WatchGuard Endpoint Security Solutions for Business

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
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		✓		✓	✓
Protection against advanced persistent threats (APTs)	✓		✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
Threat Hunting Service: Deterministic indicators attack mapped to MITRE ATT&CK			✓	✓	✓
Threat Hunting Service: Non-deterministic indicators attack mapped to MITRE ATT&CK with contextual telemetry					✓
Queries to WatchGuard's Cloud-based collective intelligence	✓	✓	✓	✓	✓
Behavioral blocking	✓	✓	✓	✓	✓
Personal and managed firewall		✓		✓	✓
IDS / HIPS		✓		✓	✓
Network attack protection			✓	✓	✓
Device control		✓		✓	✓
URL filtering by category *(web browsing monitoring)*		✓		✓	✓
Monitoring					
Endpoint risk monitoring	✓	✓	✓	✓	✓
Cloud-based continuous monitoring of all process activity	✓		✓	✓	✓
Data retention for one year for retrospective attack investigation	✓		✓	✓	✓
Vulnerability assessment		✓	✓	✓	✓
Detection					
Detection of compromised trusted applications			✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
Fully configurable and instant security risk alerts	✓	✓	✓	✓	✓
STIX IOCs and YARA rules search					✓
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		✓	✓	✓	✓
Shadow copies		✓	✓	✓	✓
Ability to block unknown and unwanted applications			✓	✓	✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Investigation					
Threat Hunting Service: Deterministic indicators attack mapped to MITRE ATT&CK			✓	✓	✓
Threat Hunting Service: Non-deterministic indicators attack mapped to MITRE ATT&CK with contextual telemetry					✓
Incident graphs and lifecycle information available from the web console	✓		✓	✓	✓
Ability to export lifecycle information for local analysis	✓		✓	✓	✓
Advanced Reporting Tool *(add-on)*			✓	✓	✓
Discovery and monitoring of unstructured personal data across endpoints *(add-on)**			✓	✓	✓
Advanced attack investigation (Jupyter Notebooks)			✓	✓	✓
Remote shell to manage processes and services, file transfers, command-line tools, get dumps, pcap, etc.					✓
Attack surface reduction					
Lock mode in the Advanced Protection			✓	✓	✓
Anti-exploit technology	✓		✓	✓	✓
Block programs by hash or name (pe.: 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)	✓	✓	✓	✓	✓
Secure access to Wi-Fi network through access points	✓	✓	✓	✓	✓
Advanced security policies					✓
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	✓	✓	✓	✓	✓
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 SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Remote Monitoring & Management (RMM) Integrations					
ConnectWise Automate	✓	✓	✓	✓	✓
Kaseya VSA	✓	✓	✓	✓	✓
N-able N-central	✓	✓	✓	✓	✓
N-able N-sight	✓	✓	✓	✓	✓
Modules					
WatchGuard Data Control*			✓	✓	✓
WatchGuard Advanced Reporting Tool			✓	✓	✓
WatchGuard Patch Management		✓	✓	✓	✓
WatchGuard Full Encryption		✓	✓	✓	✓
WatchGuard SIEMFeeder			✓	✓	✓
High availability service	✓	✓	✓	✓	✓
Host platform certifications	✓	✓	✓	✓	✓
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)**	✓	✓	✓	✓	✓

✓ Basic functionality only

✓ Full functionality

* 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 EPDR 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.

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.

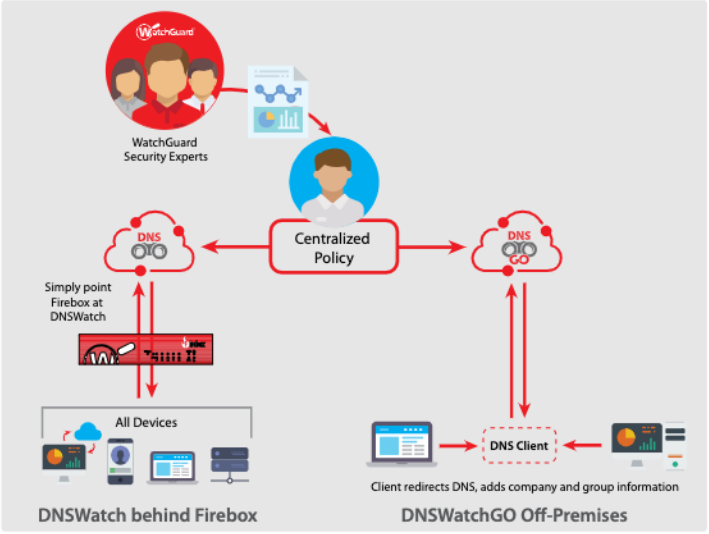
List of compatible browsers: Google Chrome, Mozilla Firefox, Microsoft Edge and Safari.

