The Advantages of AI-Driven NDR

ThreatSync+ NDR: Network Detection and Response Use Case Coverage

The use cases and value proposition of WatchGuard's Cloud-Native NDR solution and how it empowers smaller security teams to efficiently reduce cybersecurity risk

Table of Contents

Introduction

As cyber threats escalate, the techniques used to infect devices improve and become even more complicated and challenging to detect; security teams must find tools that quickly and accurately locate and stop attacks. Yet, time and again, new technologies on the market fail to give defenders the upper hand.

The network, the backbone of any IT system, is undergoing a profound transformation as it transitions to the Cloud. Despite these changes, it remains the "single source of truth" for security teams, offering them the tools to mitigate risks and identify and halt attacks. It's crucial to recognize that attackers must gain control of the network to execute a successful attack.

For many years, detection strategies primarily focused on endpoints (devices), from antivirus to endpoint detection and response (EDR), and now extended detection and response (XDR). This shift away from the network was primarily influenced by widespread adoption of encrypted traffic, which diminished the value of packet capture. Additionally, the exponential growth in traffic volume made policy-based detection complex and prone to false positives.

The widespread adoption of automation and artificial intelligence has significantly improved detection and response capabilities for EDR and XDR. It has also revolutionized network detection and response (NDR) capabilities, regardless of whether the network is on-premises or in the Cloud. With the integration of AI and automation, NDR products have transitioned from complex to simple, and detection capabilities have shifted from noisy to precise.

The Advantages of AI-Driven NDR

Unsupervised and semi-supervised machine learning runs against massive network traffic flows, eliminating the need for full packet capture and pure policy-based detection. Instead, AI models watch for risky traffic and endpoint locations, network reconnaissance, command and control, privilege escalations (1), lateral movement, data staging, backup disruption, mass encryption, and data exfiltration, effectively covering detection across the expansion and execution phases of a cyberattack.

Networks cannot be bypassed in a successful cyberattack. Attacks can attempt to hide in regular traffic, but their structure and movement will be anomalous when compared to the normal baseline for that environment, and they will be detected. NDR systems cannot be attacked and shut down by attackers as they operate outside the network, monitoring the network flows. Continuously monitoring network traffic with multiple AI models is the unquestionable source of truth for IT teams to understand their risks and threats. This paper examines the use cases that WatchGuard's ThreatSync+ NDR solution covers.

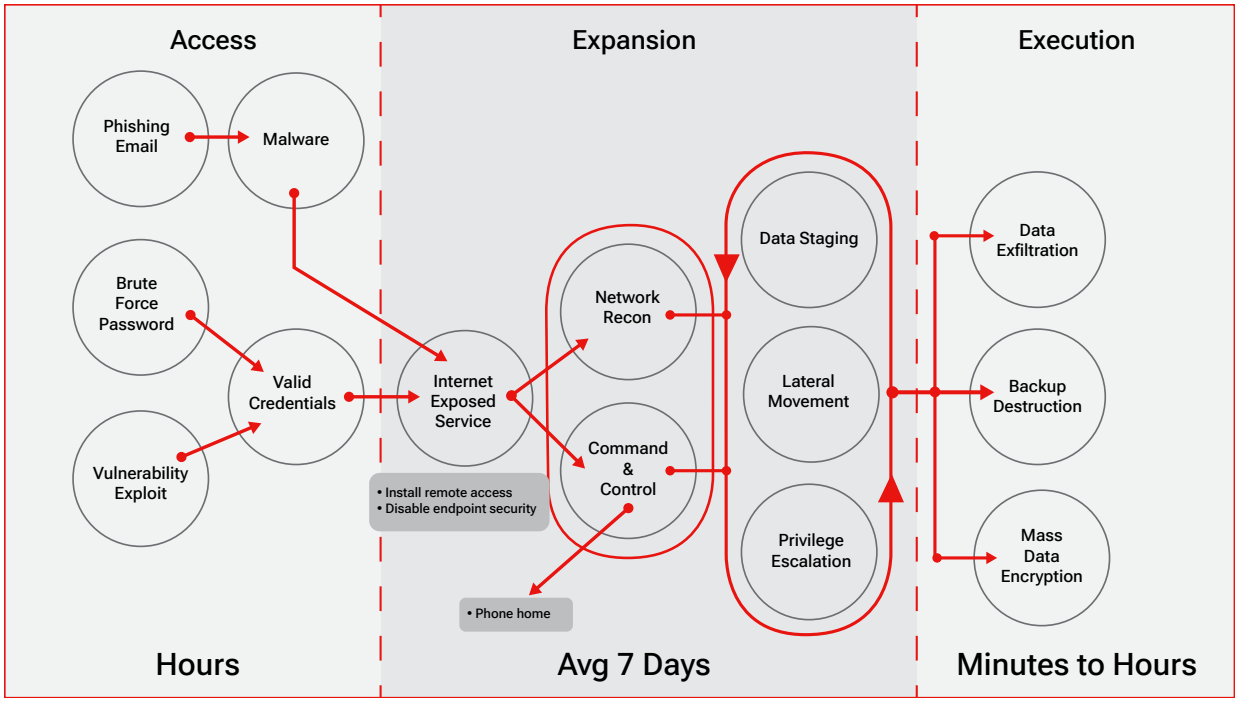


Figure 1. Cyberattack network expansion phase execution success defines the overall success of the attack.

