Betreten Sie die XDR-Welt

Ein Leitfaden für MSPs zur Realisierung moderner Sicherheit

INHALTSVERZEICHNIS

01 XDR ist die Zukunft der Cybersicherheit

02 Die wichtigsten Herausforderungen für die Cybersicherheit von heute

03 XDR: Ein intelligenterer Ansatz für moderne Cybersicherheit

04 MSPs können es sich nicht leisten, XDR zu ignorieren

05 XDR für den MSP: Wesentliche Aspekte

06 XDR mit ThreatSync Core

07 Tiefere Erkennung mit ThreatSync+

08 Funktionsweise: Bereitstellung von XDR-Diensten mit WatchGuard

09 MDR: WatchGuard als Erweiterung Ihres Teams

WatchGuard

01 XDR ist die Zukunft der Cybersicherheit

Cyberbedrohungen sind nicht nur ein Problem für große Unternehmen, sondern richten auch in kleinen Unternehmen großen Schaden an. Die Angreifer werden immer schlauer, schneller und aggressiver.

Access-for-Hire-Programme, Ransomware-as-a-Service und neue KI-Tools haben die Bedrohungslage verschärft.

Das alte Sicherheitskonzept ist nicht mehr ausreichend.

Unternehmen erwarten von ihren Managed Service Providern (MSPs) eine Sicherheit, die sich genauso schnell weiterentwickelt wie die Bedrohungen. Wenn Ihre Cybersicherheitsstrategie nicht auf Anpassungsfähigkeit ausgelegt ist, sind Sie bereits im Rückstand.

02 Die wichtigsten Herausforderungen für die Cybersicherheit von heute

Um diese Herausforderungen zu meistern, benötigen Sie einen integrierten Ansatz, der Kontext- und Telemetriedatenkorrelation über mehrere Sicherheitsschichten und IT-Domänen hinweg bietet.

> Mit stärker integrierten Sicherheitslösungen erhalten Sie einen umfassenden Überblick über Ihren Sicherheitsstatus.

Mit einem integrierten Cybersicherheit-Ansatz, der erweiterte Erkennungs- und Reaktionsfähigkeiten (Extended Detection and Response, XDR) sowie Automatisierung und KI-Technologien umfasst, können Sie die Sicherheitseffizienz gegen komplexe Bedrohungen drastisch verbessern und gleichzeitig die Sicherheitsabläufe vereinfachen.

WatchGuard®

Isolierte Sicherheit

MSPs verwalten die Sicherheit von Netzwerken, Endpoints und Identitäten und arbeiten mit mehreren Tools, um verschiedene Angriffsflächen abzudecken. Aber mehr Tools bedeuten nicht immer mehr Sicherheit. Wenn Lösungen nicht miteinander kommunizieren, bleiben Lücken, die die Angreifer ausnutzen können.

Eingeschränkte Visualisierung

Unverbundene Tools bedeuten, dass Sicherheitsteams nur Fragmente des Gesamtbildes erhalten. Wenn sie Zeit damit verschwenden, Daten aus mehreren Quellen zusammenzusuchen, haben Angreifer bei einem Cyberangriff die Oberhand. Wenn Ihr Team mit sechs verschiedenen Dashboards jongliert, nur um ein Problem zu diagnostizieren, verlieren Sie wertvolle Reaktionszeit.

Zu viele Daten

Jedes Sicherheitstool generiert seine eigenen Protokolle, Warnmeldungen und Telemetriedaten, oft in verschiedenen Formaten. Das Ergebnis? Eine Flut von Daten, die schwer zu analysieren ist. Wichtige Bedrohungen gehen im Rauschen unter, Fehlalarme verschlingen Ressourcen und reale Angriffe bleiben unerkannt. Die Integration von Lösungen mehrerer Anbieter ist komplex, und selbst wenn sie funktioniert, ist die Verwaltung eine Herausforderung.

Mangelnde Sicherheitsautomatisierung

Ohne Automatisierung sind die Sicherheitsteams auf manuelle Prozesse angewiesen, die die Erkennung von Bedrohungen verlangsamen und die Wahrscheinlichkeit von Fehlern erhöhen.

