WatchGuard Endpoint-Sicherheitslösungen für Unternehmen

ENDPOINT-SICHERHEIT UND -MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Schutz					
Schutz vor bekannter und Zero-Day-Malware	✓	✓	✓	✓	✓
Schutz vor bekannter und Zero-Day-Ransomware	✓	✓	✓	✓	✓
Schutz vor bekannten und Zero-Day-Exploits	✓	✓	✓	✓	✓
Anti-Phishing-Schutz		✓		✓	✓
Schutz mehrere Angriffsvektoren (Web, E-Mail, Netzwerk, Geräte)	✓	✓	✓	✓	✓
Traditioneller Schutz mit generischen und optimierten Signaturen		✓		✓	✓
Schutz vor Advanced Persistent Threats (APTs)	✓		✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
Abfragen von Cloud-basierten kollektiven WatchGuard-Informationen	✓	✓	✓	✓	✓
Verhaltensblockierung	✓	✓	✓	✓	✓
Persönliche und verwaltete Firewall		✓		✓	✓
IDS/HIPS		✓		✓	✓
Schutz vor Netzwerkangriffen			✓	✓	✓
Gerätesteuerung		✓		✓	✓
URL Filtering nach Kategorie (Webbrowsing-Überwachung)		✓		✓	✓
Überwachung					
Risk-Monitoring für Endpoints		✓	✓	✓	✓
Cloudbasierte ständige Überwachung aller Prozessaktivitäten	✓		✓	✓	✓
Einjährige Aufbewahrung von Daten für retrospektive Angriffsuntersuchungen	✓		✓	✓	✓
Schwachstellenanalyse		✓	✓	✓	✓
Erkennung					
Erkennung gefährdeter Treiber	✓	✓	✓	✓	✓
Erkennung von Codeinjektionen in laufenden Prozessen	✓	✓	✓	✓	✓
Vollständig konfigurierbare und sofortige Sicherheitsrisiko-Warnmeldungen	✓	✓	✓	✓	✓
Erkennung kompromittierter vertrauenswürdiger Anwendungen			✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
eXtended Detection and Response (XDR) capabilities	✓		✓	✓	✓
Threat Hunting Service: MITRE ATT&CK zugeordnete deterministische Indicators of Attack			✓	✓	✓
STIX- und YARA-Framework-Suche					✓
Threat Hunting Service: MITRE ATT&CK zugeordnete nicht-deterministische Indicators of Attack mit kontextueller Telemetrie					✓
Eindämmung					
Echtzeitisolierung von Computern über die Cloud-Konsole	✓		✓	✓	✓

ENDPOINT-SICHERHEIT UND -MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Reaktion und Abhilfe		✓			
Text für Fernzugriff auf Endpoints über die Verwaltungsbenutzeroberfläche					
Möglichkeit zum Zurücksetzen und Beheben der von Angreifern durchgeführten Aktionen		✓	✓	✓	✓
Zentrale Quarantäne		✓	✓	✓	✓
Automatische Analyse und Desinfektion		✓	✓	✓	✓
Fähigkeit, unbekannte und unerwünschte Anwendungen zu blockieren			✓	✓	✓
eXtended Detection and Response (XDR) capabilities	✓		✓	✓	✓
Schattenkopien		✓	✓	✓	✓
Untersuchung					
Threat Hunting Service: MITRE ATT&CK zugeordnete deterministische Indicators of Attack			✓	✓	✓
Ereignisdiagramme und Lebenszyklus-Informationen über die Web-Konsole	✓		✓	✓	✓
Möglichkeit zum Export von Lebenszyklus-Informationen zur lokalen Analyse	✓		✓	✓	✓
Advanced Reporting Tool *(Add-On)*			✓	✓	✓
Entdeckung und Überwachung unstrukturierter personenbezogener Daten über Endpoints hinweg *(Add-on)*			✓	✓	✓
Erweiterte Untersuchung von Angriffen (Jupyter Notebooks)			✓	✓	✓
Remote-Shell zur Verwaltung von Prozessen und Diensten, Dateiübertragungen, Befehlszeilentools, Dump-Abruf, pcap usw.					✓
Untersuchungsbereich für IoAs und verdächtige Verhaltensmuster		✓			✓
Threat Hunting Service: MITRE ATT&CK zugeordnete nicht-deterministische Indicators of Attack mit kontextueller Telemetrie					✓
Zugriff auf angereicherte Telemetriedaten, in denen MITRE ATT&CK-Taktiken und -Techniken verdächtigen Ereignissen zugeordnet sind					✓
Detaillierte Dateianalyse mit dem CAPA-Tool					✓
Detaillierter Modus für die Angriffssimulation					✓
Verkleinerung der Angriffsoberfläche					
Endpoint Access Enforcement			✓	✓	✓
Sperre im erweiterten Schutz			✓	✓	✓
Anti-Exploit-Technologie	✓		✓	✓	✓
Sperren Sie Programme nach Hash oder Namen (z. B. PowerShell)			✓	✓	✓
Gerätesteuerung		✓		✓	✓
Web-Schutz		✓		✓	✓
Automatisierte Aktualisierungen	✓	✓	✓	✓	✓
Automatische Erkennung ungeschützter Endpoints	✓	✓	✓	✓	✓
Patch Management für Betriebssysteme und Drittanbieter-Anwendungen		✓	✓	✓	✓
Sicherheit für VPN-Verbindungen (benötigt Firebox)	✓	✓	✓	✓	✓
Durchsetzung des Netzwerkzugriffs auf WLAN über Access Points	✓	✓	✓	✓	✓
Erweiterte Sicherheitsrichtlinien					✓
Möglichkeit zur Blockierung von Verbindungen von nicht autorisierten Endpoints					✓