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.

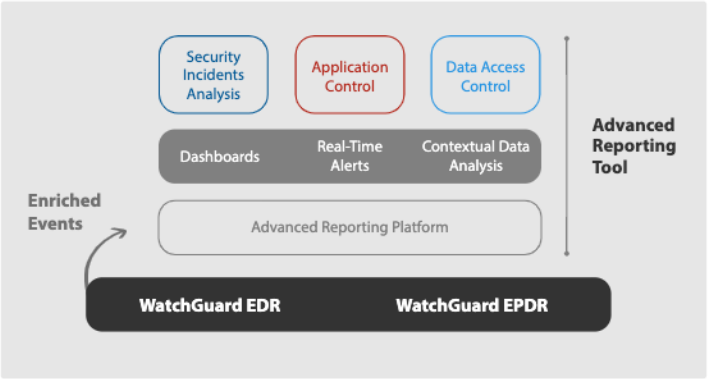
More information



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.

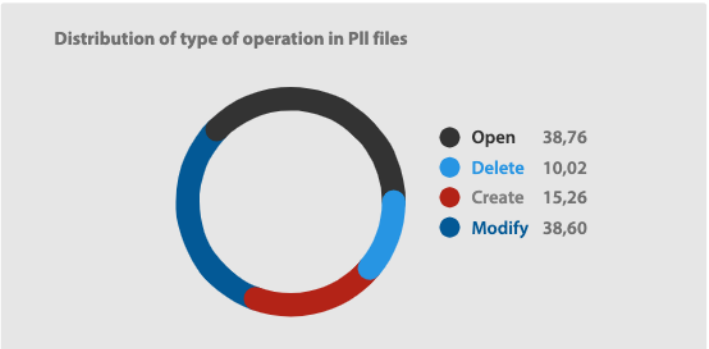
More information



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

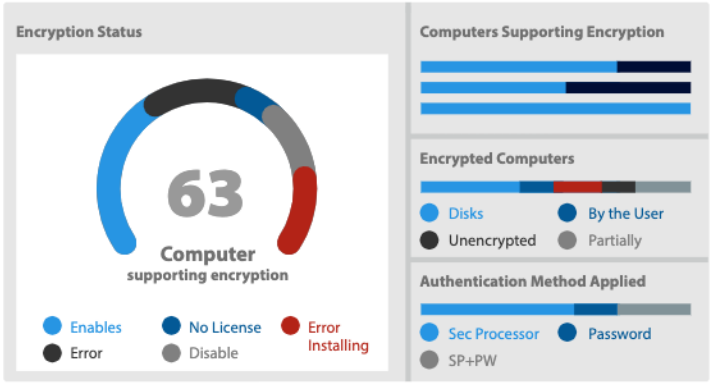


**Data Control is available in the following countries: Spain, Germany, UK, Sweden, France, Italy, Portugal, Holland, Finland, Denmark, Switzerland, Norway, Austria, Belgium, Hungary and Ireland.*

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.

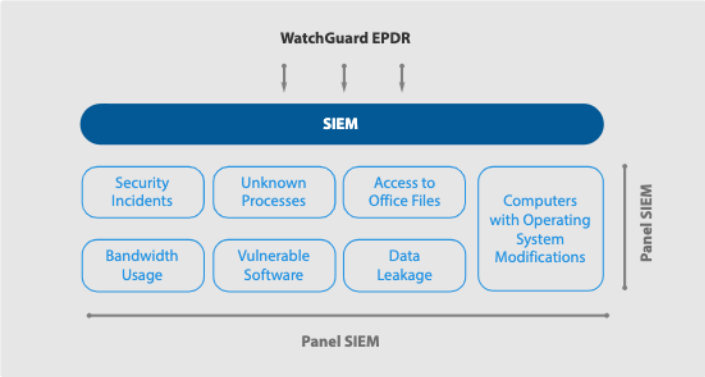
More information



SIEMFeeder

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



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