1. **Langsame Erkennung**
   Die manuelle Erkennung verlängert die Reaktionszeiten, sodass Bedrohungen eskalieren können, bevor sie erkannt werden. Ihr Team verschwendet Zeit mit der Verfolgung von Fehlalarmen, während echte Bedrohungen unbemerkt bleiben.

2. **Unklare Reaktionsmaßnahmen**
   Wenn ein Angriff erfolgt, zählt jede Sekunde. Woher wissen Sicherheitsadministratoren, welche Reaktionsmaßnahmen sie zuerst ergreifen sollten? Ohne automatisierte Reaktionsmöglichkeiten müssen Sicherheitsadministratoren die beste Vorgehensweise erraten, was das Risiko längerer Ausfallzeiten und von Datenverlusten erhöht.

Überlastete Sicherheitsteams

Unternehmen sind auf mehr Systeme, Anwendungen und Geräte als je zuvor angewiesen, und jedes einzelne muss ständig überwacht werden. MSPs, die nach neuen Ebenen der Aggregation, Zusammenführung und Analyse von Sicherheitstelemetrie suchen, erhöhen die ohnehin schon hohe Arbeitsbelastung ihrer Teams noch weiter.

Dies wird noch verstärkt durch:

1. **Fachkräftemangel im Bereich Cybersicherheit**
   Es ist schwieriger denn je, qualifizierte Sicherheitsexperten zu finden und zu halten. Die Nachfrage steigt rasant an, aber erfahrene Talente sind knapp. Unterbesetzte Teams müssen mit mehreren Sicherheitstools jonglieren, während sie versuchen, mit einer wachsenden Angriffsfläche Schritt zu halten.

2. **Warnmüdigkeit**
   Sicherheitsteams werden jede Woche mit Tausenden von Warnmeldungen überflutet. Aber nur 19 % sind es wert, untersucht zu werden, und lediglich 4 % werden überprüft. Anstatt Probleme zu lösen, erhöhen viele Sicherheitstools die Arbeitsbelastung und zwingen Teams dazu, Fehlalarme manuell zu durchsuchen, während echte Bedrohungen unentdeckt bleiben.

Sicherheitsteams werden jede Woche mit Tausenden von Warnmeldungen überflutet.

Aber nur **19 %** sind es wert, untersucht zu werden, und lediglich **4 %** werden überprüft.

03 Ein intelligenterer Ansatz für moderne Cybersicherheit

Um den Bedrohungen immer einen Schritt voraus zu sein, benötigen Sie einen integrierten Ansatz, der die Punkte Ihrer gesamten IT-Umgebung miteinander verbindet. Das bedeutet, dass Sie Sicherheitslösungen einsetzen müssen, die zusammenarbeiten und Echtzeit-Transparenz, Kontext und Korrelation über mehrere Ebenen hinweg bieten.

XDR konsolidiert Daten von **Firewalls, Servern, Workstations und Geräten,** um Angriffe schneller zu erkennen und zu stoppen. Mit der KI-gesteuerten Automatisierung wird das Rauschen unterdrückt, werden Fehlalarme reduziert und Sicherheitsteams dabei unterstützt, sich auf echte Bedrohungen zu konzentrieren.

WatchGuard

Bessere Visualisierung & Kontext

Korreliert Daten über mehrere Sicherheitsebenen hinweg, um ein vollständiges Bild zu erhalten.

Niedrigere Kosten & Höhere Effizienz

Beseitigt Redundanzen und verbessert die Sicherheitseffektivität.

Schnellere Threat Detection & Response

KI und Automatisierung identifizieren und bekämpfen Bedrohungen, bevor sie sich ausbreiten.

Vereinfachte Sicherheitsabläufe

Reduziert den Bedarf an manuellen Eingriffen und entlastet so die IT-Teams.

WatchGuard

04 MSPs können es sich nicht leisten, XDR zu ignorieren

Als MSP vertrauen Ihre Kunden darauf, dass Sie sie vor immer ausgefeilteren Angriffen schützen. **Wenn Sie Ihren Kunden eine stärkere, intelligentere Sicherheit bieten möchten, ohne die Komplexität zu erhöhen, ist XDR der richtige Weg.** MSPs können es sich nicht mehr leisten, mit nicht miteinander verbundenen Sicherheitstools zu jonglieren.

