DATASHEET

WATCHGUARD ADVANCED EPDR

CYBERSECURITY CHALLENGES

Endpoints are the primary target for most cyberattacks. As the technology infrastructure becomes more complex, organizations struggle to find the expertise necessary to monitor and manage endpoint security risks. So, what types of challenges are security teams facing when adopting endpoint security solutions?

- **Ever-evolving sophisticated threats:** Efficient, proactive security practices can mean distinguishing between a minor security operation or being a victim. These practices range from reducing the attack surface to uncovering emerging threats before an actual compromise.
- **Alert fatigue, lack of efficiency:** Security teams receive thousands of weekly alerts, of which only 19% are considered trustworthy, and only 4% are investigated. Two-thirds of security teams' time is dedicated to managing alerts and classifying suspicious files manually.
- **Poor performance:** Frequently, endpoint security solutions require installation and management of multiple agents on each monitored computer, server, and laptop, causing serious errors, poor performance and high resource consumption.

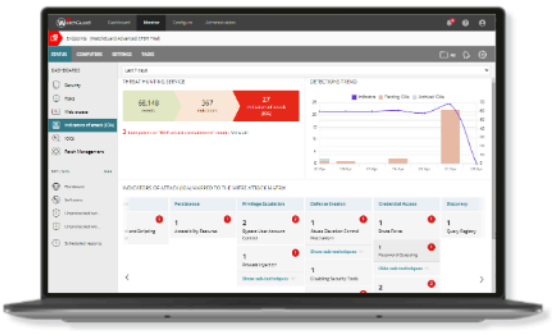
As defenders, security teams need autonomous prevention, detection, and response solutions and weapons to easily hunt, investigate, and respond to threats lurking in the environments, taking the security stack to the next level to minimize adversaries' dwell time.

LEVEL UP YOUR CYBERSECURITY SERVICES

WatchGuard Advanced EPDR is a cloud-delivered solution for computers, laptops, and servers that automates prevention, detection, containment, and response to advanced threats. It unifies preventive and EDR technologies with advanced AI-powered services:

- **Zero-Trust Application Service:** cloud-based AI sytem automatically classifies all executables, eradicating known and unknown malware.
- **Threat Hunting Service:** behavioral analytics in the cloud, to uncover threat actors utilizing living-off-the-land (LotL) techniques
- **AI/ML analytics** detect Living-off-the-land, fileless and script attacks, and blocks hidden threats in installers, PDFs, and Office files.
- **Automated Incident Reconstruction:** attack path visualization that reduces alert volume and speeds incident understanding
- **GenAI Assistant:** natural language queries over telemetry, boosting usability and team efficiency

WatchGuard Advanced EPDR extends EPDR with hunting and investigation tools, including IoC search, advanced IoA detection, enriched telemetry, and MITRE ATT&CK–mapped analytics, plus remote access to Windows, macOS, and Linux for faster investigation and response.



Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS and Android.

WatchGuard Advanced EPDR unifies preventive and EDR technologies in a single cloud-delivered solution, automating prevention, detection, containment, and response against advanced threats across endpoints.

Attack Surface Reduction

- Centralized endpoint Security Risk detection and scoring
- Unmanaged endpoint proactive detection
- Vulnerability assessment for OS and hundreds of applications

Prevention

- Firewall (IDS), device and application control
- Multi-vector anti-malware with on-demand scan
- Pre-execution heuristics and Collective Intelligence
- Self-learning AI with behavioral analytics detects malware, ransomware, fileless and script-based attacks
- ML analysis of installers, PDFs, Office files for hidden threats with automatic blocking
- URL and web filtering, anti-phishing, anti-tampering • Detection via network traffic analysis
- Endpoint Access Enforcement that blocks lateral movements

Hunting and Detection Technologies

- Continuous endpoint monitoring with EDR
- Zero Trust Application and Threat Hunting services
- Sandboxing in real environments & anti-exploit protection
- Automated detection and containment of RDP attacks
- STIX indicators of attack (IoCs) and YARA rules searches
- Execution monitoring or denial of common LotL applications
- Access to the enriched telemetry
- Events and indicators of attack (IoAs) mapped to MITRE ATT&CK
- CAPA tool: file information (behaviors, strings, imports, exports) •
- Automated incident attack path reconstruction
- GenAI Assistant to query telemetry

Containment and Remediation

- Endpoint isolation, reboot & remote shell
- Automatic remediation & rollback
- Encrypted file recovery (shadow copies)

BENEFITS

Cost-Effective Operations - No More Wasted Time on Suspicious Files
Like WatchGuard EPDR, the Zero-Trust Application Service gives your team back all that time dedicated to reverse engineering suspicious files that other solutions alert on without closing the loop and delegating the last verdict to you.