Risk Visibility

Insight into hidden network risks that attackers will exploit

Organizations must have a comprehensive view of their network traffic and systems, including IoT devices, to see and understand the risks and vulnerabilities hidden in networks. Mitigating these risks and vulnerabilities will reduce threat surfaces, harden defenses, and make organizations less vulnerable to attack.

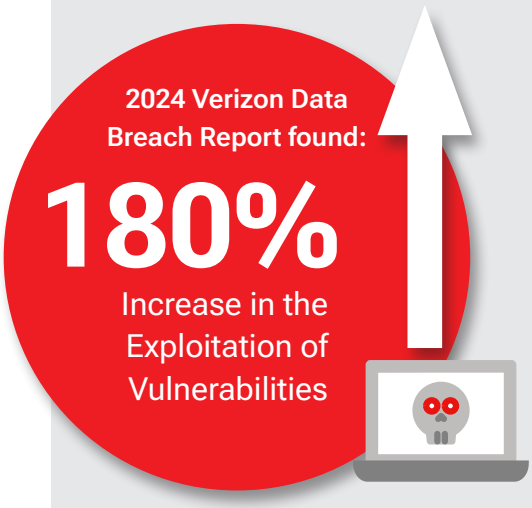
ThreatSync+ NDR enables organizations to identify network risks and vulnerabilities before they can be exploited. By monitoring network traffic and analyzing traffic behavior patterns, IT teams can quickly identify the most significant risks and allocate appropriate resources to mitigate them. Risk coverage includes north-south and east-west network traffic, VPN, and network-to-Cloud traffic.

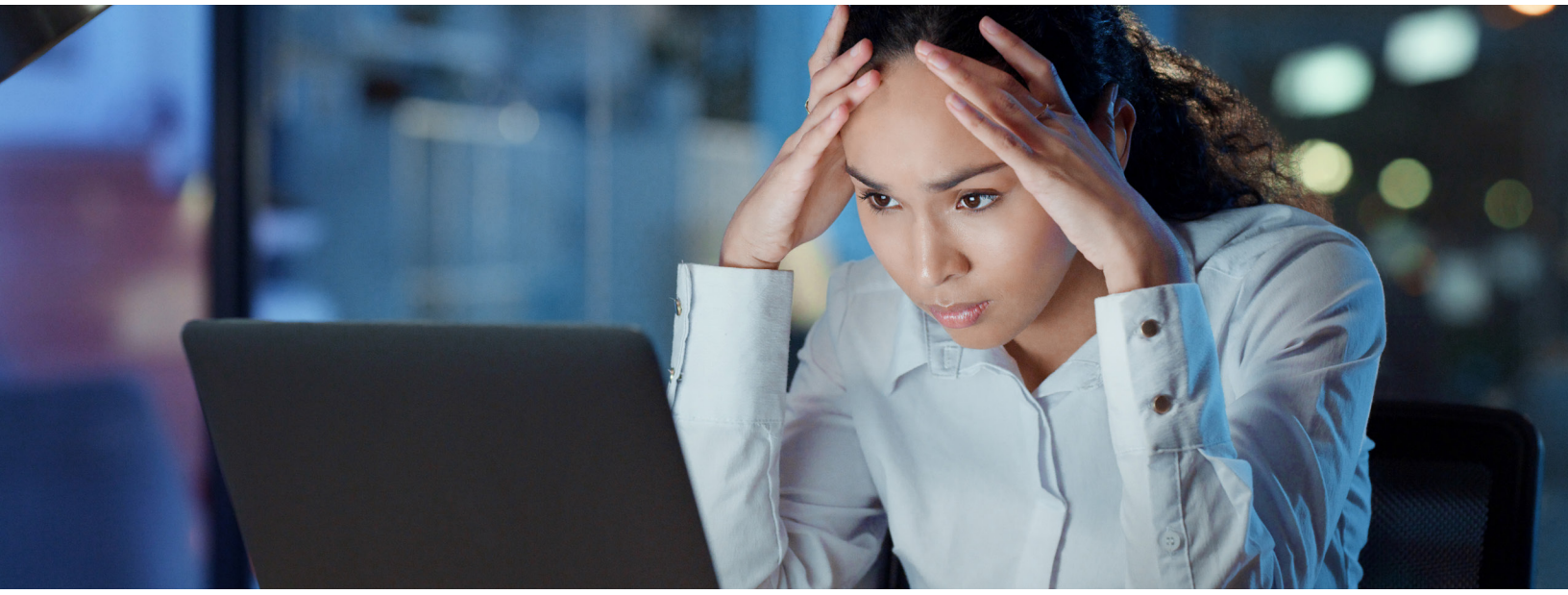
ThreatSync+ NDR provides highly effective network risk visibility because it utilizes advanced machine-learning algorithms integrated with a policy engine first to understand all of the devices operating on the network and then define which of these devices is at greatest risk based on the anomalous traffic flowing through it. ThreatSync+ NDR identifies all network devices and allows the IT/security team to tag them and apply an importance score, which is then calculated into the AI-based risk scoring. When risk scores exceed set thresholds or new devices suddenly appear on the network, ThreatSync+ NDR will alert the IT/security team to the issue.

The second level of risk visibility comes from the ThreatSync policy engine, which includes hundreds of best practices controls based on ISO and NIST standards. IT/Security teams can quickly build new controls or modify existing controls. Controls include standard firewall rules allowing ThreatSync+ NDR to monitor for rule failures across the entire network; for example, traffic flowing to a blacklisted country.

