WatchGuard

MDR-Kaufleitfaden

> So wählen Sie den richtigen Managed Detection and Response Service aus

INHALTSVERZEICHNIS

01 MDR – von Beginn an richtig

Cyberangriffe werden immer schneller, intelligenter und schwieriger zu erkennen. Viele Unternehmen können einfach nicht mehr Schritt halten, weil ihre Zeit, ihre Tools und ihr Personal begrenzt sind. Hier kommt Managed Detection and Response (MDR) ins Spiel.

MDR ist ein Service, der Bedrohungsüberwachung, Reaktionen in Echtzeit und Expertenanalyse rund um die Uhr kombiniert, um Angriffe zu stoppen, bevor sie Schaden anrichten. MDR schließt die Lücken, die herkömmliche Tools hinterlassen.

Aber da viele Anbieter behaupten, dass sie MDR anbieten, kann es schwierig sein, die richtige Wahl zu treffen.

> ***In diesem Leitfaden erhalten Sie die Informationen, die Sie benötigen, um Ihre Optionen klar bewerten und eine Lösung auswählen zu können, die echten Schutz bietet.***

02

So bewerten Sie MDR-Lösungen

Beim Vergleich von MDR-Anbietern ist es wichtig, über die Schlagworte und glänzenden Dashboards hinaus zu schauen. Die folgenden Kriterien sind grundlegend, wenn es darum geht, Bedrohungen zu stoppen und Ihr Unternehmen zu schützen:

1. Abdeckung der gesamten Angriffsfläche

Eine MDR-Lösung muss all die Orte überwachen, die Angreifer ausnutzen könnten, wie Endpoints, Netzwerk, Identitätssysteme oder Anmeldedaten und Cloud-Anwendungen. Viele Bedrohungen beginnen nicht am Endpoint und hören nicht an der Firewall auf. Eine gute MDR-Lösung folgt der Bedrohung, wo auch immer sie sich hinbewegt, und merzt sie frühzeitig aus, bevor echter Schaden angerichtet wird.

2. Antwortgeschwindigkeit

Die Erkennung ist nur der Anfang. Das zählt wirklich: wie schnell ein Anbieter die Bedrohung bestätigen, eindämmen und mit der Behebung beginnen kann. Die Branchendurchschnitte variieren stark, und viele MDR-Anbieter benötigen 30 bis 60 Minuten oder mehr, um zu reagieren.

Top-Performer wie WatchGuard liegen im Durchschnitt unter 10 Minuten, mit einer durchschnittlichen Reaktionszeit (MTTR) von 6 Minuten für kritische Bedrohungen. Diese Zeit macht den Unterschied zwischen einem Schrecken und einem ausgewachsenen Vorfall. Halten Sie Ausschau nach Anbietern, die Folgendes anbieten:

- SLA-gestützte Reaktionszeiten (15 Minuten oder weniger sind überzeugend)
- Automatisierte Eindämmung (Millisekunden, um infizierte Geräte oder Konten zu isolieren)
- Konsistente, reale Leistung (nicht nur Durchschnittswerte, sondern auch Worst-Case-Reaktionszeiten)

Je schneller die Reaktion, desto geringer die Auswirkungen. So einfach ist das.

3. Reduzierung unwichtiger Benachrichtigungen

Zu viele Warnmeldungen = Warnmüdigkeit. Die besten MDR-Anbieter verwenden KI und Menschen, um Fehlalarme angemessen zu bewerten und herauszufiltern, sodass Sie nur die wichtigen Warnungen erhalten. Sie erhalten Action, und nicht nur eine Benachrichtigungsflut. High-Fidelity-Erkennung bedeutet, dass Sie dem vertrauen, was Sie sehen – und Ihr Team konzentriert bleiben kann.

4. Integration mit vorhandenen Tools

Ein starker MDR-Service sollte in Ihre Umgebung passen und nicht dazu führen, dass Sie alles neu aufbauen müssen. Halten Sie Ausschau nach nahtloser Unterstützung für Microsoft 365, AWS, Google Workspace, Ihre Firewalls und andere bereits vorhandene Tools.

