

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EPDR	WatchGuard EDR	WatchGuard EPP
Protection			
Protection against known and zero day malware	✓	✓	✓
Protection against known and zero day ransomware	✓	✓	✓
Protection against known and zero day exploits	✓	✓	✓
Anti-spyware, anti-phishing protection, etc.	✓	✓	✓
Protection for multiple attack vectors (<i>web, email, network, devices</i>)	✓	✓	✓
Traditional protection with generic and optimized signatures	✓	✓	✓
Protection against advanced persistent threats (APTs)	✓	✓	
Zero-Trust Application Service	✓	✓	
Threat Hunting Service (indicators of attack)	✓	✓	
Queries to WatchGuard's Cloud-based collective intelligence	✓	✓	✓
Behavioral blocking and IoA detection	✓	✓	✓
Personal and managed firewall	✓		✓
IDS / HIDS	✓		✓
Authorized software by hash or program properties	✓	✓	
Ability to block unknown and unwanted applications	✓	✓	
Device control	✓		✓
URL filtering by category (<i>web browsing monitoring</i>)	✓		✓
Monitoring			
Advanced endpoint security	✓	✓	
Cloud-based continuous monitoring of all process activity	✓	✓	
Data retention for one year for retrospective attack investigation	✓	✓	
Detection			
Detection of compromised trusted applications	✓	✓	
Zero-Trust Application Service	✓	✓	
Fully configurable and instant security risk alerts	✓	✓	✓
Containment			
Real-time computer isolation from the Cloud console	✓	✓	
Response and remediation			
Ability to roll back and remediate the actions taken by attackers	✓	✓	✓
Centralized quarantine	✓	✓	✓
Automatic analysis and disinfection	✓	✓	✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EPDR	WatchGuard EDR	WatchGuard EPP
Investigation			
Threat Hunting Service (indicators of attack)	✓	✓	
Incident graphs and lifecycle information available from the web console	✓	✓	
Ability to export lifecycle information for local analysis	✓	✓	
Advanced Visualization Tool (<i>add-on</i>)	✓	✓	
Discovery and monitoring of unstructured personal data across endpoints (<i>add-on</i>)	✓	✓	
Attack surface reduction			
Information about each computer's hardware and software components	✓	✓	✓
Information about the Microsoft updates installed on endpoints	✓	✓	✓
Real-time information about the status of all protections and communications	✓	✓	✓
Automatic updates	✓	✓	✓
Automatic discovery of unprotected endpoints	✓	✓	✓
Ability to immediately protect unprotected endpoints remotely	✓	✓	✓
WatchGuard native proxy to support endpoints with no Internet connection	✓	✓	✓
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 assign custom permissions to console users	✓	✓	✓
Ability to customize local alerts	✓	✓	✓
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	✓	✓	✓
Endpoint system management			
System status reports at different levels and with multiple granularity options	✓	✓	✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EPDR	WatchGuard EDR	WatchGuard EPP
Modules			
Data Control integration - <i>COMING SOON</i>	✓	✓	
Advanced Reporting Tool integration - <i>COMING SOON</i>	✓	✓	
SIEM integration - <i>COMING SOON</i>	✓	✓	
Patch Management integration - <i>COMING SOON</i>	✓	✓	✓
Full Encryption inegration - <i>COMING SOON</i>	✓	✓	✓
High availability service	✓	✓	✓
Host platform certifications	ISO27001, SAS 70 ISO27001, SAS 70		
Supported operating systems			
Supports Windows Intel	✓	✓	✓
Support for Windows ARM	✓	✓	✓
Support for macOS ARM	✓	✓	✓
Supports macOS	✓	✓	✓
Supports Linux	✓	✓	✓
Supports Android	✓	✓	✓
Supports iOS			
Support for virtual environments - persistent and non-persistent (VDI)***	✓	✓	✓

- ✓ Basic functionality only
- ✓ Full functionality

*** 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 EPDR solution is compatible with Citrix Virtual Apps, Citrix Desktops 1906 & Citrix Workspace App for Windows.

