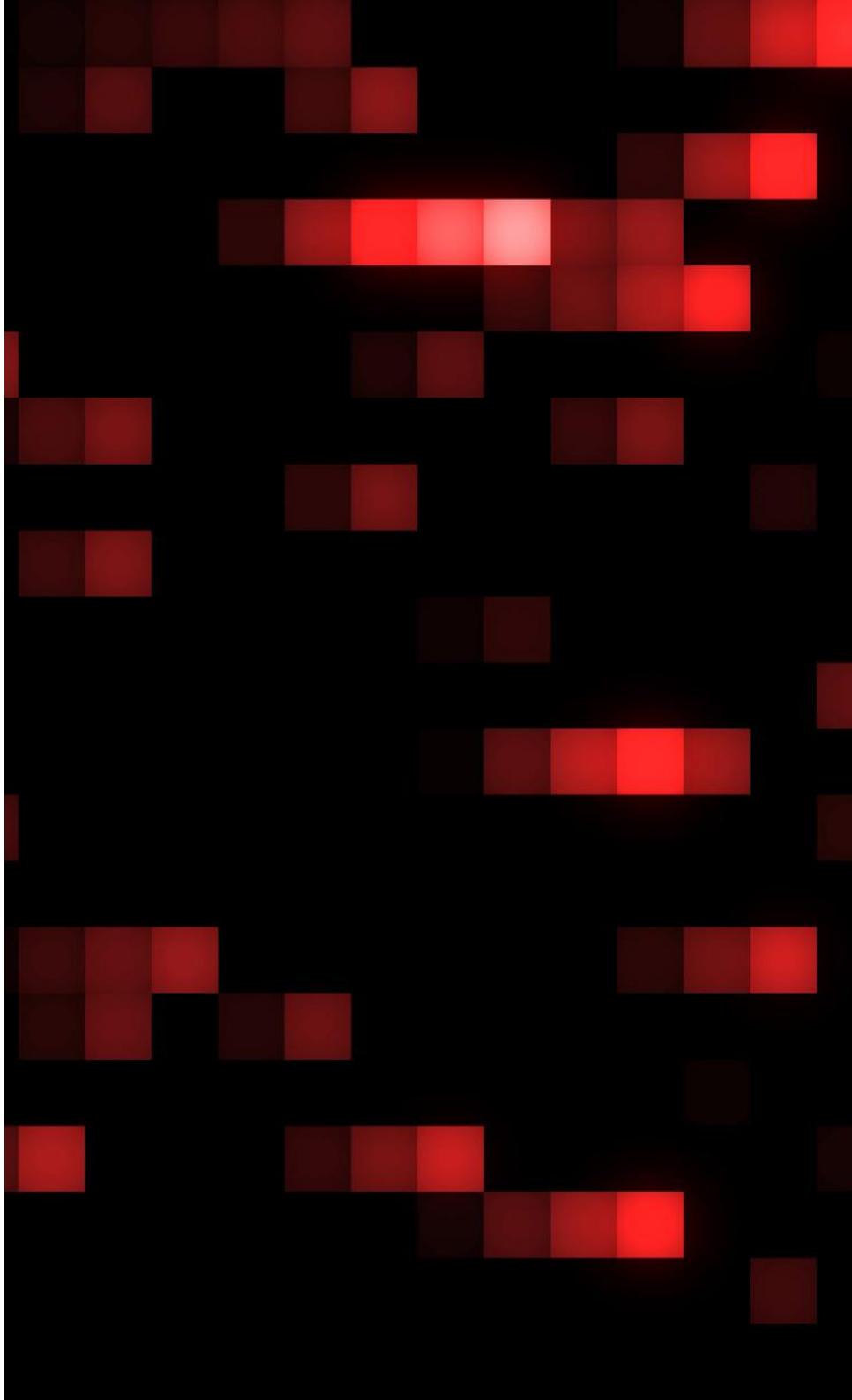
WATCHGUARD THREATSYNC®

Betreten Sie die XDR-Welt

Ein Leitfaden für MSPs zur Realisierung moderner Sicherheit

INHALTSVERZEICHNIS



01 Wichtigste Herausforderungen der heutigen Cybersicherheit

Unternehmen jeder Größe stehen vor der Herausforderung, mit der zunehmend komplexen und tückischen Cybersicherheitslandschaft Schritt zu halten. Bedrohungsakteure haben es nicht nur auf große Unternehmen abgesehen. Sie zielen mit ausgeklügelten Cyberangriffen gezielt auch auf kleine und mittelständische Unternehmen sowie deren Geschäftspartner ab.

Als Unternehmen kann man es sich nicht leisten, die Augen zu verschließen und den Status quo in Sachen Sicherheit beizubehalten. Die Bedrohungsakteure und ihre Vorgehensweisen entwickeln sich rasch weiter. Unternehmen und ihre bevorzugten Managed Service Provider (MSP) müssen entsprechend reagieren, um ihre Umgebungen, Geräte, Benutzer und Daten zu schützen. Daher benötigen Sie Sicherheitslösungen, die sich an Ihre Bedürfnisse anpassen und mit den wachsenden Bedrohungen der heutigen Zeit Schritt halten können.

F12.net

„Bei der Cybersicherheit geht es nicht um das Ziel, sondern um den Weg – was daran liegt, dass die Lage sich kontinuierlich verändert."

Calvin Engen
Chief Technology Officer bei F12.net

Was sind die wichtigsten Herausforderungen der heutigen Cybersicherheit für MSPs?

Isolierte Sicherheit

Anbieter von Sicherheitslösungen müssen eine ständig wachsende Anzahl von Schwachstellen in den Unternehmensnetzwerken, Endgeräten und Identitäten ihrer Kunden managen und schützen. Bei der Vielzahl unterschiedlicher Schwachstellen und der großen Bandbreite an potenziellen Cyberangriffen, die es zu erkennen und abzuwehren gilt, ist es sinnvoll, eine breite Palette an Sicherheitslösungen zu entwickeln. Ein breites Instrumentarium kann jedoch ein zweischneidiges Schwert sein, wenn die einzelnen Lösungen unabhängig voneinander funktionieren. Mehrere Sicherheitslösungen bedeuten nicht mehr Sicherheit [1]

Ein breites Instrumentarium kann ein zweischneidiges Schwert sein, wenn die einzelnen Lösungen unabhängig voneinander funktionieren.

[1] Panaseer 2022 Security Leaders Peer Report

19%

Die Zahl der von Unternehmen eingesetzten Sicherheitslösungen ist in den letzten zwei Jahren um 19 % gestiegen.