Microsoft 365

aws

WatchGuard

> Eine gute MDR-Lösung schützt Sie nicht nur, *sie respektiert auch Ihre Zeit.*

5. Sichtbarkeit und Transparenz

Sie sollten nicht gezwungen sein, Informationen über Ihre eigene Umgebung suchen zu müssen. Halten Sie Ausschau nach einem einzigen, benutzerfreundlichen Portal, das Erkennungen, SOC-Maßnahmen und den Bedrohungsverlauf an einem Ort anzeigt. Ein Pluspunkt ist es, wenn es Ihnen Unterstützung für Compliance-Berichte und Kundenaktualisierungen bietet.

6. Anleitung durch Experten

Sie möchten nicht noch mehr Benachrichtigungen, sondern Antworten. Die besten MDR-Anbieter schließen echte Experten wie Technical Account Manager (TAMs) in ihr Angebot ein, die kontinuierliche Bedrohungseinblicke, Eskalationsunterstützung und strategische Empfehlungen bieten. Sie helfen Ihnen, intelligentere Entscheidungen zu treffen und neuen Risiken immer einen Schritt voraus zu sein.

7. Schnelles Onboarding

Es sollte nicht Wochen dauern, bis ihr Unternehmen geschützt ist. Mit einem starken MDR-Anbieter ist Ihr Unternehmen mit nur minimalen Unterbrechungen, ohne komplizierte Einrichtung und ohne überraschende neue Anforderungen schnell geschützt.

Top-Anbieter bieten ein Onboarding am selben Tag an, insbesondere wenn Sie bereits Tools verwenden, die von diesen Anbietern unterstützt werden (wie Microsoft 365 oder WatchGuard EPDR). Halten Sie Ausschau nach Diensten, die über ein Portal aktiviert werden können, mit klaren Schritten, Automatisierung und Support, falls erforderlich.

Stellen Sie folgende Fragen:

- Wie lange dauert es, bis unser Unternehmen geschützt ist?
- Was müssen wir installieren, konfigurieren oder ändern?
- Können wir zuerst mit einer kleinen Gruppe ein Pilotprojekt oder Tests implementieren?