ENDPOINT-SICHERHEIT UND -MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Endpoint security management					
Zentrale cloudbasierte Konsole	✓	✓	✓	✓	✓
Risiko (kontinuierliche Überwachung)	✓	✓	✓	✓	✓
Vererbung von Einstellungen zwischen Gruppen und Endpoints	✓	✓	✓	✓	✓
Möglichkeit zur Konfiguration und Anwendung von Einstellungen auf Gruppenbasis	✓	✓	✓	✓	✓
Möglichkeit zur Konfiguration und Anwendung von Einstellungen pro Endpoint	✓	✓	✓	✓	✓
Echtzeit-Bereitstellung von Einstellungen der Konsole zu Endpoints	✓	✓	✓	✓	✓
Sicherheitsmanagement basierend auf Endpoint-Ansichten und dynamischen Filtern		✓	✓	✓	✓
Möglichkeit zur Planung und Ausführung von Aufgaben in Endpoint-Ansichten	✓	✓	✓	✓	✓
Möglichkeit zur Zuweisung benutzerdefinierter Berechtigungen für Konsolenanwender	✓	✓	✓	✓	✓
Möglichkeit zur individuellen Konfiguration lokaler Warnmeldungen	✓	✓	✓	✓	✓
Anwender-Aktivitätsaudits	✓	✓	✓	✓	✓
Installation über MSI-Packages, Download-URLs und an Endanwender gesendete E-Mails	✓	✓	✓	✓	✓
On-Demand-Berichte und geplante Berichte auf verschiedenen Ebenen und mit mehreren Granularitätsoptionen	✓	✓	✓	✓	✓
Sicherheits-KPIs und Management-Dashboards	✓	✓	✓	✓	✓
API-Verfügbarkeit	✓	✓	✓	✓	✓
Remote Monitoring & Management-Integrationen (RMM)					
ConnectWise Automate	✓	✓	✓	✓	✓
Kaseya VSA	✓	✓	✓	✓	✓
N-able N-central	✓	✓	✓	✓	✓
N-able N-sight	✓	✓	✓	✓	✓
NinjaOne (Automatisiertes deployment-skripting)	✓	✓	✓	✓	✓
Module					
WatchGuard Data Control*			✓	✓	✓
WatchGuard Advanced Reporting Tool			✓	✓	✓
WatchGuard Patch Management		✓	✓	✓	✓
WatchGuard Full Encryption		✓	✓	✓	✓
WatchGuard SIEMFeeder			✓	✓	✓
Hochverfügbarkeitsdienst	✓	✓	✓	✓	✓
Hostplattform-Zertifizierungen	✓	✓	✓	✓	✓

ENDPOINT-SICHERHEIT UND -MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Kompatible Betriebssysteme					
Unterstützt Windows Intel	✓	✓	✓	✓	✓
Unterstützung für Windows ARM	✓	✓	✓	✓	✓
Unterstützung für macOS ARM (M1 und M2)	✓	✓	✓	✓	✓
Unterstützt macOS	✓	✓	✓	✓	✓
Unterstützt Linux	✓	✓	✓	✓	✓
Unterstützt Android		✓		✓	✓
Unterstützt iOS		✓		✓	✓
Unterstützt virtuelle Umgebungen – persistent und nicht persistent (VDI)**	✓	✓	✓	✓	✓

✓ Nur Basisfunktionalität

✓ Volle Funktionalität

* Data Control ist in den folgenden Ländern verfügbar: Spanien, Deutschland, Vereinigtes Königreich, Schweden, Frankreich, Italien, Portugal, Niederlande, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.

** Kompatible Systeme mit folgenden virtuellen Maschinen: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop und MS Virtual Servers. Die WatchGuard EPDR-Lösung ist kompatibel mit Citrix Virtual Apps, Citrix Desktops 1906 und Citrix Workspace-App für Windows.