XDR bietet MSPs eine skalierbare Möglichkeit, fortschrittliche Cybersicherheit anzubieten, ohne dass ein teures Security Operations Center (SOC) oder kostspieliges SIEM erforderlich ist. XDR bietet einen einheitlichen, KI-gesteuerten Sicherheitsansatz zur Erkennung von und Reaktion auf Bedrohungen für Ihre Kunden über eine einzige Plattform.

Mit XDR können MSPs:

1. **Sicherheitslücken und blinde Flecken beseitigen**
   Wenn Sie sich auf ein Flickwerk unabhängiger Sicherheitswerkzeuge verlassen, führt dies zu fragmentierter Transparenz und verzögerter Reaktion auf Bedrohungen. XDR integriert alle Sicherheitsebenen in ein einziges, intelligentes System, reduziert blinde Flecken und verbessert die Erkennung von Bedrohungen.

2. **Die betriebliche Effizienz steigern und Kosten senken**
   Mit XDR verarbeiten Automatisierung und KI komplexe Bedrohungsanalysen, wodurch der manuelle Arbeitsaufwand reduziert und die Effizienz gesteigert wird. Dass bedeutet, dass Ihr Team weniger Zeit mit der Verwaltung mehrerer nicht miteinander verbundener Sicherheitstools verbringt und mehr Zeit hat, sich auf das Geschäftswachstum zu konzentrieren.

3. **Zufriedeneren Kunden mehr Sicherheit anbieten**
   Durch die Einführung von XDR erhalten Ihre Kunden eine proaktive, KI-gesteuerte Sicherheitslösung, die Echtzeiterkennung und -reaktion bietet. Dies stärkt ihre allgemeine Cybersicherheitslage und macht Sie zu einem unverzichtbaren Sicherheitspartner.

4. **Komplexere Sicherheitsprobleme lösen**
   Bei der Cybersicherheit geht es nicht mehr nur darum, sicher zu bleiben. XDR kann Ihren Kunden helfen, bei der Einhaltung von Vorschriften zu sparen, Branchenkontrollen einzuhalten, eine Cyberversicherung zu beantragen und ihren Lieferkettenpartnern Sicherheit zu demonstrieren.

5. **Einen wachstumsstarken Markt erschließen**
   XDR ist mit einer jährlichen Wachstumsrate von fast 40 % eines der am schnellsten wachsenden Segmente im Bereich der Cybersicherheit. XDR ist eine hervorragende Gelegenheit für MSPs, den Umsatz zu steigern, das Serviceangebot zu verbessern und der Konkurrenz einen Schritt voraus zu sein.

05 XDR für den MSP

Wesentliche Aspekte:

1 Umfassende Abdeckung des Bedrohungspotentials
Das Ziel von XDR ist es, die Erkennung und Reaktion auf Ihre gesamte Bedrohungsoberfläche zu vereinheitlichen, aber viele Anbieter decken nur einen kleinen Teil der erforderlichen Funktionen ab. Darüber hinaus sind viele XDR-Lösungen Erweiterungen von EDR-Tools und decken weder das Netzwerk noch die Cloud ab. Suchen Sie nach einem XDR-Partner, der eine starke Endpointabdeckung mit der Aufnahme von Daten in Ihrer gesamten Umgebung kombiniert, einschließlich lokaler Netzwerke, Rechenzentren, Firewalls, VM/Container, Anwendern und der Cloud.

