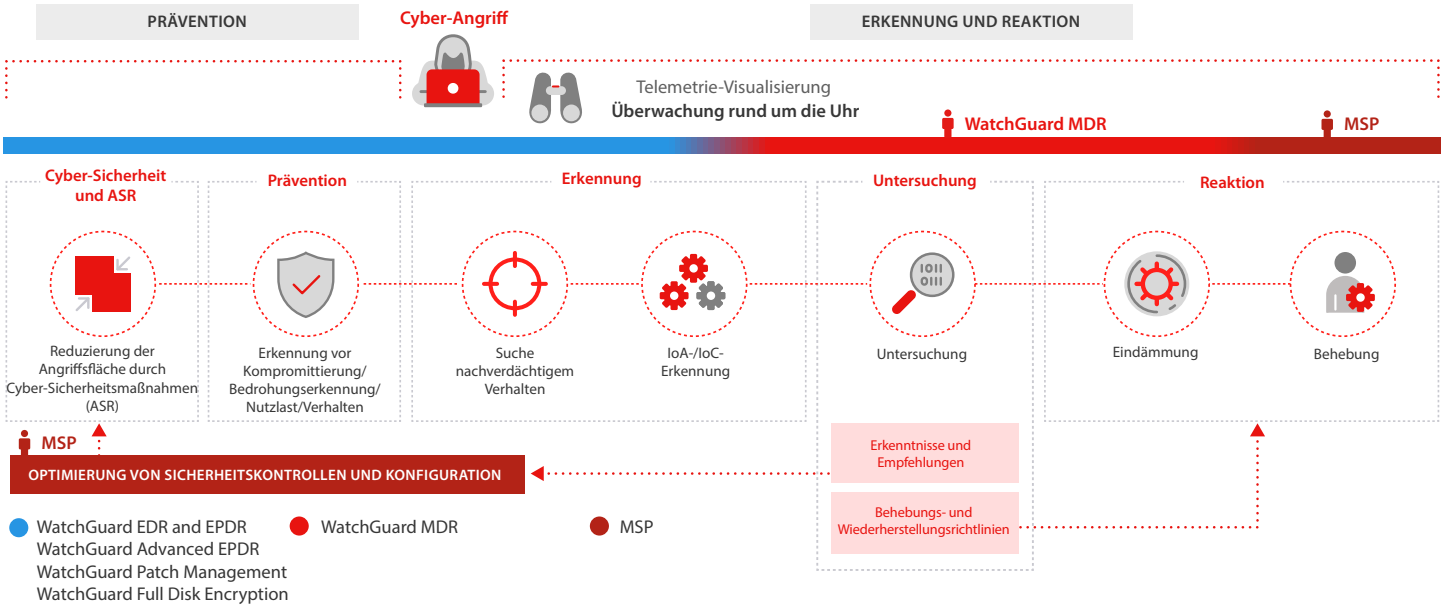

# WatchGuard MDR für MSP

## Erkennung und Reaktion rund um die Uhr ohne Mehraufwand.

Da sich die Bedrohungslandschaft weiter ausdehnt und immer ausgefeilter wird, was mit erheblichen Kosten verbunden ist – einschließlich der Kosten im Zusammenhang mit der obligatorischen Einhaltung gesetzlicher Vorschriften – haben Unternehmen mit ernsthaften Sicherheitsrisiken zu kämpfen, die auf ineffizientes Sicherheitsmanagement und einen Mangel an qualifizierten Sicherheitsteams zurückzuführen sind. Daher wenden sich viele Unternehmen an ihre MSPs, um deren Technologie, Mitarbeiter und Fachwissen zu nutzen, die zur Bewältigung dieser Herausforderungen erforderlich sind.

Die Verwaltung komplexer Sicherheitsprobleme erfordert angesichts der steigenden Anzahl an Bedrohungen jedoch hochqualifiziertes Personal und erhebliche Investitionen, was es MSPs erschwert, Managed Detection and Response Services (MDR) auf praktische, skalierbare und kostengünstige Weise anzubieten. Aus diesem Grund hat WatchGuard den Managed Service WatchGuard MDR eingeführt, der Serviceanbietern dabei helfen soll, diese Herausforderungen zu meistern. Durch die Nutzung unseres umfassenden MDR-Service können MSPs die Anforderungen ihrer Kunden erfüllen, ohne ein eigenes SOC (Security Operations Center) erstellen und rund um die Uhr betreiben zu müssen.