Unterstützte Plattformen und Systemanforderungen von WatchGuard Endpoint Security

Unterstützte Betriebssysteme: Windows (Intel und ARM), macOS (Intel und ARM), Linux iOS und Android.

EDR-Funktionen sind unter Windows, macOS und Linux verfügbar, wobei Windows sämtliche Funktionen uneingeschränkt unterstützt.

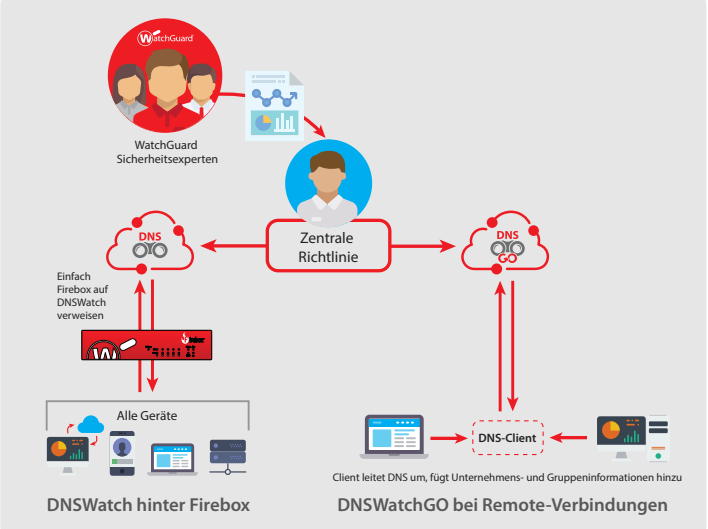
Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge und Opera.

ZUSÄTZLICHE MODULE UND PRODUKTE VON WATCHGUARD FÜR ENDPOINT-SICHERHEIT

DNSWatchGO

DNSWatchGO ist ein cloudbasierter Dienst, der Schutz auf Domain-Ebene, Inhaltsfilterung und integrierte Schulungen zur Förderung des Sicherheitsbewusstseins bietet, damit Ihre Benutzer auch außerhalb Ihres sicheren Netzwerkperimeters geschützt sind. Im Fall kritischer Warnmeldungen führen die Sicherheitsexperten von WatchGuard eine maßgeschneiderte Analyse der potenziellen Bedrohung durch und dokumentieren dann potenzielle Infektionen in einfacher Sprache und mit detaillierten Informationen. Wenn ein Benutzer auf einen bösartigen Link klickt, wird er von DNSWatchGO automatisch auf eine sichere Seite umgeleitet. Außerdem werden ihm Ressourcen angeboten, mit denen er sein Sicherheitswissen vertiefen kann.

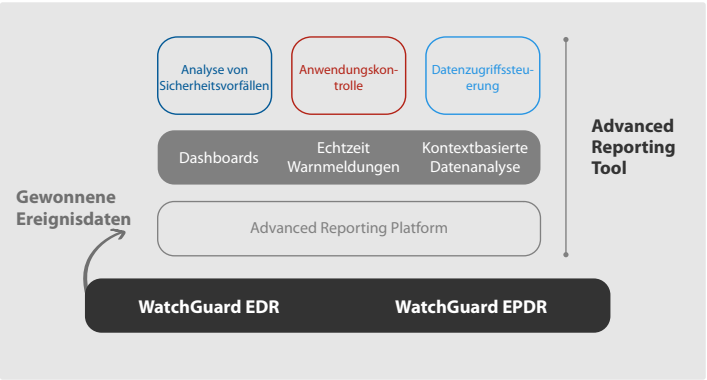
Weitere Informationen



Advanced Reporting Tool

Das Advanced Reporting Tool speichert und korreliert die Informationen in Zusammenhang mit der Prozessausführung und dem Kontext, der von WatchGuard EPDR von Endpoints extrahiert wird. Erzeugt automatisch Sicherheitsinformationen und bietet Tools, mit denen Organisationen Angriffe und ungewöhnliche Verhaltensmuster präzise bestimmen sowie internen Missbrauch der Firmennetzwerke und -systeme erkennen können, um umfassendere Sicherheitsuntersuchungen zu ermöglichen.

