



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-, 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. Unsere Live Threat Hunter sind 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 Prüfung und Maßnahmen, 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. WatchGuard MDR lässt sich in WatchGuard Endpoint oder unterstützte Endpoint-Produkte von Drittanbietern integrieren, um Verhaltensweisen wie Diebstahl von Anmeldedaten und Eskalation von Berechtigungen zu erkennen, kompromittierte Geräte zu isolieren, bösartige Prozesse zu stoppen und eine Live-Reaktion von Analysten zu ermöglichen, bevor sich Malware lateral ausbreiten und eskalieren kann.

Identitätsschutz

WatchGuard MDR lässt sich in WatchGuard AuthPoint oder Okta integrieren, um verdächtige Aktivitäten wie Login-Anomalien, fehlgeschlagene Login-Stürme oder die Erstellung von Rogue-Konten zu erkennen und darauf zu reagieren. Durch die Deaktivierung kompromittierter Konten in Echtzeit werden Angreifer daran gehindert, sich als Benutzer auszugeben oder unentdeckt 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, um interne Systeme vor heimlichen Bedrohungen zu schützen.

Cloud-Schutz

WatchGuard MDR überwacht Microsoft 365 und andere Cloud-Plattformen auf Anzeichen von Kompromittierung, einschließlich verdächtiger Anmeldungen, Berechtigungsänderungen und Postfachzugriff. 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.



Mehr Schutz mit WatchGuard MDR

ANGRIFFSVEKTOR



WATCHGUARD MDR HÄLT SIE AUF



Gestohlene Anmeldedaten

Identität: Blockiert die Übernahme von Konten

Exploits und Malware

Endpoint: Stoppt Malware und isoliert Endpoints

Laterale Bewegung

Netzwerk: Erkennt und blockiert laterale Bewegungen

Cloud-Zugriff und Exfiltration

Cloud-Integration: Widerruft den Zugriff und setzt Anmeldedaten zurück

WAS GESCHÜTZT WIRD 🔑

Identitäten

Ruhende Daten

Daten in Bewegung

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	WatchGuard Open MDR
Ideal für Partner/Kunden, die:	WatchGuard Endpoint verwenden	Microsoft Defender verwenden	WatchGuard Endpoint, NDR, Identity, Firewall verwenden	Tools von Drittanbietern verwenden
SOC-Monitoring rund um die Uhr	✓	✓	✓	✓
KI/ML-basierte Bedrohungserkennung	✓	✓	✓	✓
Incident Response (menschliche und automatisierte Reaktion, Ursachenanalyse)	✓	✓	✓	✓
Advanced Incident Response (Untersuchung, Wiederherstellung und Prävention nach einer Sicherheitsverletzung)	✓	✓	✓	✓
Threat Hunter	✓	✓	✓	✓
Verteidigungsportal	✓	✓	✓	✓
Partnerzugang zum Technical Account Manager	✓	✓	✓	✓
Endpoint-Integration	WatchGuard Endpoint	Microsoft Defender	WatchGuard Endpoint	WatchGuard Endpoint, CrowdStrike, Microsoft Defender
Netzwerkintegration			WatchGuard Firebox ThreatSync NDR	WatchGuard Firebox, ThreatSync NDR und die meisten Firewalls von Drittanbietern
Identitätsintegration			WatchGuard AuthPoint	WatchGuard AuthPoint und Okta
Microsoft 365	✓	✓	✓	✓
AWS CloudTrail-Abdeckung			✓	✓
Google Workspace			✓	✓

Über WatchGuard Technologies, Inc.

WatchGuard® Technologies gehört zu den weltweit führenden Anbietern im Bereich Cybersicherheit für Managed Service Provider. Im Gegensatz zu anderen Anbietern bietet WatchGuard über seine Unified Security Platform® echte Sicherheit für reale Umgebungen. Auf der Grundlage von künstlicher Intelligenz und Zero-Trust-Ansätzen bietet das Unternehmen starken und skalierbaren Schutz für Netzwerke, Endpoints und Identitäten. WatchGuard genießt das Vertrauen von mehr als 17.000 Vertriebspartnern und Managed Service Providern, die über 250.000 Unternehmen schützen. Das Unternehmen hilft Partnern, schnell zu wachsen, betriebliche Belastungen zu beseitigen und starke Ergebnisse zu erzielen – ohne zusätzliche Anbieter, Konsolen oder Komplexität. WatchGuard hat seinen Hauptsitz in Seattle, Washington, und unterhält Niederlassungen weltweit. Weitere Informationen finden Sie unter [WatchGuard.de](https://www.watchguard.de).