Reduce Threat Surfaces & Improve Cyber Hygiene

- Identify, tag, and monitor devices/IoT on the network
- Pinpoint failing firewall rules
- Discover misconfigured or unprotected ports
- Organize networks into zero trust security zones
- Detect network blind spots, shadow IT, & rogue devices





Proactive Risk Mitigation

ThreatSync+ NDR is designed to uncover seemingly invisible risks and provide guidance and actions to mitigate those risks and proactively improve the security posture. ThreatSync+ AI models are tuned to watch for failed firewall rules, unsecured ports, failed backups and more. Risks are identified and prioritized, and remediation actions are shared for rapid mitigation. ThreatSync+ NDR finds risks before attackers exploit them.

Reveal Rouge Devices

ThreatSync+ NDR collects and analyzes network (north-south & east-west) traffic along with user log data to identify all devices and systems on the network. Based on traffic, ThreatSync+ AI will identify the device type, including IoT devices. It detects and alerts when new devices appear; correlation will even identify the IP address and user account for each device detected. The solution delivers an accurate 360-degree operational view of your network.

Network Segmentation, Zero Trust

Organizations struggle to enforce network zero trust initiatives because zero trust often involves complex architectures, many different products, and multiple subnets. Implementing and managing zero trust controls in complex environments can be challenging, and if misconfigurations occur, environments can be compromised and data lost. ThreatSync+ NDR operates as a zero trust overwatch control.

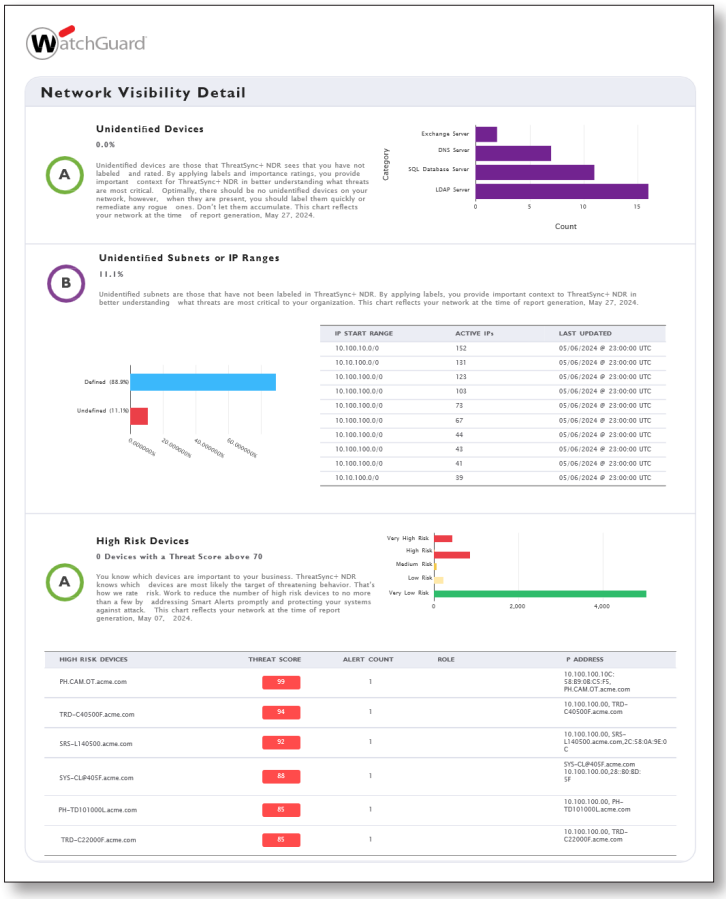


Figure 2. Network visibility reports identifying unknown or risky assets help maintain a healthy network

ThreatSync+ NDR enables IT/security teams to define and enforce zero trust network access parameters based on device and subnet tags, device type, device or traffic criticality, topology, and physical location. These parameters become zero trust monitoring layers, and ThreatSync+ NDR alerts IT/security teams when zero trust controls are violated.

Network Threat Detection and Response

Staying ahead of evolving threats that bypass traditional security solutions

The cybersecurity landscape continues to shift towards more advanced and evasive cyberattacks. The SolarWinds and MOVEit breaches are prominent examples of the consequences of undetected attacks. They highlight the need for more robust and comprehensive security measures beyond traditional perimeter protection.

A multi-layered security approach better tackles these new-generation threats. There has been an increased focus on network detection and response to meet these challenges. NDR solutions complement endpoint protection and provide greater threat detection coverage across network environments.

ThreatSync+ NDR delivers Cloud-native threat detection and response. The ThreatSync+ AI engine uses multiple unsupervised and semi-supervised machine-learning methods to determine normal activity baselines for all devices, traffic, and users across the network and Cloud.

ThreatSync+ AI continuously monitors for threatening behavior across five critical categories:

1. Indications of cyberattacks
2. Risky human behavior
3. Risky device behavior
4. Network risk
5. Network health

Each category includes multiple AI models and overlying, integrated policies to surface and prioritize threats, and correlate behaviors to eliminate false positives. Threat detection policies enrich AI results by adding threat intelligence and common attack behavior techniques. This enables automated, highly accurate, continuous monitoring of threats across networks and VPN traffic. When threats surface, ThreatSync+ NDR delivers the needed intelligence and guidance to understand the threat, its stage, and affected systems and offers immediate remediation actions via ThreatSync workflows for EDR and firewalls.

