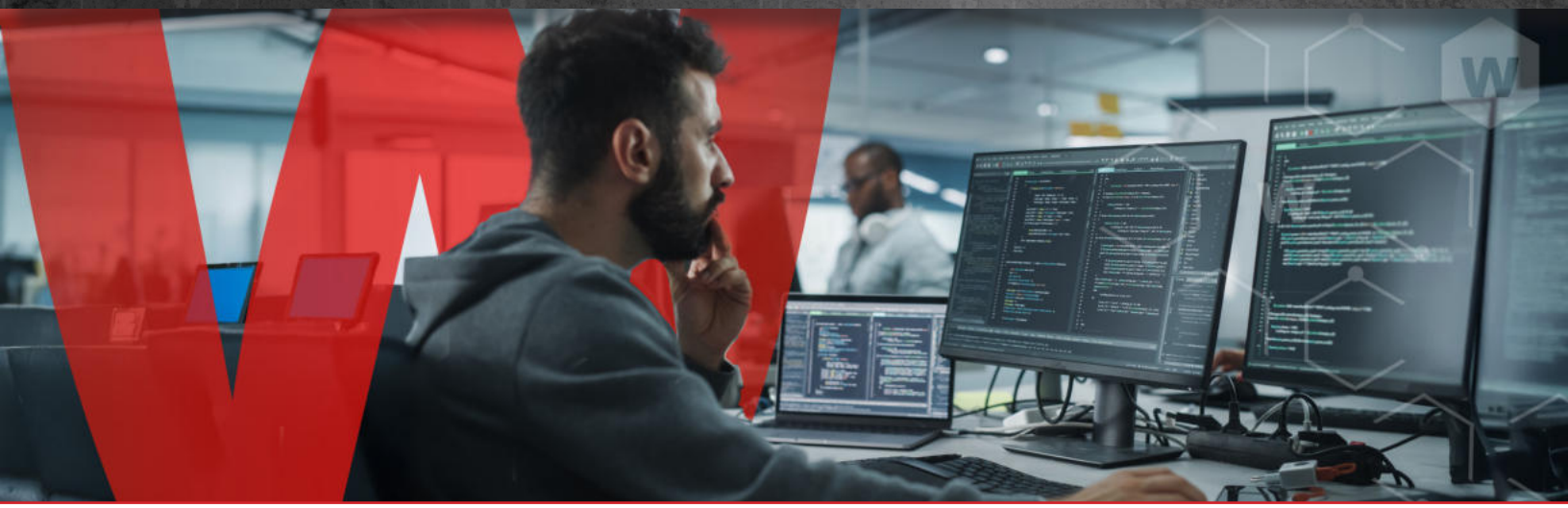
WatchGuard MDR



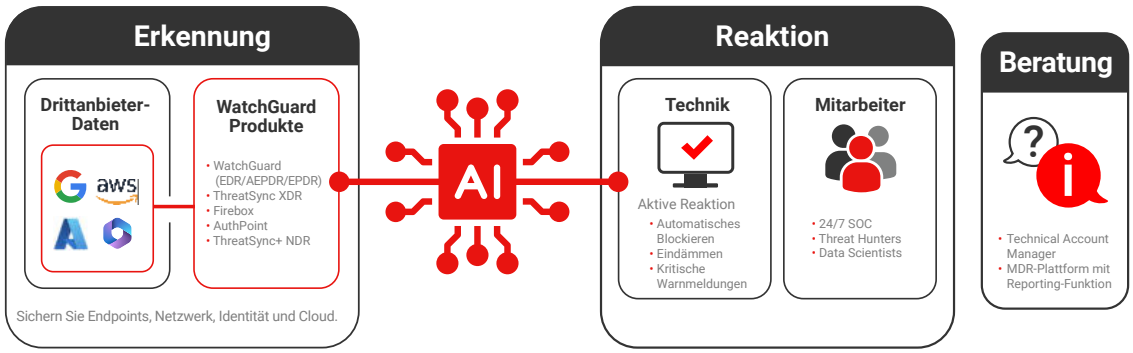
24/7-Bedrohungserkennung und -Reaktion in Ihrem gesamten Sicherheitssystem

WatchGuard MDR ist ein vollständig verwalteter 24/7-Service, der Sie nicht nur vor Bedrohungen warnt, sondern auch aktiv darauf reagiert. Unser Team hilft Ihnen, sich auf das Wesentliche zu konzentrieren und schnell auf Bedrohungen auf Ihren Laptops, Servern, Benutzeridentitäten, im Netzwerk und in der Cloud zu reagieren.