WatchGuard

03 Fragen, die Sie MDR-Anbietern stellen sollten

Frage	Worauf Sie achten sollten	✓ Gute Antwort	✗ Red Flag
Welche Teile meiner Umgebung überwachen Sie auf Bedrohungen? (Endpoints? Cloud? Firewall?)	Achten Sie auf eine breite Abdeckung über Endpoints, Cloud, Identität und Netzwerk hinweg. Je mehr Angriffsflächen überwacht werden, desto früher können Bedrohungen erkannt werden.	„Wir überwachen Ihre Endpoints, Cloud-Dienste wie Microsoft 365 oder AWS, Ihre Firewall-Aktivitäten und Benutzeridentitätsereignisse. Je mehr wir sehen, desto schneller können wir reagieren.“	„Wir konzentrieren uns hauptsächlich auf Endpoints“ oder „Der Cloud-Support ist begrenzt“. ***Lücken wie diese führen zu „toten Winkeln“, in denen sich Angreifer unentdeckt bewegen können.***
Wie schnell reagieren Sie auf eine kritische Warnung?	Fragen Sie nach tatsächlichen Kennzahlen wie der mittleren Zeit bis zur Reaktion (Mean Time to Response, MTTR) und ob die Reaktion auch die Eindämmung oder nur die Alarmierung umfasst.	„Unsere durchschnittliche Reaktionszeit beträgt weniger als 10 Minuten, wobei viele Maßnahmen in Millisekunden automatisch ergriffen werden. Dies stützen wird durch ein SLA.“	„Wir alarmieren Sie schnell, und dann entscheiden Sie, was zu tun ist.“ ***Das ist kein echtes MDR. Das ist eine reine Warnung mit „Hausaufgaben“.***
Welche Maßnahmen ergreifen Sie automatisch? Was muss ich erledigen?	Sie sollten nach einer automatisierten Eindämmung (wie das Isolieren von Geräten, das Deaktivieren von Konten) Ausschau halten, wobei Sie die klare Option haben sollten, weiter beteiligt zu sein, wenn Sie dies möchten.	„Wir isolieren automatisch Endpoints, beenden bösartige Prozesse, blockieren IPs und deaktivieren kompromittierte Konten. Sie können sich entscheiden: Bleiben Sie selber aktiv, oder lassen Sie unser SOC die Führung übernehmen.“	„Wir benachrichtigen Sie und geben Ihnen Anweisungen.“ ***Das bedeutet, dass Sie die Behebung immer noch selbst durchführen müssen, insbesondere außerhalb der Geschäftszeiten.***
Wie hoch ist Ihre Fehlalarmrate?	Niedrige Fehlalarmrate = weniger Warnmüdigkeit und mehr Vertrauen. Fragen Sie nach bestimmten Daten und geben Sie sich nicht mit vagen Behauptungen zufrieden.	„Dank KI-Filterung und menschlicher Expertise haben wir im Durchschnitt weniger als einen Fehlalarm pro Kunde und Monat.“	„Das hängt von Ihrer Umgebung ab.“ ***Wenn der Anbieter dies nicht quantifizieren kann, gehen Sie von einer hohen Falschmeldungsrate aus.***
Kann ich alle Vorfälle an einem Ort sehen?	Ein einheitliches Portal ist ein Muss. Es sollte erkannte Bedrohungen, SOC-Maßnahmen und den Untersuchungsverlauf in Echtzeit anzeigen.	„Ja, Sie erhalten ein einziges Portal mit vollständiger Transparenz über alle Vorfälle, SOC-Maßnahmen, Metriken und Berichte.“	„Wir senden Ihnen Berichte per E-Mail“ oder „Sie können über mehrere Dashboards auf Ihre Daten zugreifen.“ ***Dies ist ineffizient und schwieriger zu verwalten.***
Bieten Sie Analysen zu Vorfallreaktionen und Grundursachen an?	Sie möchten wissen, was passiert ist, wie es passiert ist und was zu beheben ist – und nicht nur, dass „etwas blockiert wurde“.	„Ja, wir bieten eine vollständige Reaktion auf Vorfälle mit Ursachenanalyse und Empfehlungen, wie sich künftige Angriffe verhindern lassen.“	"Wir isolieren nur die Bedrohung und machen dann weiter." ***Das macht Ihr Unternehmen anfällig für wiederholte Vorfälle.***
Was ist in den Preisen enthalten? Fallen zusätzliche Gebühren für Eindämmung oder Berichte an?	Die Preisgestaltung sollte transparent sein, und es sollten keine überraschenden Gebühren für Kernfunktionen wie Eindämmung, Vorfallsberichte oder grundlegende Integrationen anfallen.	„Alle Eindämmungsmaßnahmen, SOC-Reaktionen und monatlichen Berichte sind enthalten. Es fallen keine zusätzlichen Gebühren an, es sei denn, Sie fügen Dienstleistungen wie Compliance-Audits hinzu.“	„Das ist Teil unseres Tarifs auf höherer Ebene“ oder „Eindämmung ist als Add-on verfügbar.“ ***Achten Sie auf Dinge, die als Upsell angeboten werden, aber eigentlich enthalten sein sollten.***

04 So bewerten Sie Rentabilität und Wert

MDR ist nicht einfach nur ein Sicherheitsupgrade – es ist eine Geschäftsinvestition.

> So -evaluieren Sie den Wert:

Risikominderung

Wie sehr verringert MDR die Wahrscheinlichkeit eines kostspieligen Vorfalls wie Ransomware?