ThreatSync+ NDR Threat Coverage

- Ransomware
- Supply Chain
- VPN Threats
- Command & Control C2
- Man-in-the-Middle
- Unauthorized Web & DNS Activities
- Masqueraders (Tunnelling)
- Rogue Behaviors
- Insider Threats
- Lateral Movement

North-South Threat Detection

Monitoring north-south traffic for risks and threats is critical in detecting attacks that have bypassed endpoint security. ThreatSync+ NDR specifically looks for attack stages, including reconnaissance, command and control, payload entry, data exfiltration, traffic between anomalous or known harmful locations, external network scans, and internal and external traffic anomalies, including NET BIOS and AD communications events. If any of these anomalies arise, ThreatSync can immediately block them via firewall and EDR integration.

East-West Threat Detection

Monitoring east-west traffic is equally critical in detecting attacks unfolding inside your network. ThreatStnc+ NDR monitors for horizontal reconnaissance, credential escalation and access, lateral movement, data staging, anomalous access, anomalous data movement in the network, to the Cloud or in the Cloud, data stores made public, and backup disruption. Monitoring north-south, east-west, and network-Cloud communications will detect attacks that have bypassed endpoints and reduce dwell times from weeks to hours.

Automated Remediation

One of the biggest challenges facing IT and security teams is dwell time. In the latest Verizon Data Breach Report, average dwell times run from 30 to 50 days, while attack completion times average from 1 to 12 days. The math just does not work, and teams are forced into recovery mode as soon as the completed attack is detected. With the ability to detect and surface attacks inside the network, ThreatSync+ NDR, working with ThreatSync core, can automatically or manually immediately remediate attacks on detection. With these capabilities, even a small IT team can detect and stop an attack before completing its intended path. ThreatSync+ NDR operates as a zero trust overwatch control.

ThreatSync+ NDR includes over fifty out-of-the-box network defense controls delivering 24X7 monitoring across network and VPN attack surfaces to detect ransomware, APT, DOS, IP, PII, & PHI theft, and other advanced attacks.

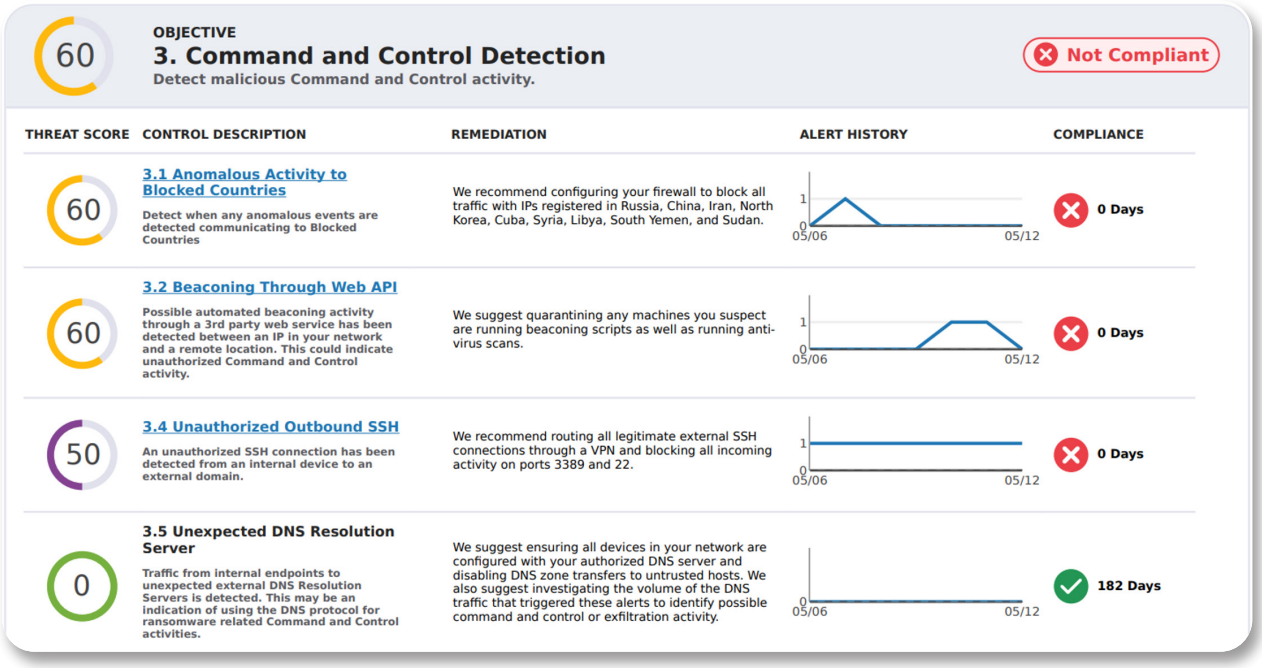


Figure 3. Command and Control Detection activity report

Continuous Compliance and Reporting

Sustainable Network Compliance for Industry Best Practices and Regulatory Frameworks

Organizations must deal with defending against cyberattacks while implementing increasingly stringent data security and privacy regulations. The cost and complexity of compliance can be challenging for any team. Still, for smaller, resource-constrained teams, the manual data collection, validation, and report-creation process can be overwhelming.

