Die Vorteile KI-basierter NDR

ThreatSync+ NDR: Netzwerkerkennung und Abwehr – Anwendungsfallabdeckung

Die Anwendungsfälle und das Wertversprechen der Cloud-nativen NDR-Lösung von WatchGuard und wie kleinere Sicherheitsteams damit Cybersicherheitsrisiken effizient reduzieren können

Inhalt

Einleitung

Da Cyberbedrohungen immer weiter zunehmen und die Techniken zur Infizierung von Geräten immer besser, komplexer und schwieriger zu erkennen werden, müssen Sicherheitsteams Tools finden, mit denen sich Angriffe schnell und präzise lokalisieren und stoppen lassen. Doch trotz neuer Schutztechnologien haben Angreifer allerdings weiterhin die Oberhand.

Das Netzwerk, das Rückgrat eines jeden IT-Systems, befindet sich im Zuge des Umstiegs auf die Cloud in einem tiefgreifenden Wandel. Trotz dieser Änderungen bleibt es die „Single Source of Truth" für Sicherheitsteams und bietet ihnen die Werkzeuge, um Risiken zu mindern und Angriffe zu identifizieren und zu stoppen. Es ist wichtig zu erkennen, dass Angreifer die Kontrolle über das Netzwerk erlangen müssen, um einen erfolgreichen Angriff auszuführen.

Viele Jahre lang konzentrierten sich Erkennungsstrategien hauptsächlich auf Endpoints (Geräte), von Antivirus über Endpoint Detection and Response (EDR) bis hin zu Extended Detection and Response (XDR). Diese Verlagerung weg vom Netzwerk wurde in erster Linie durch die weit verbreitete Einführung von verschlüsseltem Datenverkehr beeinflusst, was den Wert der Paketerfassung verringerte. Darüber hinaus machte das exponentielle Wachstum des Datenverkehrsvolumens die richtlinienbasierte Erkennung komplex und anfällig für falsch positive Ergebnisse.

Die umfangreiche Einführung von Automatisierung und künstlicher Intelligenz hat die Erkennungs- und Reaktionsfähigkeiten für EDR und XDR erheblich verbessert. Dadurch wurden auch die NDR-Funktionen (Network Detection and Response) erheblich verbessert, unabhängig davon, ob sich das Netzwerk vor Ort oder in der Cloud befindet. Durch die Integration von KI und Automatisierung sind NDR-Produkte mittlerweile nicht mehr komplex, sondern einfach, und Erkennungsfunktionen sind erheblich präziser geworden.

Die Vorteile KI-basierter NDR

Unüberwachtes und halbüberwachtes maschinelles Lernen wird mit umfangreichen Netzwerkdatenströmen durchgeführt. Dadurch entfällt die Notwendigkeit einer vollständigen Paketerfassung und einer rein richtlinienbasierten Erkennung. Stattdessen achten KI-Modelle auf riskanten Datenverkehr und Endpoint-Standorte, Netzwerkaufklärung, Befehl und Steuerung, Rechteausweitungen (1), laterale Bewegung, Daten-Staging, Backup-Unterbrechung, Massenverschlüsselung und Datenexfiltration, wodurch die Erkennung über die Expansions- und Ausführungsphasen eines Cyberangriffs hinweg effektiv abgedeckt wird.

Netzwerke können bei einem erfolgreichen Cyberangriff nicht umgangen werden. Angriffe können versuchen, sich im regulären Datenverkehr zu verstecken, aber ihre Struktur und Bewegung werden im Vergleich zur normalen Basislinie für diese Umgebung anomal sein, sodass sie erkannt werden. NDR-Systeme können von Angreifern nicht attackiert und abgeschaltet werden, da sie außerhalb des Netzwerks laufen und die Netzwerkdatenströme überwachen. Das kontinuierliche Monitoring des Netzwerkverkehrs mit mehreren KI-Modellen ist die unbestreitbare Quelle der Wahrheit für IT-Teams, um ihre Risiken und Bedrohungen zu verstehen. In diesem Artikel werden die Anwendungsfälle beschrieben, die die ThreatSync+ NDR-Lösung von WatchGuard abdeckt.

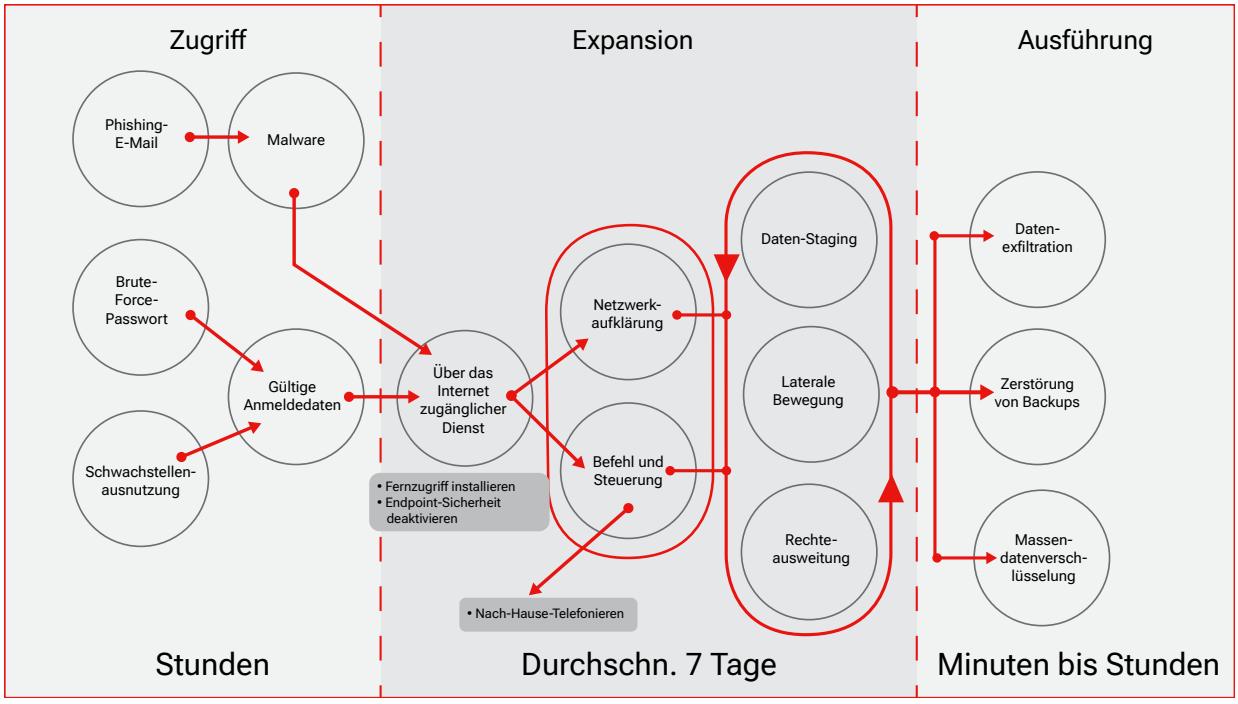


Abbildung 1. Vom Erfolg der Netzwerkexpansionsphase eines Cyberangriffs hängt der Gesamterfolg des Angriffs ab.

