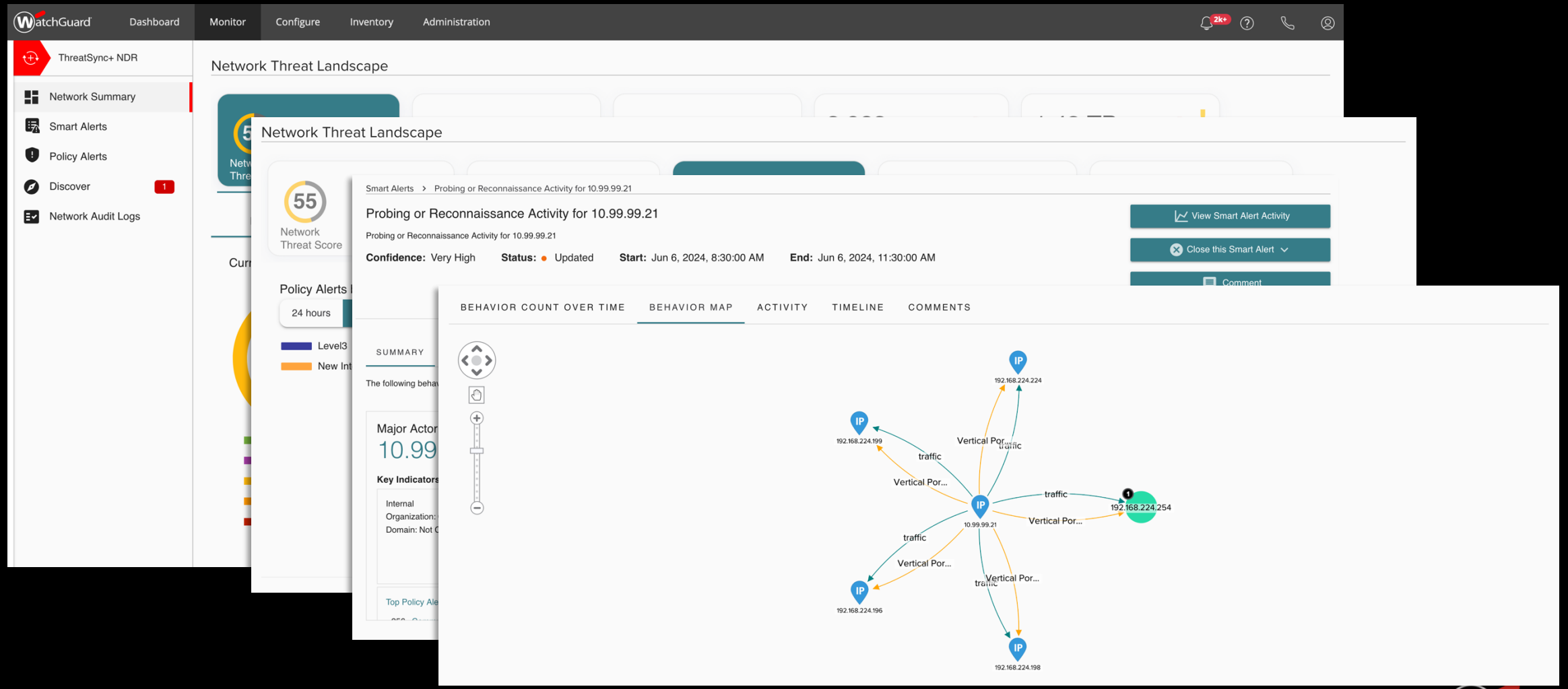


ThreatSync+ includes 36+ AI-powered detections for Ransomware Alone

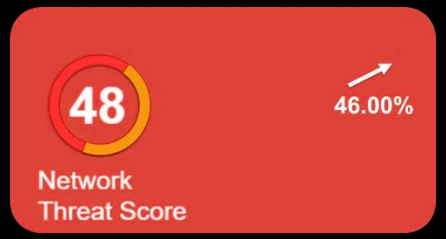
ThreatSync+ Vision: Unifying AI Analysis



ThreatSync+ NDR



ThreatSync+: Expand Use Case Coverage



Risk Visibility

Minimize Threat Surfaces & Improve Hygiene

- Identify, tag, and monitor devices/IoT
- Surface failed policies, misconfigurations, account issues across networks & Clouds
- Detect blind spots, vulnerabilities, and rogue devices

Threat Detection

Reduce Dwell Time & Stop Attack Damage

- Ransomware attacks
- Vulnerability-based attacks
- Cloud/SaaS account attacks
- Cloud to network attacks
- MITRE Attack Stage Visibility

Compliance

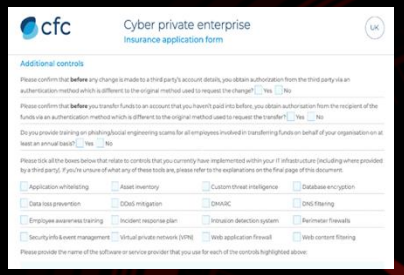
Reduce manual audit & reporting costs

- Continuous, automated control reporting
- 100+ OTB cyber & compliance policies
- UK Cyber Essentials, ISO 27001, NIST 800-53
- GDPR, FFIEC, NCUA compliance