Non-compliance with regulatory environments can result in hefty fines. In February 2023, for example, GDPR (General Data Protection Regulation) regulators fined the Bank of Ireland €750,000 for insufficient technical security controls, and in the United States, Oklahoma State University – Center for Health Services paid $875,000 in HIPAA fines for a data breach.

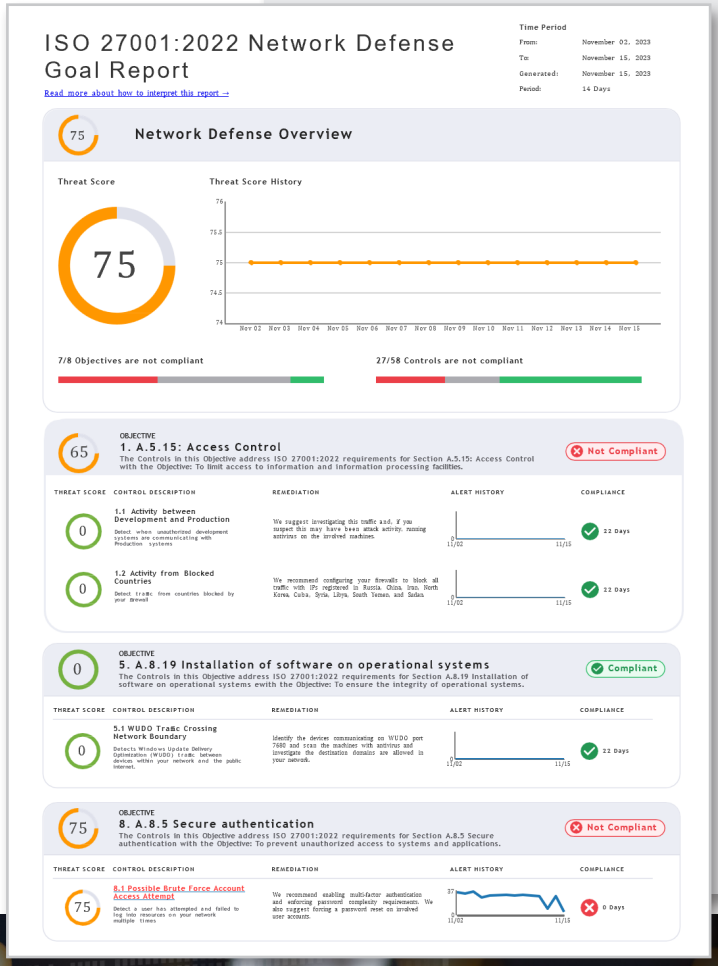
ThreatSync+ NDR, combined with WatchGuard Compliance Reporting, includes a policy engine, over a hundred Compliance Controls mapped to the most common control frameworks, and an Automated Reporting Engine to quickly and easily create configurable compliance reports for all your network controls.

Prebuilt control frameworks for ISO-27001, NIST 800-53, NIST-171/ CMMC, and Cyber Essentials are included. Easily configurable control mapping for specialized industry audits expands capabilities to cover the Motion Picture Association (MPAA) framework, CIS Critical Security Controls, IEEE standards, and most cyber insurance requirements.

Beyond audit requirements, ThreatSync+ NDR includes Network Threat Summary and Ransomware Defense reports, which combine cyber defense program goals and metrics to be tracked along with an overall risk score and trending, top-level views of risks, threats, and vulnerabilities.

Control Frameworks Covered

- ISO27001
- NIST800-53
- NIST 171
- NIST CSF
- CMMC/DFARS
- GDPR



Network Compliance Coverage

Whether proving compliance with security frameworks like NIST and ISO standards, industry standards like the Motion Picture Association (MPA) framework, or constantly changing supply chain audits from multiple ecosystem partner audits, ThreatSync+ NDR network controls have you covered with over one hundred AI-refined internet, NIST, and ISO-based network controls built into the product.

AI-Powered Compliance Controls

ThreatSync+ NDR begins by building a picture of what "normal" life looks like for your network – a baseline. Multiple baselines are created for devices, traffic flows, and applications for every moment of every day. ThreatSync AI analyzes massive amounts of network traffic to build this picture. ThreatSync+ NDR then layers in policies, including over a hundred NIST 800-53 controls out of the box. AI and policies working together are combined with threat intelligence feeds to understand what is a vulnerability (e.g., patching system failure), what is a risk (e.g., firewall rule misconfiguration), and what is a threat (e.g., probing or reconnaissance activity). Humans could never accomplish this deep level of continuous visibility. ThreatSync+ NDR can detect vulnerabilities, risks, and threats hidden from other cybersecurity tools.

Automated Continuous Compliance

Compliance is not a one-time event but an ongoing process. To remain compliant, organizations must continuously monitor their operations, policies, and practices. Standards like NIST 800-53 and ISO 27001 create the foundation for most regulatory IT control sets, and ThreatSync+ NDR comes complete with over a hundred network controls.

ThreatSync AI models continuously assess the effectiveness of these controls and alert on control violations. Controls are easily configured to match specific regulations like NIST-171 and Cyber Essentials.

Proving Compliance

Once automated compliance is achieved, the next step is to prove it through control effectiveness reporting. ThreatSync+ NDR and WatchGuard Compliance Reporting automate the compliance reporting process. Based on policy frameworks, single or multiple compliance reports are automatically generated. Reports visualize control effectiveness and provide best practice guidance on achieving compliance when controls fail. Traditionally, this process has been manual, slow, and costly. ThreatSync + NDR with WatchGuard Compliance Reporting automates this process, saving significant time and money.