WatchGuard MDR bietet die Überwachung von Endpoints und Microsoft 365-Aktivitäten, Bedrohungssuche, Erkennung, Untersuchung und Eindämmung mit Empfehlungen zur Behebung. Der Service wird von einem Elite-Team von Sicherheitsexperten verwaltet und von KI unterstützt. Er ist rund um die Uhr verfügbar und bietet flexiblen Support, der auf die betrieblichen Anforderungen von MSPs zugeschnitten ist, entweder rund um die Uhr oder während der Geschäftszeiten. Es sind keine Investitionen in traditionelle SOC-Infrastrukturen, fortschrittliche Technologien oder schwer zu findende Sicherheitsexperten erforderlich, sodass Partner den globalen Mangel an Fachkräften und Finanzmitteln bewältigen und gleichzeitig in ihrem eigenen Tempo skalieren können.



## Funktionsweise

WatchGuard MDR bietet eine rund um die Uhr verfügbare Überwachung der an den Endpoints und in Microsoft 365 registrierten Bedrohungsaktivitäten und ermöglicht die Korrelation verdächtiger Aktivitäten, um Cyber-Bedrohungen umgehend und effektiv zu erkennen, zu untersuchen und darauf zu reagieren. So funktioniert der Service:

### Service-Onboarding:

Der Onboarding-Prozess wird sofort nach der Aktivierung des MDR-Diensts im Konto des Abonnenten eingeleitet. WatchGuard SOC-Analysten arbeiten zusammen, um Reaktionstypen zu definieren und optimalen Service zu gewährleisten. Wir bestätigen die Einrichtung von WatchGuard EDR, EPDR und Advanced EPDR und arbeiten gemeinsam daran, die Funktionalität Ihrer Sicherheitskontrollen zu überprüfen, um die Eindämmung und Reaktionsbereitschaft sicherzustellen.

### Rund um die Uhr verfügbare Endpoint- und Microsoft 365-Aktivitätsüberwachung und -Datenerfassung:

WatchGuard MDR nutzt Endpoint-Daten, die von WatchGuard-Hostsensoren gesammelt und dann 365 Tage lang in unserem Cloud SOC gespeichert werden. Unsere Threat Hunting-Experten erforschen in Echtzeit und im retrospektiv mithilfe von maschinellem Lernen und fortschrittlicher Analytik neue Muster, um die Cyber-Sicherheit zu verbessern.

### 24/7 proaktive Bedrohungsjagd und -erkennung:

Wir verwenden maschinelles Lernen, um diese Daten zu analysieren und verdächtige Aktivitäten und Anomalien zu erkennen, die auf das Vorhandensein einer Bedrohung hinweisen könnten. Wir ordnen alle Angriffsindikatoren (IoA) dem MITRE ATT&CK-Framework zu, um die Bedrohungsakteure schnell zu durchschauen. Unser MDR-Personal sucht proaktiv nach Endpoint-Bedrohungen, verkürzt die Erkennungszeit und verbessert die Sicherheitseffizienz.

### 24/7 Untersuchung und Validierung :

Untersuchung und Validierung sind Schlüsselelemente unseres MDR-Service. Mithilfe von Algorithmen für maschinelles Lernen, die anhand realer Cyber-Vorfälle trainiert wurden, korrelieren unsere Experten IoA mit Vorfällen, untersuchen und validieren sie, um potenzielle Bedrohungen schnell anzugehen und die Auswirkungen zu minimieren.

### Sofortige Benachrichtigung der Partnerteams über Vorfälle:

Nach der Bestätigung eines Sicherheitsvorfalls benachrichtigt WatchGuard MDR unsere MSP-Partner umgehend mit einer Validierung nach dem Vorfall und erspart ihnen die Überprüfung unbestätigter Fälle. Die Benachrichtigungen enthalten detaillierte Informationen zu den Untersuchungen und den betroffenen Computern, sodass Partnerteams schnell und sachkundig reagieren können, um Bedrohungen zu minimieren und potenzielle Schäden oder Datenverluste effizient zu verhindern.