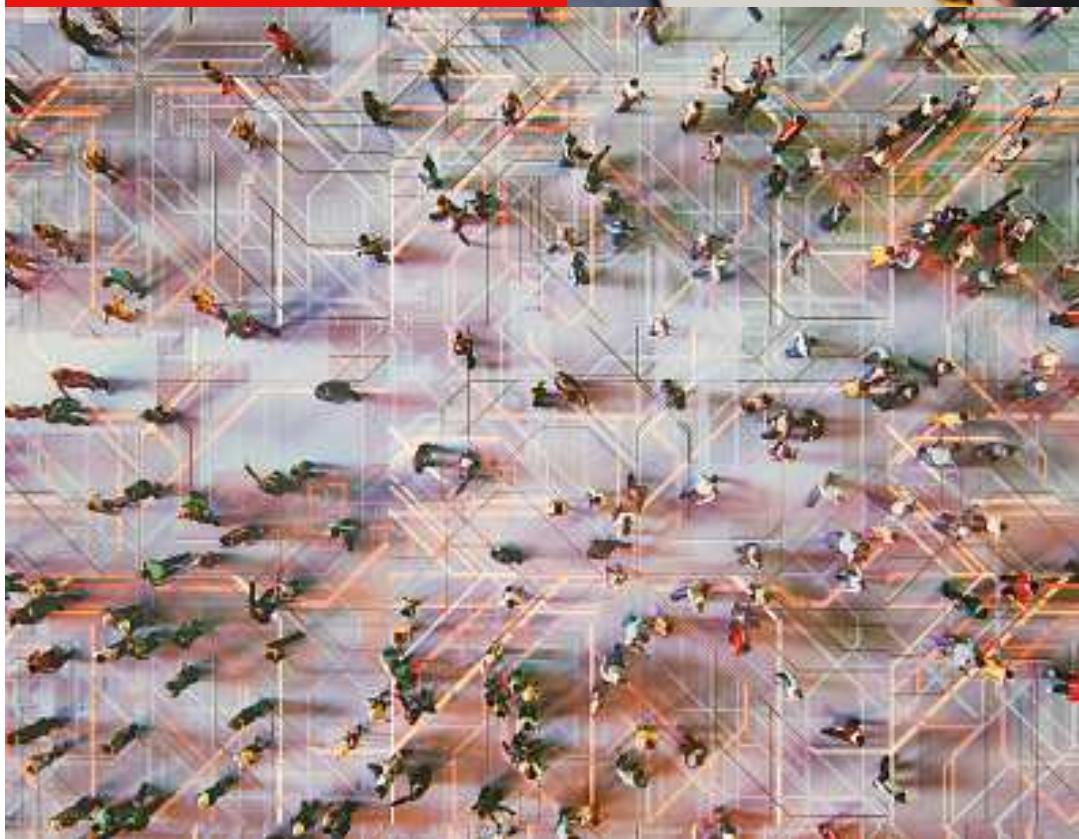
2 Einfache Bereitstellung und Integration
XDR-Lösungen, die schwer zu implementieren, zu integrieren und abzustimmen sind, sind zum Scheitern verurteilt. Anbieter von Sicherheitslösungen belasten ihre Kunden und Partner oft mit komplexen Integrations- und Tuningprozessen, die das XDR-Versprechen zunichte machen. Suchen Sie nach Lösungen, die zu 100 % Cloud-nativ sind, um eine einfache Integration und Bereitstellung zu ermöglichen, und die nur eine minimale Konfiguration erfordern, um erste Erkennungen zu erkennen.

3 Einheitliche KI-Analyse
XDR-Lösungen wenden in der Regel nur die KI-Analyse (überwachtes maschinelles Lernen) am Endpoint an. Alle anderen Bedrohungserkennungen, einschließlich der netzwerkinternen und Cloud-basierten, sind richtlinienbasiert. Suchen Sie nach Lösungen, die Bedrohungsdaten vom Endpunkt, von Netzwerken, Cloud-Plattformen, SaaS-Anwendungen und VPN-Protokollen für eine tiefergehende Analyse durch KI-Tools vereinen.

4 Entwickelt für den MSP
Da sie für große SOCs entwickelt wurden, konzentrieren sich viele XDR-Angebote auf ausgefallene Analyse- und Visualisierungstools und berücksichtigen kleinere Teams kaum. Infolgedessen produzieren sie eine überwältigende Anzahl von Warnmeldungen und Fehlalarmen. Wenn eine XDR-Lösung Ihr Team überfordert, ist sie ineffektiv.

XDR-Lösungen sollten auch nicht die Einstellung neuer Experten oder umfangreiche Umschulungen Ihres Teams erfordern. Suchen Sie nach Anbietern, die die Minimierung von Warnungen priorisieren, und über klare Workflows, Bedrohungsbewertungen und Funktionen zur Automatisierung der Reaktion verfügen, die Ihr Team effektiver machen.

> Suchen Sie nach Anbietern, die die Minimierung von Warnungen priorisieren, und über klare Workflows, Bedrohungsbewertungen und Funktionen zur Automatisierung der Reaktion verfügen, die Ihr Team effektiver machen.



