SERVICE-BRIEFING

WatchGuard Gesamt-MDR

Total MDR unterstützt Sie bei der Skalierung Ihrer Sicherheitsdienstleistungen mit minimalem betrieblichem Aufwand. Bieten Sie rund um die Uhr Schutz, Bedrohungsabwehr und fachkundige Beratung, ohne ein SOC mit Mitarbeitern zu besetzen oder mehrere Tools zusammenzufügen.

Vorteile für Partner mit Total MDR

Beschleunigtes Onboarding: Aktivieren Sie umfassenden Schutz ohne komplexe Bereitstellungen. Schnelles Onboarding bedeutet schnellere Einnahmen.

Für den WatchGuard Stack entwickelt: Partner, die bereits Firebox, AuthPoint oder WatchGuard EDR vertreiben, können ihre Abdeckung und ihren Leistungsumfang ohne zusätzliche Tools erweitern

Einheitliches Portal = Verkaufsförderung: Zeigen Sie Ihren Kunden, wie Sie sie schützen – Endpoints, Netzwerk, Identität und Cloud – alles von einem Ort aus.

Geringe Störgeräusche, hohe Zuverlässigkeit: Weniger Fehlalarme bedeuten weniger Arbeitsaufwand und mehr Zeit, um sich auf die Wertschöpfung und den Aufbau des Kundenvertrauens zu konzentrieren.

Die gesamte MDR-Bedrohungserkennung und -reaktion umfasst:

Endpunkte:
WatchGuard EDR, EPDR, AEPDR

Firewall:
WatchGuard Firebox

Identität:
AuthPoint

Netzwerk:
ThreatSync+ NDR

Cloud:
Microsoft 365/Azure, AWS CloudTrail, Google Workspace

Hauptmerkmale & Vorteile

Einheitliche Bedrohungssichtbarkeit
Erhalten Sie einen vollständigen Überblick über Ihre Sicherheitslage an einem Ort. WatchGuard Total MDR vereint Daten aus Endpunkt-, Firewall-, Identitäts-, Netzwerk- und Cloud-Umgebungen in einem einzigen, benutzerfreundlichen Portal. Sie müssen nicht mehr zwischen den Tools wechseln oder das Gesamtbild übersehen – nur klare, zentralisierte Einblicke, um Bedrohungen schneller zu erkennen und darauf zu reagieren.

24/7 SOC-Abdeckung
Unsere erfahrenen Sicherheitsanalysten überwachen, untersuchen und reagieren rund um die Uhr auf Bedrohungen, sodass Sie dies nicht tun müssen. Egal, ob es 14:00 Uhr oder 02:00 Uhr ist, das WatchGuard SOC arbeitet aktiv daran, Organisationen zu schützen, ohne die Kosten oder die Komplexität des internen Aufbaus eines SOC zu verursachen.

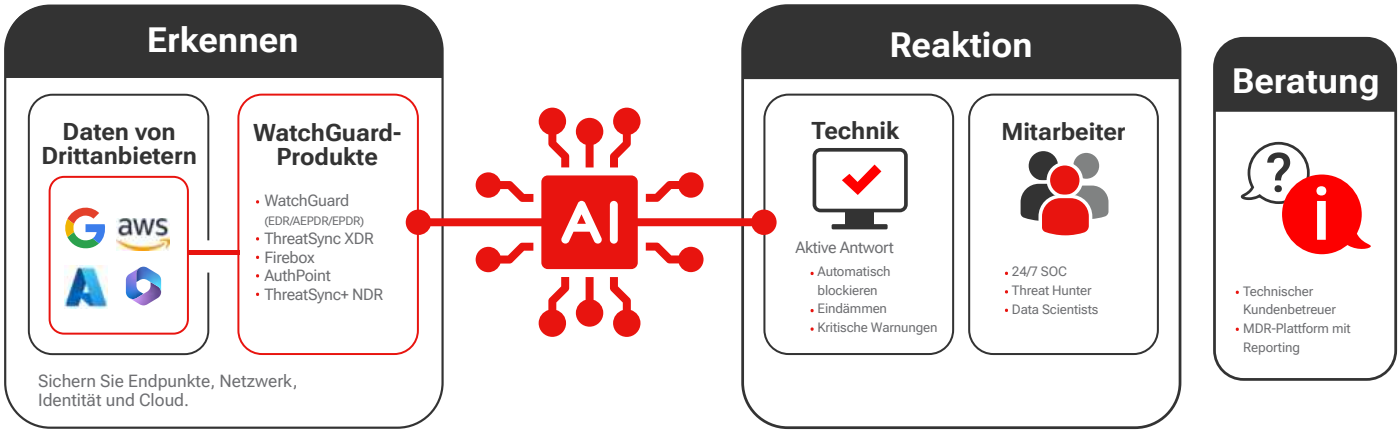
KI-gesteuerte Erkennung
Maschinelles Lernen analysiert ständig Tausende von Signalen, um verdächtige Aktivitäten in Echtzeit zu erkennen. Es durchschneidet Alarmgeräusche, erkennt Anomalien und passt sich schneller an neue Bedrohungen an als herkömmliche regelbasierte Tools und bietet besseren Schutz mit weniger manuellem Aufwand.

