DATENBLATT

ThreatSync+ NDR

Unified Network Security leicht gemacht

ThreatSync+ NDR ist eine Erweiterung der ThreatSync XDR-Lösung von WatchGuard. Durch die Verwaltung in der WatchGuard Cloud bietet sie eine hocheffektive Lösung für Netzwerkerkennung, Reaktion und Compliance für Cybersicherheitsteams mit verteilten Netzwerken. ThreatSync + NDR fasst mittels KI-gesteuerten Sicherheitsrichtlinien das massive Volumen an Netzwerkverkehr in priorisierte intelligente Warnungen, Untersuchungsansichten und Compliance-Berichte zusammen.

Sobald Netzwerkrisiken und Bedrohungsereignisse identifiziert wurden, sendet ThreatSync+ NDR sie zur Behebung an ThreatSync XDR und bietet somit eine einheitliche Orchestrierungsreaktion. Gemeinsam optimieren sie die Cybersicherheit, verbessern die Transparenz, beschleunigen die automatisierten Reaktionsmaßnahmen im gesamten Unternehmen, reduzieren Risiken und Kosten und bieten mehr Präzision.

Risiken und Bedrohungen in Ihrem gesamten Netzwerk identifizieren

Für Netzwerk- und Cloud-Betriebsleiter bietet ThreatSync + NDR einen umfassenden Überblick über abnormale riskante Aktivitäten von Remote-Mitarbeitern sowie in lokalen und Cloud-Umgebungen. Diese Transparenz ermöglicht es ihnen, ungeschützte oder nicht geschützte Geräte, Bedrohungen für IoT-Geräte, falsch konfigurierte Ports, riskanten Datenverkehr und Backup-Systemausfälle schnell zu identifizieren, ohne die IT-Teams zu überlasten.

Bedrohungen erkennen und stoppen, Verweildauer verkürzen

ThreatSync+ NDR ermöglicht eine automatisierte, kontinuierliche Überwachung von Bedrohungen über Netzwerke, die Cloud und VPNs hinweg. Mit einer einzigartigen Kombination aus Cyber-TTP-Richtlinien, Threat Intelligence und KI stellt es eine kurze, priorisierte Liste mit intelligenten Warnungen und Bedrohungsberichten bereit. Cyber- und IT-Manager können Cyberangriffe so rund um die Uhr schnell untersuchen und beheben.

Kontinuierliche Compliance nachweisen

Vorgefertigte, automatisierte Compliance-Richtlinien und -Berichte werden mithilfe der Compliance-Berichterstattung von WatchGuard auf Knopfdruck aktiviert. Weisen Sie Compliance durch vorgefertigte Berichte, einschließlich Kontrolleffektivität, SLA-Verfolgung und Zielmetriken nach. Compliance-Richtlinien umfassen mehrere zusammengeführte Regeln, KI-Modelle, Kontrollziele und Sicherheitsberichte für ISO 27001, NIST 800-53, Cyber Essentials, FFIEC, NIAC, CMMC und mehr.

Entwickelt für kleine IT-Sicherheitsteams

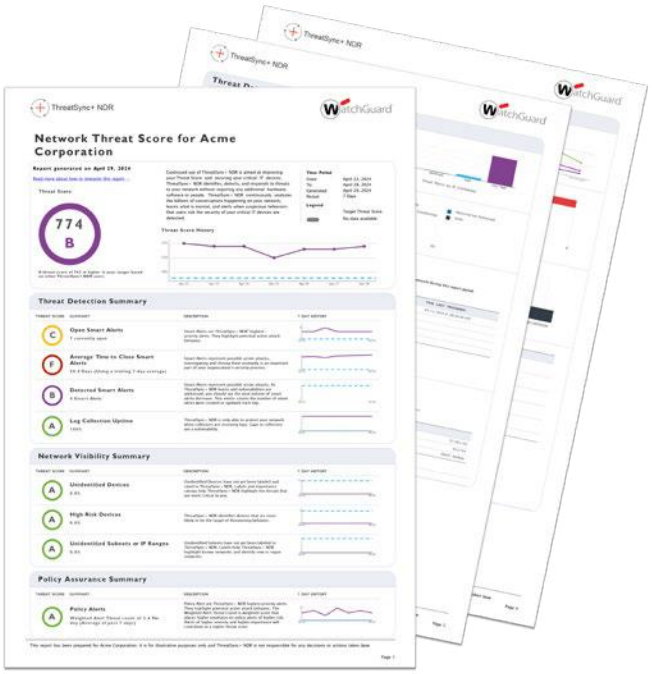
Das einzigartige cloudnative Bereitstellungsmodell von ThreatSync + NDR bietet Cybersicherheit auf Enterprise-Niveau zu einem Bruchteil der Kosten herkömmlicher NDR- oder SIEM-Tools. In nur wenigen Stunden bereitgestellt, ist ThreatSync + NDR für den operativen Erfolg in jeder Umgebung konzipiert.