### Minderungs- und Behebungsleitlinien:

Wenn Sicherheitsvorfälle auftreten, arbeitet das WatchGuard MDR-Team eng mit MSP zusammen, um klare, umsetzbare Anleitungen für die Reaktion auf Vorfälle und die Schadensbegrenzung bereitzustellen. Dazu gehören detaillierte Empfehlungen für Eindämmungsmaßnahmen, Abhilfemaßnahmen und die Verbesserung der zukünftigen Sicherheitslage. Unsere Richtlinien helfen Partnern, schnell und effektiv auf Bedrohungen zu reagieren, die Auswirkungen von Vorfällen zu minimieren und die allgemeine Sicherheitslage der Kunden zu verbessern, um zu verhindern, dass ähnliche Vorfälle erneut auftreten.

### Rund um die Uhr verfügbare Reaktion und Schadensbegrenzung durch WatchGuard oder das Partnerteam:

Unsere MDR-Experten erstellen benutzerdefinierte automatisierte Playbooks, um validierte Bedrohungen zu minimieren und einzudämmen, einschließlich solcher, die eine potenzielle Endpoint-Isolierung umfassen. Wenn sich die Partner dafür entscheiden, ihre eigenen Teams mit der Eindämmung zu beauftragen, bietet das WatchGuard MDR-Team Unterstützung an.

### Reaktion und Behebung durch das Partnerteam:

Unter der Leitung von Watch Guard Partnern werden in der Phase nach dem Vorfall die Spuren des Angreifers verfolgt, Daten wiederhergestellt und Schwachstellen behoben. Dies kann auch die Verbesserung bestehender Sicherheitseinstellungen oder die Implementierung neuer Sicherheitskontrollen umfassen, um ähnliche Vorfälle in Zukunft zu verhindern.

### Wöchentliche und monatliche Berichterstellung:

WatchGuard MDR-Experten liefern wöchentliche und monatliche Sicherheitsberichte an Partner, die erkannte IoA, Untersuchungen, identifizierte Vorfälle und eine Sicherheitszustandsanalyse umfassen, um potenzielle Bedrohungen zu antizipieren. Partner können Berichte anpassen, um die Kundenbindung mit ihrem MDR-Service zu verbessern.

**Vorteile für unsere Partner**

| Funktionen | MSP-Vorteile |
|---|---|
| Rund um die Uhr verfügbare Überwachung, Datenerfassung durch WatchGuard SOC in der Cloud | Nutzen Sie die MDR-Möglichkeiten, ohne in ein modernes SOC zu investieren. |
| Rund um die Uhr verfügbare Erkennung, Thread Hunting und Untersuchung durch die Experten von WatchGuard | Erweitern Sie Ihr Team mit qualifizierten Mitarbeitern für Cyber-Sicherheit, um MDR rund um die Uhr bereitzustellen. |
| Rund um die Uhr verfügbare unbeaufsichtigte Bedrohungseindämmung | Beauftragen Sie uns mit der Eindämmung von unentdeckten Bedrohungen rund um die Uhr. |
| Sofortige Benachrichtigung des MSP-Teams | Übernehmen Sie die Führung bei Ihren Kundenbeziehungen, während wir sicherstellen, dass Sie immer informiert sind. |
| Minderungs- und Behebungsleitlinien | Erhalten Sie Zugriff auf Sicherheitswissen und bewährte Methoden, die Ihnen einen Wettbewerbsvorteil verschaffen. |
| Service-Onboarding und regelmäßige Zustandsprüfungen | Verhindern Sie Angriffe durch unzureichende Sicherheit oder nicht verwaltete Endpoints. |
| Wöchentlicher Wellness-Status- und monatliche Aktivitätsberichte | Erhöhen Sie die Sicherheit Ihrer Kunden, indem Sie Bedrohungen, die Sicherheitsrisiken ausnutzen, immer einen Schritt voraus sind. |

## MDR-Modell und Anwendungsfälle

### 1. MDR von einem internen Security Operations Center (SOC):

Ein internes SOC ist eine dedizierte Einrichtung und ein Team innerhalb eines MSP, das für das Management und die Reaktion auf Cyber-Sicherheitsprobleme in der Umgebung seiner Kunden verantwortlich ist.

- **Kontrolle:** Volle Kontrolle über alle Prozesse, Tools und Daten.
- **Kosten:** Hoch – umfasst Investitionen in Technologie und qualifiziertes Personal.
- **Skalierbarkeit:** Die Skalierung erfordert zusätzliche Investitionen in Personal und Technologie.
- **Management:** Das gesamte Management und der Betrieb werden intern geregelt.

