



WatchGuard Endpoint Security-Module

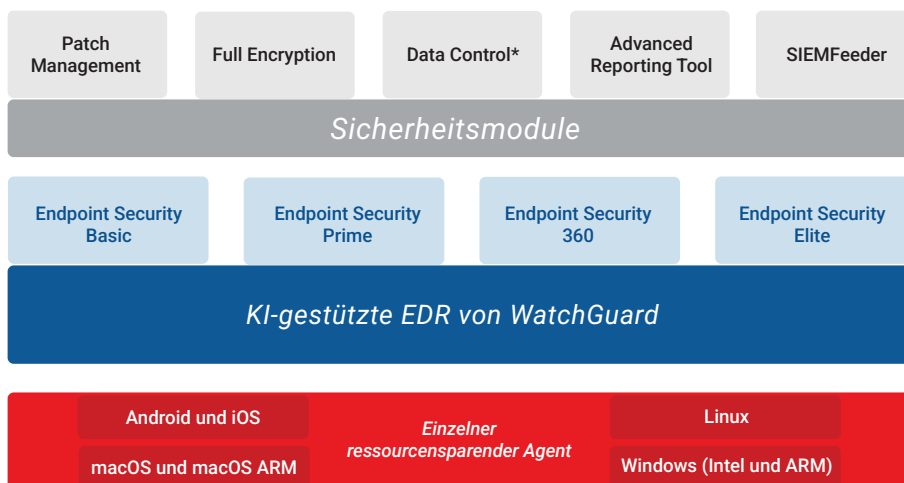
Analysen als Schlüssel zum Vorbeugen von Cyberangriffen

Erweitertes Sicherheitsrisikomanagement und Transparenz

Die heutige Bedrohungslandschaft ist ausgefeilter denn je, und Sicherheitsteams sind zunehmendem Druck ausgesetzt, mit begrenzter Zeit und begrenzten Ressourcen mehr zu leisten. Die WatchGuard Endpoint Security-Module erweitern den Schutz, die Transparenz und die Kontrolle in Ihrer Umgebung durch Funktionen, die automatisiertes Patchen, Verschlüsselung, Überwachung sensibler Daten, erweiterte Berichterstellung und SIEM-Integration ermöglichen. Gemeinsam helfen sie Unternehmen, die Sicherheit zu stärken, das Management zu vereinfachen und die betriebliche Komplexität zu reduzieren, ohne unnötigen Aufwand zu verursachen.

Wie hilft Ihnen WatchGuard dabei, diese Herausforderung zu meistern?

Die WatchGuard Endpoint Security-Lösungen bieten KI-gestützte EDR, die fortgeschrittene Cyberangriffe verhindert, solche erkennt und darauf reagiert – mit Funktionen, die von grundlegendem Schutz bis hin zu erweiterten Untersuchungen reichen. Integrierte Module für das Patch-Management, den Schutz sensibler Daten, die Verschlüsselung von Festplatten und USB-Laufwerken sowie Erkenntnissen aus Sicherheitsanalysen: All dies wird über einen einzigen ressourcensparenden Agenten bereitgestellt und von einer einzigen Cloud-basierten Plattform verwaltet und bietet Unternehmen die Flexibilität, Sicherheitsmaßnahmen auf ihre Bedürfnisse zuzuschneiden.



WatchGuard Cloud

WatchGuard Patch Management

Sichern Sie Betriebssysteme und Anwendungen und halten Sie sie auf dem neuesten Stand, während Sie gleichzeitig die Angriffsfläche Ihres Netzwerks verringern. Vereinfachen Sie das Patchen mit automatisierter Erkennung, Priorisierung und Bereitstellung kritischer Windows-, macOS-, Linux- und Drittanbieteranwendungen. Mit der stufenweisen Patch-Bereitstellung können Sie Patches in kontrollierten Umgebungen testen und nur geeignete Updates in die Produktion übernehmen, um ein konsistentes Patching und ein reduziertes Risiko zu gewährleisten.

WatchGuard Full Encryption

Eine umfassende Datenträgerverschlüsselung ist die vorderste Verteidigungslinie für einen effektiven Schutz Ihrer Daten. WatchGuard Full Encryption nutzt Microsoft BitLocker und macOS FileVault zur Ver- und Entschlüsselung von Datenträgern und ermöglicht Unternehmen durch den Einsatz der Pre-Boot-Authentifizierung, mit der die Identität von Anwendern verifiziert wird, bevor das Betriebssystem geladen wird, den Verlust und Diebstahl von Laptops sowie den unbefugten Zugriff auf Daten zu verhindern.

WatchGuard Advanced Reporting Tool

Das WatchGuard Advanced Reporting Tool bietet durch leistungsstarke Dashboards, Such- und Analysefunktionen einen umfassenden Einblick in die Endpunktaktivität. Identifizieren Sie schnell Sicherheitsrisiken, generieren Sie umsetzbare Sicherheitsinformationen, decken Sie IT-Ressourcennutzungsmuster auf und konfigurieren Sie Warnungen basierend auf Unternehmensrichtlinien.

WatchGuard Data Control*

WatchGuard Data Control* vereinfacht die Verwaltung des Schutzes von personenbezogenen und sensiblen Daten und liefert die erforderliche Transparenz darüber, wo diese sich zu jeder Zeit befinden. Data Control ermöglicht Unternehmen das Erkennen, Klassifizieren, Prüfen und Überwachen von unstrukturierten personenbezogenen Daten in Endpoints. Es unterstützt Benutzer außerdem bei der ordnungsgemäßen Verwaltung von Daten in Bezug auf Einwilligung, zur Kenntnisnahme und gesetzliche Vorgaben wie die DSGVO.

WatchGuard SIEMFeeder

WatchGuard SIEMFeeder integriert Endpunkt-Telemetrie nahtlos in Ihr SIEM. Erhalten Sie einen besseren Einblick in Sicherheitsvorfälle, das Systemverhalten und Schwachstellen in Ihrer Umgebung.

* Verfügbar in Spanien, Deutschland, Großbritannien, Schweden, Frankreich, Italien, Portugal, den Niederlanden, Finnland, Dänemark, der Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.

Klicken Sie [hier](#) oder besuchen Sie <https://wgrd.tech/4wahrBr>, um beliebte IT-Managementanwendungen von Drittanbietern zu sehen.