EPP AND EDR SOLUTIONS

WatchGuard Endpoint Security

Extensible Protection to Prevent, Detect and Respond to Advanced Threats

The endpoint is a favorite target for cybercriminals, with plenty of known vulnerabilities to be exploited and software versions that are often out of date. These devices are frequently on the Internet without protection from corporate perimeter security, and worse yet, employees can unwittingly enable hackers to make their way onto corporate endpoints and networks. It's past the time when businesses of all sizes need to implement powerful endpoint security that includes endpoint protection (EPP) integrated with advanced endpoint detection and response (EDR) technologies.

WatchGuard's Endpoint Security platform delivers maximum protection with minimal complexity to take the guesswork out of endpoint security. Our user-centric security products and services offer advanced EPP and EDR approaches with a full suite of security and operations tools for protecting people, devices, and the networks they connect to from malicious websites, malware, spam, and other targeted attacks. Uniquely powered by automated, AI-driven processes and security analyst-led investigation services, our WatchGuard EPDR, Advanced EPDR and WatchGuard EDR products provide threat hunting services and 100% classification of the applications, certifying the legitimacy and safety of all running applications – a critical need for any company implementing a zero trust security model.

Good or Bad – Know with 100% Confidence

Most endpoint security products block what is known to be bad, investigate what is suspicious, and allow what is not known – enabling malware that rapidly morphs to bypass defenses with other unknown traffic. By contrast, the WatchGuard EDR, Advanced EPDR and WatchGuard EPDR products feature a Zero-Trust Application Service that classifies 100% of executables by analyzing all suspicious and unknown processes and applications using special machine-learning algorithms in our Cloud platform, and even verifying with our lab technicians when needed. As a result, all executables are known to be goodware or malware, so that customers receive only confirmed alerts and enjoy the ultimate protection that comes from the default-deny position of a zero trust model.

Find Lurking Threats Without Adding Staff

Threat hunting usually requires a highly skilled resource and consumes many hours before they detect threats and return the insights that make it clear how to remediate them. Our advanced EDR solutions offer a threat hunting service where our security analysts monitor the customer endpoint environment and provide information about potential ongoing attacks including root cause analysis, anomalies detected, relevant IT insights and potential attack surface reduction plans. This is a standard feature that comes with our WatchGuard EDR. Advanced EPDR and WatchGuard EPDR products and saves companies from having to allocate IT staff time and energy on investigating infected endpoints themselves.

Enjoy Intuitive, Cloud-Based Management

Companies with limited IT staff and security expertise benefit from WatchGuard Cloud. This Cloud-based management platform makes it simple to deploy, configure and manage your endpoint security products. It provides real-time protection and communication with endpoints including our security engine and signatures, and URL filtering capabilities that allow users to send tasks and configurations to thousands of computers in seconds. In addition, WatchGuard Cloud allows you to manage the whole portfolio from a single pane of glass, reducing infrastructure costs and minimizing time spent on reporting and operational tasks.

Extend Security, Visibility and Operations Capabilities

Optional modules are available for all EPP and EDR security products. Add Patch Management to centrally manage updates and patches for operating systems for third-party applications and unsupported (EOL) software programs; deploy Full Encryption to encrypt and decrypt endpoint information; rely on our Advanced Reporting Tool to generate security intelligence and to pinpoint attacks and unusual behaviors; and include Data Control to discover, classify, audit, and monitor unstructured personal data stored on endpoints. SIEMFeeder creates a new source of critical information that monitors all the processes running on your devices. And Systems Management, our RMM tool, to manage, monitor, and maintain all your IT infrastructure.

A Complete Package with Flexible Options to Meet Every Need

WatchGuard EDR and WatchGuard EPDR

- Provides powerful endpoint detection and response (EDR) protection from zero day attacks, ransomware, cryptojacking and other advanced targeted attacks using new and emerging machine-learning and deep-learning AI models.
- Get 100% classification with Zero-Trust Application Service – creating the kind of response required for deployment of a zero trust model. Increase staff utilization and efficiency with insights from the Threat Hunting Service.
- Implement defense-in-depth endpoint security with WatchGuard EPDR, which includes all the benefits of our WatchGuard EDR and EPP products in one package.