Comprehensive Endpoint Security to Tailor to Your Services
WatchGuard Advanced EPDR provides a comprehensive range of capabilities to strengthen endpoint security programs, including attack surface reduction, threat prevention, detection, and response, proactive hunting tools and remote endpoint connection for prompt response.

Enhanced Hunting and Response at Your Fingertips
Thanks to centralized IoC searches, WatchGuard Advanced EPDR enables security teams to discover threats without dealing with complex queries. The Threat Hunting Service delivers IoAs contextualized with telemetry. IoAs and events are enriched with MITRE tactics and techniques for swift correlation and response.

Scalable Managed Security Services to Grow at Your Pace
WatchGuard's Unified Security Platform architecture brings comprehensive security from network to endpoint, Wi-Fi, and identity, with unparallel platform features, at no additional cost. The more services you adopt, the greater your operational and business benefits.

ZERO TRUST MODEL: A LAYERED PROTECTION

WatchGuard's Endpoint Security platform doesn't rely on just one single technology. We implement layers of tools together to reduce the opportunity for a threat actor to succeed. Working in concert, these technologies utilize resources at the endpoint to minimize the risk of a breach.

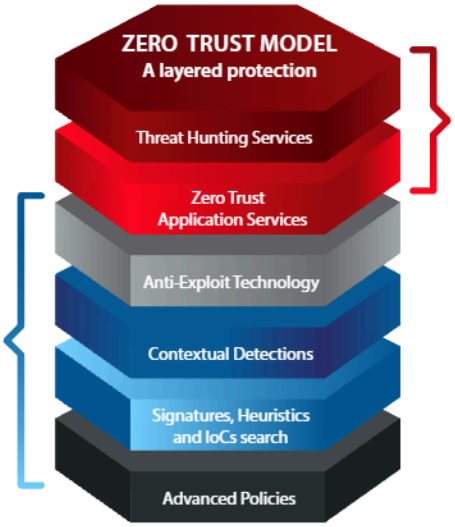
ENDPOINT LAYERS:

Layer 1/ / Enhanced Security Policies
Detect or block the execution of common attack techniques

Layer 2 / Signature Files, Heuristic Technologies and STIX IoCs Search Engine enables security teams to hunt for recently disclosed attacks by hash, filename, path, C2 domain, IP, and YARA Rules

Layer 3 / Contextual Detections of malwareless attacks using OS tools such as PowerShell, WMI, web browsers, and other commonly targeted applications such as Java, Adobe, and more.

Layer 4 / Anti-Exploit Technology
It enables us to detect fileless attacks designed to exploit vulnerabilities



CLOUD-NATIVE LAYERS

Layer 5 / Zero-Trust Application Service
Classifies 100% of processes before they run, denying any execution until it is certified as trusted

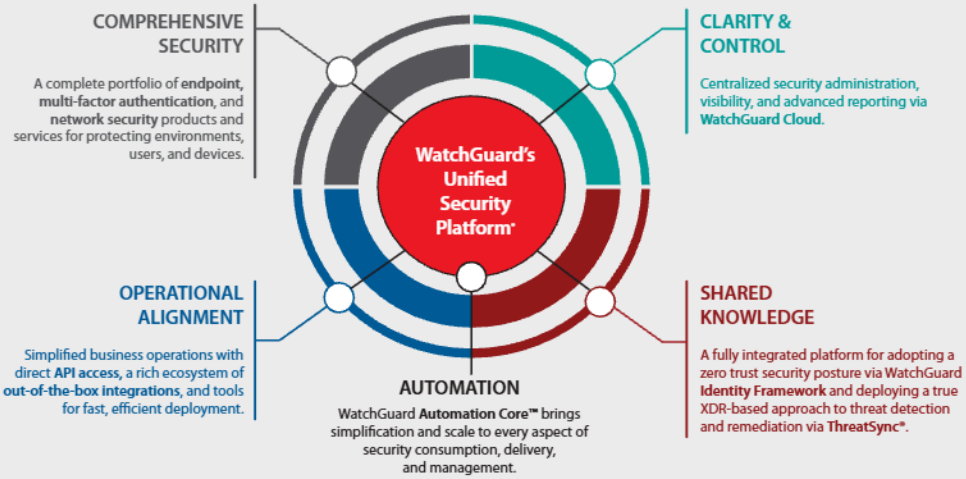
Layer 6 / Threat Hunting Service
It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs. Non-deterministic IoAs are contextualized in the Cloud-based console with the associated telemetry, enabling security analysts to investigate potential attack attempts.

IMPLEMENT POWERFUL, SIMPLIFIED SECURITY WITH WATCHGUARD'S UNIFIED SECURITY PLATFORM

WatchGuard Unified Security Platform architecture is a single platform for elevating modern security delivery.

Our platform approach helps you deliver powerful security services for every threat vector with increased scale and velocity while supporting operational efficiencies and greater profitability. Learn more here.

A single, scalable platform for elevating modern security delivery.



U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com
WatchGuard Technologies, Inc.