

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Schutz				
Schutz vor Exploits		•	•	•
Schutz vor bekannter und Zero-Day-Malware	•	•	•	•
Schutz vor bekannter und Zero-Day-Ransomware	•	•	•	•
Schutz vor bekannten und Zero-Day-Exploits		•	•	•
Anti-Phishingschutz	•	•	•	•
Schutz für mehrere Angriffsvektoren (Web, E-Mail, Netzwerk, Geräte)	•	•	•	•
Traditioneller Schutz mit generischen und optimierten Signaturen	•	•	•	•
Zero-Trust Application Service			•	•
Abfragen von Cloud-basierten kollektiven WatchGuard-Informationen	•	•	•	•
Selbstlernende KI – Kontextbasierte Verhaltenserkennung	•	•	•	•
Selbstlernende KI – Malicious Installer (MSI)-Blockierung	•	•	•	•
Selbstlernende KI – Erkennung von böartigen .NET-Aktionen	•	•	•	•
Selbstlernende KI – Skriptschutz	•	•	•	•
Persönliche und verwaltete Firewall	•	•	•	•
IDS/HIPS	•	•	•	•
Netzwerkangriffsschutz		•	•	•
Geräteststeuerung	•	•	•	•
URL Filtering nach Kategorie (Web-Browsing-Überwachung)	•	•	•	•
Monitoring				
Risk-Monitoring für Endpoints	•	•	•	•
Ständige Überwachung aller Prozessaktivitäten	•	•	•	•
Datenaufbewahrung	30 Tage*	30 Tage	90 Tage	90 Tage
Add-on für 1-Jahres-Datenaufbewahrung		•	•	•
Schwachstellenanalyse	•	•	•	•
Detection				
Erkennung gefährdeter Treiber		•	•	•
Vollständig konfigurierbare und sofortige Warnmeldungen für Sicherheitsrisiken	•	•	•	•
Erkennung von kompromittierten vertrauenswürdigen Anwendungen			•	•
Zero-Trust Application Service			•	•
ThreatSync eXtended Detection and Response (XDR) – Erkennungsfähigkeiten	•	•	•	•
Vorfallvisualisierung (Vorfalldiagramm und Signalpanel mit Zeitleiste)	•	•	•	•
MITRE ATT&CK zugeordnete Vorfallssignale		•	•	•
Suche nach STIX IoCs und YARA-Regeln				•
Eindämmung				
Isolierung, Scan und Neustart von Computern in Echtzeit		•	•	•

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Reaktion und Abhilfemaßnahmen				
Fähigkeit, die von Angreifern durchgeführten Ransomware-Aktionen rückgängig zu machen und zu beheben (Schattenkopien)	•	•	•	•
Zentralisierte Quarantäne	•	•	•	•
Automatische Analyse und Desinfektion	•	•	•	•
Fähigkeit, unbekannte und unerwünschte Anwendungen zu blockieren			•	•
ThreatSync eXtended Detection and Response (XDR) – Behebungsmaßnahmen		•	•	•
Untersuchung				
Interaktive Multisignal-Vorfallansicht für eine umfassende Ursachenanalyse (Root Cause Analysis, RCA)		•	•	•
Automatische Erkennung und Korrelation eines Angriffs mit Alarmen, die dem MITRE ATT&CK® Framework zugeordnet sind		•	•	•
Deep Context und Echtzeit-Computerforensik-Telemetrie				•
Fortgeschrittene Abfrage für Untersuchungen				•
GenAI-Untersuchungsassistent				•
Erweiterte Angriffsuntersuchung (Jupyter Notebooks)				•
Remote-Shell für schnellere MTTR und kürzere Dauer von Sicherheitsverletzungen				•
Detaillierte Dateianalyse mit dem CAPA-Tool				•
Verbose-Modus für Angriffssimulation				•
Advanced Reporting Tool (Add-on)		•	•	•
Erkennung und Überwachung unstrukturierter personenbezogener Daten über Endpoints hinweg (Add-on)**		•	•	•
Reduzierung der Angriffsfläche				
Endpoint Access Enforcement			•	•
Sperrmodus im Advanced-Protection-Modul			•	•
Anti-Exploit-Technologie		•	•	•
Blockierung von Programmen nach Hash oder Name (z. B. PowerShell)			•	•
Gerätesteuerung	•	•	•	•
Internetschutz	•	•	•	•
Automatische Updates	•	•	•	•
Automatische Erkennung ungeschützter Endpoints	•	•	•	•
Patch-Management für Betriebssysteme und Anwendungen von Drittanbietern (Add-on)	•	•	•	•
Sicherheit für VPN-Verbindungen (erfordert Firebox)	•	•	•	•
Erweiterte Sicherheitsrichtlinien				•