36%

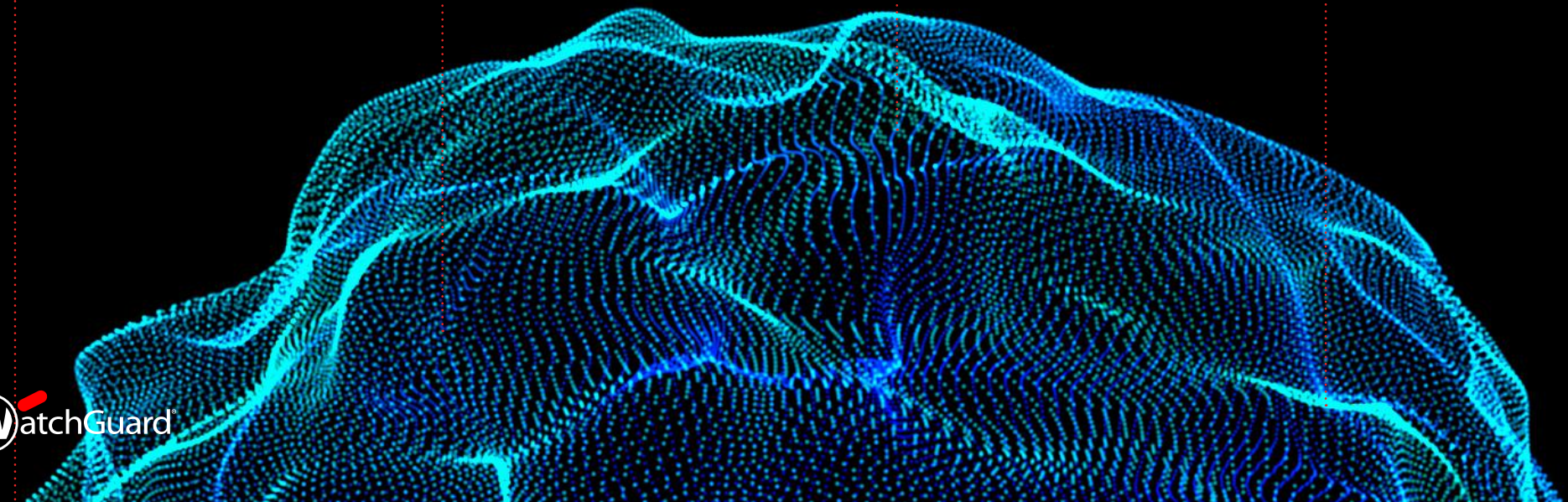
Nur 36 % der Unternehmen erklären, dass sie „sehr zuversichtlich“ in Bezug auf die Funktionsfähigkeit der Sicherheitskontrollen sind.

64 auf 76

Die Zahl der von Großunternehmen verwendeten Sicherheitslösungen ist von durchschnittlich 64 auf 76 Anwendungen gestiegen.

82 %

Außerdem erlebten 82 % der Befragten Sicherheitsvorfälle, die bestehende Lösungen nicht verhindern konnten.



WatchGuard®

Transparenzlücken

Mit all den isolierten Sicherheitslösungen ist es für MSPs auch schwierig, sich einen umfassenden Überblick über die Sicherheitslage eines Kunden zu verschaffen. Jedes Lösung bietet nur einen begrenzten Einblick in den eigenen Spezialbereich. Das Ergebnis ist eine Sammlung von Puzzlestücken, die Sie manuell klassifizieren und zu einem vollständigen Bild zusammensetzen müssen.

Schlimmer noch: Im Falle eines aktiven Cyberangriffs vergeuden Sie beim Zusammenfügen dieser Puzzleteile entscheidende Zeit. Wenn sich Ihre Sicherheitsadministratoren bei mehreren Konsolen anmelden und zwischen einem halben Dutzend verschiedener Tools umschalten müssen, nur um festzustellen, was überhaupt passiert, dann haben Bedrohungsakteure einen erheblichen Vorteil.

> MSPs müssen diese Isoliertheit überwinden, um vergeudete Zeit zu vermeiden und eine Chance zu haben, mit den sich rasant entwickelnden Cyberangriffen Schritt zu halten.

Solange diese Sicherheitslösungen jedoch nicht von ein und demselben Anbieter implementiert werden, bieten auf unterschiedliche Sicherheitsbereiche ausgerichtete Lösungen selten die Interoperabilität, die für einen wirksamen Schutz erforderlich ist.

Probleme mit der Zusammenführung und mit kontextbasierten Daten

Alle Sicherheitslösungen, wie z. B. Netzwerklösungen, Firewalls, Endpoint-Sicherheit oder Identitäts-Tools, stellen Protokolle, Telemetriedaten und Warnmeldungen auf unterschiedliche Weise dar. Sie haben jeweils ein eigenes Format und eine eigene Frequenz.

Gleichzeitig kann es schwierig sein, die riesige Menge an Sicherheitsdaten, die von diesen Lösungen erfasst werden, manuell zu verwalten, zusammenzuführen und zu analysieren. Man kann leicht wichtige Bedrohungsindikatoren übersehen oder sich mit Fehlmeldungen (False Positives) herumschlagen, wenn man in Daten ertrinkt, die von mehreren unterschiedlichen Produkten erzeugt werden. Letztlich führt dies dazu, dass Bedrohungen übersehen werden, die für die Kunden ein Risiko darstellen.

Die Integration mehrerer Sicherheitslösungen von verschiedenen Anbietern kann kompliziert und zeitaufwändig sein und erfordert spezielle Kenntnisse. Das Management dieser Lösungen kann selbst bei erfolgreicher Integration eine Herausforderung darstellen, vor allem wenn es um komplexe und heterogene IT-Umgebungen geht.

Mangelnde Sicherheitsautomatisierung

Als MSP verlassen sich Ihre Kunden darauf, dass Sie ihre wertvollen Daten schützen und für die Unversehrtheit ihres Unternehmens sorgen. Ohne Automatisierung kann die Erkennung von Sicherheitsvorfällen und die Reaktion darauf langsam und ineffektiv sein, was Ihre Kunden dem Risiko kostspieliger Datenschutzverletzungen und Rufschädigungen aussetzt.

1. **Langsame und längere Erkennungszeiten**
   Ohne automatisierte Erkennung müssen sich Ihre Sicherheitsteams auf manuelle Prozesse verlassen, die die mittlere Zeit bis zur Erkennung (MTTD) erheblich beeinträchtigen, Bedrohungen übersehen, False Positives auslösen und die Reaktionszeiten bei Vorfällen verlängern. Diese Verzögerung bei der Erkennung von Sicherheitsbedrohungen kann dazu führen, dass Ihr Team kritische Bedrohungen übersieht und unnötige Untersuchungen unbedeutender Warnungen durchführt, was zu höheren Kosten führt und potenziellen Sicherheitsverletzungen Tür und Tor öffnet.