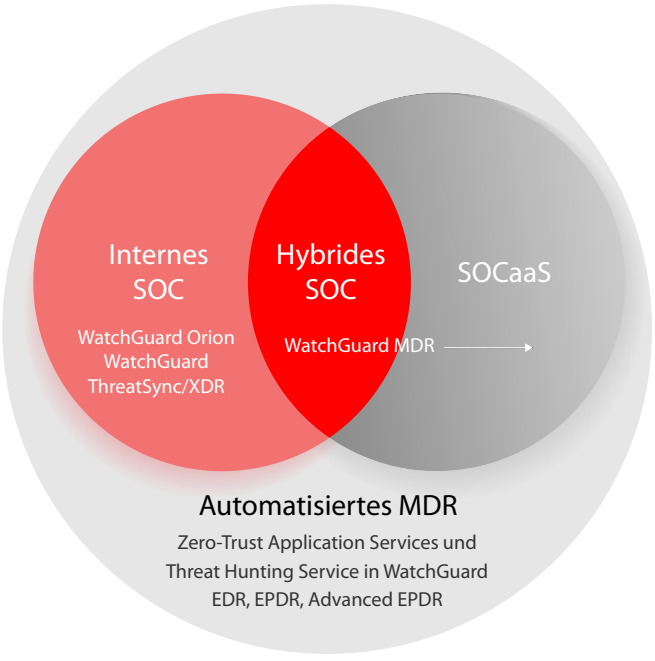
★ **Anwendungsfall:** Ideal für große Unternehmen mit erheblichen Budgets für Cyber-Sicherheit und hohen Sicherheitsanforderungen.

### 2. MDR von einem SOC-as-a-Service (SOCaaS):

SOCaaS ist ein Dienst, der ausgelagerte Überwachungs-, Erkennungs-, Untersuchungs- und Reaktionsfunktionen für die Cyber-Sicherheit durch einen externen MDR bereitstellt.

- **Kontrolle:** Eingeschränkte Kontrolle, da die Prozesse vom MDR-Anbieter abgewickelt werden.
- **Kosten:** Niedriger – Betriebskosten anstelle einer Kapitalinvestition.
- **Skalierbarkeit:** Kann je nach gewähltem Service skalierbar sein.
- **Management**: Verwaltet durch Cyber-Sicherheitsexperten von Drittanbietern.

★ Anwendungsfall: Geeignet für kleine und mittelgroße Unternehmen oder Organisationen mit begrenzten Budgets und Mitarbeitern für Cyber-Sicherheit.




### 3. MDR von einem Hybrid-SOC:

Ein hybrides SOC-Modell kombiniert interne und ausgelagerte SOC-Funktionalitäten, um ein Gleichgewicht zwischen internen und externen Cyber-Sicherheitsfunktionen herzustellen.

- **Kontrolle:** Moderate Kontrolle – intern verwaltet, nutzt aber externe Ressourcen.
- **Kosten:** Kann je nach dem Verhältnis zwischen internen und ausgelagerten Funktionen optimiert werden.
- **Skalierbarkeit:** Höher – interne Maßnahmen können durch externe Möglichkeiten ergänzt werden.
- **Management:** Bezieht sowohl das interne Management als auch das Management von Drittanbietern ein.

★ Anwendungsfall: Ideal für Unternehmen, die ihre bestehenden SOC-Funktionen ohne erhebliche Investitionen erweitern möchten.

### 4. Automatisiertes MDR (Services)

Im Kontext der automatisierten MDR spielt die Technologie eine zentrale Rolle bei der Stärkung der Cyber-Sicherheitsabwehr, indem sie verschiedene Funktionen rationalisiert und oft automatisch abwickelt, um die Effizienz und Reaktionsfähigkeit zu verbessern.

- **Kontrolle:** Erkennungs- und Reaktionsaktivitäten werden automatisiert. Ermöglicht es IT-Teams, sich auf strategische, komplexe oder eskalierte Probleme zu konzentrieren.
- **Kosten:** Es sind keine zusätzlichen Kosten erforderlich, da alle Technologien, einschließlich KI in der Cloud, qualifiziertes Personal, Tools und Bedrohungsanalysen, in den Produktkosten enthalten sind.
- **Skalierbarkeit:** Erleichtert die Anpassung an die sich entwickelnde Größe und Komplexität von Unternehmensumgebungen.
- **Management:** Bietet einen systematischen Ansatz zur Erkennung und Reaktion auf Bedrohungen und minimiert so den Verwaltungsaufwand.