Supply Chain Defense

Protect Ecosystem / Maintain Contracts & Revenue

- Quickly recognize attacks across your cloud and network
- Share critical threat intelligence with partners
- Prove security posture/ continuous audits
- Impact on sales contracts



Cyber Insurance

Acquire and Maintain Cyber Insurance / Assure Payouts

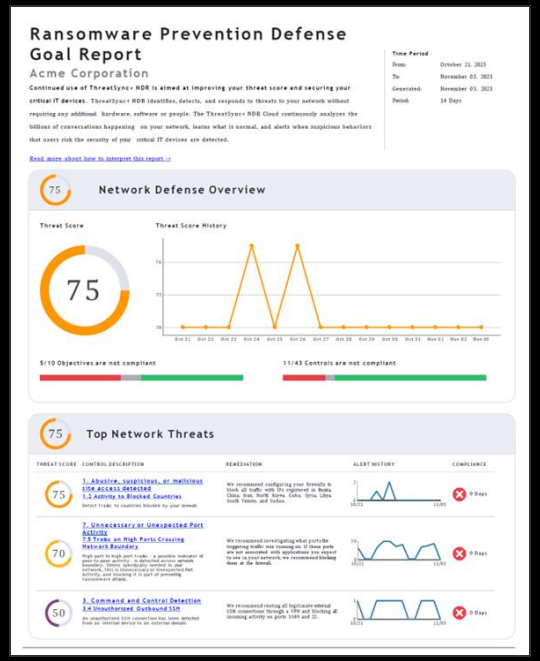
- Network & Cloud cyber hygiene standards upgrade
- Ensure cost reduction and renewals, pre-breach posture
- Ensure post-breach payout standard met

Risk, Compliance and Threat Reporting

Immediate Global Risk and Threat Visibility

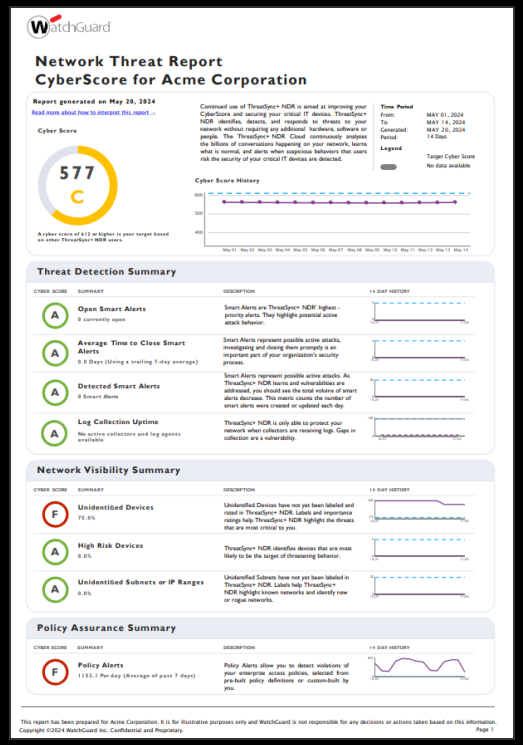
- Unifies all firewall, router, and switch data to deliver a global view of risks and threats
- Network Threat Reports
  - Top risks and threats, guidance on mitigation
  - Program definition, goal setting
  - SLA metrics
  - Management reporting
- Ransomware Defense Reports include 15 objectives and 56 controls defined by CISA to protect your network
  - Top risks and threats, guidance on mitigation
  - Program definition, goal setting
  - Management reporting

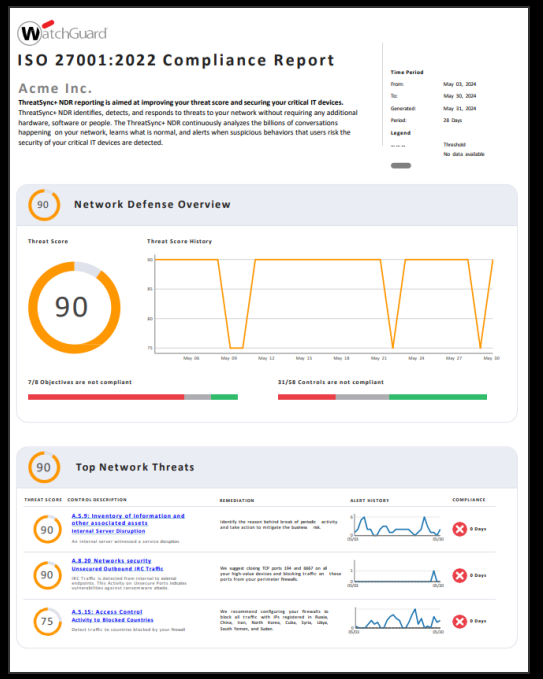
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE



Ransomware Defense Report

Network Threats Report





Compliance Reports

Live Demo

Real Security for the Real World

WatchGuard

Thank you!

Questions?