Mitarbeitereffizienz

Lässt sich damit die Einstellung eines rund um die Uhr verfügbaren Sicherheitsteams vermeiden (das mindestens 6–7 Vollzeitkräfte erfordert)?

Zeitersparnis

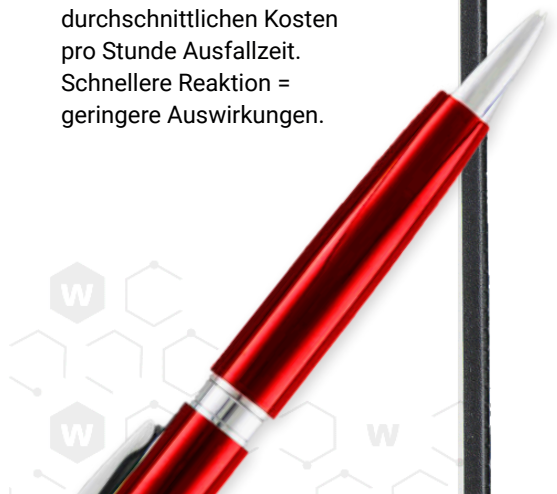
Wie viel Zeit spart Ihr Team, wenn es sich nicht mehr mit Falschmeldungen beschäftigen oder mehrere Tools verwalten muss?

Vermiedene Kosten für Ausfallzeiten

Berücksichtigen Sie die durchschnittlichen Kosten pro Stunde Ausfallzeit. Schnellere Reaktion = geringere Auswirkungen.

Compliance-Ausrichtung

Bietet der Service Berichte für Cyberversicherungen oder -vorschriften?



> Unverzichtbare Funktionen:

- 24/7-Überwachung durch ein echtes SOC-Team
- Abdeckung der gesamten Umgebung
- Schnelle, automatisierte Bedrohungseindämmung
- Niedrige Fehlalarmrate (idealerweise < 1/Monat)
- KI/ML zum Erkennen und Auffinden von Anomalien in der Umgebung und der Reaktion darauf
- Einheitliche Ansicht über Sicherheitsebenen hinweg
- Von Menschen durchgeführte Ermittlungen und Threat Hunting
- Unterstützung für Ihre bestehende Umgebung (z. B. Microsoft 365)
- Schnelles Onboarding

> Wünschenswert (aber nicht kritisch):

- Benutzerdefinierte Dashboards
- Anpassung und Alarmregeln als Selfservice
- Optionale Add-ons wie Phishing-Simulationen oder Schulungsmodule

WatchGuard

05 Welche Rolle spielen KI und maschinelles Lernen wirklich bei MDR?

Die meisten MDR-Anbieter sagen, dass sie KI verwenden – und das ist nicht nur ein Schlagwort. In der heutigen Bedrohungslandschaft benötigen Sie KI und maschinelles Lernen, um Schritt zu halten.

Angreifer gehen äußerst schnell vor und nutzen oft Automatisierung und KI, um groß angelegte Phishing-Kampagnen zu starten, Malware im Handumdrehen zu verändern oder sich unter normal erscheinendem Verhalten zu verstecken. Menschliche Analysten allein können nicht jede Bedrohung erkennen oder schnell genug reagieren, besonders nicht mitten in der Nacht. Hier kommt KI ins Spiel.

KI ermöglicht eine schnellere Erkennung, intelligentere Priorisierung und Reaktionen in Echtzeit. KI filtert unwichtige Benachrichtigungen heraus, weist auf Anomalien hin und handelt in Millisekunden, damit sich Ihr Team auf das Wesentliche konzentrieren kann.

Hierauf sollten Sie bei der Bewertung von KI in MDR achten:

> **KI, die unwichtige Benachrichtigungen filtert**
KI sollte Fehlalarme reduzieren und nicht zu noch mehr Warnmeldungen führen. Halten Sie nach Lösungen Ausschau, die Aktivitäten mit geringem Risiko automatisch herausfiltern und ermöglichen, dass sich Analysten nur auf die wichtigen Bedrohungen konzentrieren können.