Risikovisualisierung

Einblick in versteckte Netzwerkrisiken, die von Angreifern ausgenutzt werden

Unternehmen müssen einen umfassenden Überblick über ihren Netzwerkverkehr und ihre Systeme, einschließlich IoT-Geräte, haben, um die in Netzwerken verborgenen Risiken und Schwachstellen zu erkennen und zu verstehen. Die Minderung dieser Risiken und Schwachstellen verringert die Bedrohungsoberflächen, verbessert die Abwehr und macht Unternehmen weniger anfällig für Angriffe.

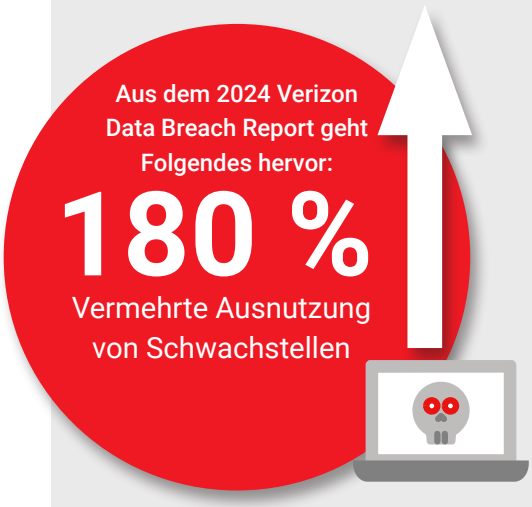
ThreatSync+ NDR ermöglicht es Unternehmen, Netzwerkrisiken und Schwachstellen zu identifizieren, bevor sie ausgenutzt werden können. Durch das Monitoring des Netzwerkdatenverkehrs und die Analyse von Verkehrsverhaltensmustern können IT-Teams die wichtigsten Risiken schnell identifizieren und geeignete Ressourcen zuweisen, um sie zu mindern. Die Risikoabdeckung umfasst Nord-Süd- und Ost-West-Netzwerkdatenverkehr, VPN und Netzwerk-Cloud-Datenverkehr.

ThreatSync+ NDR bietet eine hocheffektive Risikotransparenz für Netzwerke, da fortschrittliche Machine-Learning-Algorithmen verwendet werden, die in eine Richtlinien-Engine integriert sind, um zunächst alle im Netzwerk betriebenen Geräte zu verstehen und dann basierend auf dem anomalen Datenverkehr, der durch das Netzwerk fließt, zu definieren, welches dieser Geräte am stärksten gefährdet ist. ThreatSync+ NDR identifiziert alle Netzwerkgeräte und ermöglicht es dem IT-/Sicherheitsteam, sie zu markieren und einen Wichtigkeitswert anzuwenden, der dann in das ermittelte KI-basierte Risiko einfließt. Wenn die Risikowerte die festgelegten Schwellenwerte überschreiten oder plötzlich neue Geräte im Netzwerk auftauchen, macht ThreatSync+ NDR das IT-/Sicherheitsteam auf das Problem aufmerksam.

Die zweite Ebene der Risikovisualisierung basiert auf der Richtlinien-Engine von ThreatSync, die Hunderte von Best-Practice-Kontrollen auf der Grundlage von ISO- und NIST-Standards umfasst. IT-/Sicherheitsteams können schnell neue Kontrollen erstellen oder bestehende Kontrollen ändern. Zu den Kontrollen zählen Standard-Firewall-Regeln, die es ThreatSync+ NDR ermöglichen, Regelfehler im gesamten Netzwerk zu überwachen, z. B. Datenverkehr, der in ein Land auf der schwarzen Liste fließt.

Bedrohungspotenziale reduzieren und die IT-Hygiene verbessern

- Geräte/IoT im Netzwerk identifizieren, markieren und überwachen
- Fehlerhafte Firewall-Regeln lokalisieren
- Falsch konfigurierte oder ungeschützte Ports ermitteln
- Netzwerke in Zero-Trust-Sicherheitszonen aufteilen
- Blinde Flecken im Netzwerk, Schatten-IT und nicht autorisierte Geräte finden



Proaktive Risikominderung

ThreatSync+ NDR wurde entwickelt, um scheinbar unsichtbare Risiken aufzudecken und Leitlinien und Maßnahmen bereitzustellen, um diese Risiken zu mindern und den Sicherheitsstatus proaktiv zu verbessern. ThreatSync+-KI-Modelle sind so eingestellt, dass sie auf fehlgeschlagene Firewall-Regeln, ungesicherte Ports, fehlgeschlagene Backups und mehr achten. Risiken werden identifiziert und priorisiert und für eine schnelle Minderung werden Abhilfemaßnahmen bereitgestellt. ThreatSync+ NDR findet Risiken, bevor sie von Angreifern ausgenutzt werden.

Nicht autorisierte Geräte erkennen

ThreatSync+ NDR sammelt und analysiert den Netzwerkdatenverkehr (Nord-Süd und Ost-West) zusammen mit den Anwenderprotokolldaten, um alle Geräte und Systeme im Netzwerk zu identifizieren. Auf der Grundlage des Datenverkehrs identifiziert ThreatSync+ KI den Gerätetyp, einschließlich IoT-Geräte. Die Lösung erkennt, wenn neue Geräte verbunden werden, und gibt entsprechende Warnmeldungen aus. Anhand von Korrelation werden sogar die IP-Adresse und das Anwenderkonto für jedes erkannte Gerät identifiziert. Die Lösung liefert eine detaillierte 360-Grad-Betriebsansicht Ihres Netzwerks.

Netzwerksegmentierung, Zero Trust

Unternehmen haben Schwierigkeiten, Zero-Trust-Initiativen im Netzwerk durchzusetzen, da Zero-Trust oft komplexe Architekturen, viele verschiedene Produkte und mehrere Subnetze umfasst. Die Implementierung und Verwaltung von Zero-Trust-Kontrollen in komplexen Umgebungen kann eine Herausforderung darstellen und bei Fehlkonfigurationen können Umgebungen kompromittiert werden und Daten verloren gehen. ThreatSync+ NDR agiert als Zero-Trust-Überwachungskontrolle.