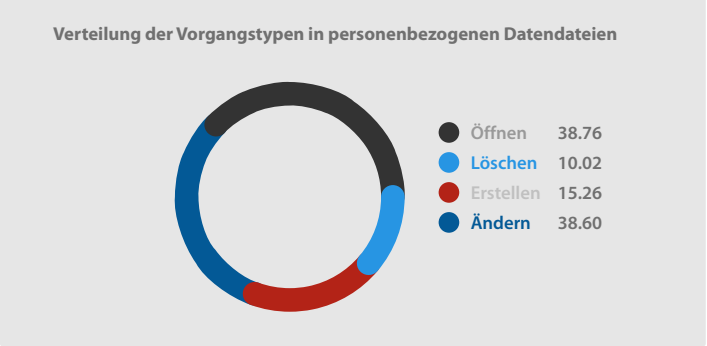
Weitere Informationen



Data Control

Data Control ist ein Modul für unstrukturierte Datensicherheit und ist darauf ausgelegt, Unternehmen bei der Einhaltung von Datenschutzrichtlinien zu helfen sowie personenbezogene und vertrauliche Daten zu entdecken und zu schützen, sowohl in Echtzeit als auch über den Lebenszyklus der Daten auf Endpoints und Servern hinweg. Data Control entdeckt, auditiert und überwacht unstrukturierte personenbezogene Daten auf Endpoints: Von ruhenden Daten bis hin zu verwendeten Daten und Daten in Bewegung.

Weitere Informationen

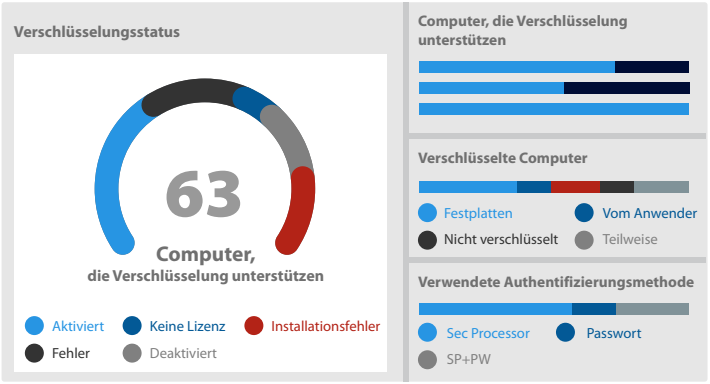


**Data Control ist in den folgenden Ländern verfügbar: Spanien, Deutschland, Vereinigtes Königreich, Schweden, Frankreich, Italien, Portugal, Niederlande, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.*

Full Encryption

Full Encryption ist ein zusätzliches Modul für den WatchGuard Endpoint-Schutz und hochentwickelte, anpassungsfähige Sicherheitslösungen, das auf zentrales Management der vollständigen Festplattenverschlüsselung ausgelegt ist. Es bietet die folgenden Funktionen: Vollständige Festplattenverschlüsselung und -Entschlüsselung, zentrale Verwaltung und Wiederherstellung von Verschlüsselungsschlüsseln, Listen und Berichte und zentrale Anwendung von Richtlinien.

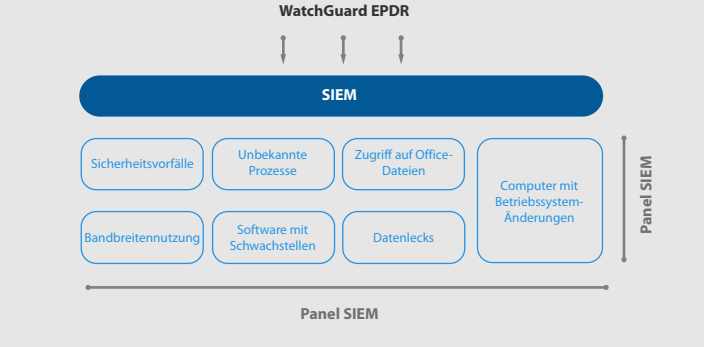
Weitere Informationen



SIEM Feeder

SIEM Feeder. WatchGuard EDR und WatchGuard EPDR integriert auf geschützten Endpoints erfasste Ergebnisse nahtlos in bestehende Unternehmens-SIEM-Lösungen, ohne weitere Bereitstellungen auf Anwendergeräten. Überwachte Ereignisse werden sicher, entweder direkt oder indirekt über Plug-Ins, über das LEEF/CEF-Format gesendet, das mit den meisten SIEM-Systemen auf dem Markt kompatibel ist.

Weitere Informationen



WatchGuard-Verteilung. Kauf und Einrichtung benötigen Unterstützung durch WatchGuard-Mitarbeiter.

Patch Management

ist ein Modul zum Schwachstellenmanagement von Betriebssystemen und Drittanbieter-Anwendungen auf Windows-Workstations und -Servern.

Die Lösung erfordert keine neuen Endpoint-Agents oder Managementkonsolen, da sie vollständig in alle Endpoint-Lösungen von WatchGuard integriert ist. Zudem bietet sie zentrale Echtzeit-Transparenz des Sicherheitsstatus hinsichtlich Software-Schwachstellen, fehlender Patches, Aktualisierungen und nicht unterstützter EOL-Software. Sie ist einfach zu verwenden und installiert und überwacht Aktualisierungen in Echtzeit.

Weitere Informationen