06 XDR mit ThreatSync Core

ThreatSync Core ist eine native XDR-Lösung, die MSPs mit einer zentralen Konsole für Intelligence und Reaktion auf Vorfälle ausstattet.

ThreatSync ist einfach zu verwenden und bereitzustellen. Außerdem ist es leistungsstark. Mit nur wenigen Klicks können Sie die Erkennung über alle WatchGuard-Sicherheitsebenen hinweg vereinheitlichen und so eine schnellere Reaktion auf Bedrohungen über eine einzige Schnittstelle ermöglichen.

Zentralisiert WatchGuard-Warnmeldungen

Vereint Vorfall-Workflows

Ermöglicht automatische und manuelle Reaktions-maßnahmen

WatchGuard

ThreatSync bietet XDR-Funktionen, indem es Indikatoren für Kompromittierungen (IoCs) aus allen WatchGuard-Sicherheitsprodukten korreliert.

Einzelne Sicherheitsereignisse werden zu bewerteten Vorfällen zusammengefasst, die mehr Einblicke und einen domänenübergreifenden Kontext bieten, um die Erkennung von Bedrohungen zu beschleunigen. Es gibt keine komplexe Orchestrierung; die Sicherheitsteams implementieren und verwalten einfache Richtlinien, um die Transparenz und Kontrolle sofort zu verbessern.

Mit ThreatSync können Response-Experten automatisch Maßnahmen ergreifen, mit denen sie Schäden am effektivsten verhindern und die Ausbreitung eines Angriffs begrenzen können. Bedrohungen werden bewertet, damit die Teams das Risikoniveau der Bedrohung verstehen, genau wissen, wo sie ansetzen müssen, und schneller die richtigen Entscheidungen treffen können.

Mit ThreatSync können Response-Experten automatisch Maßnahmen ergreifen, mit denen sie Schäden am effektivsten verhindern und die Ausbreitung eines Angriffs begrenzen können. Bedrohungen werden bewertet, damit die Teams das Risikoniveau der Bedrohung verstehen, genau wissen, wo sie ansetzen müssen, und schneller die richtigen Entscheidungen treffen können.

ThreatSync korreliert die Erkennung und Reaktion über:

1. **WatchGuard Firebox und Unified Security Platform®**
2. **WLAN**
3. **WatchGuard EDR/EPDR**
4. **WatchGuard AuthPoint**

Keine zusätzlichen Kosten für die Freischaltung von XDR

WatchGuard ist der Ansicht, dass die XDR-Funktionen heute für alle Unternehmen einen kritischen Cybersicherheitsschutz darstellen. Aus diesem Grund haben wir ThreatSync, unsere native XDR-Lösung, ohne zusätzliche Kosten in die WatchGuard Unified Security Platform integriert.

07 Tiefere Erkennung mit ThreatSync+

ThreatSync+ ist die fortschrittliche KI-Engine von WatchGuard für XDR. Sie nutzt ein neuronales Netzwerk von über 95 Lernmodellen, die darauf trainiert sind, Anzeichen von Angriffen zu suchen und zu erkennen. ThreatSync + arbeitet sicher aus der Cloud heraus und ist die zentrale Informationsquelle für die Identifizierung laufender Bedrohungen. Sie bietet eine Rund-um-die-Uhr-Überwachung der gesamten Angriffsfläche Ihrer Kunden.

Mit ThreatSync+ können Sicherheitsteams leicht Hinweise auf Bedrohungen aufdecken, während diese sich durch die Cyber-Kill-Chain bewegen, von Netzwerk-Reconnaissance (Externe Erkundung), Befehls-und Steuerungsfunktionen, Berechtigungseskalationen, lateraler Bewegung, Dateninszenierung, Backup-Unterbrechung und Massenverschlüsselung bis hin zur Datenexfiltration.

Funktionsweise:

Intelligentes Baselining
ThreatSync+ durchläuft einen intensiven Lernprozess, der mit der Ermittlung normaler Verhaltensmuster beginnt, die mit Ihrem Netzwerk, Ihren Anwendern, Diensten und den zugehörigen Assets korreliert sind. Dieser Kontext ermöglicht es ThreatSync + auch, bisher unbekannte Assets und Geräte zu identifizieren und zu klassifizieren, sodass Sie deren Rolle verstehen und deren Bedeutung einschätzen können.