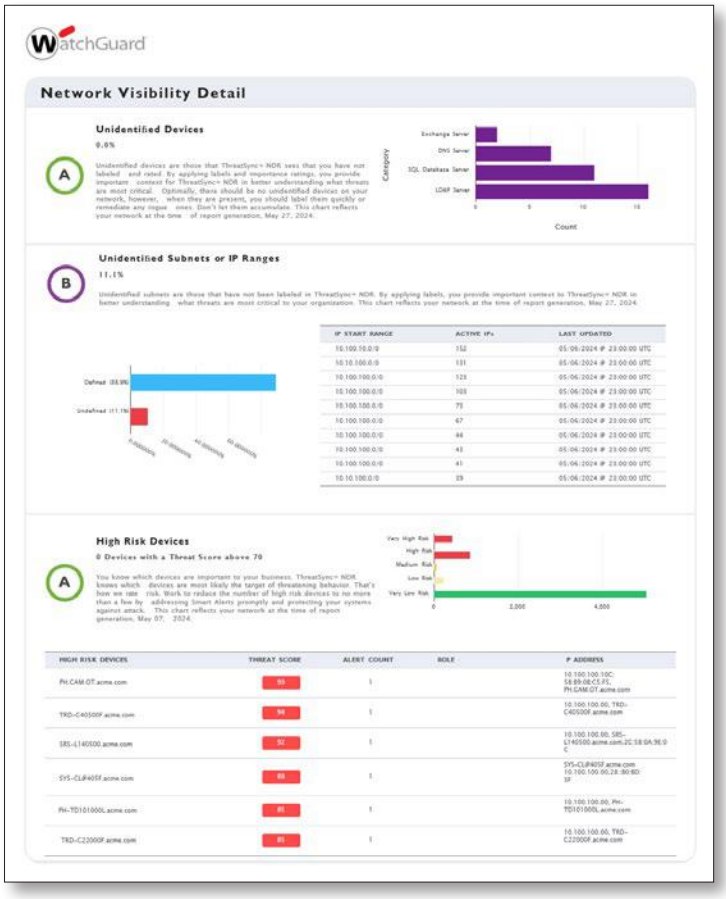


Abbildung 2: Berichte zur Netzwerkvisualisierung, die unbekannte oder risikoreiche Geräte identifizieren, tragen zur Aufrechterhaltung eines fehlerfreien Netzwerks bei

ThreatSync+ NDR ermöglicht es IT-/Sicherheitsteams, basierend auf Geräte- und Subnetz-Tags, Gerätetyp, Geräte- oder Datenverkehrskritikalität, Topologie und physischem Standort Parameter für einen Zero-Trust-Netzwerkzugriff zu definieren und durchzusetzen. Diese Parameter werden zu Zero-Trust-Überwachungsebenen und ThreatSync+ NDR alarmiert IT-/Sicherheitsteams, wenn Zero-Trust-Kontrollen verletzt werden.

Netzwerkbedrohungsanalysen

Sich entwickelnden Bedrohungen, die traditionelle Sicherheitslösungen umgehen, immer einen Schritt voraus bleiben

Die Cybersicherheitslandschaft verlagert sich weiter in Richtung fortgeschrittener und getarnter Cyberangriffe. Die Sicherheitsverletzungen bei SolarWinds und MOVEit sind bekannte Beispiele für die Folgen unentdeckter Angriffe. Sie unterstreichen die Notwendigkeit robusterer und umfassenderer Sicherheitsmaßnahmen, die über den traditionellen Perimeterschutz hinausgehen.

Mit einem mehrschichtigen Sicherheitsansatz lassen sich diese Bedrohungen der neuen Generation besser bekämpfen. Der Schwerpunkt liegt zunehmend auf der Netzwerkerkennung und Abwehr, um diese Herausforderungen zu meistern. NDR-Lösungen ergänzen den Endpoint-Schutz und ermöglichen eine bessere Bedrohungserkennung in Netzwerkumgebungen.

ThreatSync+ NDR bietet eine Cloud-native Bedrohungserkennung und -abwehr. Die KI-Engine von ThreatSync+ verwendet mehrere unüberwachte und halbüberwachte maschinelle Lernmethoden, um normale Aktivitätsbasislinien für alle Geräte und Anwender sowie den gesamten Datenverkehr im Netzwerk und in der Cloud zu bestimmen.

ThreatSync+ KI überwacht Systeme in fünf kritischen Kategorien kontinuierlich auf bedrohliches Verhalten:

1. Hinweise auf Cyberangriffe
2. Riskantes menschliches Verhalten
3. Riskantes Geräteverhalten
4. Netzrisiken
5. Netzwerkzustand

Jede Kategorie umfasst mehrere KI-Modelle und allgemeine, integrierte Richtlinien, um Bedrohungen zu erkennen und zu priorisieren und Verhaltensweisen zu korrelieren und so falsch positive Ergebnisse zu eliminieren. Richtlinien zur Bedrohungserkennung bereichern die KI-Ergebnisse, indem sie Bedrohungsinformationen und gängige Angriffsverhaltenstechniken hinzufügen. Dies ermöglicht ein automatisiertes, äußerst präzises und kontinuierliches Monitoring von Bedrohungen über Netzwerke und VPN-Datenverkehr hinweg. Wenn Bedrohungen auftauchen, liefert ThreatSync+ NDR die erforderlichen Informationen und Anleitungen, um die Bedrohung, die entsprechende Phase und die betroffenen Systeme zu verstehen, und bietet sofortige Abhilfemaßnahmen über ThreatSync-Workflows für EDR und Firewalls.

Bedrohungsabdeckung von ThreatSync+ NDR

- Ransomware
- Lieferkette
- VPN-Bedrohungen
- Befehl und Steuerung (Command and Control, C2)
- Man-in-the-Middle
- Nicht autorisierte Web- und DNS-Aktivitäten
- Masquerading (Tunneling)
- Rogue-Verhalten
- Insider-Bedrohungen
- Laterale Bewegung

Nord-Süd-Bedrohungserkennung

Das Monitoring des Nord-Süd-Datenverkehrs auf Risiken und Bedrohungen ist entscheidend für die Erkennung von Angriffen, die die Endpoint-Sicherheit umgangen haben. ThreatSync+ NDR sucht speziell nach Angriffsphasen, einschließlich Aufklärung, Befehl und Steuerung, Nutzlasteingabe, Datenexfiltration, Datenverkehr zwischen anomalen oder bekannten schädlichen Standorten, externe Netzwerkscans sowie interne und externe Datenverkehrsanomalien, einschließlich NET BIOS- und AD-Kommunikationsereignissen. Wenn eine oder mehrere dieser Anomalien auftreten, kann ThreatSync sie sofort über Firewall und EDR-Integration blockieren.