Supported platforms and systems requirements of Watchguard EPDR

Supported operating systems: [Windows \(Intel & ARM\)](#), [macOS \(Intel & ARM\)](#), [Linux and Android](#).

Support to legacy systems starting in Windows XP SP3 and Server 2003.

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

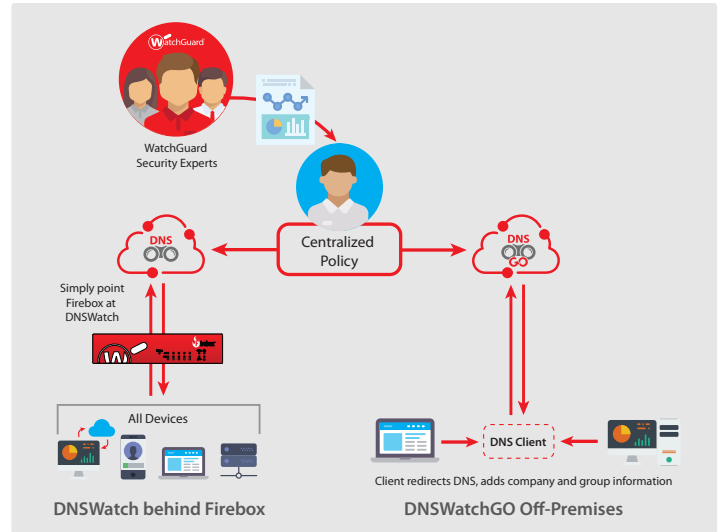
List of compatible browsers: [Google Chrome](#), [Mozilla Firefox](#), [Internet Explorer](#), [Microsoft Edge and Opera](#).

ADDITIONAL WATCHGUARD ENDPOINT SECURITY MODULES AND PRODUCTS

DNSWatchGO

DNSWatchGO is a Cloud-based service that provides domain-level protection, content filtering, and integrated security awareness training to keep your users safe when they travel outside of your secure network perimeter. When critical alerts are seen, WatchGuard's team of security experts performs a tailored analysis of the potential threat, following up with an easy-to-understand accounting that includes detailed insights about the potential infection. When a user clicks a malicious link, DNSWatchGO automatically redirects them to a safe page and offers resources that reinforce security education.

[More information](#)

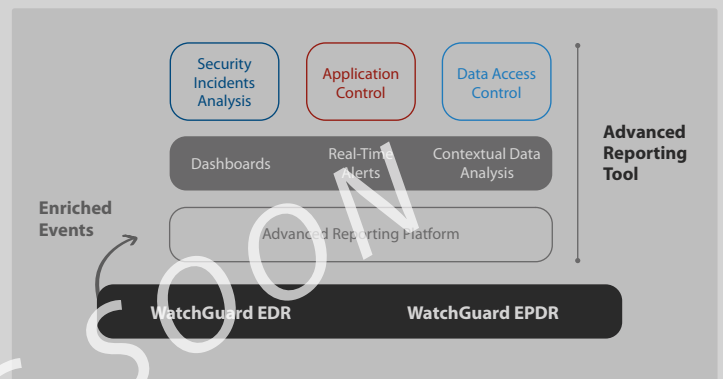


Advanced Reporting Tool

The Advanced Reporting Tool stores and correlates the information related to process execution and its context extracted by WatchGuard EPDR from endpoints. Automatically generates security intelligence and provides tools that allow organizations to pinpoint attacks and unusual behaviors, detecting internal misuse of the corporate systems and network to go deeper in a security investigation.