★ Anwendungsfall: Automatisierte MDR-Services sind für Unternehmen mit begrenztem Personal/Budget für Cyber-Sicherheit von entscheidender Bedeutung und bieten einen robusten, erschwinglichen Schutz.

## Argumente für WatchGuard MDR

Mit Lösungen wie Advanced EPDR, WatchGuard Orion und WatchGuard ThreatSync für XDR unterstützt WatchGuard MSP beim Aufbau eigener interner SOC und sorgt gleichzeitig für eine hohe Effizienz ihrer Cyber-Sicherheitsteams. Wir ermöglichen automatisiertes MDR mit dem Zero-Trust Application Service und dem Threat Hunting Service in WatchGuard EDR, EPDR und Advanced EPDR.

Mit der Einführung von WatchGuard MDR können unsere MSP-Partner jetzt Services für Managed Detection and Response bereitstellen, um die laufenden Herausforderungen in Bezug auf Kompetenz- und Finanzierunglücken für die Cyber-Sicherheit zu bewältigen.

Mehr als Erkennung und Reaktion: MDR-Anbieter sind langfristige, strategische Geschäftspartner

**MDR wird zu einer Mainstream-Sicherheitsstrategie**

## WatchGuard-Portfolio

### Netzwerksicherheit

WatchGuard bietet eine breite Palette an Netzwerksicherheitslösungen, von Tabletops und 1-HE 19 Zoll Rackmount-Appliances bis hin zu cloudbasierten und virtuellen Firewalls. Unsere Firebox® Appliances bieten wichtige Sicherheitsdienste, von Standard-IPS, URL-Filterung, Gateway-AV, Anwendungskontrolle und Antispam bis hin zu erweiterten Schutzfunktionen wie Datei-Sandboxing, DNS-Filterung und mehr. Dank der leistungsstarken Deep Packet Inspection (DPI) können Sie alle unsere Sicherheitsdienste gegen Angreifer einsetzen, die versuchen, sich hinter verschlüsselten Kanälen wie HTTPS zu verstecken. Außerdem bietet jede Firebox standardmäßig SD-WAN, was die Ausfallsicherheit und Leistung des Netzwerks erhöht.

### Identitätssicherheit

WatchGuard AuthPoint® schließt passwortbasierte Sicherheitslücken mit Multi-Faktor-Authentifizierung auf einer einfach zu bedienenden Cloud-Plattform. 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. AuthPoint bietet ebenfalls eine optimierte Benutzererfahrung mit Online- und Offline-Authentifizierungsmethoden sowie ein Webanwendungsportal für einfachen Single Sign-On-Zugriff.

### Sicheres, cloudverwaltetes WLAN

Die sicheren, cloudverwalteten WLAN-Lösungen von WatchGuard bieten einen sicheren, geschützten Rahmen für WLAN-Umgebungen, ohne dass Sie sich um die Verwaltung kümmern müssen. Gleichzeitig werden die Kosten erheblich gesenkt. Von Heimbüros bis hin zu großflächigen Firmengeländen stellt WatchGuard die WLAN 6-Technologie mit sicherer WPA3-Verschlüsselung bereit. Dank WatchGuard Cloud sind WLAN-Netzwerkkonfiguration und Richtlinienverwaltung, Zero-Touch-Bereitstellung, benutzerdefinierte Captive Portals, VPN-Konfiguration, umfangreiche Interaktionstools, Einblicke in Geschäftsanalysen und Upgrades nur einen Klick entfernt.

### Endpoint-Sicherheit

Mit den Lösungen von WatchGuard Endpoint Security schützen Sie Ihre Geräte vor Cyber-Angriffen. WatchGuard EPDR und Advanced EPDR, unsere erstklassigen KI-gestützten Endpoint-Lösungen, verbessern Ihre Sicherheitslage durch die nahtlose Integration von Endpoint Protection (EPP) mit Funktionen für Detection and Response (EDR) und unseren Zero-Trust Application und Threat Hunting Services. Diese sind alle vollständig in die WatchGuard Cloud und ThreatSync integriert und bieten wertvolle Einblicke und Erkenntnisse, wobei sie gleichzeitig die produktübergreifende Erkennung und Reaktion (XDR) stützen.

## Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. 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 sowie 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.de**.