Ost-West-Bedrohungserkennung

Das Monitoring des Ost-West-Datenverkehrs ist ebenso wichtig, um Angriffe in Ihrem Netzwerk zu erkennen. ThreatSync+ NDR überwacht das System auf horizontale Aufklärung, Rechteausweitung und Zugriff auf Anmeldeinformationen, laterale Bewegung, Daten-Staging, anomalen Zugriff, anomale Datenbewegung im Netzwerk, in die Cloud oder in der Cloud, veröffentlichte Datenspeicher und Backup-Unterbrechung. Durch das Monitoring der Nord-Süd-, Ost-West- und Netzwerk-Cloud-Kommunikation werden Angriffe erkannt, die Endpoints umgangen haben, und die Verweildauer wird von Wochen auf Stunden reduziert.

Automatisierte Behebung

Eine der größten Herausforderungen für IT- und Sicherheitsteams ist die Verweildauer. Im neuesten Verizon Data Breach Report liegen die durchschnittlichen Verweildauern zwischen 30 und 50 Tagen, während die Angriffsabschlusszeiten durchschnittlich zwischen 1 und 12 Tagen liegen. Die Rechnung geht nicht auf und Teams müssen in den Wiederherstellungsmodus wechseln, sobald der abgeschlossene Angriff entdeckt wird. Da ThreatSync+ NDR Angriffe innerhalb des Netzwerks erkennen und aufdecken kann, können Angriffe in Kombination mit ThreatSync Core automatisch oder manuell sofort nach der Erkennung beseitigt werden. Mit diesen Funktionen kann selbst ein kleines IT-Team einen Angriff erkennen und stoppen, bevor der beabsichtigte Angriffspfad abgeschlossen ist. ThreatSync+ NDR agiert als Zero-Trust-Überwachungskontrolle.

ThreatSync+ NDR enthält über fünfzig sofort einsatzbereite Kontrollen für den Netzwerkschutz, die ein Rund-um-die Uhr-Monitoring über Netzwerk- und VPN-Angriffsflächen hinweg ermöglichen, um Ransomware, APT, DOS- und IP-Angriffe, den Diebstahl personenbezogener Daten und geschützter Gesundheitsdaten sowie andere elaborierte Bedrohungen zu erkennen.

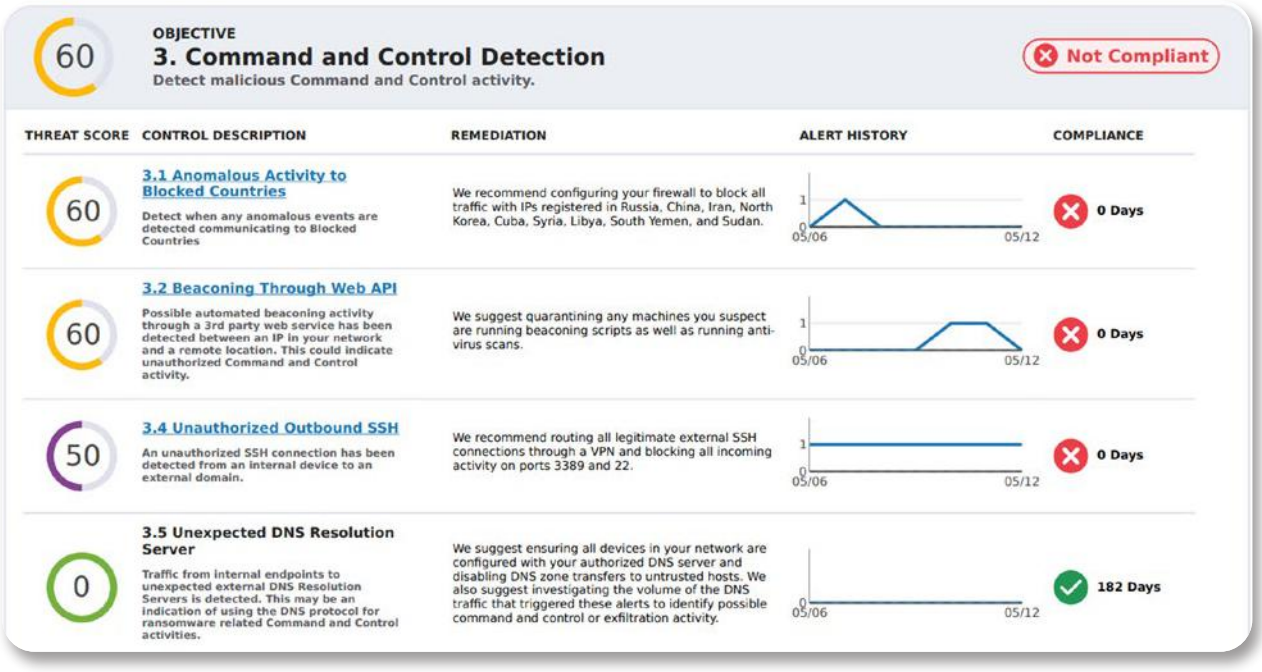


Abbildung 3. Aktivitätsbericht zur Befehls- und Steuerungserkennung

Kontinuierliche Compliance und Berichterstattung

Nachhaltige Netzwerk-Compliance für Best Practices und regulatorische Rahmenbedingungen der Branche

Unternehmen müssen sich mit der Abwehr von Cyberangriffen befassen und gleichzeitig immer strengere Vorschriften zur Datensicherheit und zum Datenschutz umsetzen. Die Kosten und die Komplexität im Zusammenhang mit Compliance können für jedes Team eine Herausforderung darstellen. Für kleinere Teams mit beschränkten Ressourcen kann der manuelle Aufwand für Datenerfassung, Validierung und Berichterstellung jedoch sehr hoch sein.

Vorschriftenverstöße können zu hohen Bußgeldern führen. Im Februar 2023 beispielsweise verhängten die Aufsichtsbehörden der DSGVO (Datenschutz-Grundverordnung) gegen die Bank of Ireland wegen unzureichender technischer Sicherheitskontrollen eine Geldbuße von 750.000 EUR. In den Vereinigten Staaten zahlte die Oklahoma State University – Center for Health Services HIPAA-Bußgelder in Höhe von 875.000 USD für eine Datensicherheitsverletzung.