Datenbreite
ThreatSync+ nutzt mehrere Datenquellen, um einen Kontext für die Verhaltensweisen in Ihrer Umgebung zu erstellen. ThreatSync+ erfasst Telemetriedaten aus Verkehrsprotokollen, NetFlow, DHCP, VPN, Entr ID/ AD, M365 und Azure Cloud Workloads/Arbeitsbereichen, Anwendungsaktivitäten und WatchGuard Endpoint-Lösungen.

Intelligente Warnmeldungen
Intelligente Warnmeldungen enthalten Diagramme und Karten mit Informationen zum Verhalten nach historischen Aktivitäten und Zeitleiste. Dazu gehört eine Verhaltenskarte, die die Verbindungen zwischen dem wichtigsten Akteur und den verschiedenen Verhaltenstypen zeigt. Sie können auf jeden Verhaltenstyp und jede IP-Adresse verweisen, um Details zum Gerätetyp, zur Organisation oder zum Standort des Verhaltens anzuzeigen.

KI-gestütztes XDR aus der Cloud
ThreatSync+ erweitert die Abdeckung von WatchGuard, um unterschiedliche Umgebungen von Sicherheits- und Netzwerkwerkzeugen von Drittanbietern über ein einziges Analyse-Dashboard zu überlagern und zu verwalten. Mit einer Open XDR-Lösung können MPSs ihr Anbieter-Ökosystem aus Firewalls, Routern und Switches von Drittanbietern nutzen und gleichzeitig die Sicherheitstransparenz und -kontrolle mit ThreatSync + verbessern.

WatchGuard

08 Funktionsweise: Bereitstellung von XDR-Diensten mit WatchGuard

Zentrales Bedrohungs-Dashboard

Das Bedrohungs-Dashboard bietet MSPs eine aggregierte Ansicht der gesamten XDR-Bereitstellung ihrer Kunden, beginnend mit offenen Bedrohungswarnungen, die zu „Vorfällen" korreliert und nach Schweregrad geordnet sind. Auf diese Weise können Teams auf einfache Weise erkennen, wo sie Prioritäten setzen müssen. Bei jedem Vorfall kann das Sicherheitsteam weitere Informationen abrufen und in den meisten Fällen Maßnahmen ergreifen, um die Bedrohung zu stoppen.

Reaktionsmaßnahmen

ThreatSync ermöglicht die automatische Erkennung und Reaktion auf Bedrohungen, die im Netzwerk, auf Endgeräten oder in der Identitätsinfrastruktur erkannt werden.

Zu den Reaktionsmaßnahmen gehören:

- IP-Adresse der Bedrohungsquelle blockieren
- Datei löschen
- Gerät isolieren
- Bösartigen Prozess beenden
- Anwender blockieren