2. **Unklarheit in Bezug auf Reaktionsmaßnahmen**
   Woher wissen Sicherheitsadministratoren, welche Reaktionsmaßnahmen sie zuerst ergreifen sollten? Wenn ein Unternehmen von einem Sicherheitsvorfall betroffen ist, kann die Schnelligkeit und Genauigkeit der Reaktion den Ausschlag geben, wenn es um die Auswirkungen und das Ausmaß des Angriffs geht. Ohne automatisierte Reaktionsmöglichkeiten ist es jedoch mitunter schwierig zu wissen, welche Reaktionsmaßnahme die Bedrohung beseitigt und die mittlere Zeit bis zur Reaktion (MTTR) verkürzt.

Zeit ist der entscheidende Faktor. Langsame Erkennungszeiten und ungenaue Reaktionsmaßnahmen können dazu führen, dass sich Angriffe auf das gesamte Unternehmen ausbreiten, was oft zu längeren Ausfallzeiten und Datenverlusten führt.

Mit der Sicherheitsautomatisierung können Sie einheitliche und wirksame Sicherheitsdienste für eine Vielzahl von Kunden anbieten und ein einheitliches Sicherheitsniveau für alle Kunden aufrechterhalten.

Komplexe Sicherheit und überlastete IT-Sicherheitsteams

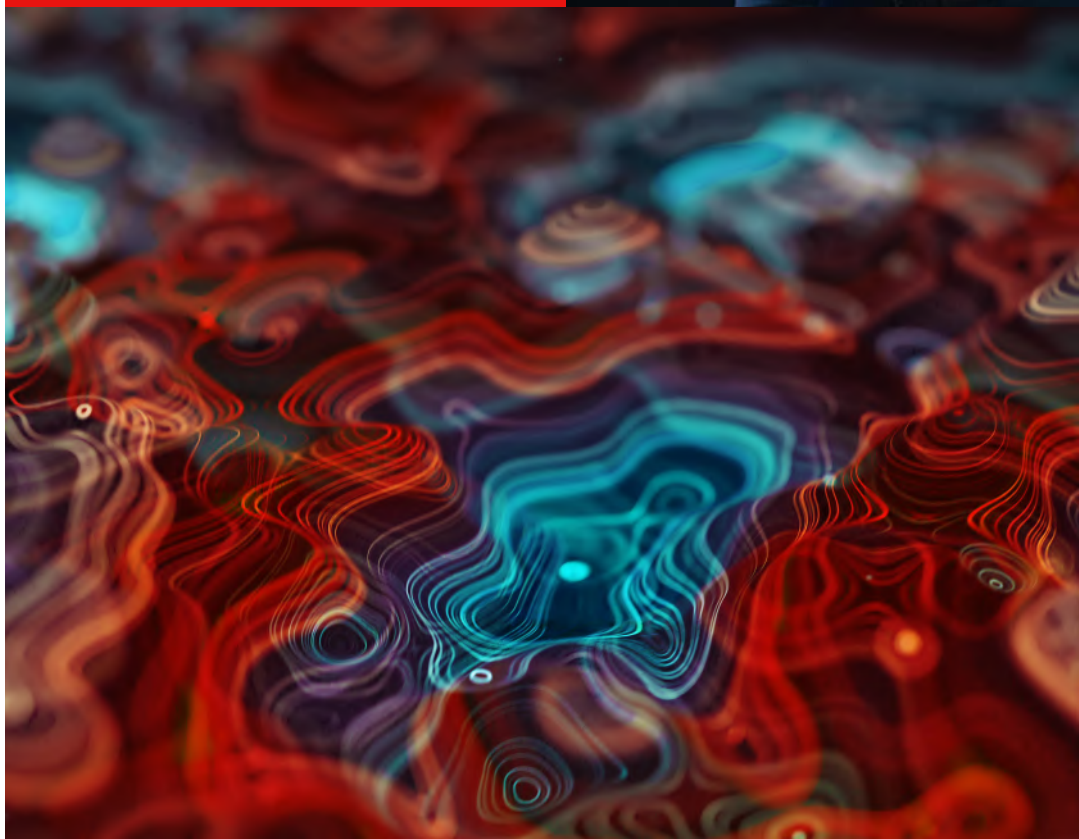
Im Zuge des technologischen Fortschritts werden IT-Umgebungen immer komplexer. Sie umfassen zahlreiche Systeme, Anwendungen und Geräte, die zur Gewährleistung ihrer Sicherheit ständig überwacht und gewartet werden müssen. Darüber hinaus kommen immer neue, ausgefeilte Bedrohungen hinzu, die die MSP-Teams unter enormen Druck setzen.

MSPs, die nach neuen Ebenen der Aggregation, Zusammenführung und Analyse von Sicherheitstelemetrie suchen, erhöhen die ohnehin schon hohe Arbeitsbelastung ihres Sicherheitspersonals. Administratoren müssen mit einer ständigen und wachsenden Flut von Warnmeldungen umgehen und eine zunehmend vielfältige Angriffsfläche schützen, bei der die Erkennung von Bedrohungen immer komplexer geworden ist.

1 **Mangel an qualifizierten Fachkräften für Cybersicherheit**
Die Einstellung und Bindung von qualifiziertem und erfahrenem Personal wird immer schwieriger, da die Nachfrage nach hochqualifizierten Fachkräften in diesem Bereich steigt. Vor diesem Hintergrund ist es für MSPs mit knappem Personal schwierig, ein breites Spektrum an spezialisierten Sicherheitslösungen zu verwalten und gleichzeitig die nötige Zeit für die Erkennung und Eindämmung von Bedrohungen aufzubringen.

2 **Alert Fatigue:**
Durchschnittlich erhalten Unternehmen pro Woche Tausende von Warnmeldungen zu Malware, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % überhaupt geprüft werden. Hinzu kommt, dass einige herkömmliche Sicherheitslösungen eigentlich keine spezifischen Anwendungsfälle lösen, sondern zusätzliche Arbeitsbelastung verursachen, da sie die Verantwortung für die Verwaltung von Warnmeldungen an die Dienstanbieter delegieren und diese dazu zwingen, die Bedrohungen manuell zu klassifizieren.

Die Einstellung und Bindung von qualifiziertem und erfahrenem Personal wird immer schwieriger, da die Nachfrage nach hochqualifizierten Fachkräften in diesem Bereich steigt.