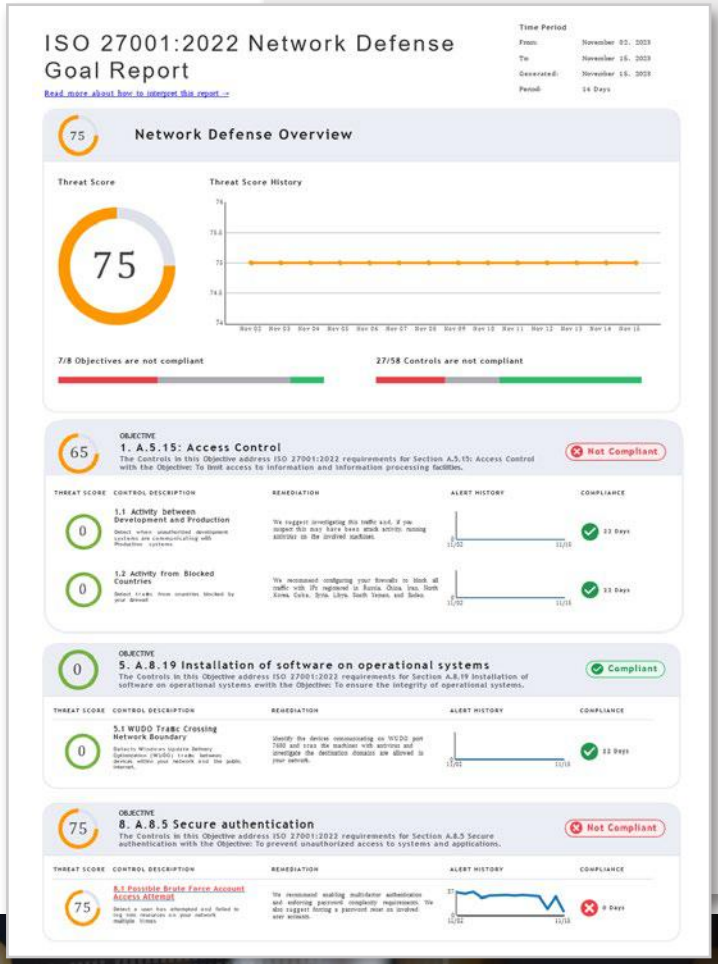
ThreatSync+ NDR umfasst in Kombination mit der Compliance-Berichterstattung von WatchGuard eine Richtlinien-Engine, über hundert Compliance-Kontrollen, die den gängigsten Standards zugeordnet sind, und eine automatisierte Berichtserstattungs-Engine, um schnell und einfach konfigurierbare Compliance-Berichte für alle Ihre Netzwerkkontrollen zu erstellen.

Vorgefertigte Kontrollmechanismen für ISO-27001, NIST 800-53, NIST-171/ CMMC und Cyber Essentials sind enthalten. Die einfach konfigurierbare Kontrollzuordnung für spezialisierte Branchenaudits erweitert die Funktionen, um das Framework der Motion Picture Association (MPAA), CIS Critical Security Controls, IEEE-Standards und die meisten Anforderungen von Cyberversicherungen abzudecken.

Neben den Auditanforderungen umfasst ThreatSync+ NDR Berichte zur Zusammenfassung von Netzwerkbedrohungen und zum Schutz vor Ransomware, in denen Ziele und Kennzahlen des Cyberabwehrprogramms mit einem allgemeinen Risikowert und Trends sowie übergreifenden Ansichten zu Risiken, Bedrohungen und Schwachstellen kombiniert werden.

Abgedeckte Standards

- ISO27001
- NIST800-53
- NIST 171
- NIST CSF
- CMMC/DFARS
- Datenschutz-Grundverordnung (DSGVO)



Netzwerk-Compliance-Abdeckung

Ob Sie die Einhaltung von Sicherheits-Frameworks wie NIST- und ISO-Standards, Branchenstandards wie das Framework der Motion Picture Association (MPA) nachweisen oder sich ständig verändernde Lieferketten-Audits von mehreren Ökosystem-Partnern bestehen möchten: In ThreatSync+ NDR sind über hundert KI-optimierte Internet-, NIST- und ISO-basierte Netzwerkkontrollen integriert.

KI-basierte Compliance-Kontrollen

ThreatSync+ NDR erstellt zunächst eine Basislinie des normalen Netzwerkverhaltens. Für jeden Moment eines jeden Tages werden mehrere Basislinien für Geräte, Datenverkehrsströme und Anwendungen erstellt. Dazu analysiert ThreatSync KI riesige Mengen an Netzwerkdatenverkehr. ThreatSync+ NDR fügt dann Richtlinien hinzu, darunter über hundert NIST 800-53-Kontrollen, die sofort einsatzbereit sind. KI und Richtlinien werden mit Bedrohungsdaten kombiniert, damit erkannt werden kann, was eine Schwachstelle (z. B. ein Fehler im Patching-System), was ein Risiko (z. B. eine Fehlkonfiguration der Firewall-Regeln) und was eine Bedrohung (z. B. eine Test- oder Aufklärungsaktivität) ist. Ein derartiges Niveau an kontinuierlicher Sichtbarkeit könnte der Mensch niemals erreichen. ThreatSync+ NDR kann Schwachstellen, Risiken und Bedrohungen erkennen, die vor anderen Cybersicherheitstools verborgen bleiben.

Automatisierte kontinuierliche Compliance

Compliance ist kein einmaliges Ereignis, sondern ein fortlaufender Prozess. Um konform zu bleiben, müssen Unternehmen ihre Abläufe, Richtlinien und Praktiken kontinuierlich überwachen. Standards wie NIST 800-53 und ISO 27001 bilden die Grundlage für die meisten IT-Kontrollvorschriften und im Lieferumfang von ThreatSync+ NDR sind über hundert Netzwerkkontrollen enthalten.

ThreatSync-KI-Modelle bewerten kontinuierlich die Wirksamkeit dieser Kontrollen und geben bei Kontrollverletzungen Warnmeldungen aus. Kontrollen können einfach konfiguriert und an bestimmte Vorschriften wie NIST-171 und Cyber Essentials angepasst werden.

Nachweis der Compliance

Sobald eine automatisierte Compliance erreicht wurde, besteht der nächste Schritt darin, diese durch die Berichterstattung über die Wirksamkeit der Kontrollen nachzuweisen. ThreatSync+ NDR und die Compliance-Berichterstattung von WatchGuard automatisieren den Prozess der Compliance-Berichterstattung. Auf der Grundlage von Richtliniensystemen werden automatisch einzelne oder mehrere Compliance-Berichte generiert. Die Berichte veranschaulichen die Wirksamkeit der Kontrollen und bieten Best-Practice-Anleitungen für die Einhaltung der Vorschriften, wenn die Kontrollen versagen. Bislang war dies ein manueller, langsamer und kostspieliger Prozess. ThreatSync+ NDR mit Compliance-Berichterstattung von WatchGuard automatisiert diesen Prozess und spart Ihnen dadurch viel Zeit und Geld.

