WatchGuard Endpoint Security

The last endpoint solution you will ever need.

www.watchguard.com

WatchGuard Endpoint Security

WatchGuard Endpoint Security solutions deliver the technologies required to stop advanced cyberattacks on endpoints including next-gen antivirus (EPP) and Endpoint Detection and Response (EDR). Add a full stack of integrated modules for patch management, encryption of disks and USB drives, and security intelligence insights, delivered via a single lightweight agent and managed from a single Cloud-based platform.

Endpoint Protection
WatchGuard EPP is an effective Cloud-native security solution that centralizes next-generation antivirus for all your Windows, macOS and Linux desktops, laptops, and servers.

Endpoint Detection and Response
WatchGuard EDR complements other EPP solutions by adding a full stack of EDR capabilities to automate the detection, containment, and response to any advanced threat.

Endpoint Protection Detection & Response
WatchGuard EPDR combines our broad set of EPP technologies with our EDR capabilities for computers, laptops and servers to detect threats that traditional solutions cannot even see.

Patch Management
Discover, prioritize, and deploy critical Windows operating system and third-party application patches to prevent cyberattacks and mitigate known vulnerabilities with WatchGuard Patch Management.

Full Disk Encryption
WatchGuard Full Encryption strengthens control over hard disks and USB drives containing sensitive data, ensuring that the data remains protected from theft and unauthorized access.

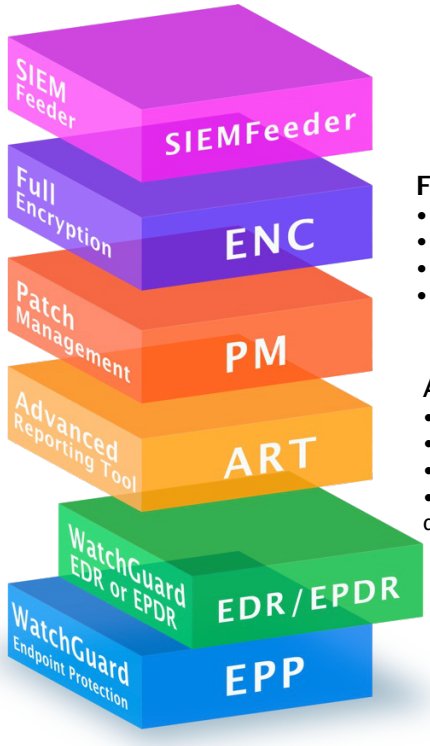
Advanced Reporting Tool
WatchGuard Advanced Reporting Tool generates security intelligence in real time by delivering deep insights into your applications, network, and users' day-to-day operations and actions.

Single-agent Endpoint Security architecture

SIEMFeeder
- Integration with corporate SIEM platforms
- Details and context of all endpoint activity
- CEF, LEEF, Syslog and Kafka support

Patch Management (PM)
- Microsoft and 3rd party applications patching
- End-of-Life application management
- Patch rollback and Windows Update service control
- On-demand or scheduled patching tasks

WatchGuard EPP
- Anti-malware and HIPS protection
- Managed Endpoint Firewall
- Device Control
- Hardware/software inventory
- Web browsing monitoring and filtering



Full Encryption (ENC)
- Managed Full Disk Encryption with BitLocker
- Centralized management of recovery keys
- Centralized encryption policies
- Encryption dashboards, widgets and reporting

Advanced Reporting Tool (ART)
- Preconfigured dashboards, reports and alerts
- Widgets, and predefined queries for security KPIs
- KPIs for vulnerable applications, access data and files
- Raw data from: endpoint operations, network connections, data access, processes with 12-month retention

WatchGuard EPDR
- Protection against sophisticated targeted attacks
- Detection of unknown exploits
- Virtual patching for unsupported systems
- Machine Learning and Deep Learning
- Zero-Trust Application Service
- Containment and Remediation features
- Threat Hunting Service

Threat Hunting Service

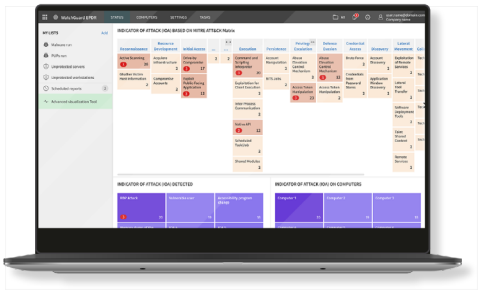
Hunting the Unknown

WatchGuard's continuous monitoring of endpoint activity allows the agent to act as a sensor and inform the Cloud platform not only about the files being run, but also about their context of execution (what happened right before, which users are trying to run which command or application, what network traffic is generated, which data files are being accessed, parameters, etc.).

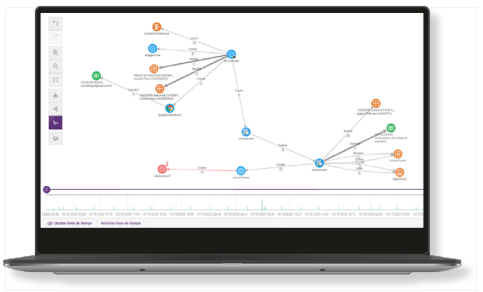
This allows our Threat Hunting Service to identify abnormal behavior and suspicious activity and their categorization as indicators of attack with a high degree of confidence and without false positives.

