infinigate | WatchGuard

MDR Spickzettel

Leistungsstarke Funktionen mit WatchGuard MDR

Bedrohungsüberwachung und -bekämpfung rund um die Uhr

Mit Automatisierung und menschlicher Expertise untersucht ein globales SOC Warnungen, bestätigt deren Echtheit und reagiert innerhalb weniger Minuten.

Proaktive Bedrohungsanalyse und schnelle Eindämmung

Analysten identifizieren versteckte oder neu auftretende Bedrohungen, die von Tools möglicherweise übersehen werden, und isolieren und stoppen dann schnell bestätigte Angriffe, um eine Ausbreitung und wiederholte Vorfälle zu verhindern.

Schnelle Einführung und unkomplizierte Skalierbarkeit

Sie können den Schutz innerhalb weniger Stunden aktivieren und ihn für hybride Umgebungen oder für mehrere Tools skalieren.

Einheitliches Portal

Das zentrale Portal für Managed Services von WatchGuard bietet Einblicke in Echtzeit, Zeitleisten zu Incidents sowie Schutznachweise für Compliance- und Cybersecurity-Anforderungen.

Technischer Kundenbetreuer (Technical Account Manager, TAM)

Ein Experte, der SOC-Aktivitäten interpretiert, regelmäßige Sicherheitsprüfungen durchführt und Ihnen dabei hilft, Stakeholdern den Mehrwert aufzuzeigen.

WatchGuard Managed Detection and Response (MDR) ist ein vollständig verwalteter Service, der alle Bestandteile Ihrer IT-Umgebung schützt: die Geräte, die Benutzerkonten, die Cloudanwendungen und den Datenverkehr dazwischen. Statt überflüssige Warnungen auszulösen, filtert er unnötige Daten heraus, untersucht Bedrohungen und bekämpft sie in Ihrem Auftrag.

Die Unified Security Platform von WatchGuard unterstützt diesen Rund-um-die-Uhr-Schutz. Dadurch kommt jedes Signal an, ist jede Reaktion schneller und wird jede Aktion an einem zentralen Ort angezeigt. Erkennung alleine genügt nicht, die Reaktion ist wichtig.

WatchGuard MDR kombiniert KI und Expertenreaktion, um Bedrohungen in den Bereichen Endpunkte, Netzwerk, Identität und Cloud über eine einheitliche Plattform hinweg zu erkennen, zu untersuchen und zu stoppen. MDR kann nicht nur Warnmeldungen aussprechen. Es kombiniert kontinuierliche Überwachung, Untersuchungen durch Experten und reale Reaktionen auf Bedrohungen in einem Service. MDR zeigt Ihnen keine Warnmeldungen, mit denen Sie alleine fertig werden müssen, sondern validiert die Bedrohungen und ergreift Maßnahmen zu ihrer Bekämpfung – Tag und Nacht.

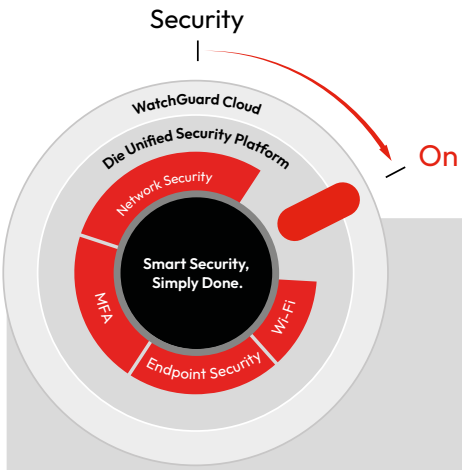
WatchGuard MDR bietet rund um die Uhr für alle Geräte, Benutzeridentitäten, Cloud-Services und Netzwerke übergreifende Überwachung, Untersuchung und Bedrohungsbekämpfung in Echtzeit. Durch die Zusammenarbeit von KI und menschlichen Analysten werden unnötige Daten beseitigt, Angriffe schnell unterbunden und auf einer zentralen Plattform volle Transparenz und Klarheit beim Reporting geschaffen. WatchGuard MDR nutzt eine zentrale Plattform für Endpunkte, Identitäten, die Cloud und Netzwerkaktivitäten. Alle Daten werden an einem Ort angezeigt. Die Plattform von WatchGuard erleichtert die Bereitstellung, vereinfacht die Betriebsabläufe und verbessert die Abdeckung der Angriffsflächen. Dadurch werden die Kosten gesenkt, Risiken minimiert und hochkomplexe Angriffe schnell abgewehrt.

