WatchGuard Endpoint Security Solutions for MSPs

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Protection				
Protection against known and zero-day malware	●	●	●	●
Protection against known and zero-day ransomware	●	●	●	●
Protection against known and zero-day exploits		●	●	●
Anti-phishing protection	●	●	●	●
Protection for multiple attack vectors (web, email, network, devices)	●	●	●	●
Traditional protection with generic and optimized signatures	●	●	●	●
Anti-exploit protection		●	●	●
Zero-Trust Application Service			●	●
Queries to WatchGuard's cloud-based collective intelligence	●	●	●	●
Self-learning AI context-based behavioral detection	●	●	●	●
Self-learning AI Malicious Installer (MSI) blocking	●	●	●	●
Self-learning AI malicious .NET detection	●	●	●	●
Self-learning AI script protection	●	●	●	●
Personal and managed firewall	●	●	●	●
IDS / HIPS	●	●	●	●
Network attack protection		●	●	●
Device control	●	●	●	●
URL filtering by category (web browsing monitoring)	●	●	●	●
Monitoring				
Endpoint risk monitoring	●	●	●	●
Continuous monitoring of all process activity	●	●	●	●
Data retention	30 Days*	30 days	90 days	90 days
1 year data retention add-on		●	●	●
Vulnerability assessment	●	●	●	●
Detection				
Detection of vulnerable driver		●	●	●
Fully configurable and instant security risk alerts	●	●	●	●
Detection of compromised trusted applications			●	●
Zero-Trust Application Service			●	●
ThreatSync eXtended Detection and Response (XDR) – detection capabilities	●	●	●	●
Incident visualization (incident graph and signals panel with timeline)	●	●	●	●
Incident signals mapped to MITRE ATT&CK		●	●	●
STIX IoCs and YARA rules search				●
Containment				
Real-time computer isolation, scan and restart		●	●	●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Response and Remediation				
Ability to roll back and remediate the ransomware actions taken by attackers (shadow copies)	●	●	●	●
Centralized quarantine	●	●	●	●
Automatic analysis and disinfection	●	●	●	●
Ability to block unknown and unwanted applications			●	●
ThreatSync eXtended Detection and Response (XDR) – remediation actions		●	●	●
Investigation				
Interactive, multi-signal incident view for comprehensive Root Cause Analysis (RCA)		●	●	●
Automatic detection and correlation of an attack, with alerts, mapped to the MITRE ATT&CK® framework		●	●	●
Deep context and real-time computer forensics telemetry				●
Advanced Querying for investigations				●
GenAI Investigation Assistant				●
Advanced attack investigation (Jupyter Notebooks)				●
Remote shell for faster MTTR and reduced breach dwell time				●
Deep file analysis with CAPA tool				●
Verbose Mode for attack simulation				●
Advanced Reporting Tool (add-on)		●	●	●
Discovery and monitoring of unstructured personal data across endpoints (add-on)**		●	●	●
Attack Surface Reduction				
Endpoint Access Enforcement			●	●
Lock mode in the Advanced Protection module			●	●
Anti-exploit technology		●	●	●
Block programs by hash or name (e.g. PowerShell)			●	●
Device control	●	●	●	●
Web protection	●	●	●	●
Automatic updates	●	●	●	●
Automatic discovery of unprotected endpoints	●	●	●	●
Patch Management for OS and third-party applications (add-on)	●	●	●	●
Security for VPN connections (requires Firebox)	●	●	●	●
Advanced security policies				●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Endpoint Security Management				
Centralized cloud-based console	●	●	●	●
Settings inheritance between groups and endpoints	●	●	●	●
Ability to configure and apply settings on a group basis	●	●	●	●
Ability to configure and apply settings on a per-endpoint basis	●	●	●	●
Real-time deployment of settings from the console to endpoints	●	●	●	●
Security management based on endpoint views and dynamic filters	●	●	●	●
Ability to schedule and perform tasks on endpoint views	●	●	●	●
Ability to assign preconfigured roles to console users	●	●	●	●
Ability to customize local alerts	●	●	●	●
Ability to control restarts for Patch & Engine Update	●	●	●	●
User activity auditing	●	●	●	●
Installation via MSI packages, download URLs, and emails sent to end users	●	●	●	●
On-demand and scheduled reports at different levels and with multiple granularity options	●	●	●	●
Security KPIs and management dashboards	●	●	●	●
API availability	●	●	●	●
Remote Monitoring & Management (RMM) Integrations				
ConnectWise Automate	●	●	●	●
Kaseya VSA	●	●	●	●
N-able N-central	●	●	●	●
N-able N-sight	●	●	●	●
NinjaOne (Automated Deployment Scripting)	●	●	●	●
Modules				
Patch Management	●	●	●	●
Full Encryption	●	●	●	●
Advanced Reporting Tool		●	●	●
Data Control**		●	●	●
SIEMFeeder		●	●	●
MDR		●	●	●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Supported Operating Systems				
Supports Windows Intel	●	●	●	●
Support for Windows ARM	●	●	●	●
Support for macOS ARM (M1 and M2)	●	●	●	●
Supports macOS Intel	●	●	●	●
Supports Linux	●	●	●	●
Supports Android	●	●	●	●
Supports iOS	●	●	●	●
Support for virtual environments - persistent and non-persistent (VDI)***	●	●	●	●

Where is WatchGuard EDR?

Our EDR solution has been removed from this matrix because it is selling to a specific use case, in which a customer who has AV/EPP is looking to layer an EDR solution on top.

* Incident-related retention in management UI only.

** WatchGuard Data Control is supported in the following countries only: Spain, Germany, UK, Sweden, France, Italy, Portugal, Holland, Finland, Denmark, Switzerland, Norway, Austria, Belgium, Hungary, and Ireland.

*** Compatible systems with the following types of virtual machines: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop and MS Virtual Servers. WatchGuard Endpoint Security 360 solution is compatible with Citrix Virtual Apps, Citrix Desktops 1906 & Citrix Workspace App for Windows.

Supported platforms and systems requirements of WatchGuard Endpoint Security

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS and Android.

EDR capabilities are available on Windows, macOS, and Linux, with Windows being the platform that provides all the capabilities in their entirety.

List of compatible browsers: Google Chrome, Mozilla Firefox, Microsoft Edge and Safari.