ThreatSync+ NDR's integrated policy engine and AI analyze billions of network flows, combining them into millions of network events and reducing them to hundreds of anomalous behaviors and finally into just a handful of alerts that need immediate action.

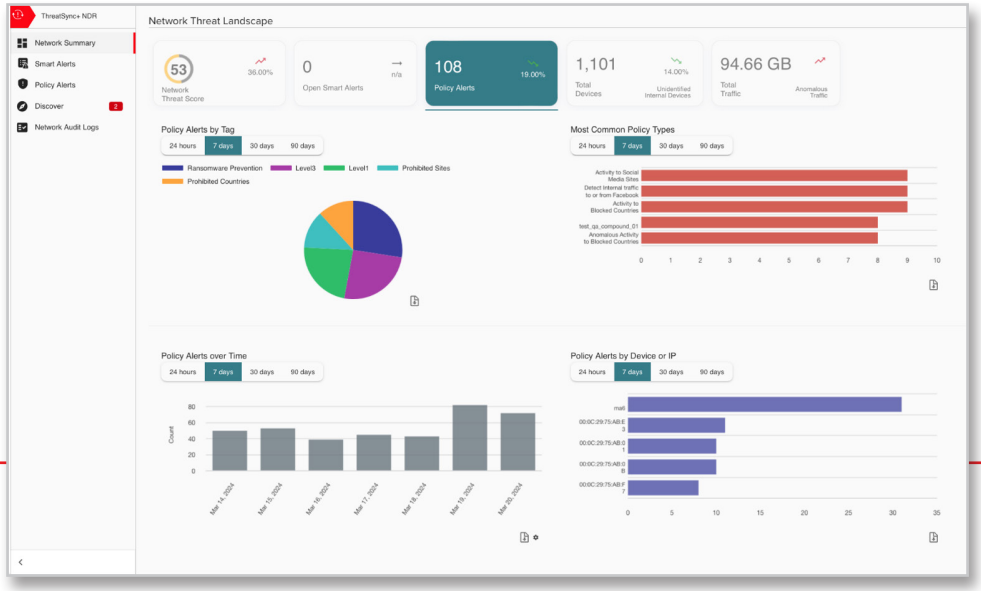


Figure 4. ThreatSync+ NDR available in WatchGuard Cloud

Ransomware Detection

Looking Inside Your Network to Where Ransomware Can't Hide

Ransomware is one of the most significant cybersecurity threats facing organizations today. Unfortunately, traditional efforts to thwart ransomware attacks, which focus on preventing account or endpoint compromise, are insufficient. Cybercriminals are becoming more sophisticated, and successful ransomware attacks continue to rise even with these defenses in place.

New, sophisticated ransomware attacks use tactics and techniques to bypass and evade traditional cyber defenses, such as firewalls, strong authentication, and EDR/EPP tools. Many attacks are even successful at shutting off EDR agents and backup systems.

ThreatSync+ NDR monitors for indicators of a ransomware attack, even if endpoints are compromised, and sends you real-time alerts so you can stop the attack from spreading. The ThreatSync AI engine uses multiple unsupervised and semi-supervised machine-learning methods to determine normal baselines of activities for all devices, traffic, and users across the network. These models are specifically tuned to watch for the indicators of a ransomware attack and will automatically monitor, alert, and remediate attacks 24/7.

The Ransomware Threat Is Real

- 41% of small businesses fell victim to a cyberattack in 2023, a rise from 38%[1]
- The human element is the cause of 74% of breaches[2]
- 538 new ransomware variants were discovered in 2023[3]
- Ransomware payments hit $1billion in 2023[4]
- Sophistication is increasing as attacks look to freeze backups and bypass endpoint security.
  - Mespinoza/Pysa (PowerShell)
  - Sodinokibi (REvil) (Turn off Security)
  - Bitpaymer/DoppelPaymer (RDP)
  - Ryuk (PowerShell, Registry Access)

1. https://www.insurancebusinessmag.com/us/news/cyber/despite-awareness-small-businesses-still-highly-vulnerable-to-cyber-attacks
2. https://apnews.com/article/small-business-cyberattacks-hack-ransomware
3. https://securityintelligence.com/articles/ransomware-all-time-high-attackers-struggle
4. https://securityintelligence.com/articles/ransomware-all-time-high-attackers-struggle/