Ihr Unternehmen steht nicht still, und das sollte auch Ihre Sicherheit nicht. WatchGuard MDR bietet Ihnen rund um die Uhr volle Transparenz und kompetenten Schutz. Ob riskante Anmeldungen, verdächtige E-Mails oder versteckte Bedrohungen in Ihrem Netzwerk – wir erkennen sie schnell und stoppen sie, bevor Schaden entsteht, ohne Ihr Team zusätzlich zu belasten.

Was Sie mit WatchGuard MDR erhalten

- Erkennung Sie rund um die Uhr Bedrohungen in Ihrer gesamten Umgebung – Endpoint, Identität, Netzwerk und Cloud.
- Filtern Sie Störsignale heraus, um nur zuverlässige Warnmeldungen zu erhalten.
- Reagieren Sie automatisch oder eskalieren Sie je nach Schweregrad an Experten.
- Reduzieren Sie Risiken, indem Sie die Ursachen identifizieren und Lücken schließen.
- Bieten Sie Echtzeit-Transparenz und Berichte zu Bedrohungsaktivitäten, Reaktionsmaßnahmen und SOC-Leistung.



Wichtigste Funktionen

Eine einzige Ansicht für Ihre gesamte Sicherheitsstruktur
Erhalten Sie eine einheitliche Ansicht der Bedrohungsaktivitäten über Endpoint-, Firewall-, Identitäts-, Netzwerk- und Cloud-Aktivitäten hinweg von einem Ort aus, sparen Sie Zeit und reduzieren Sie die Komplexität.

Überwachung und Reaktion rund um die Uhr
Unser globales SOC ist immer im Einsatz. Echte Menschen und leistungsstarke Automatisierung arbeiten zusammen, um Bedrohungen zu erkennen und zu stoppen. Unser Live-Support ist immer für Sie da. Das WatchGuard Security Operations Center ist auf mehrere Standorte verteilt und bietet so Redundanz und eine echte 24 Stunden Abdeckung.

Intelligentere Erkennung mit KI/ML
KI und maschinelles Lernen scannen Tausende von Signalen in Echtzeit, erkennen Muster, die Menschen möglicherweise übersehen, und lernen, wie neue Bedrohungen gestoppt werden können. Das System lernt aus jedem Vorfall und wird jeden Tag intelligenter, um Bedrohungen schneller zu erkennen und zu reagieren.

Proaktives Threat Hunting
Unsere Analysten suchen nach versteckten Bedrohungen, die automatisierte Tools übersehen können, damit Sie auch dann geschützt sind, wenn Angreifer versuchen, schlau zu sein.

Schnell reagierende Automatisierung
Wir automatisieren manuelle Aufgaben, filtern Störsignale, eskalieren nur das, was wichtig ist, und handeln schnell, um Bedrohungen einzudämmen, bevor sie sich ausbreiten können.

Präzise Reaktion auf Bedrohungen
Wir handeln schnell, um Bedrohungen einzudämmen, Endpunkte zu isolieren, bösartige Dateien zu blockieren und Aktivitäten in Ihrer Umgebung zu untersuchen.

Flexible Reaktionsoptionen
Sie entscheiden, wie die Reaktion gehandhabt wird: Handeln Sie selbst, lassen Sie uns übernehmen oder teilen wir die Verantwortung. Sie entscheiden.

Echtzeit-Visualisierung
Das MDR-Portal bietet Ihnen an einem zentralen Ort einen Live-Überblick über Ihre gesamte Umgebung, einschließlich Warnmeldungen, ergriffener Maßnahmen und Kennzahlen, die zeigen, wie gut Sie geschützt sind.

