DATENBLATT

WatchGuard CORE MDR

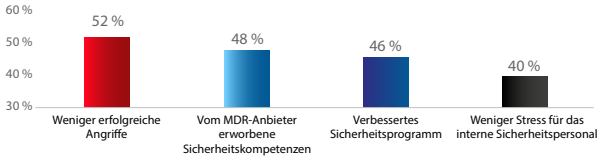
Mehr Möglichkeiten für unsere Partner mit WatchGuard SOC-Know-how

Das Potenzial von MDR ausschöpfen

Mit der Weiterentwicklung des Bedrohungsumfelds stehen Unternehmen vor dem Problem komplexer Sicherheitsherausforderungen in Kombination mit einem Mangel an Cyber-Sicherheitsexperten. Es fehlen Ressourcen und Zeit, um die Cyber-Sicherheit erfolgreich in den Griff zu bekommen. Zur Lösung dieser Probleme lagern Unternehmen den Cyber-Sicherheitsbetrieb an Managed Security Provider (MSP) aus.

Der Betrieb von Security Operations Centern (SOC) setzt jedoch qualifiziertes Personal und hohe Investitionen voraus, was MSP vor Probleme bei der Bereitstellung von Managed Detection and Response (MDR) stellt. Damit Partner diese Hürden überwinden können, führt WatchGuard seine Lösung WatchGuard Core MDR ein. Partner, die unseren umfassenden Erkennungs- und Reaktionsservice in ihr Portfolio aufnehmen, erfüllen die Erfordernisse ihrer Kunden, ohne ein eigenes SOC aufbauen zu müssen, und schließen so die Kompetenz- und Finanzierunglücke für die Cyber-Sicherheit.

Vorteile durch MDR für Mittelstandsunternehmen[2]



Im Team mit unseren Cyber-Experten erstklassige MDR bereitstellen

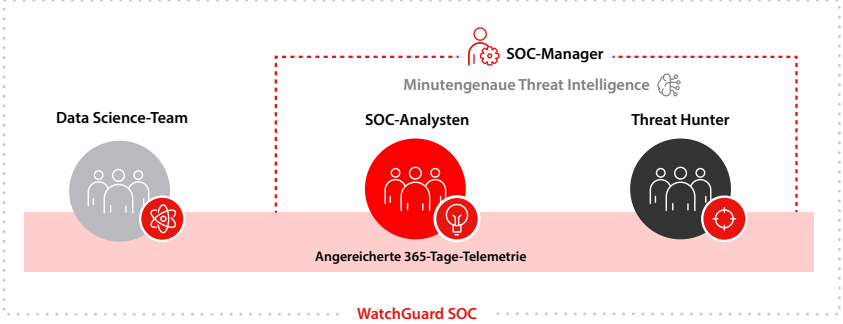
Ein qualifiziertes Team von WatchGuard-Cybersicherheitsexperten schützt die Endpoints und Office 365-Instanzen Ihrer Kunden rund um die Uhr mit Aktivitätsüberwachung, Bedrohungssuche, Erkennung, Untersuchung und optional auch mit selektiver und maßgeschneiderter Eindämmung für jeden Kunden.

Im Falle eines Cyberangriffs führt Sie das Team durch den Reaktionsprozess, um Bedrohungen zu stoppen und zu beheben. Für zusätzlichen Komfort und zur Minimierung der Reaktionszeit können Sie die Eindämmung auch standardmäßig an das SOC delegieren – entweder rund um die Uhr oder außerhalb Ihrer Geschäftszeiten.

Im Rahmen des Service-Onboarding bewertet unser Team außerdem die Angriffsfläche an den Endpoints und verbessert so unmittelbar ihre Sicherheit und die allgemeine Resilienz gegenüber Cyber-Bedrohungen.

WatchGuard Core MDR unterstützt Sie mit automatisch gelieferten regelmäßigen Berichten über die Service-Aktivitäten und den Sicherheitsstatus, die Ihnen helfen, präventive und die Angriffsfläche reduzierende Services anzubieten.

Unser Expertenteam von WatchGuard SOC transformiert die Endpoint-Überwachung und die 365-Tage-Telemetrie in verwertbare Sicherheitsanalysen, die durch branchenführendes, verlässliches maschinelles Lernen/KI und minutengenaue Threat Intelligence rund um die Uhr ergänzt werden.



