DATASHEET

ThreatSync+ NDR

Unified Network Security Made Simple

ThreatSync+ NDR is an extension of WatchGuard's ThreatSync XDR solution. Managed in the WatchGuard Cloud, it delivers a highly effective network detection, response, and compliance solution for cybersecurity teams with distributed networks. Utilizing AI-driven security policies, ThreatSync+ NDR reduces the massive volume of network traffic into prioritized smart alerts, investigative views, and compliance reports.

Once network risks and threat events are identified, ThreatSync+ NDR sends them to ThreatSync XDR for remediation, providing a unified orchestration response. Together, they streamline cybersecurity, enhance visibility, automate response actions across the organization more quickly, reduce risk and cost, and offer greater accuracy.

See Risks and Threats Across Your Network

For network & Cloud operations managers, ThreatSync+ NDR offers a comprehensive view of abnormal risky activities across remote workers, on-premises, and Cloud environments. This visibility allows managers to swiftly identify unprotected or rogue devices, threats to IoT devices, misconfigured ports, risky traffic, and backup system failures without overburdening IT teams.

Detect and Stop Threats, Reduce Dwell Time

ThreatSync+ NDR enables automated, continuous monitoring for threats across networks, the Cloud, and VPNs. Utilizing a unique combination of cyber TTP policies, threat intelligence, and AI, it delivers a short, prioritized list of smart alerts and threat reports. Cyber and IT managers can then quickly investigate and remediate cyberattacks 24x7.

Prove Continuous Compliance

Prebuilt, automated compliance policies and reports are activated with the push of a button using WatchGuard's Compliance Reporting. Prove compliance through prebuilt reporting, which includes control effectiveness, SLA tracking, and compliance objective metrics. Compliance policies include multiple aggregated rules, AI models, control objectives, and assurance reports for ISO 27001, NIST 800-53, Cyber Essentials, FFIEC, NIAC, CMMC, and more.

Built for Small IT Security Teams

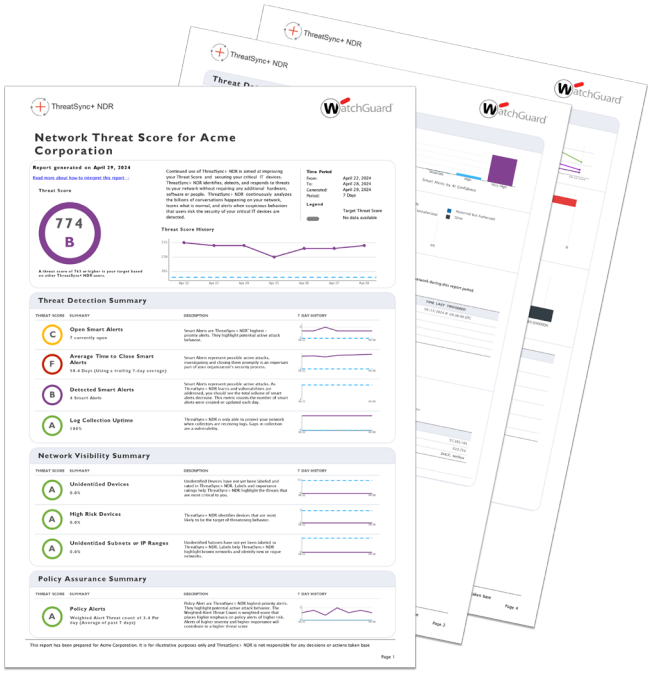
ThreatSync+ NDRs' unique Cloud-native delivery model provides enterprise-class cybersecurity at a fraction of the cost of traditional NDR or SIEM tools. Deployed in just hours, ThreatSync+ NDR is designed for operational success in any environment.

Benefits

- Compliance status is evaluated with a button click. Reports are generated quickly for auditors, partners, suppliers, and insurance providers.
- Cost of compliance is reduced by automating highly manual processes, reducing workloads on IT teams.
- Compliance posture is improved through control effectiveness reports and take practical remediation actions with improvement guidance.
- Simplified compliance process includes easy-to-configure, out-of-the-box control sets and reports to support new and changing requirements.