Geringe Störsignale, hohe Signalqualität
Sie erhalten nur zuverlässige Warnmeldungen mit weniger als einem Fehlalarm pro Monat, sodass Ihr Team sich auf das Wesentliche konzentrieren kann.

Integrierte fachkundige Anleitung
Technische Kundenbetreuer (TAMs) bieten kontinuierliche Sicherheitsberatung und helfen, SOC-Aktivitäten zu verstehen, Trends zu erkennen und den Schutz im Laufe der Zeit zu verbessern. Mit ständig verfügbarer kompetenter Unterstützung können Sie Ihren Kunden zuverlässig bessere Ergebnisse liefern.

Warum WatchGuard? Wettbewerbsvorteil

Bewährter führender Anbieter für Cybersicherheit
Mit über 25 Jahren Erfahrung im Bereich der Cybersicherheit hat sich WatchGuard einen Namen für die Bereitstellung von Schutz für Unternehmen gemacht, der einfach, skalierbar und zugänglich ist. Heute tragen wir zum Schutz von über 10 Millionen Endpoints in 250.000 Unternehmen weltweit bei.

Wirklich integrierte Sicherheit
Im Gegensatz zu MDR-Anbietern, die nur Endpoints überwachen oder noch Cloud-Support hinzufügen, kombinieren wir Endpoint-, Identitäts-, Firewall- und Netzwerkerkennung.

Partnerorientiertes Design
Unsere Lösungen sind für MSPs und kleinere Organisationen konzipiert – ohne aufgeblähte Tools die umständlich angepasst werden müssen. Sie behalten die Kontrolle über Kundenbeziehungen und die Erbringung von Dienstleistungen.

Weniger Alarmmüdigkeit, mehr Maßnahmen
Im Vergleich zu einigen Anbietern, die täglich mehr als 15 Fehlalarme generieren, verzeichnen wir durchschnittlich weniger als einen Fehlalarm pro Monat. Das bedeutet weniger Ablenkungen und schnellere Reaktion.

Schnellere Bereitstellung von Schutz
Ein schnelles Onboarding, vorgefertigte Integrationen und starker Partner-Support sorgen dafür, dass Sie ohne großen Aufwand schnell einsatzbereit sind.

Entwickelt für moderne Strukturen
Mit nativer Unterstützung für Microsoft 365, Azure, AWS und Google Workspace tragen wir zum sofortigen Schutz von Hybrid- und Cloud-First-Umgebungen bei.

Bewährte Technologie, vertrauenswürdiges Team
Unser SOC kombiniert fundiertes Sicherheits-Know-how mit leistungsstarker KI, um Bedrohungen schnell zu erkennen und zu stoppen. Die MDR-Plattform von WatchGuard wurde in Branchenbewertungen wie MITRE getestet und basiert auf jahrzehntelanger Erfahrung mit zuverlässigem, leistungsstarkem Schutz für Unternehmen weltweit.

Sichern Sie die gesamte Angriffsfläche

Endpoint Protection
Endpoints sind ein primäres Ziel für Ransomware, Phishing und dateilose Angriffe. Total MDR nutzt WatchGuard EDR/EPDR/AEPDR, um Verhaltensweisen wie den Diebstahl von Anmeldedaten und die Eskalation von Berechtigungen zu erkennen, kompromittierte Geräte zu isolieren, bösartige Prozesse zu stoppen und eine Live-Reaktionen von Analysten zu ermöglichen, bevor sich Malware lateral ausbreiten und eskalieren kann.

Identitätsschutz
Total MDR lässt sich in WatchGuard AuthPoint integrieren, um verdächtige Aktivitäten wie Anomalien bei der Anmeldung, fehlgeschlagene Anmeldeversuche oder die Erstellung von betrügerischen Konten zu erkennen und darauf zu reagieren. Durch die Deaktivierung kompromittierter Konten in Echtzeit werden Angreifer daran gehindert, sich als Benutzer auszugeben oder unbemerkt auf Cloud-Plattformen zuzugreifen.