AI-Driven Ransomware Detection and Response

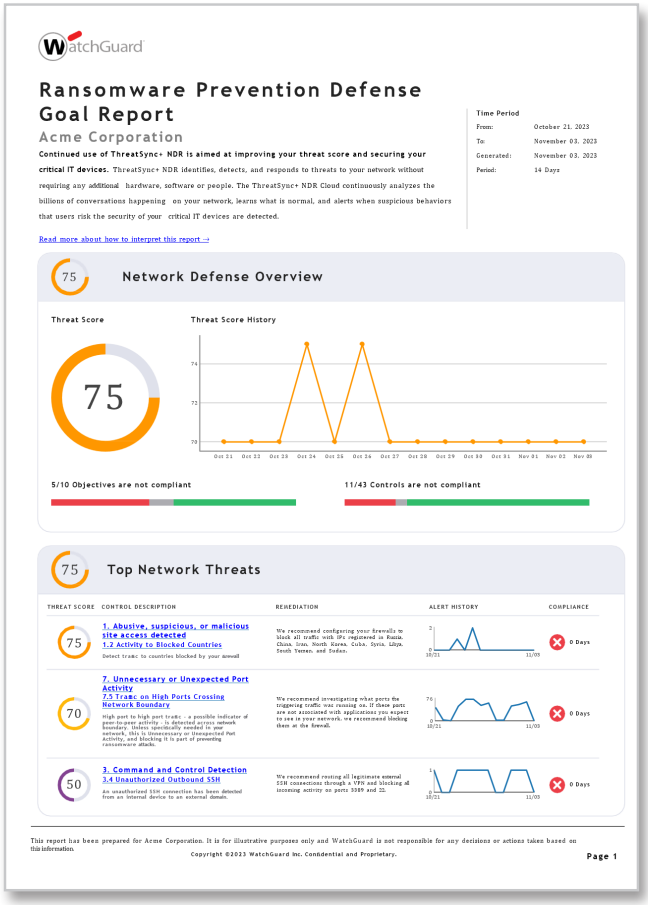
There are over 40 machine-learning models specifically focused on ransomware detection, capable of surfacing and stopping ransomware attacks before they harm your organization. Detection models include identifying rogue network devices, reconnaissance traffic, command and control, lateral movement, abnormal encrypted RDP and DNS tunnels, and abnormal VPN activity. Remediation efforts are quickly executed via ThreatSync, including automated IP blocking and EPDR endpoint quarantine.

Continuous Ransomware Monitoring

Continuously monitor and reduce network risks that leave you exposed to ransomware attacks. ThreatSync+ NDR ransomware defense policies derived from the CISA ransomware defense best practices constantly monitor, analyze, and refine your network risks, including unsecured ports, traffic to unknown or risky locations, ineffective firewall rules, unpatched systems, failed backups, and rogue network behavior that can lead to attacks.

Ransomware Risk Reporting

ThreatSync+ NDR includes an automatically generated Ransomware Defense Report presenting the top CISA ransomware defense controls and their effectiveness in your environment. Controls include disrupted backup system schedules, unauthorized remote access, unusual admin activity, and many more.



WatchGuard

Ransomware Prevention Defense Goal Report

Acme Corporation

Continued use of ThreatSync+ NDR is aimed at improving your threat score and securing your critical IT devices. ThreatSync+ NDR identifies, detects, and responds to threats to your network without requiring any additional hardware, software or people. The ThreatSync+ NDR Cloud continuously analyzes the billions of conversations happening on your network, learns what is normal, and alerts when suspicious behaviors that users risk the security of your critical IT devices are detected.

Time Period
From: October 21, 2023
To: November 03, 2023
Generated: November 03, 2023
Period: 14 Days

Read more about how to interpret this report →

75 Network Defense Overview

Threat Score

75

Threat Score History

5/10 Objectives are not compliant

11/43 Controls are not compliant

75 Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	1. Abusive, suspicious, or malicious site access detected 1.2 Activity to Blocked Countries Detect traffic to countries blocked by your firewall	We recommend configuring your firewall(s) to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		0 Days
70	7. Unnecessary or Unexpected Port Activity 7.5 Traffic on High Ports Crossing Network Boundary High port to high port traffic - a possible indicator of unwanted traffic crossing the network boundary. Unless specifically needed in your network, this is Unnecessary or Unexpected Port Activity, and blocking it is part of preventing ransomware attacks.	We recommend investigating what ports the triggering traffic was running on. If these ports are not associated with applications you expect to see in your network, we recommend blocking them at the firewall.		0 Days
50	3. Command and Control Detection 3.4 Unauthorized Outbound SSH An unauthorized SSH connection has been detected from an internal device to an external domain.	We recommend routing all legitimate external SSH connections through a VPN and blocking all incoming activity on ports 5985 and 22.		0 Days

This report has been prepared for Acme Corporation. It is for illustrative purposes only and WatchGuard is not responsible for any decisions or actions taken based on this information.

Page 1

ThreatSync+ NDR includes policy-driven controls and objectives that cover the 40 CISA-defined critical network ransomware defense policies. These policies and their effectiveness are clearly shown in the solution's Ransomware Prevention Defense Goal Report.

Supply Chain Defense

Be a strong link, not a weak link, in the cyber defense supply chain

Digital transformation has connected businesses to create unparalleled efficiency in the accuracy and volume of supply chain movement and transactions, forever removing boundaries between company systems and processes. There is, unfortunately, a downside: this web of interconnected systems has opened opportunities for cybercriminals to enter via the weakest links and navigate the digital supply chain to their intended target via the connected ecosystem.

To mitigate third-party supply chain risk, prominent vendors and ecosystem associations have joined to set cybersecurity standards that must be met before integrated supply chain contracts are signed. These standards are enforced via stringent audits, and contract termination can result from an audit failure.

Implementing and remaining compliant with these standards creates a significant challenge for resource-constrained companies, who must improve their security hygiene across hybrid networks while managing operations and human costs. They must also demonstrate continuous compliance to enter or remain a part of the supply chain ecosystem.