> **KI, die nicht nur beobachtet, sondern auch handelt**
Die beste KI-gestützte MDR-Lösung beschränkt sich nicht auf die Erkennung. Sie reagiert automatisch, indem sie Hosts isoliert, schädliche IP-Adressen blockiert und kompromittierte Konten deaktiviert. In vielen Fällen greift sie ein, bevor überhaupt ein Mensch hinzugezogen werden muss.

> **KI, die im Laufe der Zeit lernt**
Wird das System intelligenter, je mehr Bedrohungen es verarbeitet? Fragen Sie nach, ob die KI vergangene Vorfälle nutzt, um die Genauigkeit bei künftigen Vorfällen zu verbessern – insbesondere bei der Erkennung von heimlichen oder dateilosen Angriffen.

> **KI, die mit Menschen arbeitet, und nicht an ihrer Stelle**
KI ist großartig, wenn es um Geschwindigkeit und Skalierbarkeit geht. Menschliche Threat Hunter sind großartig, wenn es um Kontext und Nuancen geht. Die besten MDR-Lösungen kombinieren beides, um schnellere und genauere Entscheidungen zu treffen.

06 Ist MDR für Ihr Unternehmen das Richtige? Wichtige Überlegungen:

1. Verfügen Sie über das Personal, das die Sicherheit rund um die Uhr überwacht?

Die meisten kleinen und mittleren Unternehmen haben solches Personal nicht. MDR bietet Ihnen ein Security Operations Center (SOC), das rund um die Uhr verfügbar ist – so entfallen die Kosten für die Einstellung und Bindung eines Analystenteams. Sie würden 6–8 Mitarbeitende in Vollzeit benötigen, um all dies selbst zu tun. Und hierbei sind Tools, Schulungen und Burnout nicht berücksichtigt.

2. Müssen Sie Compliance- oder Versicherungsanforderungen erfüllen?

Für viele Branchen (Gesundheitswesen, Finanzen, Bildung) ist eine Überwachung und Reaktion auf Vorfälle rund um die Uhr zwingend erforderlich. Außerdem verlangen Cyberversicherer MDR zunehmend als Bedingung für die Versicherungsabdeckung.

MDR bietet die Dokumentation und Reaktion in Echtzeit, die erforderlich sind, um diese Anforderungen zu erfüllen und im Ernstfall entsprechende Beweise zu liefern.

3. Wie könnten Sie erkennen, dass Sie genau jetzt einem Angriff ausgesetzt sind?

Kann Ihr Team einen Ransomware-Versuch, eine Cloud-Kompromittierung oder einen Diebstahl von Zugangsdaten innerhalb von Minuten erkennen und darauf reagieren? Wenn die Antwort lautet: „Wir würden es wahrscheinlich zu spät herausfinden“, kann MDR diese Lücke schließen.

4. Sie werden von Warnmeldungen überflutet, oder erhalten gar keine?

Wenn Sie:

- von Warnmeldungen ohne Kontext überwältigt werden,
- sich auf Tools wie Antivirus- oder Firewall-Protokolle ohne echte Analyse verlassen,
- überhaupt keine Warnmeldungen erhalten,

dann gehen Ihnen Bedrohungen entweder durch die Lappen, oder Sie verschwenden Ihre Zeit mit Falschmeldungen. MDR liefert High-Fidelity-Warnmeldungen und die Reaktion darauf, und nicht nur Protokolle.

5. Können Sie es sich finanziell leisten, nichts zu tun?

Ausfallzeiten, Datenverlust, Lösegeldzahlungen, Compliance-Bußgelder und Reputationsschäden kosten mehr als MDR.

Laut dem Cybersicherheitsbericht von Microsoft für KMUs im Jahr 2024 belaufen sich die durchschnittlichen Gesamtkosten pro Cyberangriff auf rund 250.000 USD, schwerere Vorfälle können jedoch bis zu 7 Millionen USD kosten.