Netzwerkschutz
Angriffe, die Endpoints umgehen, wie z. B. laterale Bewegungen, Port-Scans oder C2-Datenverkehr, werden durch die Firebox und ThreatSync+ NDR identifiziert. Total MDR reagiert sofort, indem es schädliche IP-Adressen blockiert, Ports schließt oder die Datenexfiltration stoppt und so interne Systeme vor versteckten Bedrohungen schützt.

Cloud-Schutz
Total MDR überwacht Microsoft 365 und andere Cloud-Plattformen auf Anzeichen von Kompromittierung, einschließlich verdächtiger Anmeldungen, Berechtigungsänderungen und Zugriff auf Postfächer. Bei Microsoft 365 reagiert es über API-Integrationen, um den Zugriff zu widerrufen, Anmeldedaten zurückzusetzen und Bedrohungen einzudämmen, bevor es zu E-Mail-Betrug oder Datenverlust kommt.

<6 Minuten durchschnittliche Dauer bis zur ersten Reaktion

„Wir benötigen Lösungen, die einfach bereitzustellen und zu warten sind. Umfangreiche, komplizierte Werkzeuge können wir uns nicht leisten. Dadurch gewinnen wir Zeit und können uns auf die strategische Unterstützung konzentrieren. Mehrere Konsolen parallel zu bedienen ist nicht mehr nötig – für ein kleines Team wäre das auf Dauer auch nicht machbar."
~ Julien Perret, Eiffie

KI-gesteuertes Threat Hunting + Automatisierung

Integrierte Unterstützung für Firebox, AuthPoint, ThreatSync+ NDR und WatchGuard EDR/EPDR/AEPDR

Unterstützung für Microsoft 365, Azure, AWS CloudTrail und Google Workspace

Ein einziges Portal für Visualisierung, Reaktion und Berichterstattung

Vollständig verwaltete oder gemeinsam verwaltete Optionen verfügbar

<1 Fehlalarm pro Monat

Mehr Schutz mit Total MDR

ANGRIFFSVEKTOR	TOTAL MDR ABWEHRREAKTION	WAS GESCHÜTZT WIRD
Gestohlene Anmeldedaten	**AuthPoint**: Blockiert die Übernahme von Konten	Identitäten
Exploits und Malware	**EDR**: Stoppt Malware und isoliert Endpunkte	Ruhende Daten
Laterale Bewegung	**NDR + Firebox**: Erkennt und blockiert laterale Bewegungen	Daten in Bewegung
Cloud-Zugriff und Exfiltration	**Cloud-Integration**: Widerruft den Zugriff und setzt Anmeldedaten zurück	Anwendungen

Welcher MDR-Service ist der richtige für Sie?

Nicht jede Umgebung ist gleich. Einige Kunden nutzen bereits Microsoft Defender. Andere wünschen sich umfassenden WatchGuard-Schutz. Mit WatchGuard MDR können Sie jedem Kunden das richtige Schutzniveau bieten.

	WatchGuard Core MDR	WatchGuard Core MDR für MS	WatchGuard Total MDR
Ideal für Partner/Kunden, die:	WatchGuard Endpoint verwenden	Microsoft Defender verwenden	WatchGuard Endpoint, NDR, Identity, Firewall verwenden
SOC-Monitoring rund um die Uhr	✓	✓	✓
KI/ML-basierte Bedrohungserkennung	✓	✓	✓
Automatisierte Reaktion auf Bedrohungen/Echtzeit-Warnmeldungen	✓	✓	✓
Ursachenanalyse	✓	✓	✓
Threat Hunter	✓	✓	✓
Reaktion auf Vorfälle			✓
Verteidigungsportal	✓	✓	✓
Partnerzugang zum Technical Account Manager	✓	✓	✓
Endpoint-Integration	WatchGuard EDR/EPDR/AEPDR	Microsoft Defender	WatchGuard EDR/EPDR/AEPDR
Netzwerkintegration			WatchGuard Firebox ThreatSync+ NDR
Identitätsintegration			WatchGuard AuthPoint
Threat Sync + XDR			✓
Microsoft 365	✓	✓	✓
AWS CloudTrail-Abdeckung			✓
Google Workspace			✓

Über WatchGuard Technologies, Inc.

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 and 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 Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter watchguard.de.