Die Fallstricke von Sicherheitsansätzen mit spezialisierten Sicherheitskonzepten

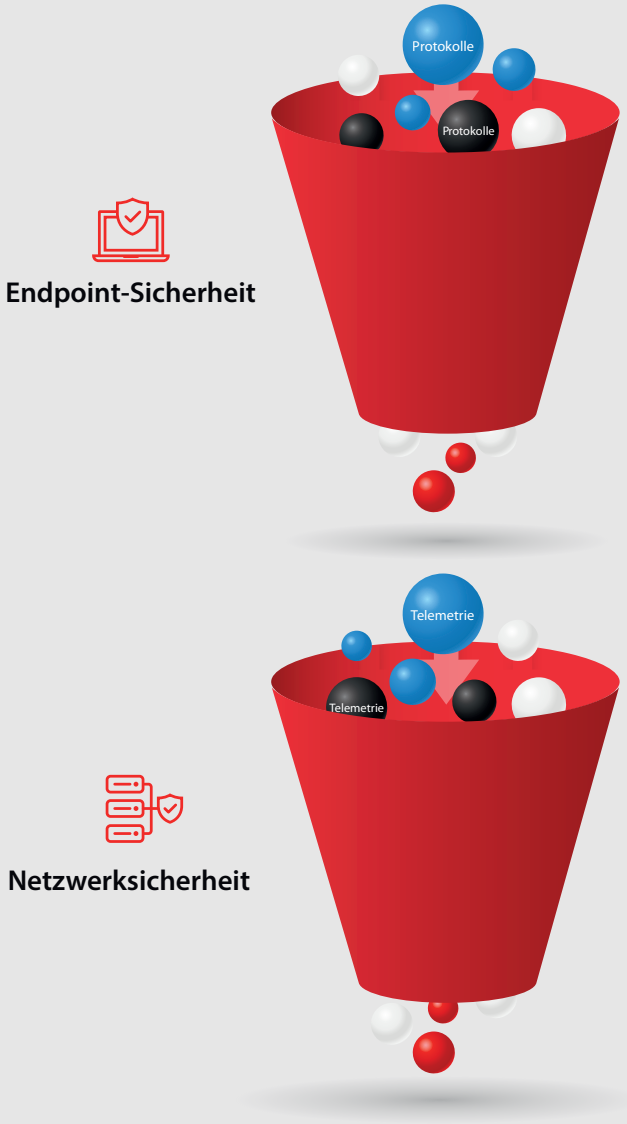
Endpoint Detection and Response (EDR) und Netzwerksicherheitslösungen sind zwei entscheidende Komponenten einer modernen Cybersicherheitsstrategie. Dank dieser Lösungen können Unternehmen komplexe Bedrohungen gegen kritische Bereiche erkennen und entsprechende Reaktionsmaßnahmen ergreifen.

Obwohl die passenden Netzwerksicherheits- und EDR-Lösungen bei der Erkennung von und der Reaktion auf komplexe Bedrohungen äußerst effektiv sind, bieten sie MSPs Einblick in bestimmte Bereiche der IT-Infrastruktur. Netzwerksicherheitslösungen wie Firewalls und Intrusion-Detection-Systeme basieren auf einem netzwerkperimeterzentrierten Modell und bieten einfach nicht genügend Einblick in die Endpoints. Ihr Schwerpunkt liegt dabei auf dem Schutz der Eingangs- und Ausgangspunkte des Netzwerks und der Überwachung des Datenverkehrs am Netzwerkrand. Mit der Verbreitung der hybriden Arbeitsmodelle werden die Netzwerkgrenzen jedoch immer durchlässiger, was die Aufrechterhaltung einer wirksamen Sicherheit erschwert.

Analog dazu sind EDR-Lösungen für MSPs, die Endpoint-Bedrohungen erkennen und verhindern wollen, zu einem unverzichtbaren Hilfsmittel geworden. Sie allein bieten jedoch keinen Einblick in die Bedrohungen, die in den Netzwerkumgebungen der Kunden auftreten.

Aus diesem Grund sehen sich MSPs oft gezwungen, auf einen Flickenteppich von Sicherheitsprodukten zurückzugreifen, um Bedrohungen auf mehreren Sicherheitsebenen erkennen zu können. Fragmentierte Ansätze wie diese, bei denen Sicherheitslösungen unabhängig voneinander funktionieren, schaffen blinde Flecken. Sie schränken die Sichtbarkeit, die kontextbezogenen Ergebnisse und die Effektivität von Erkennung und Reaktion ein und erschweren dadurch die Bereitstellung eines umfassenden End-to-End-Schutzes für Kunden.

Diese Herausforderungen sind wahrscheinlich nur zu gut bekannt. MSPs müssen sich schon viel zu lange mit ihnen auseinandersetzen. Aber tatsächlich ist der Großteil dieser Hindernisse einfach das Nebenprodukt veralteter Sicherheitsansätze. Ihre Überwindung erfordert die Bereitschaft, den eigenen Kurs zu ändern und sich auf eine neue Sicherheitsstrategie einzulassen.



02 XDR: Ihr Tor zur modernen Sicherheit

Um diese Herausforderungen zu meistern, müssen MSPs einen integrierten Ansatz verfolgen, der die Zuordnung von Kontext- und Telemetriedaten über mehrere Ebenen in den komplexen IT-Umgebungen von heute ermöglicht. Sie müssen eng miteinander verzahnte Sicherheitslösungen einsetzen, um einen umfassenden Überblick über den Sicherheitsstatus Ihrer Kunden zu erhalten.

> 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.

Wie funktioniert XDR?

Wir leben in einer Welt, in der Cyberangriffe eher die Regel als die Ausnahme sind – nichts könnte einem Unternehmen mehr Schaden zufügen als ein erfolgreicher Angriff. Vor dem Hintergrund, dass sich Sicherheitsfachkräfte mit persistenten und sich weiterentwickelnden Angriffen auseinandersetzen und gleichzeitig eine Vielzahl von Systemen und Tools verwalten müssen, ist jetzt der richtige Zeitpunkt für eine umfassende Lösung zur Erkennung und Abwehr von Bedrohungen, die MSPs neue Möglichkeiten eröffnet. XDR ist diese Lösung.

XDR bietet MSPs einen umfassenden Sicherheitsansatz, der auf Automatisierung und KI-Technologien setzt, um Bedrohungen über Firewalls, Server, Workstations und Geräte hinweg zu erkennen und entsprechend zu reagieren.

> Mit einer integrierten XDR-Lösung können Sie Ihre Sicherheitsabläufe straffen, die Betriebskosten senken und Ihren Kunden helfen, ein effektiveres und umfassenderes Sicherheitskonzept zu erreichen.