6. Haben Sie bereits in Sicherheitstools investiert, die Sie nicht umfassend nutzen?

Vielleicht haben Sie Microsoft 365, Defender, eine Firewall oder EDR. Aber wenn niemand diese Tools aktiv überwacht, Signale korreliert oder in Echtzeit reagiert, haben Sie zwar die Tools, aber keinen Schutz.

Mit MDR funktionieren diese Tools intelligenter, weil MDR die Signale erkennt und Maßnahmen ergreift.

7. Was passiert, wenn es um 2 Uhr morgens zu einem Vorfall kommt?

Haben Sie einen Plan? Jemanden in Bereitschaft? Oder hoffen Sie einfach, dass schon nichts Schlimmes passiert, während alle schlafen?

Die meisten Angriffe scheren sich nicht um Geschäftszeiten, und wenn niemand das Geschehen aktiv überwacht und bereit ist zu reagieren, können wenige Minuten zu einem großen Schaden führen.

MDR ist nicht nur eine Versicherung: Es ist eine Versicherung mit Action. Wenn eine Bedrohung eintritt, reagiert MDR in Echtzeit, um sie einzudämmen, die Auswirkungen zu minimieren und den Betrieb Ihres Unternehmens aufrechtzuerhalten. Selbst wenn Sie schlafen.

07

Warum Tools allein nicht ausreichen

Möglicherweise verfügen Sie bereits über solide Sicherheitstools wie Antivirus, EDR, Firewalls und sogar MFA. Vielleicht haben Sie in Benutzerschulungen oder Protokollverwaltung investiert. Die Wahrheit ist jedoch, dass kein Tool alleine jede Bedrohung erkennen, darauf reagieren und sie stoppen kann.

Während die meisten Tools gute Arbeit leisten, funktionieren sie in der Regel nur in ihrem jeweiligen Bereich gut. Und Angreifer wissen, wie sie sich unentdeckt zwischen diesen Bereichen bewegen können. MDR ersetzt Ihre Tools nicht, sondern verbindet sie, stärkt sie und füllt die kritischen Lücken, die sie zurücklassen. ***Hier ist eine Erläuterung dazu, was gängige Sicherheitstools tun, woran es ihnen mangelt und wie MDR dort weitermacht, wo sie aufhören:***