Richtlinienwarnungen und Rahmenzuordnung

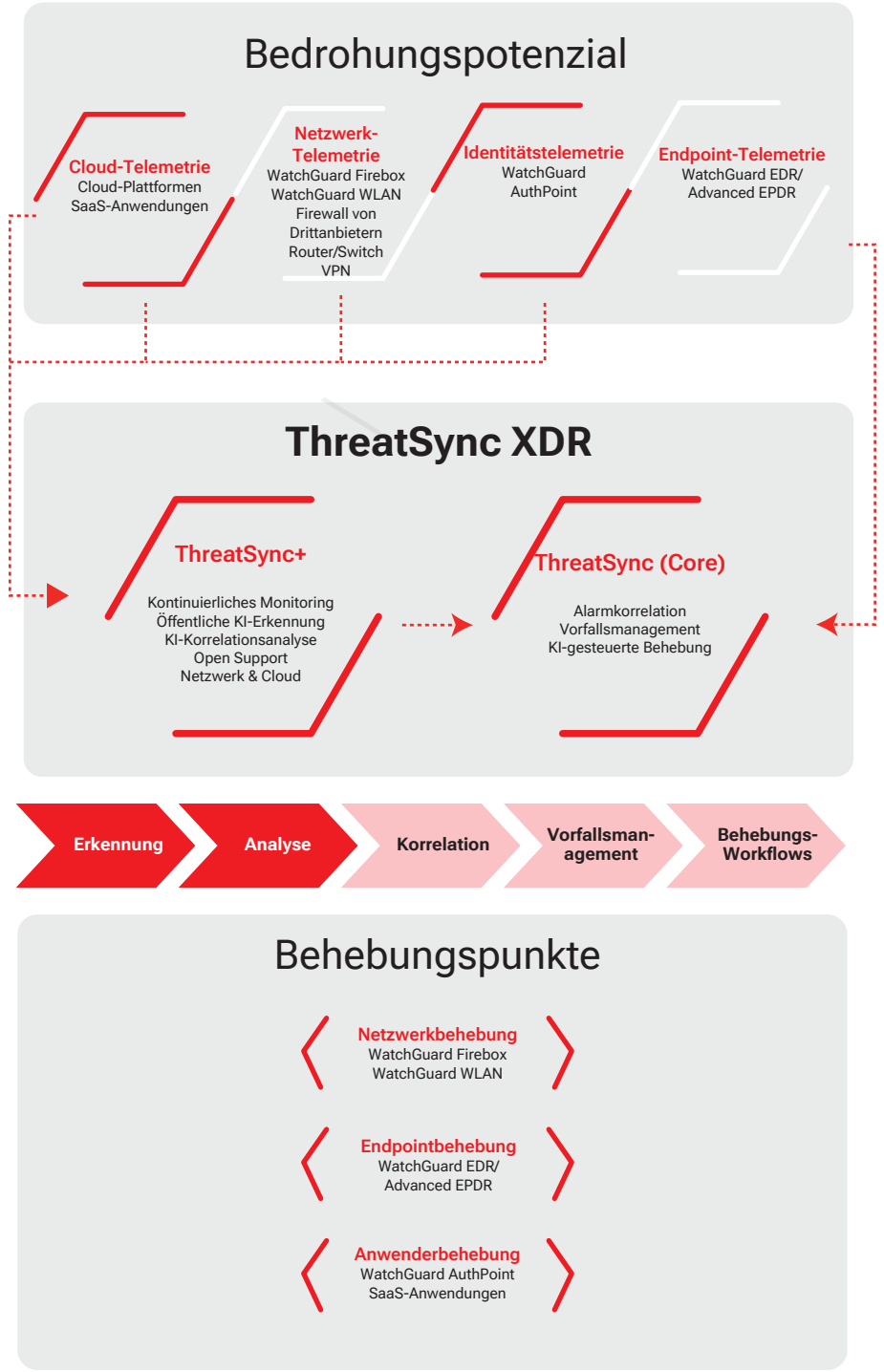
Wenn Sie sich auf ein Flickwerk unabhängiger Sicherheitswerkzeuge verlassen, führt dies zu fragmentierter Transparenz und verzögerter Reaktion auf Bedrohungen. XDR integriert alle Sicherheitsebenen in ein einziges, intelligentes System, reduziert blinde Flecken und verbessert die Erkennung von Bedrohungen.

Kontinuierliche Compliance mit Berichterstattung

Keine manuellen Bewertungen und Erstellungen von Berichte mehr in Excel. ThreatSync kombiniert Hunderte von vorgefertigten Richtlinienkontrollen mit der kontinuierlichen automatisierten Compliance-Reporting-Engine von WatchGuard, um das Compliance-Reporting zu automatisieren.

Kosteneinsparungen

ThreatSync ist zu 100 % cloudbasiert, macht neue Hardware überflüssig und automatisiert manuelle Prozesse wie Bedrohungsüberwachung, Bedrohungssuche und Compliance-Reporting – alles in einer einfach bereitzustellenden, benutzerfreundlichen XDR-Lösung auf Enterprise-Niveau.



09 MDR: WatchGuard als Erweiterung Ihres Teams

Sie sind noch nicht bereit, Ihr XDR-Programm rund um die Uhr zu unterstützen? Arbeiten Sie mit unseren Cyber-Experten zusammen und nutzen Sie unseren erstklassigen Managed Detection and Response (MDR) -Service. Ein qualifiziertes Team von WatchGuard-Cybersicherheitsexperten bietet rund um die Uhr Aktivitätsüberwachung, Bedrohungssuche, Erkennung, Untersuchung und optionale, selektive und maßgeschneiderte Eindämmungsmaßnahmen für jeden Kunden. WatchGuard MDR bietet Ihnen den Schutz, den Sie benötigen, und ermöglicht es Ihnen, Ihr Managed Security Service-Portfolio um ein MDR-Angebot unter Ihrer eigenen Marke zu erweitern.