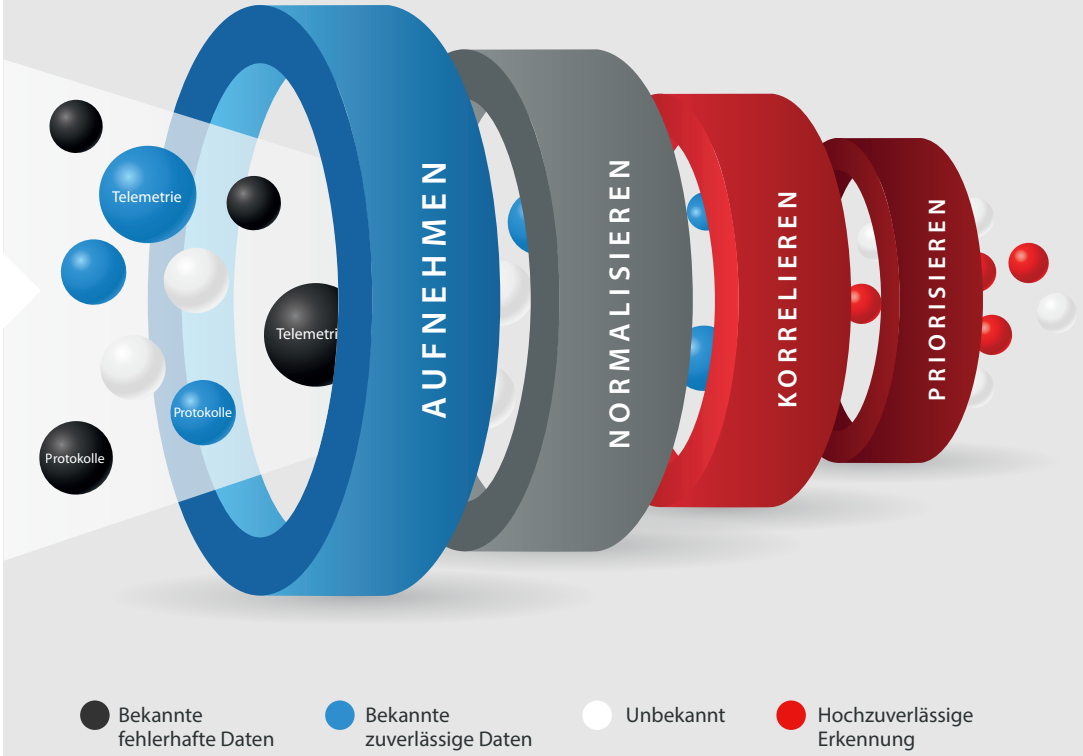
XDR bietet deutliche Vorteile gegenüber unverbundenen Sicherheitstools. Mit XDR verfügen Sie über den Kontext und die Übersicht, die Sie zur schnelleren und effizienteren Erkennung und Bekämpfung von Cyberangriffen benötigen. Wenn Sie Ihre Kunden mit einem vereinfachten und effizienteren Ansatz unterstützen wollen, ist die Einführung einer XDR-Lösung die richtige Wahl.

Endpoint-Sicherheit

XDR

Netzwerksicherheit

WATCHGUARD THREATSYNC®



XDR auf der Ebene des Sicherheitsmanagements

Bewertung und Priorisierung von Bedrohungen

XDR korreliert und kombiniert Aktivitätsdaten auf verschiedenen Sicherheitsebenen und liefert eine priorisierte Ansicht der wichtigsten Bedrohungen

Vereinfachte, konsolidierte Sicherheit

Integrierte Sicherheitsinformationen (Threat Intelligence) aus Umgebungen, Benutzern und Geräten machen den Einsatz mehrerer Einzellösungen überflüssig und optimieren die Sicherheitsabläufe.

Geschwindigkeit und Sicherheit

XDR bietet erweiterte Funktionen, die eine frühere Erkennung, schnellere Reaktionen, höhere Zuverlässigkeit und bessere Sicherheit ermöglichen.

Kontextbezogene Threat Intelligence

Viele Einzelereignisse können in ihrer Gesamtheit Indikatoren für einen Vorfall sein. XDR ermöglicht aufschlussreichere Daten sowie eine bereichsübergreifende Kontextualisierung zur schnelleren Erkennung von Bedrohungen.

03 Betreten Sie die XDR-Welt und profitieren Sie von umfassender Sicherheit

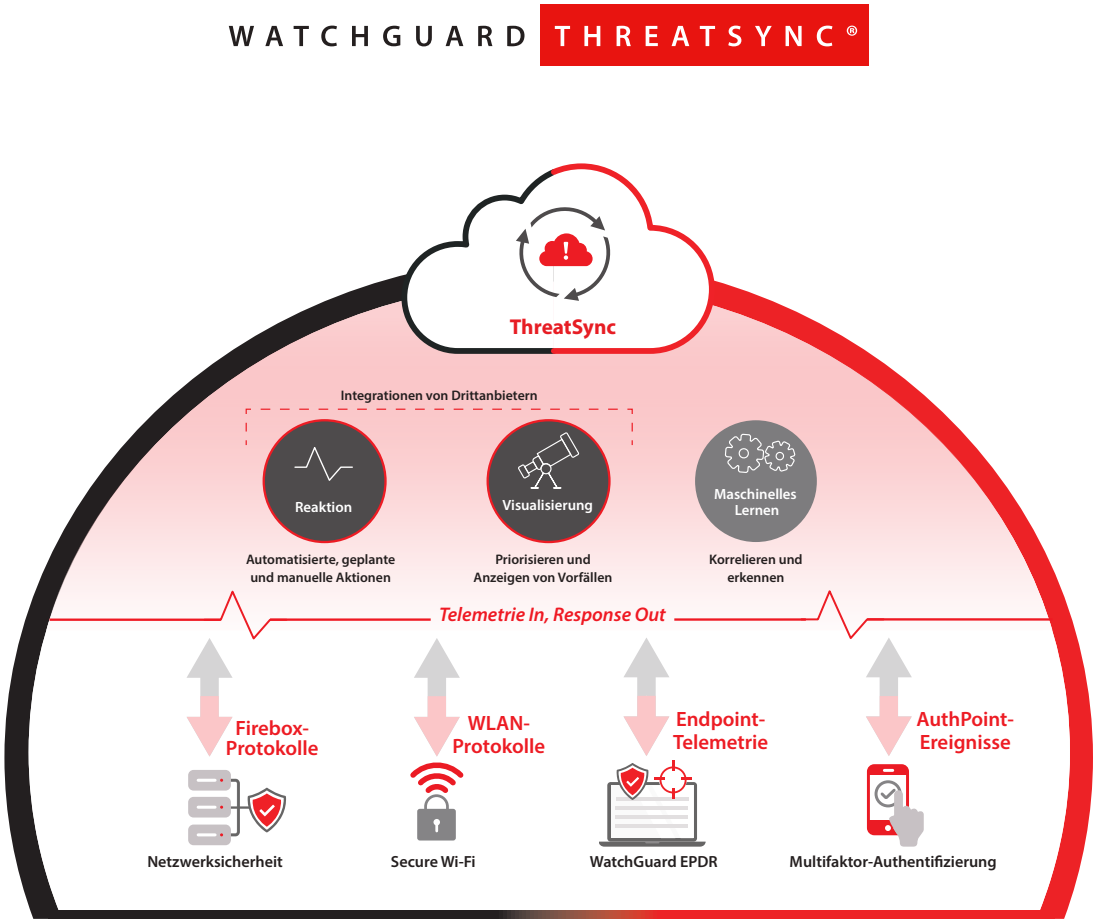
ThreatSync ist eine umfassende und einfach zu bedienende XDR-Lösung, die als Teil der Unified Security Platform®-Architektur von WatchGuard enthalten ist und produktübergreifende Erkennungen vereinheitlicht und die Reaktion auf Bedrohungen über eine einzige Schnittstelle beschleunigt.