AUF einen Blick

Profitieren Sie von der Leistungsstärke proaktiver Cyber-Sicherheit und verlassen Sie sich für den Schutz Ihrer Kunden auf kompetente Sicherheitsexperten. Vorteile von WatchGuard Core MDR:

- 100 % MDR für Partner – 100 % der Zeit
- Service-Onboarding zur Minimierung der Endpoint-Angriffsfläche
- Kontinuierliche Endpoint- und Microsoft 365-Aktivitätsüberwachung
- 365-Tage-Telemetrieaufbewahrung in der Cloud
- Proaktive Verfolgung, Verhaltenserkennung und Untersuchung rund um die Uhr
- Sofortbenachrichtigung des bevorzugten Ansprechpartners per E-Mail oder Telefon bei Vorfällen
- Ausführliche Angriffsberichte nach dem MITRE ATT&CK-Framework
- Kundenspezifische Playbooks, die auf die betrieblichen Anforderungen zugeschnitten sind, rund um die Uhr oder zu Geschäftszeiten
- Vom Kunden festgelegte, automatisierte Regeln zur Eindämmung speziell für jeden Endpoint
- Minderungs- und Behebungsleitlinien
- Fortlaufende Bewertung der Angriffsfläche
- Wöchentliche Berichte zum Endpoint-Status
- Wiederkehrende Berichte zu Office 365-Verteidigungszielen

[2] What security teams want from MDR providers ESG, Mai 2023.

Vorteile für MSPs

- Erweitern Sie Ihr Managed Security Service Portfolio mit Ihren MDR-Angeboten und eigenem Logo
- Greifen Sie auf ein modernes SOC zu, ohne Ihr eigenes zu erstellen – ohne große Investitionen
- Erweitern Sie Ihr Team um qualifizierte Cybersicherheitsexperten
- Geben Sie Ihren Kunden Sicherheit durch Überwachung, Erkennung und Reaktion rund um die Uhr
- Flexibler, jederzeit verfügbarer MDR-Service für den Betrieb rund um die Uhr oder zu Geschäftszeiten – skalieren Sie den Service in Ihrem eigenen Tempo
- Passen Sie Playbooks an die Bedürfnisse jedes Kunden an
- Schnelle und einfache Bereitstellung, insbesondere mit WatchGuard Advanced Endpoint Security

Vorteile für Ihre Kunden

- Komplexe Bedrohungen werden proaktiv mit Überwachung rund um die Uhr gestoppt
- Die Erkennung, Untersuchung und schnelle Reaktion auf Vorfälle erfolgt durch qualifizierte Cybersicherheitsexperten
- Der Schutz kann ausgeweitet werden, wenn sich Bedrohungen weiterentwickeln und das Unternehmen wächst
- Vollständiger Einblick in Angriffsflächen, um die Sicherheit zu stärken
- Bessere Einhaltung proaktiver Schutzmaßnahmen
- Kostengünstige Sicherheit ohne internes SOC
- Ihr langjähriger Anbieter kümmert sich um die Konsolidierungsstrategie, damit kein Wechsel zu einem neuen Partner erforderlich ist

