Endpoint Protection, Detection and Response

One Solution for Complete Endpoint Security

WatchGuard EPDR brings together our Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) capabilities into one easy-to-buy product for maximum security against sophisticated endpoint threats. We layer on traditional, signature-based techniques with advanced features and services for a unique, comprehensive offering. By enabling continuous endpoint monitoring, detection and classification of all activity, we are able to reveal and block anomalous behaviors of users, machines and processes. At the same time, we proactively discover new hacking and evasion techniques and tactics to quickly arm our customers. These advances are included at no extra cost and immediately add an additional intelligent layer of protection to get ahead of attackers.

Key Features

- EDR for continuous monitoring that prevents the execution of unknown processes
- Automatic detection and response for targeted attacks and in-memory exploits
- Zero-Trust Application and Threat Hunting features delivered as managed services
- Behavioral analysis and detection of IoAs (indicators of attack) scripts, macros, etc.
- Endpoint protection capabilities such as URL filtering, device control and managed firewall
- Lightweight agent and easy-to-use Cloud-based console with detailed reporting

Protection Against Modern Cyberattacks

WatchGuard EPDR is an innovative cybersecurity solution for laptops, computers and servers that combines the widest range of endpoint protection (EPP) technologies with EDR capabilities. It protects users from advanced threats, APTs, zero day malware, ransomware, phishing, rootkits, in-memory exploits and malware-less attacks, and also provides IDS, firewall, device control, and URL & content

filtering capabilities. EPDR uniquely automates the prevention, detection, containment, and response actions for ultimate security that is easy to manage and deploy.

100% Confidence with Zero Trust

With this service, processes are classified as either malware or as trusted prior to letting only the trusted execute on each endpoint, thereby enabling the ultimate default-deny posture. Our AI system automatically classifies 99.98% of all running processes with the remaining percentage manually classified by our cybersecurity experts. This approach allows us to classify 100% of all binaries without creating false positives or false negatives.

Eliminate Threats Uncertainty >

Anticipate Attackers with Threat Hunting

Our team of cybersecurity experts analyze any suspicious activity potentially related to hacking and investigate the indicators of attack to find evasion and compromise techniques. Our hunters also proactively search for patterns of anomalous behavior not previously identified on the network to help EPDR customers:

- Reduce the MTTD and MTTR (mean time to detect and mean time to respond).
- Create new rules representing new IoAs that can be delivered to the endpoints to rapidly protect them against new attacks.
- Get recommendations on how to mitigate an attack and reduce the attack surface to avoid falling victim to future attacks.

Stay One Step Ahead of Threats >

Unify Network and Endpoint Defenses

WatchGuard EPDR is managed in WatchGuard Cloud, providing a single-pane-of-glass view into our entire Unified Security Platform architecture. WatchGuard Cloud is a single, centralized interface for delivering and managing network security, advanced threat detection, multi-factor authentication, and endpoint security.

Simplify Your Security >

Uncover Your Vulnerability Risks

Why start patching when it's already too late? Identify potential vulnerabilities and take proactive measures to mitigate them before attackers exploit them. The vulnerability assessment tool helps businesses to evaluate and prioritize security weaknesses and vulnerabilities in applications and systems, so you improve your security posture and ensure your organization stays ahead of the latest threats.

Is Your Team Ready to Elevate Their Security Operations Practice?

Attackers are using legitimate tools and behaviors to avoid detection. Cybersecurity teams must shift to security operations and connect suspicious indicators to mitigate damage. WatchGuard Advanced EPDR provides automatic detection of malicious files and behavioral analysis, making it easier for analysts to hunt down weaker threat signals and quickly take control of compromised endpoints to investigate and prevent breaches.

Empower Your Team >