„eXtend, Detect and Respond“ mit ThreatSync

1 **eXtend**
Erstellen Sie Ihre XDR-Strategie mit gezielten Integrationen und domänenübergreifender Datentelemetrie aus den neuesten Technologien von WatchGuard. Indem Sie mehr verschiedene Daten aus Ihrem wachsenden Sicherheitspaket einspeisen, erreichen Sie eine höhere Visualisierung sowie stärkeren Schutz.

2 **Detect**
Verabschieden Sie sich von einem isolierten Sicherheitsansatz und wenden Sie eine intelligenten Gefahrenerkennung aus unterschiedlichen Quellen an. ThreatSync nutzt KI und maschinelles Lernen, um bereichsübergreifend potenzielle Bedrohungen in Echtzeit zu erkennen, die Erkennungszeiten zu verkürzen und den Schweregrad und den Umfang der Bedrohungen schnell einzudämmen.

3 **Respond**
Implementieren Sie XDR und reagieren Sie blitzschnell auf Bedrohungen. Mit ThreatSync können automatisierte Reaktionsmaßnahmen koordiniert werden, um Bedrohungen im gesamten Unternehmen von einer einzigen Stelle aus in einem einfacheren und schnelleren Prozess zu neutralisieren, wodurch das Risiko verringert und die Genauigkeit erhöht wird.



* Secure Wi-Fi und AuthPoint werden in Kürze verfügbar sein und in ThreatSync integriert werden.

Leistungsstarke XDR leicht gemacht

Plattformübergreifende Erkennung von Bedrohungen

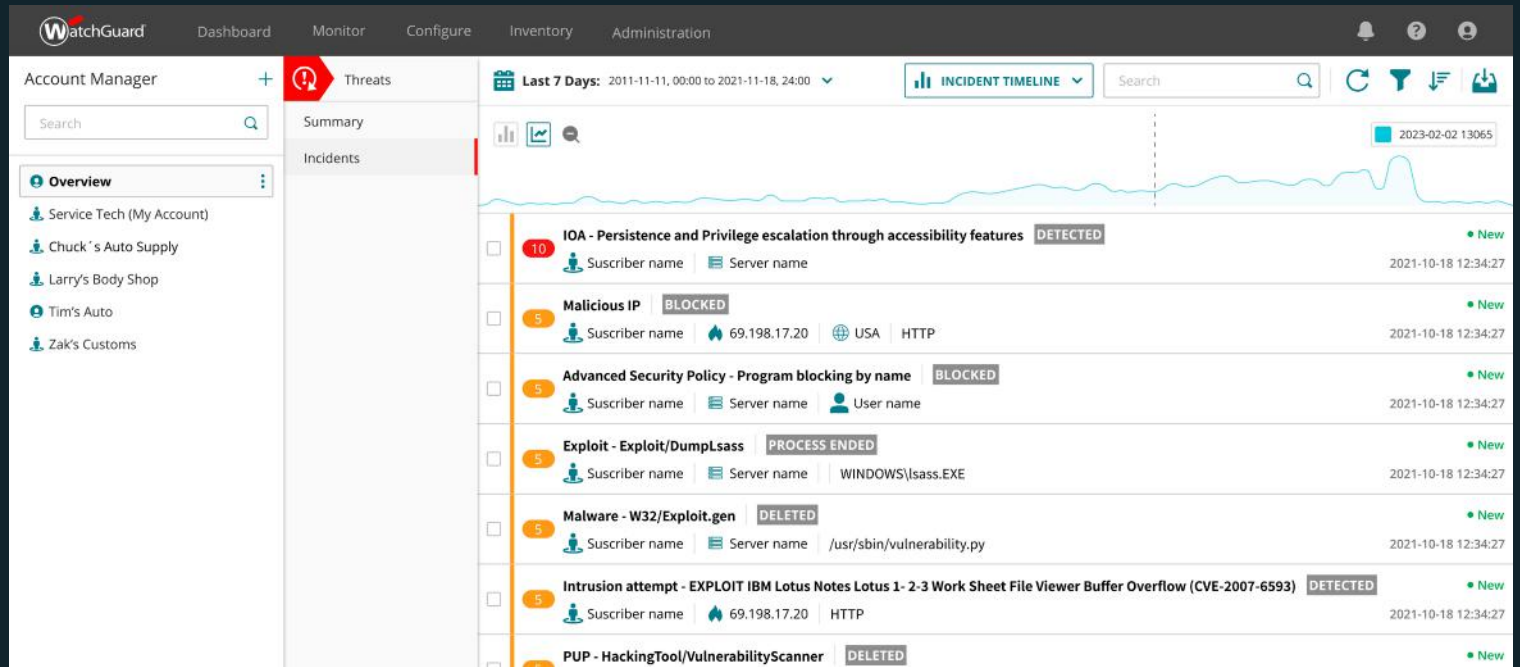
ThreatSync bietet erweiterte Erkennungsfunktionen, indem sie Gefährdungsindikatoren (IoCs) aus allen WatchGuard-Sicherheitsprodukten nutzt und entsprechend korreliert. Durch die bereichsübergreifende Korrelation und den Kontext ist die Lösung in der Lage, potenziell bösartige Aktivitäten in Bezug auf bestimmte Umgebungen, Benutzer und Geräte zu erkennen und zu bewerten, um die MTTD zu reduzieren, die Genauigkeit zu verbessern und letztendlich eine schnellere Abhilfe zu ermöglichen.

Einheitliche Sicherheitsorchestrierung und Reaktion auf Bedrohungen

Wenn Sicherheits- und IT-Administratoren einen ganzheitlichen Überblick über ihre Bedrohungslandschaft haben, können sie Bedrohungen schnell und zuverlässig nach ihrem Schweregrad einstufen und entsprechend reagieren. ThreatSync ermöglicht es Ihnen, mit intelligenter Alarmbewertung, automatisierten Abhilfemaßnahmen und Optionen für manuelle Eingriffe effizienter zu arbeiten. Dieser Grad der Orchestrierung von Bedrohungsreaktionen erweitert sowohl den Umfang als auch die Genauigkeit für Sicherheitsteams.