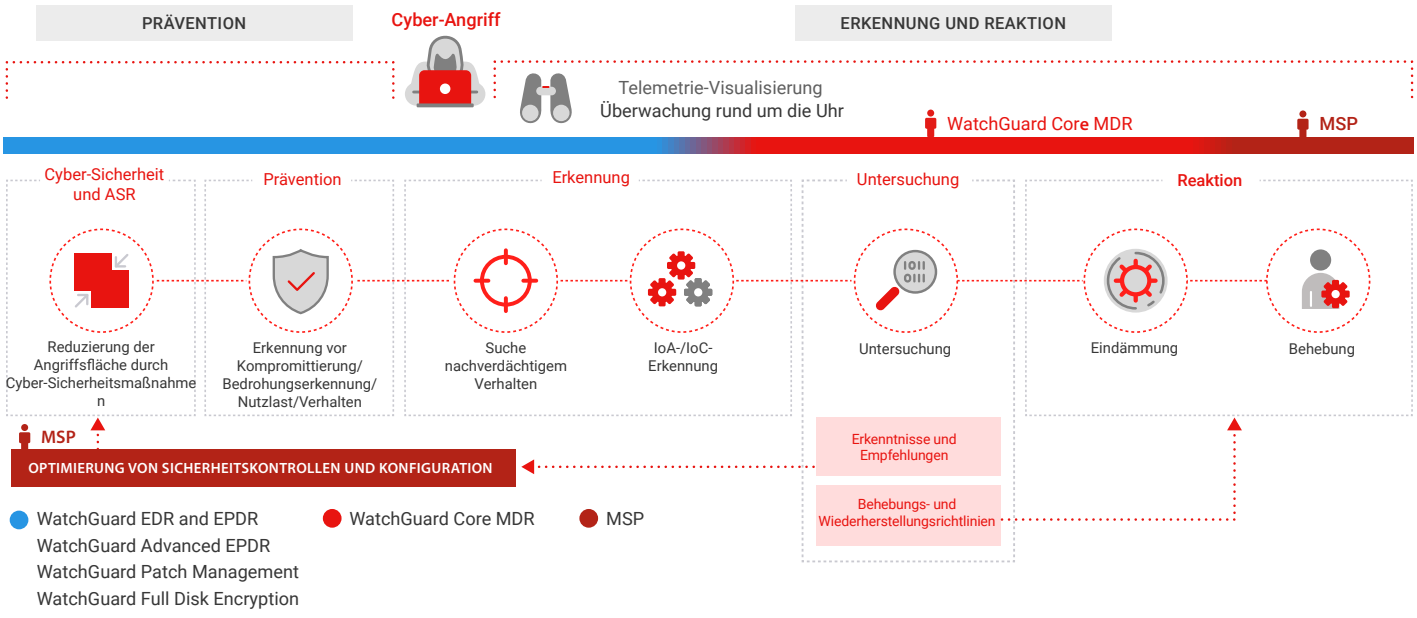
Die Leistungsstärke effizienter Prävention, Verfolgung, Erkennung und Reaktion

Wenn Sie die Cyber-Sicherheitslage für Ihre Kunden verbessern möchten, sollten Sie unbedingt der Kombination aus Prävention und Reduzierung der Angriffsfläche mit einer proaktiven Erkennung und Reaktion Priorität einräumen. Diese Sicherheitsstrategien sind sämtlich miteinander verknüpft. Die Prävention minimiert Vorfälle und die damit verbundenen Kosten. Erkennung und Reaktion eliminieren Bedrohungen, die es schaffen, die Präventionsstufe zu überwinden, und minimieren die Zeit, die bis zu ihrer Erkennung und der Reaktion darauf verstreicht. So senken Sie insgesamt die Sicherheitskosten.

WatchGuard Core MDR sorgt für maximale automatisierte Bedrohungsprävention, Erkennung und Reaktion und nutzt dazu WatchGuard EDR, EPDR oder Advanced EPDR mit den zugehörigen Managed Services. Der Zero-Trust Application Service minimiert eigenständig die Angriffsfläche für Malware. Das verbessert die Sicherheitslage und erlaubt die skalierbare Erkennung und Reaktion.

Mit dem Threat Hunting Service untersuchen qualifizierte Cybersicherheitsanalysten IoA und schwache Anzeichen, um komplexe Cyberangriffe zu erkennen. Der Service überprüft fortlaufend die Sicherheitslage, um Konfiguration und Angriffsfläche zu bewerten. Unsere Cyber-Sicherheitsanalysten stellen Leitlinien zur Minimierung der Endpoint-Angriffsfläche, zur Verbesserung der Sicherheitskontrollen und zur genauen Abstimmung der Einstellungen bereit und empfehlen das frühzeitige Patchen.

Mit der Kombination aus reduzierter Angriffsfläche, Prävention und effektiven Erkennungs- und Reaktionsstrategien eröffnen WatchGuard EDR, EPDR oder Advanced EPDR und WatchGuard MDR MSP mit einem robusten Framework für die Cyber-Sicherheit neue Möglichkeiten.



Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.com/de WatchGuard Technologies, Inc.