Vorteile

- Der Compliance-Status wird mit nur einem Knopfdruck ausgewertet. Berichte für Auditoren, Partner, Lieferanten und Versicherungen werden schnell erstellt.
- Die Compliance-Kosten werden durch die Automatisierung hochmanueller Prozesse reduziert, wodurch die Arbeitsbelastung der IT-Teams reduziert wird.
- Das Compliance-Verhalten wird durch Berichte zur Kontrollwirksamkeit verbessert und es können praktische Behebungsmaßnahmen mit Hilfe von Hinweisen zur Optimierung ergriffen werden.
- Der vereinfachte Compliance-Prozess umfasst einfach zu konfigurierende, sofort einsatzbereite Kontrollsätze und Berichte, um neue und sich ändernde Anforderungen zu unterstützen.

Kontinuierliche Compliance

Die kontinuierliche Überwachung der Ziele des Cybersicherheitsprogramms und der Kontrollen zur Einhaltung gesetzlicher Vorschriften eliminiert manuelle Prozesse und senkt die Kosten. Gleichzeitig gewährleistet die automatisierte On-Demand-Berichterstattung den Nachweis der Einhaltung. Die Compliance-Framework-Modelle decken Regulierungs-, Lieferketten-, Branchenstandards und die Einhaltung von Versicherungspolicen ab.



Wichtige Funktionen

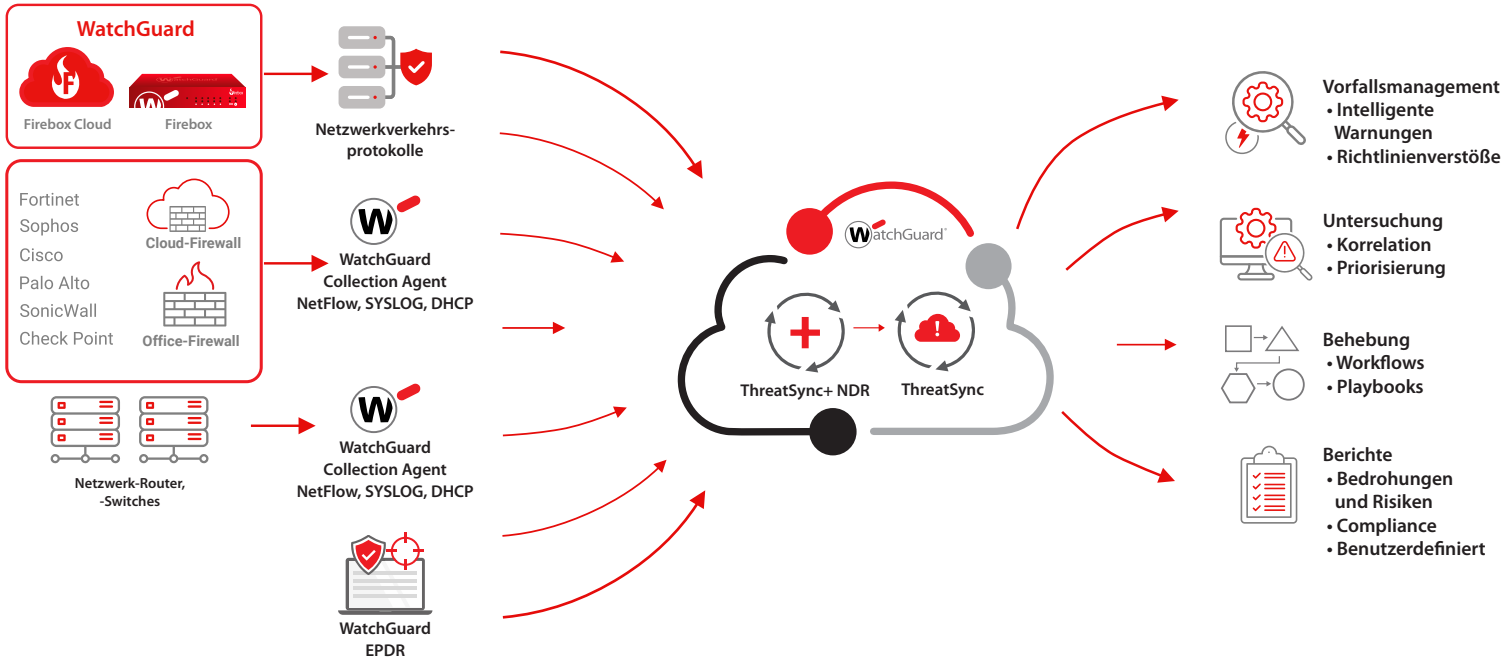
KI-gesteuerte Präzision bei der Erkennung von Angriffen in Ihrem Netzwerk, einschließlich:

- Ransomware
- Angriffe über Lieferketten
- Schwachstellen
- VPN-Bedrohungen
- Command & Control (C2)
- Man-in-the-Middle
- Nicht autorisierte Web- und DNS-Aktivitäten
- Masquerading (Tunneling)
- Kompromittierung der Anmeldeinformationen
- Rogue-Verhalten
- Insider-Bedrohungen
- Laterale Bewegung
- Datenexfiltration

NIST- und ISO-Richtlinienbasierte, KI-gestützte Kontroll-Frameworks unterstützen kontinuierliche Compliance und Compliance-Berichte.

ThreatSync und Firebox ermöglichen die Koordinierung und Automatisierung mehrerer Prozesse und Tools mithilfe der Sicherheitsorchestrierung zur Förderung eines einheitlichen Sicherheitskonzepts.

ThreatSync und ThreatSync+ NDR bieten erschwingliche, umfassende und einheitliche Bedrohungsanalysen



DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.