Einfache Bereitstellung und Verwaltung

WatchGuard ThreatSync macht die Einführung eines XDR-Ansatzes mit seinen intuitiven cloudbasierten Verwaltungs- und Automatisierungsfunktionen für einen Markt einfach, bei dem Zeit und Leistung eine wichtige Rolle spielen. Als robuste XDR-Ebene im Rahmen der Unified Security Platform-Architektur von WatchGuard integriert ThreatSync produktübergreifende Intelligenz, um die Kosten und den Verwaltungsaufwand beim Einsatz von mehreren Punktlösungen zur Erkennung und Reaktion auf Bedrohungen zu reduzieren.



Mehr Transparenz bei Netzwerk- und Endpunktaktivitäten, um Bedrohungen zu erkennen, die andernfalls unentdeckt bleiben könnten

Umfassende Sicherheit durch die Zusammenführung von Daten und Warnmeldungen auf einer einzigen Plattform, auf der Lösungen zusammenarbeiten können, um Bedrohungen zu priorisieren und darauf zu reagieren

Verringerte Belastung des Sicherheitsteams durch Automatisierung des Prozesses zur Erkennung von und Reaktion auf Bedrohungen und Freisetzung von Zeit und Ressourcen für wichtige Aufgaben

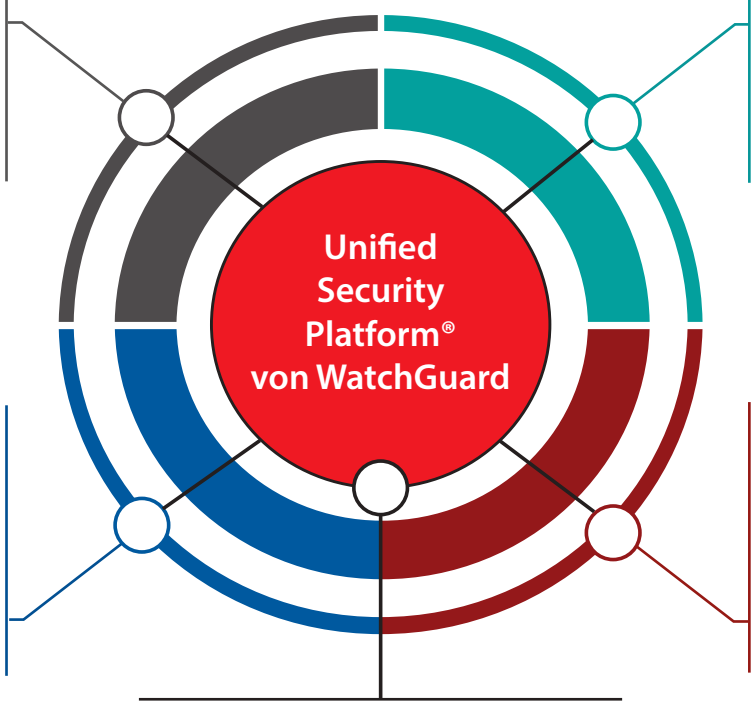
Optimierung des Reaktionsprozesses durch die Bereitstellung koordinierter und automatisierter Reaktionen auf erkannte Bedrohungen

Keine zusätzlichen Kosten XDR ist ein zentrales Element der modernen Cybersicherheit, das jedem Unternehmen zugänglich sein sollte. Deshalb ist ThreatSync bei WatchGuard ohne zusätzliche Kosten verfügbar

04 ThreatSync und die Unified Security Platform von WatchGuard

ThreatSync ist ein wichtiger Bestandteil der Unified Security Platform-Architektur von WatchGuard, einer einzigen Plattform zur Vereinfachung und Stärkung aller Aspekte der Sicherheitsnutzung, -bereitstellung und -verwaltung.

Unser einheitlicher Sicherheitsansatz bietet umfassende Sicherheit, Transparenz und Kontrolle, kollektive Intelligenz, betriebliche Ausrichtung und Automatisierung – alles, was Sie für das Wachstum und die Skalierung Ihrer Sicherheitsstrategie benötigen.



UMFASSENDE SICHERHEIT

Ein umfassendes Portfolio aus Produkten und Services für **Endpoint-Sicherheit, Multifaktor-Authentifizierung und Netzwerksicherheit** zum Schutz von Umgebungen, Anwendern und Geräten.

TRANSPARENZ UND KONTROLLE

Zentralisierte Sicherheitsverwaltung, Transparenz und erweitertes Reporting über die **WatchGuard Cloud.**

BETRIEBLICHE AUSRICHTUNG

Vereinfachte Geschäftsabläufe mit direktem API-Zugang, einer umfangreichen Auswahl an sofort einsatzbereiten **Integrationen** und Unterstützung für alle Zahlungs- und Verbrauchsmodelle über **FlexPay.**

KOLLEKTIVE INTELLIGENZ

Eine umfassend integrierte Plattform zur Einführung eines Zero-Trust-Sicherheitskonzepts über das **Identity Framework** von WatchGuard und zur Bereitstellung eines echten XDR-basierten Ansatzes für Bedrohungserkennung und -beseitigung über **ThreatSync®**.

AUTOMATISIERUNG

Automation Core® von WatchGuard ermöglicht die Vereinfachung und Skalierung sämtlicher Aspekte der Nutzung, Bereitstellung und Verwaltung von Sicherheitsdiensten.

Eine speziell entwickelte Plattform für MSPs

MSPs müssen sicherstellen, dass die Lösungen ihres Sicherheitsanbieters innovativ sind, umfassend integriert werden und die Anforderungen ihrer Kunden erfüllen können, insbesondere wenn diese über weltweit verteilte Netzwerke und hybride oder Remote-Arbeitsplätze verfügen. Darüber hinaus sollte der Anbieter über starke Supportkapazitäten verfügen, damit MSPs alle Probleme, die während der Servicebereitstellung auftreten, schnell beheben können.

WatchGuard stellt mit Threatsync nicht nur XDR zur Verfügung, sondern auch ein breites Spektrum an Sicherheitsservices und MSP-Funktionen, die dazu beitragen können, Sicherheitsstrategien zu optimieren und zu stärken, die Verwaltungskosten zu senken und das Umsatzwachstum zu steigern.

Skalierbarkeit

WatchGuard bietet ein skalierbares Framework zur Unterstützung von Kundenwachstum und Portfolioübernahme.