[More information](#)

[Supported platforms & requirements](#)

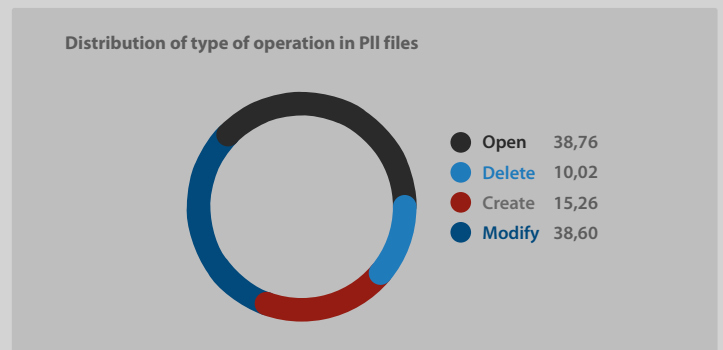


Data Control

Data Control is an unstructured data security module, designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data both in real time and throughout its lifecycle on endpoints and servers. Data Control discovers, audits and monitors unstructured personal data on endpoints: from data at rest to data in use and data in motion.

[More information](#)

[Supported platforms & requirements](#)



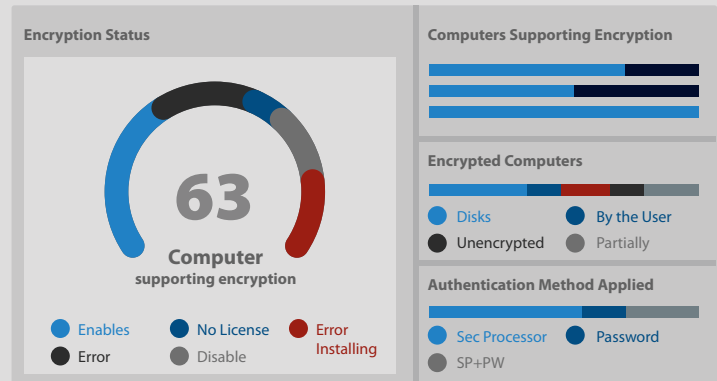
*Data Control is available in the following countries: Spain, Germany, UK, Sweden, France, Italy, Portugal, Holland, Finland, Denmark, Switzerland, Norway, Austria, Belgium, Hungary and Ireland.

Full Encryption

Full Encryption is an additional module for WatchGuard's endpoint protection and advanced adaptive security solutions, designed to centrally manage full disk encryption and provide the following features: Full drive encryption and decryption, centralized management and recovery of encryption keys, lists and reports and centralized policy application.

[More information](#)

[Supported platforms & requirements](#)



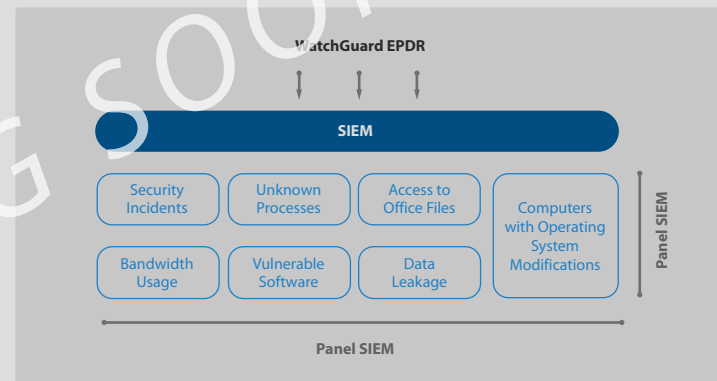
SIEM Feeder

SIEM Feeder. WatchGuard EDR and WatchGuard EPDR seamlessly integrate events gathered from protected endpoints with existing corporate SIEM solutions without additional deployments on user devices. Monitored events are sent securely using the LEEF/CEF formats compatible with most SIEM systems on the market either directly or indirectly via plugins.

[More information](#)

[Supported platforms & requirements](#)

WatchGuard distribution. Purchase and set up requires assistance from WatchGuard staff.



Patch Management

Patch Management is a module for managing vulnerabilities of the operating systems and third-party applications on Windows workstations and servers.

It does not require the deployment of any new endpoint agents or management console as it is fully integrated in all of WatchGuard's endpoint solutions. Plus, it provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates and unsupported end of life (EOL) software, and is easy to install and monitor updates in real time.

[More information](#)

[Supported platforms & requirements](#)