The traditional enterprise security mix of SIEM/EDR/NDR tools is a non-starter for most organizations. Yet, they require a solution that can deliver the critical features of these tools, including:

- The automatic discovery of vulnerable assets with the capability to identify and prioritize mitigation based on risk
- 24/7 threat monitoring and remediation covering event correlation and alerting for malware, risky activity, IoT threats, and high-risk traffic on the network
- AI-driven automated threat hunting, investigation, and response with the ability to alert IT teams and offer rapid containment
- The effective use of AI and automation to overcome staffing and budget constraints while delivering enterprise-class cybersecurity hygiene
- Continuously compliant processes and controls on demand utilizing risk and threat dashboards and security process scorecards

5. https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/
6. https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends

East-West Threat Detection

ThreatSync+ NDR intelligently detects supply chain vulnerabilities and attacks by analyzing network data for anomalous activity representing vulnerabilities, risks, and threats. Data is collected from existing network devices, routers, firewalls, directories, and Cloud systems to build a 360-degree operational view of your network. IT teams are presented with risk-scored alerts and mitigating actions to prioritize resources, including visibility into new devices on the network.

Automated Threat Hunting

Supply chains operate 24/7, and ThreatSync+ NDR AI continuously monitors hybrid networks for the IoCs of supply chain attacks even when humans cannot. Automated AI-driven threat hunting detects supply chain attack IoCs, alerts security teams to the threat, and guides them through the actions needed to remediate the attack before it spreads to other systems or across ecosystems to partners.

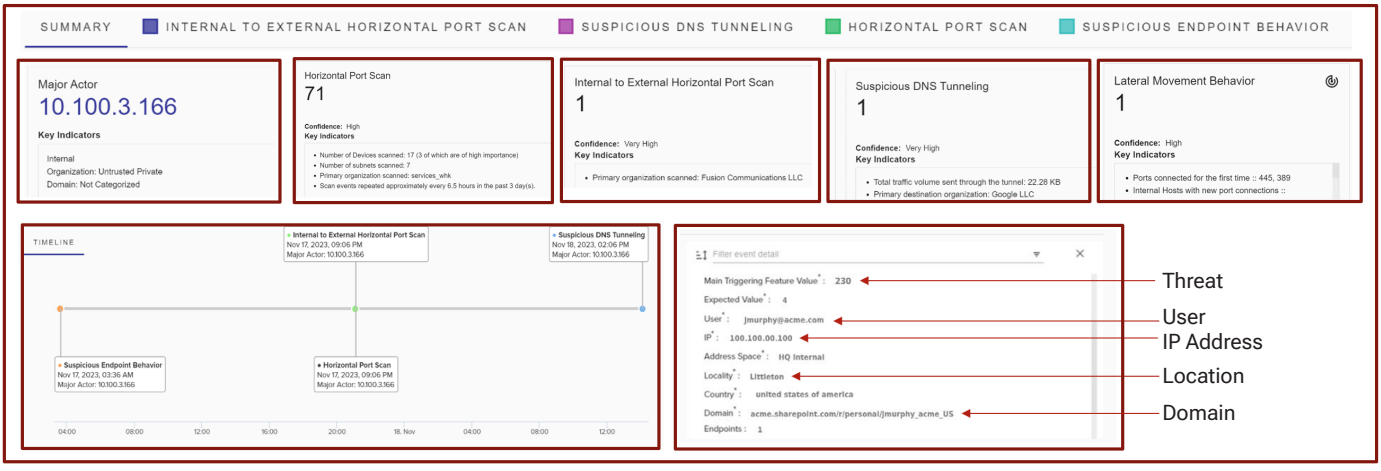
Configurable Compliance Reporting

Implement, report, and remain compliant with cybersecurity standards set and enforced by ecosystem partners, auditors, and associations. ThreatSync+ NDR enables security teams to quickly build and implement custom compliance controls and report their effectiveness. Businesses can rapidly advance security hygiene while demonstrating continuous compliance to win and maintain lucrative supply chain contracts.

Simplicity of Operation

ThreatSync+ NDR takes an intelligent route to detecting risks and vulnerabilities across highly distributed networks. ThreatSync+ NDR uses data as its intelligence source, and our advanced artificial intelligence/machine learning (AI/ML) analyzes network data for anomalous activity that represents vulnerabilities, risks, and threats. Data is collected from existing network devices, firewalls, and VPN systems to build a 360-degree operational view of your network. IT teams are presented with risk-scored alerts and mitigating actions to prioritize resources, including visibility into unknown and rogue devices on the network.

ThreatSync+ NDR investigative views enable teams to quickly identify potential supply chain threats and understand incidents and their relationships, timelines, and assets involved.



Conclusion

In the new reality of network environments, cyberattackers can now compromise an application, service, or account inside the network or in the Cloud. The combination of legacy networks with private and public Clouds means IT and security managers must monitor and manage:

- Data movement, especially when sensitive data moves from inside the network to partner and customer networks.
- Network activity that includes risky and anomalous traffic across the network boundary and then to sensitive data locations or devices.
- Rogue devices that can access sensitive areas of the network.
- Hazardous network traffic like reconnaissance, command and control, extensive data movements to risky locations, and unusual devices accessing sensitive application zones.

ThreatSync+ NDR delivers cost-effective network visibility, defense, and compliance services from the WatchGuard Cloud. Advanced AI and automation can operate as a 24/7 continuous monitoring solution, watching the organization's users, devices, and network services, and supporting immediate remediation of threats when needed. With award-winning artificial intelligence, ThreatSync+ NDR provides highly effective and affordable network threat detection and response across various use cases, ensuring a positive return on investment (ROI) and a lower total cost of ownership (TCO) than existing appliance-based NDR products and complex SIEM tools.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com