Die integrierte Richtlinien-Engine und KI von ThreatSync+ NDR analysieren Milliarden von Netzwerkdatenströmen, kombinieren sie zu Millionen von Netzwerkereignissen und reduzieren sie auf Hunderte von anomalen Verhaltensweisen und schließlich auf nur eine Handvoll Warnungen, die sofortiges Handeln erfordern.

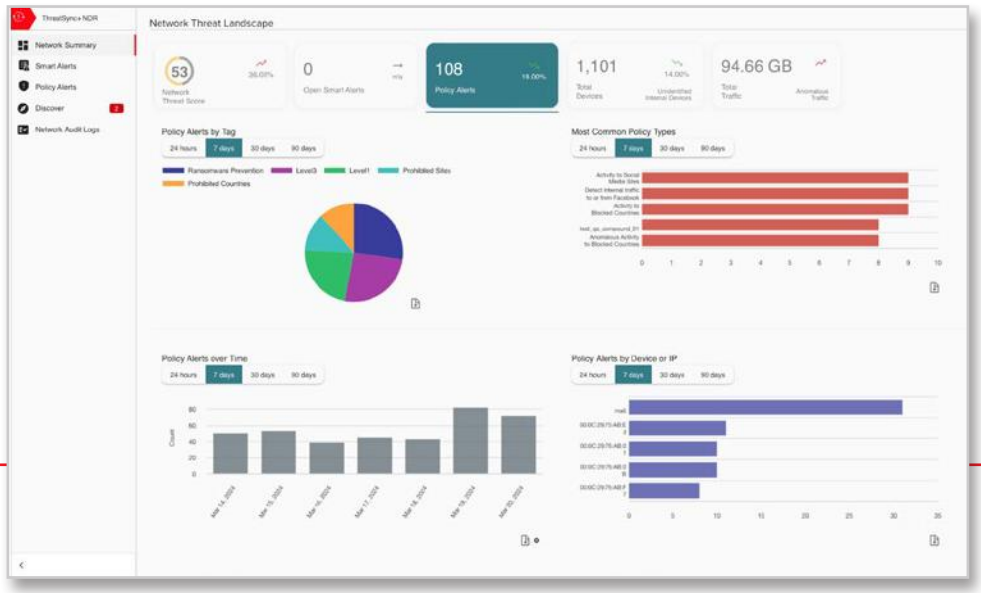


Abbildung 4. ThreatSync+ NDR ist in WatchGuard Cloud verfügbar

Ransomware-Erkennung

Ein Blick in Ihr Netzwerk, wo sich Ransomware nicht verstecken kann

Ransomware stellt eine der wichtigsten Bedrohungen für die Cybersicherheit dar, mit denen Unternehmen heute konfrontiert sind. Die herkömmlichen Bemühungen zur Abwehr von Ransomware-Angriffen, die sich auf die Verhinderung der Kompromittierung von Konten und Endpoints konzentrieren, sind allerdings leider unzureichend. Cyberkriminelle werden immer raffinierter und erfolgreiche Ransomware-Angriffe nehmen trotz dieser Abwehrmaßnahmen weiter zu.

Neue, ausgeklügelte Ransomware-Angriffe verwenden Taktiken und Techniken, um traditionelle Cyber-Abwehrmechanismen wie Firewalls, starke Authentifizierung und EDR/EPP-Tools zu umgehen. Angreifer schaffen es sogar oft, EDR-Agenten und Backup-Systeme abzuschalten.

ThreatSync+ NDR überwacht das System auf Anzeichen eines Ransomware-Angriffs, auch wenn Endpoints gefährdet sind, und sendet Ihnen Echtzeitwarnungen, damit Sie die Ausbreitung des Angriffs verhindern können. Die KI-Engine von ThreatSync verwendet mehrere unüberwachte und halbüberwachte maschinelle Lernmethoden, um normale Aktivitätsbasislinien für alle Geräte und Anwender sowie den gesamten Datenverkehr im Netzwerk zu bestimmen. Diese Modelle sind speziell auf die Erkennung der Indikatoren eines Ransomware-Angriffs ausgelegt und ermöglichen die automatische Überwachung, Alarmierung und Behebung von Angriffen rund um die Uhr.

Bedrohungen durch Ransomware sind Realität

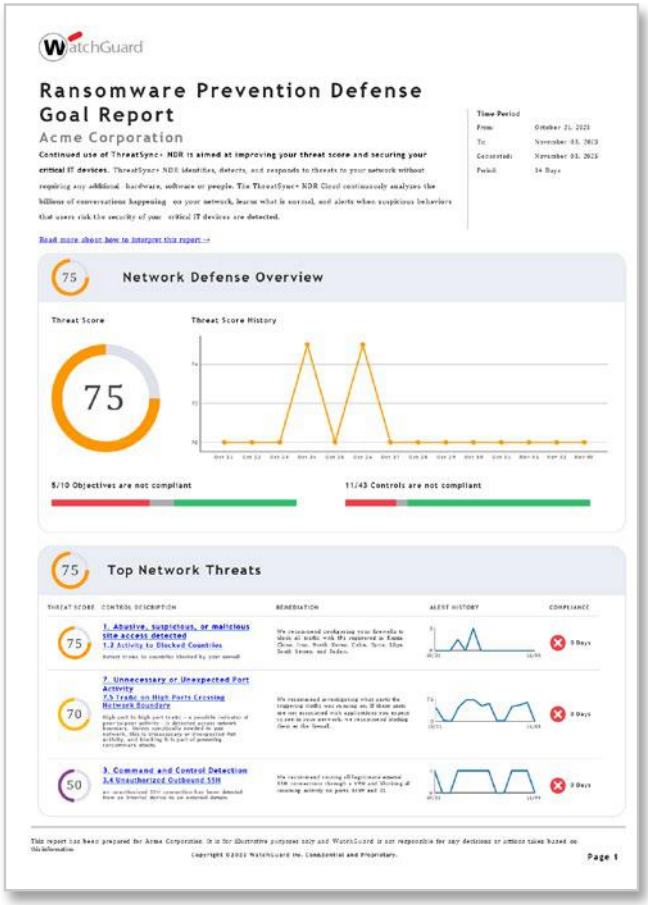
- 41 % der kleinen Unternehmen wurden 2023 Opfer eines Cyberangriffs – ein Anstieg von 38 %[1]
- Der Mensch ist die Ursache für 74 % der Verstöße[2]
- Im Jahr 2023 wurden 538 neue Ransomware-Varianten entdeckt[3]
- Ransomware-Zahlungen erreichen im Jahr 2023 die Marke von 1 Milliarde USD[4]
- Angriffe werden immer ausgefeilter und zielen darauf ab, Backups einzufrieren und die Endpoint-Sicherheit zu umgehen.
    - Mespinoza/Pysa (PowerShell)
    - Sodinokibi (REvil) (Sicherheit abschalten)
    - Bitpaymer/DoppelPaymer (RDP)
    - Ryuk (PowerShell, Registrierungszugriff)