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Sicherheitsmanagement für Endpoints				
Zentralisierte Cloud-basierte Konsole	•	•	•	•
Einstellungsvererbung zwischen Gruppen und Endpoints	•	•	•	•
Möglichkeit, Einstellungen auf Gruppenbasis zu konfigurieren und anzuwenden	•	•	•	•
Möglichkeit, Einstellungen pro Endpoint zu konfigurieren und anzuwenden	•	•	•	•
Bereitstellung von Einstellungen in Echtzeit von der Konsole zu den Endpoints	•	•	•	•
Sicherheitsmanagement basierend auf Endpoint-Ansichten und dynamischen Filtern	•	•	•	•
Möglichkeit zur Planung und Ausführung von Aufgaben in Endpoint-Ansichten	•	•	•	•
Möglichkeit, Konsolenanwendern vorkonfigurierte Rollen zuzuweisen	•	•	•	•
Möglichkeit zur individuellen Konfiguration lokaler Warnmeldungen	•	•	•	•
Möglichkeit zur Steuerung von Neustarts für Patch- und Engine-Updates	•	•	•	•
Benutzeraktivitätsprüfung	•	•	•	•
Installation über MSI-Pakete, Download-URLs und E-Mails, die an Endanwender gesendet werden	•	•	•	•
On-demand- 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 Bereitstellungs-Scripting)	•	•	•	•
Module				
Patch Management	•	•	•	•
Full Encryption	•	•	•	•
Advanced Reporting Tool		•	•	•
Data Control**		•	•	•
SIEMFeeder		•	•	•
MDR		•	•	•

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Unterstützte Betriebssysteme				
Unterstützt Windows Intel	•	•	•	•
Unterstützung für Windows ARM	•	•	•	•
Unterstützung für macOS ARM (M1 und M2)	•	•	•	•
Unterstützt macOS Intel	•	•	•	•
Unterstützt Linux	•	•	•	•
Unterstützt Android	•	•	•	•
Unterstützt iOS	•	•	•	•
Unterstützung für virtuelle Umgebungen – persistent und nicht persistent (VDI)***	•	•	•	•

Wo ist WatchGuard EDR?

Unsere EDR-Lösung wurde aus dieser Matrix entfernt, da sie für einen bestimmten Anwendungsfall verkauft wird, bei dem ein Kunde mit AV/EPP eine EDR-Lösung darüber schichten möchte.

* Vorfallsbezogene Bindung nur in der Management-Benutzeroberfläche.

** WatchGuard Data Control wird nur in den folgenden Ländern unterstützt: Spanien, Deutschland, Großbritannien, Schweden, Frankreich, Italien, Portugal, Holland, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.

*** Kompatible Systeme mit den folgenden Arten virtueller Geräte: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop und MS Virtual Servers. WatchGuard Endpoint Security 360-Lösung ist kompatibel mit Citrix Virtual Apps, Citrix Desktops 1906 und Citrix Workspace-App für Windows.

Unterstützte Plattformen und Systemanforderungen für 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](#), [Microsoft Edge](#) und [Safari](#).