Continuous Compliance

Continuous monitoring of cybersecurity program goals and regulatory compliance controls eliminates manual processes and reduces costs, while on-demand automated reporting ensures proof of compliance. Compliance framework models cover regulatory, supply chain, industry standards, and insurance policy compliance.



Key Features

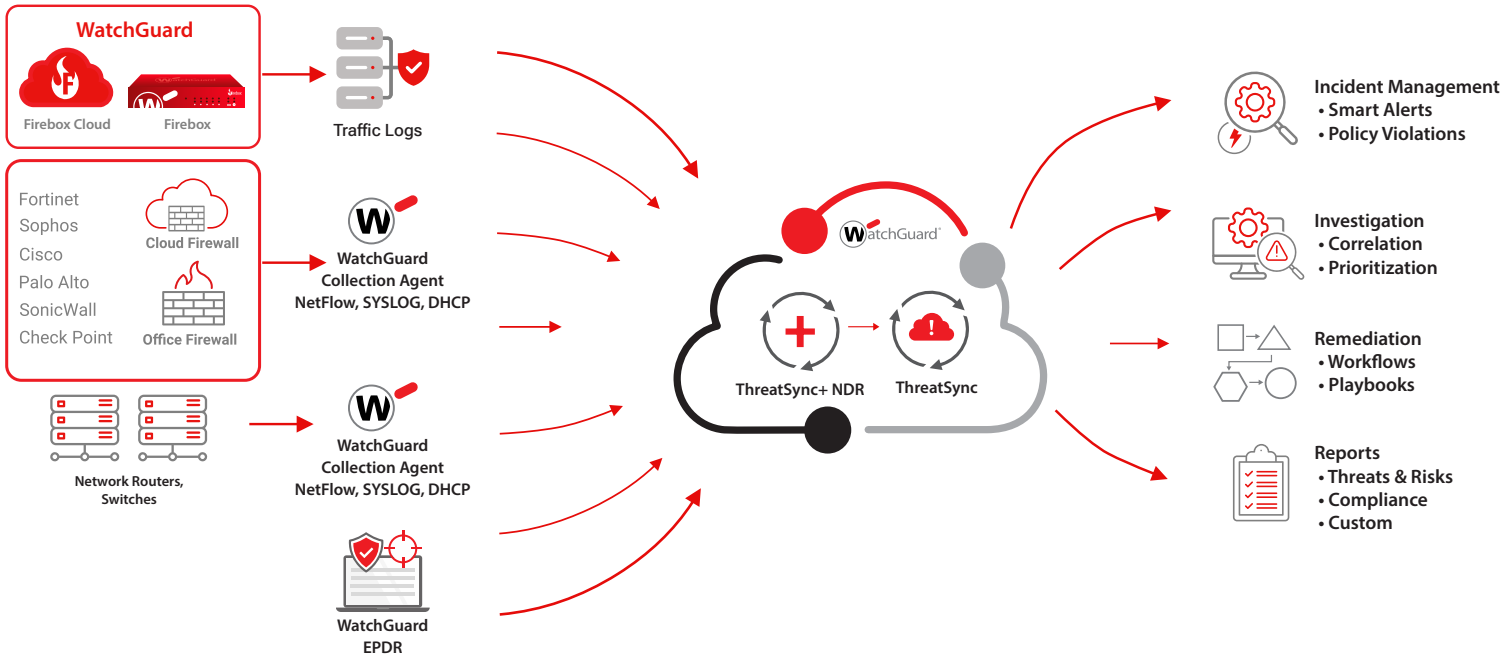
Enterprise AI-driven accuracy in detecting attacks operating inside your network, including:

- Ransomware
- Supply Chain Attacks
- Vulnerabilities
- VPN Threats
- Command & Control (C2)
- Man-in-the-Middle
- Unauthorized Web & DNS Activities
- Masqueraders (Tunneling)
- Credential Compromise
- Rogue Behaviors
- Insider Threats
- Lateral Movement
- Data Exfiltration

Out-of-the-box NIST and ISO policy-based, AI-powered control frameworks support continuous compliance and compliance reporting.

ThreatSync and Firebox integration enables the coordination and automation of multiple processes and tools with security orchestration, providing a cohesive security posture.

ThreatSync and ThreatSync+ NDR
Deliver Affordable, Expansive, and Unified Threat Detection and Response



WatchGuard Technologies, Inc.