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/

So hilft ThreatSync+ NDR

KI-basierte Ransomware-Erkennung und -Abwehr

Es gibt über 40 maschinelle Lernmodelle, die sich speziell auf die Ransomware-Erkennung konzentrieren und Ransomware-Angriffe erkennen und stoppen können, bevor sie Ihrem Unternehmen schaden. Zu den Erkennungsmodellen gehören die Identifizierung von nicht autorisierten Netzwerkgeräten, Aufklärungsdatenverkehr, Befehl und Steuerung, lateraler Bewegung, abnormalen verschlüsselten RDP- und DNS-Tunneln und abnormalen VPN-Aktivitäten. Abhilfemaßnahmen werden schnell über ThreatSync durchgeführt, einschließlich automatisierter IP-Blockierung und EPDR-Endpoint-Quarantäne.



Kontinuierliches Ransomware-Monitoring

Überwachen und reduzieren Sie kontinuierlich Netzwerkrisiken, die Sie Ransomware-Angriffen aussetzen. Die Richtlinien zur Ransomware-Abwehr von ThreatSync+ NDR, die sich aus den Best Practices der CISA-Ransomware-Abwehr ableiten, überwachen, analysieren und verfeinern ständig Ihre Netzwerkrisiken, einschließlich ungesicherter Ports, Datenverkehr an unbekannten oder riskanten Standorten, ineffektiver Firewall-Regeln, ungepatchter Systeme, fehlgeschlagener Backups und unerwünschten Netzwerkverhaltens, das zu Angriffen führen kann.

Berichterstattung zu Ransomware-Risiken

ThreatSync+ NDR enthält einen automatisch generierten Bericht zur Ransomware-Abwehr, der die wichtigsten CISA-Kontrollen zur Ransomware-Abwehr und deren Wirksamkeit in Ihrer Umgebung darstellt. Zu den Kontrollen gehören gestörte Backup-Systemzeitpläne, unbefugter Fernzugriff, ungewöhnliche Administratoraktivitäten und vieles mehr.

ThreatSync+ NDR enthält richtlinienbasierte Kontrollen und Ziele, die die 40 CISA-definierten Richtlinien zum Schutz vor kritischer Netzwerk-Ransomware abdecken. Diese Richtlinien und deren Wirksamkeit werden im Bericht zum Ziel der Ransomware-Abwehr der Lösung übersichtlich dargestellt.

Schutz der Lieferketten

Seien Sie in der Cyberabwehr-Lieferkette ein starkes und kein schwaches Glied

Die digitale Transformation verbindet Unternehmen miteinander, wodurch Genauigkeit und Umfang von Lieferkettenbewegungen und -transaktionen eine einzigartige Effizienz erreichen und die Grenzen zwischen Unternehmenssystemen und -prozessen endgültig aufgehoben werden. Leider gibt es einen Nachteil: Dieses Netz verbundener Systeme hat Cyberkriminellen die Möglichkeit eröffnet, über die schwächsten Glieder in die digitale Lieferkette einzudringen und über das vernetzte Ökosystem zu ihrem anvisierten Ziel zu navigieren.

Um das Risiko in der Lieferkette von Drittanbietern zu mindern, haben führende Anbieter und Branchenverbände gemeinsame Cybersicherheitsstandards festgelegt, die vor der Unterzeichnung von Verträgen über integrierte Lieferketten erfüllt werden müssen. Diese Standards werden über strenge Audits durchgesetzt und wenn ein Audit nicht bestanden wird, kann dies zur Vertragskündigung führen.

Die Implementierung und Einhaltung dieser Standards stellt für Unternehmen mit beschränkten Ressourcen, die ihre Sicherheitshygiene in hybriden Netzwerken verbessern und gleichzeitig den Betrieb am Laufen und die Personalkosten eindämmen müssen, eine enorme Herausforderung dar. Außerdem müssen sie die kontinuierliche Einhaltung nachweisen, um in das Lieferkettensystem einzutreten oder ein Teil davon zu bleiben.

Große Unternehmen setzen üblicherweise eine Kombination aus SIEM/EDR/NDR-Tools ein. Für die meisten Unternehmen kommt das nicht infrage. Sie benötigen jedoch eine Lösung, die die wichtigen Funktionen dieser Tools bereitstellen kann, darunter:

- Die automatische Erkennung anfälliger Geräte mit der Fähigkeit, Behebungsmaßnahmen zu identifizieren und auf der Grundlage des Risikos zu priorisieren
- Bedrohungsüberwachung und -behebung rund um die Uhr, einschließlich Ereigniskorrelation und Warnmeldungen für Malware, riskante Aktivitäten, IoT-Bedrohungen und risikoreicher Datenverkehr im Netzwerk
- KI-basierte automatisierte Bedrohungssuche, -untersuchung und -reaktion mit der Fähigkeit, IT-Teams zu warnen und eine schnelle Eindämmung zu bieten
- Der effektive Einsatz von KI und Automatisierung zur Überwindung von Personal- und Budgetbeschränkungen bei gleichzeitiger Bereitstellung von IT-Hygienemaßnahmen der Enterprise-Klasse
- Kontinuierlich konforme Prozesse und Kontrollen on demand unter Verwendung von Risiko- und Bedrohungs-Dashboards und Sicherheitsprozess-Scorecards

Cyberangriffe auf die Lieferkette in den USA betrafen 2769 Einrichtungen

58 %

Anstieg gegenüber 2022[5]

97 %

Zero-Day-Schwachstellen wurden 2023 ausgenutzt, alle wurden bei Supply-Chain-Angriffen verwendet[6]

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

Ost-West-Bedrohungserkennung

ThreatSync+ NDR erkennt Schwachstellen und Angriffe in der Lieferkette auf intelligente Weise, indem Netzwerkdaten auf anomale Aktivitäten hin analysiert werden, die Schwachstellen, Risiken und Bedrohungen darstellen. Daten werden von vorhandenen Netzwerkgeräten, Routern, Firewalls, Verzeichnissen und Cloud-Systemen gesammelt, um eine 360-Grad-Betriebsansicht Ihres Netzwerks zu erstellen. IT-Teams erhalten Warnungen mit Risikowerten und Behebungsmaßnahmen zur Priorisierung von Ressourcen, einschließlich Einblicken in neue Geräte im Netzwerk.