Benutzerfreundlichkeit

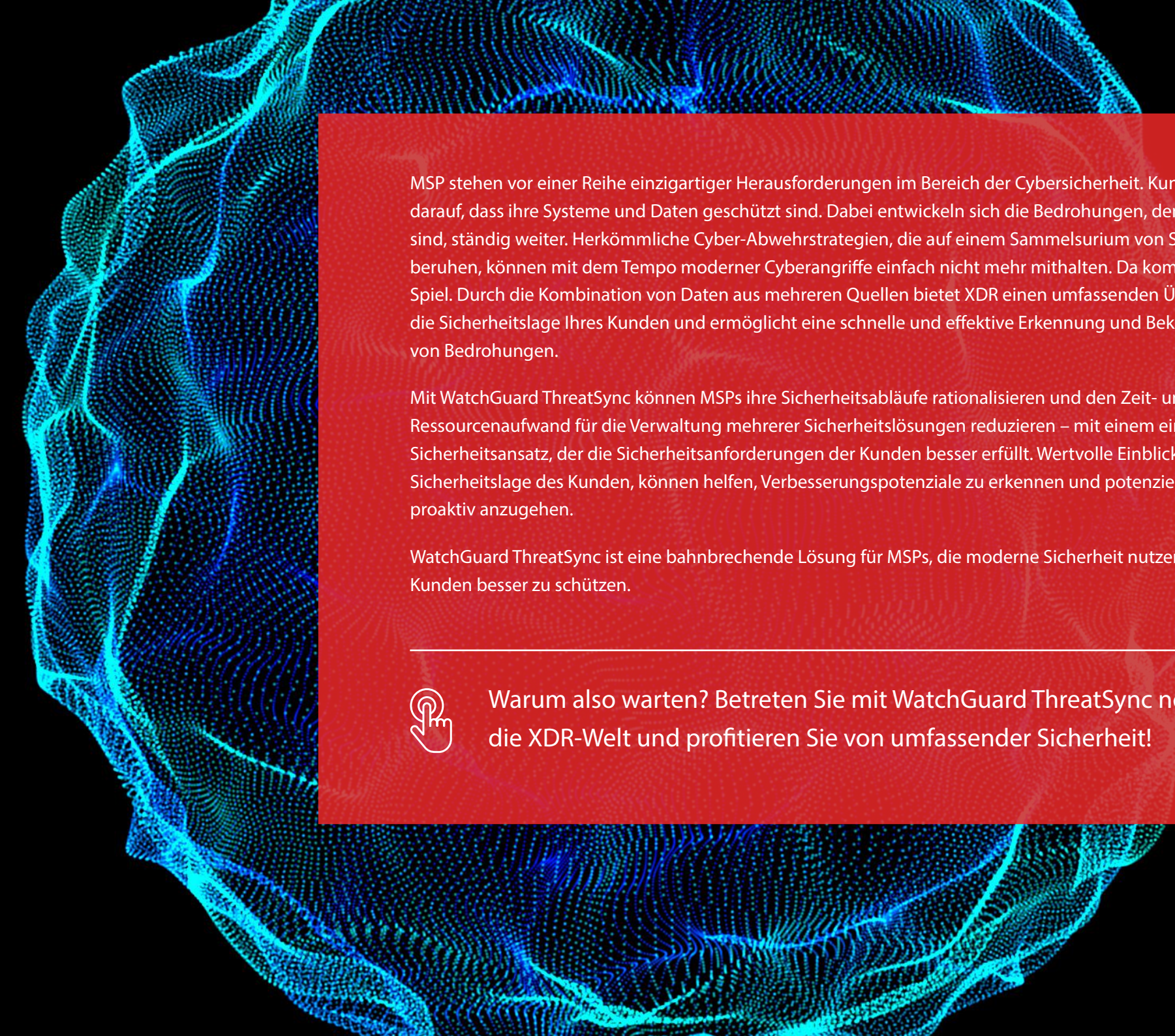
Mit einer benutzerfreundlichen Oberfläche und übersichtlichen Dashboards lässt sich die WatchGuard Cloud leicht bedienen und verwalten. ThreatSync bietet die Möglichkeit, Bedrohungen schnell zu erkennen und entsprechend zu reagieren.

Integration

WatchGuard bietet eine enge Integration im gesamten Sicherheitskonzept. WatchGuard Cloud lässt sich leicht implementieren und unterbricht keine bestehenden Workflows.

Support

WatchGuard bietet MSPs ausgezeichneten Support und Kundenservice mit zeitnahen Antworten auf Anfragen sowie kontinuierlichen Schulungen zu den neuesten Sicherheitstrends und Best Practices.



MSP stehen vor einer Reihe einzigartiger Herausforderungen im Bereich der Cybersicherheit. Kunden verlassen sich darauf, dass ihre Systeme und Daten geschützt sind. Dabei entwickeln sich die Bedrohungen, denen sie ausgesetzt sind, ständig weiter. Herkömmliche Cyber-Abwehrstrategien, die auf einem Sammelsurium von Sicherheitslösungen beruhen, können mit dem Tempo moderner Cyberangriffe einfach nicht mehr mithalten. Da kommt XDR ins Spiel. Durch die Kombination von Daten aus mehreren Quellen bietet XDR einen umfassenden Überblick über die Sicherheitslage Ihres Kunden und ermöglicht eine schnelle und effektive Erkennung und Bekämpfung von Bedrohungen.

Mit WatchGuard ThreatSync können MSPs ihre Sicherheitsabläufe rationalisieren und den Zeit- und Ressourcenaufwand für die Verwaltung mehrerer Sicherheitslösungen reduzieren – mit einem einheitlichen Sicherheitsansatz, der die Sicherheitsanforderungen der Kunden besser erfüllt. Wertvolle Einblicke in die Sicherheitslage des Kunden, können helfen, Verbesserungspotenziale zu erkennen und potenzielle Schwachstellen proaktiv anzugehen.

WatchGuard ThreatSync ist eine bahnbrechende Lösung für MSPs, die moderne Sicherheit nutzen wollen, um ihre Kunden besser zu schützen.

Warum also warten? Betreten Sie mit WatchGuard ThreatSync noch heute die XDR-Welt und profitieren Sie von umfassender Sicherheit!

WatchGuard-Portfolio

Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Secure Wi-Fi

Die sicheren WLAN-Lösungen von WatchGuard sind eine richtungsweisende Neuerung für den Markt von heute: Sie schaffen eine sichere, geschützte WLAN-Umgebung, eliminieren den Verwaltungsaufwand und ermöglichen beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach geschlossen werden. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones" als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein cloudnatives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Die auf künstlicher Intelligenz basierende Flagship-Lösung WatchGuard EPDR verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres 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 and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung und 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.com/de.

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