Tools	Funktionsweise	Mangel	So füllt MDR die Lücke
Antivirus	Blockiert bekannte Malware basierend auf Signaturen.	Erkennt dateilose Angriffe, Zero-Day-Angriffe oder alles, was ihm nicht „bekannt“ ist, nicht. Kann nicht reagieren, falls Malware „durchrutscht“.	MDR nutzt verhaltensbasierte Erkennung und kann Bedrohungen eindämmen, auch wenn sie brandneu oder unbekannt sind.
EDR (Endpoint Detection & Response)	Erkennt verdächtige Aktivitäten auf Endpoints (z. B. abnormales Verhalten, bösartige Skripte).	Generiert Warnmeldungen, erfordert jedoch häufig, dass Ihr Team Nachforschungen anstellt und Maßnahmen ergreift. Keine Überwachung oder Priorisierung durch Menschen.	MDR analysiert, priorisiert und reagiert auf Endpoint-Bedrohungen, indem Geräte automatisch isoliert und Prozesse beendet werden.
Firewall	Blockiert oder filtert den Datenverkehr zwischen Ihrem Netzwerk und der Außenwelt.	Kann interne Bedrohungen oder laterale Bewegungen nicht erkennen. Kann infizierte Endpoints oder Benutzer nicht isolieren.	MDR überwacht die internen Aktivitäten und laterale Bewegungen und fängt Bedrohungen auch dann ab, wenn sie den Perimeter bereits durchbrochen haben.
MFA (Multi-Faktor-Authentifizierung)	Erweitert den Schutz bei der Anmeldung um eine zweite Form der Identitätsüberprüfung.	Erkennt nicht, ob eine Sitzung gekapert wurde oder ob Anmeldedaten in einer SaaS-App wiederverwendet werden. Kann einen Angreifer nicht aufhalten, sobald er eingedrungen ist.	MDR erkennt anomales Anmeldeverhalten, z. B. Zugriff von ungewöhnlichen Standorten, und kann kompromittierte Konten deaktivieren.
Cloud-Überwachung	Protokolliert Kontoaktivitäten, Berechtigungsänderungen und Anmeldeereignisse.	Große Mengen an Warnmeldungen, sehr wenig Kontext. Blockiert Angriffe nicht aktiv oder setzt Anmeldedaten nicht zurück.	MDR überwacht Microsoft 365, AWS, Google Workspace und mehr und widerruft bei Bedarf automatisch den Zugriff oder sperrt Konten.
Schulungen zur Benutzersensibilisierung	Schult Mitarbeitende darin, Phishing und riskantes Verhalten zu erkennen.	Trotzdem sind sie oft verleitet und klicken einfach. Es braucht nur einen Fehler. Schulungen können keine aktiven Angriffe stoppen.	MDR geht davon aus, dass Fehler passieren, und reagiert sofort, wenn sie passieren.
SIEM/Protokollverwaltung	Speichert Protokolle für Analyse und Compliance an einem zentralen Ort.	Erfordert Feinabstimmung, Interpretation und engagierte Analysten, um die Daten zu verstehen.	MDR automatisiert die Analyse, deckt echte Bedrohungen auf und ergreift Maßnahmen, ohne dass eine Feinabstimmung oder das Durchforsten von Protokollen erforderlich ist.
Backup/DR	Hilft bei der Wiederherstellung nach einer Sicherheitsverletzung oder einem Ransomware-Ereignis.	Verhindert Angriffe nicht oder verringert ihre Auswirkungen nicht. Die Wiederherstellung kann Tage dauern.	MDR hilft, Angriffe frühzeitig zu stoppen, sodass Sie nie eine Wiederherstellung aus dem Backup benötigen.

Kurzer Überblick über WatchGuard MDR

WatchGuard MDR bietet Ihnen rund um die Uhr Bedrohungsüberwachung, schnelle Reaktionen und kompetente Anleitung in puncto Sicherheit – bereitgestellt durch Ihren vertrauenswürdigen IT-Anbieter. MDR schützt Ihre gesamte Umgebung, einschließlich Endpoints, Firewalls, Benutzeridentitäten und Cloud-Plattformen wie Microsoft 365 und AWS.

Und das ist nicht einfach nur ein Strom an Warnmeldungen. Wenn etwas schief geht, ergreift der Dienst Sofortmaßnahmen, um die Bedrohung einzudämmen. Die meisten kritischen Bedrohungen werden in weniger als 6 Minuten behandelt, mit weniger als einer Falschmeldung pro Monat. Für Ihr Unternehmen bedeutet das weniger unwichtige Benachrichtigungen, eine schnellere Lösung und stärkeren Schutz.

Sie bleiben über ein einziges Portal auf dem Laufenden, in dem Sie und Ihr Anbieter Warnungen, Fallaktivitäten und Reaktionsmaßnahmen in Echtzeit sehen können. Sie profitieren außerdem von der Beratung durch Sicherheitsexperten von WatchGuard und arbeiten dennoch direkt mit dem Partner zusammen, den Sie kennen und dem Sie vertrauen.

Ihr Partner bleibt Ihr Hauptansprechpartner. Ihr Partner ist für die Servicebeziehung verantwortlich und stellt sicher, dass alles zu Ihrer Umgebung und Ihren Geschäftszielen passt. WatchGuard bietet die Technologie und die Reaktion auf Bedrohungen – aber Ihr Anbieter ist derjenige, der die Strategie leitet.

Informationen zu WatchGuard

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.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB www.watchguard.de