WatchGuard Advanced EPDR

- Centralized management and search engine of IoCs compatible with STIX and YARA rules enabling analysts to quickly hunt for recently disclosed incidents, exchange security intelligence, and find impacted endpoints in an incident analysis.
- Advanced EPDR discovers advanced, non-deterministic IoAs mapped to the MITRE ATT&CK framework. The contextual telemetry associated with those IoAs allows analysts to investigate deeper.
- Remote shell allows further investigation, containment, and mitigation of threats. Advanced EPDR enables security analysts to remotely connect to the organization's endpoints from the web console to assess their status, investigate an incident, and take action to contain an attack.

WatchGuard EPP

- Protects endpoints from viruses, malware, spyware, and phishing with signatures, local cache, and even our own proprietary intelligence feeds derived from the malware previously detected from our EDR solutions.
- WatchGuard was built for organizations supporting many different devices. WatchGuard EPP centralizes next-generation antivirus for all your Windows, macOS, and Linux desktops, laptops, and servers, in addition to the leading virtualization systems and Android and iOS devices.

Additional Security Modules

Add optional modules available with all EPP and EDR security products:

WatchGuard Patch Management

WatchGuard Patch Management is a solution to centrally manage updates and patches for operating systems and for hundreds of third-party applications and unsupported (EOL) software programs.

WatchGuard Full Encryption

WatchGuard Full Encryption leverages Microsoft's BitLocker technology to encrypt and decrypt endpoint information with central management of the recovery keys from our WatchGuard Cloud management platform.

Extend with more optional modules available only with WatchGuard EPDR and WatchGuard EDR products:

WatchGuard Advanced Reporting Tool

WatchGuard Advanced Reporting Tool automatically generates security intelligence and provides tools to pinpoint attacks and unusual behaviors and to detect internal misuse of the corporate network.

WatchGuard Data Control*

WatchGuard Data Control* discovers, classifies, audits and monitors unstructured personal data stored on endpoints and servers throughout its lifecycle.

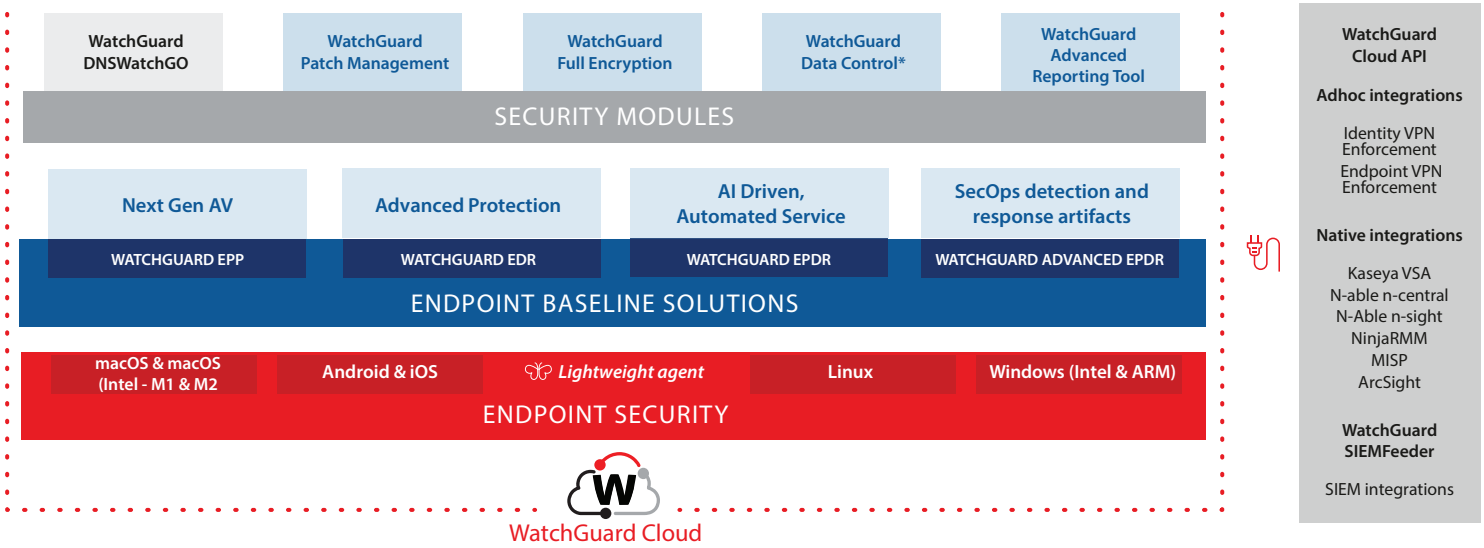
**Available in Spain, Germany, UK, Sweden, France, Italy, Portugal, Holland, Finland, Denmark,Switzerland, Norway, Austria, Belgium, Hungary, and Ireland.*