Schnelle aktive Reaktion
Mit durchschnittlichen Reaktionszeiten unterhalb von sechs Minuten werden Bedrohungen gestoppt, bevor sie sich ausbreiten. WatchGuard Total MDR isoliert kompromittierte Geräte, enthält schädliche Dateien und eskaliert Vorfälle nur bei Bedarf, damit sich die Teams auf das Wesentliche konzentrieren können und nicht in Warnmeldungen vergraben sind.

Hohe Wiedergabetreue, geringe Geräuschentwicklung
WatchGuard Total MDR liefert im Durchschnitt weniger als einen Fehlalarm pro Monat. Das bedeutet, dass Sie Warnungen mit hohem Vertrauen und klaren Aktionsplänen erhalten – wodurch die Ermüdung der Warnungen verringert, Vertrauen aufgebaut und Ihnen geholfen wird, entscheidend zu reagieren, wenn es darauf ankommt.

Experten-Support-Team
Technical Account Manager (TAMs) bieten fortlaufende Sicherheitshinweise, Bedrohungseinblicke und Eskalationsunterstützung. Sie helfen, komplexe Aktivitäten und Oberflächentrends zu verstehen, und empfehlen Verbesserungen, um den Schutz im Laufe der Zeit zu stärken.

Übersicht über den gesamten MDR-Service



Sichern Sie die gesamte Angriffsfläche

Endpoint Protection
Endpunkte sind ein primäres Ziel für Ransomware, Phishing und dateilose Angriffe. Total MDR verwendet WatchGuard EDR, EPDR, AEPDR, um Verhaltensweisen wie Diebstahl von Anmeldeinformationen und Eskalation von Berechtigungen zu erkennen, dann kompromittierte Geräte zu isolieren, bösartige Prozesse zu stoppen und Live-Analysten-Reaktionen zu ermöglichen, bevor sich Malware seitlich ausbreiten und eskalieren kann.*

Identitätsschutz
Total MDR lässt sich in WatchGuards AuthPoint 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 Endpunkte umgehen, wie seitliche Bewegung, Port-Scans oder C2-Verkehr, werden über Firebox und 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
Total MDR überwacht Microsoft 365 und andere Cloud-Plattformen auf Anzeichen von Kompromittierung, einschließlich verdächtiger Anmeldungen, Berechtigungsänderungen und Postfachzugriff.

*Partner, die bereits WatchGuard Core MDR verwenden, können auf Total MDR upgraden, um zusätzliche Funktionen für Firebox, AuthPoint und NDR freizuschalten.

Metriken, die wichtig sind

<1 Falsch-Positiv
pro Monat

Durchschnittlich
6 Benachrichtigungen
pro Monat

6 Minuten
mittlere Zeit bis zur ersten Antwort

10 Millisekunden,
um Bedrohungen automatisch einzudämmen

US-UMSATZ 1.800.734.9905 INTERNATIONALER VERTRIEB +1.206.613.0895 WEB www.watchguard.com/de WatchGuard Technologies, Inc.