Die Leistungsfähigkeit von MDR auf vorhandene Tools ausweiten

WatchGuard Open MDR bietet Managed Detection and Response auf Enterprise-Niveau, das mit bestehenden Sicherheitsinvestitionen funktioniert. Der MDR-Dienst lässt sich in unterstützte Sicherheitstools von Drittanbietern und WatchGuard integrieren, um den Schutz auf Endpoint-, Identitäts-, Netzwerk- und Cloud-Umgebungen zu erweitern.

Durch die Kombination von Automatisierung, menschlicher Bedrohungssuche und 24/7 SOC-Überwachung identifiziert Open MDR Bedrohungen schnell, validiert verdächtige Aktivitäten und ergreift Sofortmaßnahmen, um sie einzudämmen. Kontinuierliche Überwachung und koordinierte Reaktion stärken die Verteidigung und rationalisieren das Sicherheitsmanagement, ohne bestehende Systeme zu stören.

infinigate | WatchGuard



Zum Vergleich

Eigenständiger SOC-Aufbau

- Hoher Initialaufwand für Tools, Plattformen und Integrationen
- 24x7 Betrieb erfordert Schichtmodelle und spezialisiertes Fachpersonal
- Hohe Fixkosten für Personal, Training, Playbooks und Betrieb
- Know how und Threat Intelligence müssen selbst aufgebaut und gepflegt werden
- Lange Time-to-Value, bis ein SOC effektiv arbeitet
- SkalierungSkalierung bei steigenden Events oder neuen Use Cases ist komplex

WatchGuard MDR

- Sofort einsatzbereit
- 24x7x365 Monitoring durch globale SOC-Analysten
- Technischer Kundenbetreuer
- Vorkonfigurierte Use Cases, Playbooks und Automatisierung
- Klare SLAs für Eskalation
- Planbare Kosten statt hoher Investitionen
- Nahtlose Integration in die Unified Security
- Ideal als SOC-Ersatz oder SOC-Erweiterung

Offene Fragen

- Verfügt Ihr Unternehmen über ein eigenes SOC – oder fehlt es an Zeit, Budget oder Fachpersonal?
- Wer überwacht aktuell sicherheitsrelevante Logs außerhalb der Geschäftszeiten?
- Wie hoch ist die False-Positive-Rate Ihrer aktuellen Sicherheitslösungen?
- Werden Security Events heute priorisiert oder lediglich gesammelt?
- Wie schnell werden kritische Incidents erkannt und eskaliert?
- Gibt es definierte Reaktionszeiten für Sicherheitsvorfälle?
- Nutzen Sie bereits WatchGuard Firewalls, Endpoint Lösungen oder Identity Management?
- Besteht Bedarf an 24x7-Monitoring ohne Aufbau eines eigenen SOCs?
- Müssen mehrere Standorte oder Kundenumgebungen zentral überwacht werden?
- Gibt es Anforderungen an Compliance, Reporting oder Audits (z. B. NIS2, ISO 27001)?

Sie haben Fragen zu WatchGuard MDR?

Unser Experte kennt die Antworten.

Florian Fabbro
Business Development Manager
T +49 40 237301 244
M +49 170 5587885
E Florian.Fabbro@infinigate.de

Weiterführende Informationen zu WatchGuard

Jetzt informieren

https://www.infinigate.com/de/hersteller/watchguard/

Alle Trainings, Termine & Webinare

Jetzt ansehen

https://qrco.de/INF-WatchGuard-Events

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

+49 89 89048-553
watchguard@infinigate.de
www.infinigate.de

infinigate
spark your growth