WatchGuard SIEMFeeder

WatchGuard SIEMFeeder enables a new source of critical information to the security intelligence of all the processes run on your devices while being continuously monitored.

WatchGuard DNSWatchGO

WatchGuard DNSWatchGO provides DNS-level protection and content filtering that keeps businesses safe from phishing, ransomware, and other attacks even when users are outside of the network, without requiring a VPN.



Reasons to Upgrade Your Security

1. Add protection for a distributed workforce as company work-from-home policies expand.

WatchGuard Passport includes WatchGuard EPDR, WatchGuard DNSWatchGO, and WatchGuard AuthPoint for multi-factor authentication. These solutions combine to protect users from the widest range of threats; and beyond endpoint security, it protects company resources from infiltration due to lost or stolen employee credentials – an attack vector used in some of the largest published breaches.

★ Recommended Solution: **WatchGuard Passport**

2. Recover after an attack, or after discovery of latent malware on endpoints or corporate networks when the malware originated on an endpoint.

Companies in this position know two things – first, that they are certainly of interest to cyber criminals and second, that their current level of protection is not adequate. As the advanced protection of WatchGuard EPDR has evolved with the Zero-Trust Application Service and Threat Hunting Service, the number of malware-based attacks that our support team has investigated/remediated has trended to nearly zero – meaning that our customers aren't experiencing them. Combine this with the visibility and management tools to increase the productivity of an over-burdened IT team, and it delivers what's needed to prevent repeated attacks and expensive remediations.

★ Recommended Solution: **WatchGuard EPDR**

3. Elevate Your Detect and Respond capabilities by upgrading to Advanced EPDR.

Designed to empower security teams, WatchGuard Advanced EPDR is the ultimate tool for them to mature their security operations practices. The automated prevention, detection, and response capabilities of WatchGuard EPDR, combined with the advanced version's additional tools, allow security teams to keep organizations ahead in the dynamic and ever-evolving threat landscape and provide unparalleled protection, detection, and response without huge investments.

★ Recommended Solution: **WatchGuard Advanced EPDR**

4. Add EDR to an existing AV solution as a planned security investment.

These companies understand the security risks on the endpoint and have deployed an AV product, but they realize that they need an EDR solution in order to stay ahead of hackers. There's no need to wait for AV contract renewal; our WatchGuard EDR solution layers on top of an existing AV deployment so that customers can quickly benefit from our advanced, differentiated approach.