Funktionsweise:

- Unser Expertenteam von WatchGuard SOC transformiert die Endpoint-Überwachung und die 365-Tage-Telemetrie in verwertbare Sicherheitsanalysen, die durch branchenführendes, verlässliches maschinelles Lernen/KI und minutengenaue Threat Intelligence rund um die Uhr ergänzt werden.
- WatchGuard MDR unterstützt Sie mit automatisch gelieferten regelmäßigen Berichten über die Service-Aktivitäten und den Sicherheitsstatus, die Ihnen helfen, präventive und die Angriffsfläche reduzierende Services anzubieten.
- Im Rahmen des Service-Onboarding bewertet unser Team die Angriffsfläche an den Endpoints und verbessert so unmittelbar ihre Sicherheit und die allgemeine Resilienz gegenüber Cyber-Bedrohungen.
- Im Falle eines Cyberangriffs führt Sie das Team durch den Reaktionsprozess, um Bedrohungen zu stoppen und zu beheben. Für zusätzlichen Komfort und zur Minimierung der Reaktionszeit können Sie die Eindämmung standardmäßig an das SOC delegieren – rund um die Uhr oder außerhalb Ihrer Geschäftszeiten.

WatchGuard®

- Ein qualifiziertes Team von WatchGuard-Cybersicherheitsexperten bietet rund um die Uhr Aktivitätsüberwachung, Bedrohungssuche, Erkennung, Untersuchung und optionale, selektive und maßgeschneiderte Eindämmungsmaßnahmen für jeden Kunden.

WatchGuard-Portfolio

UMGEBUNGSSCHUTZ

Network Security

Die Firewalls und Netzwerksicherheitsdienste von WatchGuard kombinieren essentiellen Schutz mit fortschrittlicher Bedrohungsabwehr, einschließlich leistungsstarker Deep Packet Inspection und integriertem SD-WAN. Unsere sicheren, Cloud-verwalteten WLAN-Lösungen schaffen einen geschützten Luftraum für drahtlose Netzwerke mit umfangreichen Funktionen, die die Konnektivität verbessern, ohne die Sicherheit zu beeinträchtigen.

ANWENDERSCHUTZ

Multifaktor-Authentifizierung

WatchGuard AuthPoint® bietet eine starke, benutzerfreundliche Authentifizierung über eine leistungsstarke Cloud-native Plattform. Mit der mobilen AuthPoint-App können Anwender Anmeldeversuche über einfache Push-Benachrichtigungen genehmigen oder ablehnen, sodass jeder Anmeldeversuch in Echtzeit sichtbar und überprüfbar ist.

GERÄTESCHUTZ

Endpoint-Sicherheit

Mit der umfassenden Endpoint Security Suite von WatchGuard lassen sich Sicherheitsverletzungen, Datenverluste und Cyberangriffe ganz einfach verhindern. Diese schlanken, cloudverwalteten Lösungen integrieren erstklassige Technologie, Bedrohungsinformationen und von Experten gesteuerte Kontrollen, um erweiterte Funktionen für Prävention, Erkennung, Eindämmung und Reaktion bereitzustellen.

SCHÜTZEN SIE DAS GESAMTE UNTERNEHMEN

Managed Detection and Response

WatchGuard MDR erweitert Ihr Team um eine rund um die Uhr von Experten geleitete Überwachung und Reaktion, ohne dass Sie die Kosten für den Aufbau eines internen SOC tragen müssen. Dieser Service wird von vertrauenswürdigen WatchGuard Partnern bereitgestellt und überwacht Endpoints, Netzwerke und Microsoft-Umgebungen, um verdächtige Aktivitäten zu erkennen, Ereignisse zu korrelieren, Bedrohungen zu untersuchen und schnell und effektiv auf komplexe Angriffe zu reagieren.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security und Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von über 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.com.

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

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2025 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox, ThreatSync, Unified Security Platform und AuthPoint sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67661_071625