At WatchGuard, we have implemented the MITRE ATT&CK™ Framework (a globally accessed knowledge base of adversary tactics and techniques based on real-world observations) across multiple WatchGuard Endpoint Security processes and product features to help improve analysts' productivity and prevent breaches.

Detecting indicators of attack (IoAs) before data is exfiltrated (or encrypted in the case of a ransomware attack) is a very effective defense mechanism, especially against living-off-the-land (LotL) attacks, even if endpoints may have already been compromised.



WatchGuard EDR and WatchGuard EPDR integrate, within the same protection agent, a complete technology stack to detect IoAs in different attack phases. Far from being static technologies, they are updated continuously with new attack patterns and techniques that are discovered by the Threat Hunting Service.



Hackers are launching **extremely sophisticated cyber attacks**. There are no security measures that can ensure 100% protection. Fileless attacks in particular are a growing concern, being increasingly difficult to detect. **But hackers still leave traces** that enable us to detect unknown attacks that leverage living-off-the-land techniques. **The WatchGuard automated Threat Hunting Service continuously monitors** everything that happens in the endpoints in real time in the form of **event telemetry**. In case of a **validated breach** with a living-off-the-land technique, the indicator of attack is shown and recorded in the web console.

RDP brute force attacks, privilege escalation, fileless attacks, and lateral movements are examples of IoAs detected thanks to the Threat Hunting Service, included at no extra cost in our EDR solutions.

The Automated Threat Hunting Service – Revealing the undetectable

Our Threat Hunting Service, included in WatchGuard EDR and WatchGuard EPDR, is based on a set of threat hunting rules created by threat specialists that are automatically processed against all data gathered from telemetry, which triggers IoAs of high confidence and with a low rate of false positives to minimize MTTD and MTTR (Mean Time To Detect and Mean Time To Respond).

These indicators of attack are the result of a continuous process to discover threat actors, using advanced data analytics, our proprietary threat intelligence, and the expertise of our analysts.

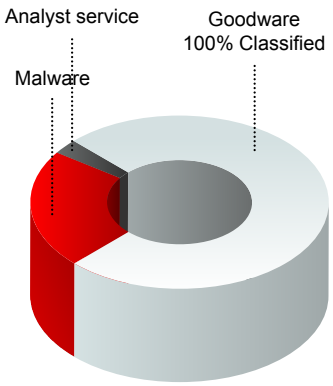
This service inherits all the cyber intelligence that we have perfected thanks to our years of experience in threat research and the historical visibility offered by a registry of application behaviors that has received more than 10 billion events per day, user and machine for more than 30 years. We have strategic alliances with international organizations such as the Cyber Threat Alliance, where we exchange indicators of attack (IoAs), indicators of compromise (IoCs), and their corresponding responses.

Should they come across an anomalous situation, the customer is notified via the web console showing details and graphs of the anomaly, providing forensic analysis of the affected systems, the origin of the attack, and the techniques used. They also provide recommendations on how to mitigate the attack and reduce the attack surface to avoid falling victim to future attacks.

Zero-Trust Application Service

Disruptive innovation in security

The Zero-Trust Application Service is a managed service included as part of the WatchGuard EPDR and WatchGuard EDR solutions. The service classifies 100% of running processes in real time, monitors endpoint activity, and blocks the execution of applications and malicious processes (pre-execution, in-execution and post-execution).



Based on the classification of all running processes on managed endpoints.

- All application activities are analyzed and monitored in real time.
- All behaviors are verified by WatchGuard analysts. Admins don't have to investigate anything.
- No application, process or DLL will execute unless it is trusted.
- Higher protection rate with minimum effort.

WatchGuard Endpoint Security Collective Intelligence

This is another key component hosted in the Cloud that increases the efficiency of the Zero-Trust Application Service. Collective Intelligence represents the consolidated and incremental knowledge repository of all applications, binaries and other files containing interpreted code, both trusted and malicious. This repository in the Cloud is continuously fed by the AI system and by expert analysts, and at the same time is continuously being queried by the solutions and services of WatchGuard Endpoint Security prior to any execution.

How the Zero-Trust Application Service works:

100% of Processes Are Accurately Classified

99.98% AUTOMATIC CLASSIFICATION | 0.02% HUMAN CLASSIFICATION

01 Deny List

FOR KNOWN MALWARE

This classification is based on our Collective Intelligence, which includes more than 2.4 billion known malware.

02 Allow List

FOR KNOWN GOODWARE

Secondly, our Collective Intelligence also includes more than 3.3 billion known goodware to complement the classification.

03 Machine Learning

FOR UNKNOWN PROCESSES

Next, our artificial intelligence and deep learning algorithms are in charge of boosting the automatic classification.

04 Cybersecurity Experts

FOR NEW ATTACK PATTERNS

Finally, our malware analysts and threat hunters manually complete the classification process and enrich our algorithms.

The graphic above shows how the technologies in the stack seamlessly work together, enabling the classification of all applications, binaries and files with interpreted code, in real time.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than 18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com