★ Recommended Solution: **WatchGuard EDR**

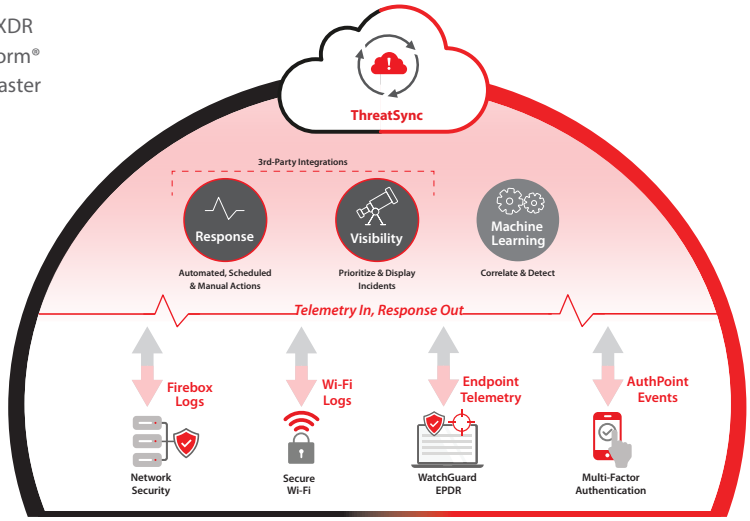
5. Upgrade from a free or consumer-grade endpoint AV product.

Sometimes, small companies or those that have few devices that cross the network perimeter are banking on a reduced risk profile, and so they've put off making investments in security. However, the world is changing, and as businesses become more exposed and need to meet stricter data security and privacy regulations, they move to a business-grade solution like the WatchGuard EPP product. With strong signature-based prevention, including signatures from malware seen in our installed base, as well as behavioral analysis and web content filtering products, WatchGuard EPP is a smart choice that's future-proofed since the platform scales with business growth.

★ Recommended Solution: **WatchGuard EPP**

Access the XDR Realm and Unleash Unified Security

WatchGuard ThreatSync is a comprehensive and simple-to-use XDR solution included as part of WatchGuard's Unified Security Platform® architecture that unifies cross-product detections and enables faster threat remediation from a single interface.



* Secure Wi-Fi and AuthPoint will be available soon, integrated into ThreatSync.

THE WATCHGUARD PORTFOLIO

Network Security

WatchGuard offers a wide range of network security solutions, including everything from tabletop and 1U rack-mounted appliances to Cloud and virtual firewalls. Our Firebox® appliances deliver critical security services, from standard IPS, URL filtering, gateway AV, application control, and antispam, to advanced protections such as file sandboxing, DNS filtering, and more. High-performance deep packet inspection (DPI) means you can leverage all our security services against attacks attempting to hide in encrypted channels like HTTPS. Additionally, every Firebox offers SD-WAN right out of the box for improved network resiliency and performance.

Identity Security

WatchGuard AuthPoint Identity Security solutions are designed to provide top-rated multi-factor authentication (MFA) and zero trust risk policies for maximum online protection. Enjoy the convenience of a corporate password manager that automatically fills in credentials across browsers like Chrome, Edge, Safari, and Firefox. Leverage our dark web monitoring services to mitigate the risks of widespread workforce credential attacks. AuthPoint also delivers optimized user experience with online and offline authentication methods, along with a web application portal for easy single sign-on access.

Secure Cloud Wi-Fi

WatchGuard's secure, Cloud-managed Wi-Fi solutions provide safe, protected airspace for Wi-Fi environments while eliminating administrative headaches and greatly reducing costs. From home offices to expansive corporate campuses, WatchGuard offers Wi-Fi 6 technology with secure WPA3 encryption. With WatchGuard Cloud, Wi-Fi network configuration and policy administration, zero-touch deployment, customized captive portals, VPN configuration, expansive engagement tools, visibility into business analytics, and upgrades are only a click away.

Endpoint Security

WatchGuard Endpoint Security solutions help you safeguard devices against cyber threats. WatchGuard EPDR and Advanced EPDR, our AI-powered flagship endpoint solutions, enhance your security posture by seamlessly integrating endpoint protection (EPP) with detection and response (EDR) capabilities alongside our Zero-Trust Application and Threat Hunting Services. All are tightly integrated within WatchGuard Cloud and ThreatSync, delivering valuable visibility and intelligence while fortifying cross-product detection and response (XDR).

Find out more

For additional details, talk to an authorized WatchGuard reseller or visit **https://www.watchguard.com.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world- class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.