Automatisierte Bedrohungssuche

Lieferketten arbeiten rund um die Uhr und ThreatSync+ NDR KI überwacht hybride Netzwerke kontinuierlich auf die IoCs von Lieferkettenangriffen, auch wenn Menschen dies nicht können. Die automatisierte KI-basierte Bedrohungssuche erkennt IoCs in der Lieferkette, weist Sicherheitsteams auf die Bedrohung hin und führt diese durch die erforderlichen Maßnahmen, um den Angriff zu beheben, bevor er sich auf andere Systeme oder über Ökosysteme hinweg auf Partner ausbreitet.

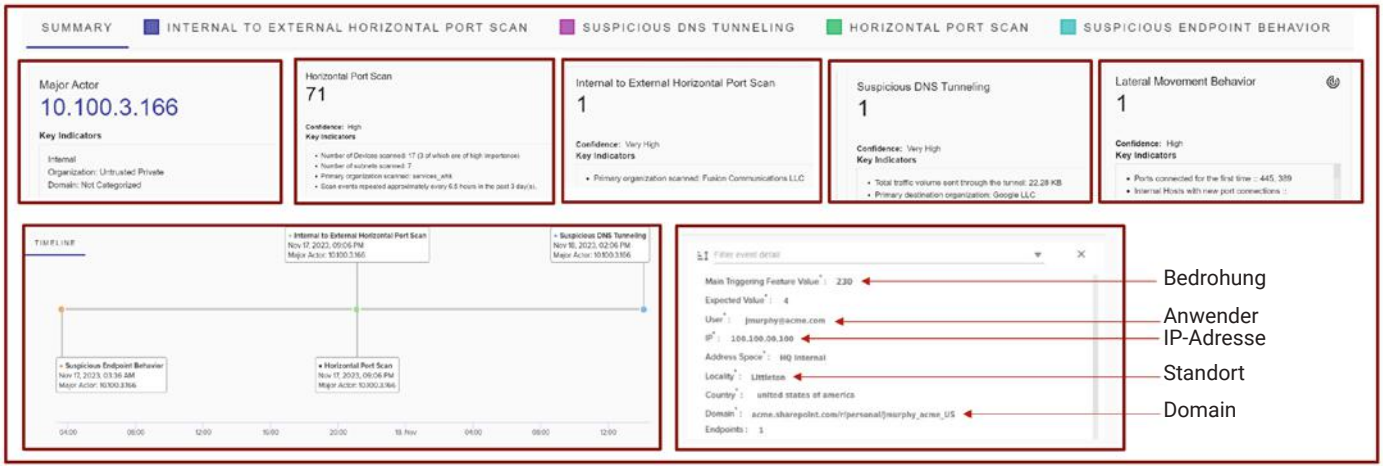
Konfigurierbare Compliance-Berichterstattung

Sie können Cybersicherheitsstandards, die von Ökosystempartnern, Auditoren und Verbänden festgelegt und durchgesetzt werden, implementieren, entsprechende Berichte erhalten und die Compliance aufrechterhalten. ThreatSync+ NDR ermöglicht es Sicherheitsteams, schnell benutzerdefinierte Compliance-Kontrollen zu erstellen und zu implementieren und Berichte zu deren Wirksamkeit zu erstellen. Unternehmen können die Sicherheitshygiene schnell vorantreiben und gleichzeitig die kontinuierliche Compliance nachweisen, um lukrative Lieferkettenverträge zu erhalten und aufrechtzuerhalten.

Vereinfachter Betrieb

ThreatSync+ NDR geht einen intelligenten Weg, um Risiken und Schwachstellen in hochgradig verteilten Netzwerken zu erkennen. ThreatSync+ NDR verwendet Daten als Informationsquelle und unsere fortschrittlichen Modelle für künstliche Intelligenz/maschinelles Lernen (KI/ML) analysieren Netzwerkdaten auf anomale Aktivitäten, die Schwachstellen, Risiken und Bedrohungen darstellen. Daten werden von vorhandenen Netzwerkgeräten, Firewalls und VPN-Systemen gesammelt, um eine 360-Grad-Betriebsansicht Ihres Netzwerks zu erstellen. IT-Teams erhalten Warnungen mit Risikowerten und Behebungsmaßnahmen zur Priorisierung von Ressourcen, einschließlich Einblicken in unbekannte und unerwünschte Geräte im Netzwerk.

Die Untersuchungsansichten von ThreatSync+ NDR ermöglichen es Teams, potenzielle Bedrohungen der Lieferkette schnell zu identifizieren und Vorfälle und ihre Beziehungen, Zeitpläne und beteiligten Ressourcen zu verstehen.



Fazit

In der neuen Realität von Netzwerkumgebungen können Cyberangriffe nun eine Anwendung, einen Dienst oder ein Konto im Netzwerk oder in der Cloud gefährden. Die Kombination von Legacy-Netzwerken mit privaten und öffentlichen Clouds bedeutet, dass IT- und Sicherheitsmanager Folgendes überwachen und verwalten müssen:

- Datenbewegung, insbesondere wenn sensible Daten aus dem Netzwerk zu Partner- und Kundennetzwerken übertragen werden
- Netzwerkaktivitäten, die riskanten und anomalen Datenverkehr über die Netzwerkgrenze hinweg und dann zu Speicherorten oder Geräte für sensible Daten umfassen
- Unerwünschte Geräte, die auf sensible Bereiche des Netzwerks zugreifen können
- Gefährlicher Netzwerkdatenverkehr wie Aufklärung, Befehl und Steuerung, umfangreiche Datenbewegungen zu riskanten Standorten und ungewöhnliche Geräte, die auf sensible Anwendungszonen zugreifen

ThreatSync+ NDR bietet kostengünstige Services für Netzwerkvisualisierung, Abwehr und Compliance über die WatchGuard Cloud. Fortschrittliche KI und Automatisierung können als kontinuierliche 24/7-Monitoring-Lösung betrieben werden, die die Anwender, Geräte und Netzwerkdienste des Unternehmens überwacht und bei Bedarf die sofortige Behebung von Bedrohungen unterstützt. Mit prämierter künstlicher Intelligenz bietet ThreatSync+ NDR eine hocheffektive und erschwingliche Erkennung und Abwehr von Netzwerkbedrohungen in verschiedenen Anwendungsfällen und gewährleistet einen positiven Return on Investment (ROI) und niedrigere Gesamtbetriebskosten (TCO) als bestehende appliancebasierte NDR-Produkte und komplexe SIEM-Tools.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unsere Unified Security Platform® ist speziell auf Managed Service Providers ausgelegt, damit sie erstklassige Sicherheit bieten können, mit der ihre Unternehmen an Größe und Geschwindigkeit gewinnen und gleichzeitig die betriebliche Effizienz verbessern können. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

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

WatchGuard Technologies, Inc.