DATASHEET

WATCHGUARD EPDR

Endpoint Protection Detection and Response

ORGANIZATIONAL CYBERSECURITY CHALLENGES

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

- **Alert fatigue:** organizations receive thousands of weekly malware alerts, of which only 19% are considered trustworthy, and only 4% of which are ever investigated. Two-thirds of cybersecurity admins' time is dedicated to managing malware alerts.
- **Complexity:** too many disconnected cybersecurity tools can be hard to manage for security professionals, due to the number of enabling technologies, the lack of in-house skills, and the time needed to identify threats.
- **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.

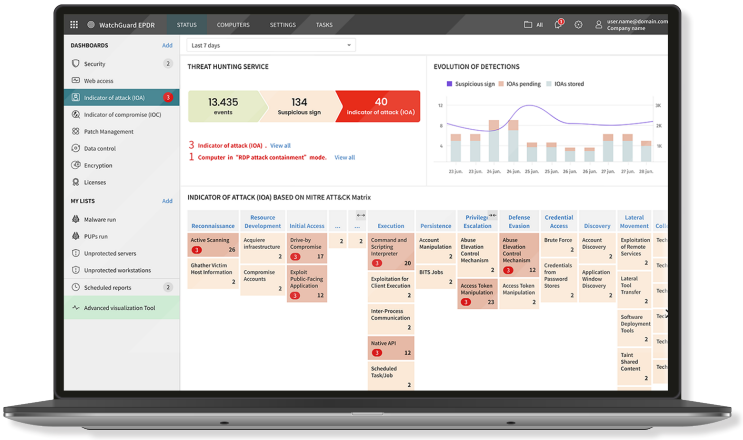
Traditional endpoint protection technologies focused on prevention are valid for known threats and malicious behaviors, but they are not enough against advanced cyber threats. From common compromise vectors to new threats, attackers are always looking for ways to escape IT notice, evade defense measures and exploit emerging weaknesses.

FROM PREVENTION TO RESPONSE - AUTOMATED ENDPOINT SECURITY

WatchGuard EPDR is an innovative cybersecurity solution for computers, laptops and servers, delivered from the Cloud. It automates the prevention, detection, containment and response to any advanced threat, zero day malware, ransomware, phishing, in-memory exploits, and fileless and malwareless attacks, inside and outside the corporate network.

Unlike other solutions, it combines the widest range of endpoint protection technologies (EPP) with automated detection and response (EDR) capabilities. It also has two services, managed by WatchGuard experts, that are delivered as a feature of the solution:

- **Zero-Trust Application Service:** 100% classification of the applications
- **Threat Hunting Service:** detecting hackers and insiders



WatchGuard EPDR integrates traditional endpoint technologies with innovative, adaptive protection, detection and response technologies in a single solution. This allows IT pros to deal with advanced cyber threats, including the following advanced security technologies:

Traditional Preventive Technologies

- Personal or managed firewall (IDS)
- Device control
- Collective Intelligence
- Deny list / Allow list
- Permanent multi-vector anti-malware & on-demand scan
- Pre-execution heuristics
- URL filtering – web browsing
- Anti-phishing
- Anti-tampering
- Remediation and rollback

Advanced Security Technologies

- Continuous endpoint monitoring with EDR
- Cloud-based machine that learns to classify 100% of processes (APTs, ransomware, rootkits, etc.)
- Sandboxing in real environments
- Anti-exploit protection
- Threat hunting, including behavioral analysis and detection of IoAs (indicators of attack) to detect LotL (living off the land attacks)
- Indicators of attack mapped to MITRE ATT&CK Framework
- Detection and prevention of RDP attacks
- Containment and remediation capabilities such as computer isolation and program blocking by hash or name

BENEFITS

Simplifies & Maximizes Security

- Its automated services reduce the costs of expert personnel. There are no false alerts to manage, no time wasted on manual settings, and no responsibility is delegated.
- No management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted since it is based on a lightweight agent and Cloud-native architecture.

Easy to Use and Easy to Manage

- Endpoint Security portfolio handles all needs of your endpoint protection in a remarkably simple way from a single web console.
- Easy to set up. Cross-platform endpoint management from a single pane of glass.
- It provides a clean and obvious user interface design that can be quickly mastered.

Automated EDR Features

- Detects and blocks hacking techniques, tactics and procedures, and malicious in-memory activity (exploits) before it can cause damage.
- Resolution and response: forensic information to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each action: actionable visibility into the attacker and their activity, facilitating forensic investigation.

ZERO-TRUST MODEL: A LAYERED PROTECTION

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

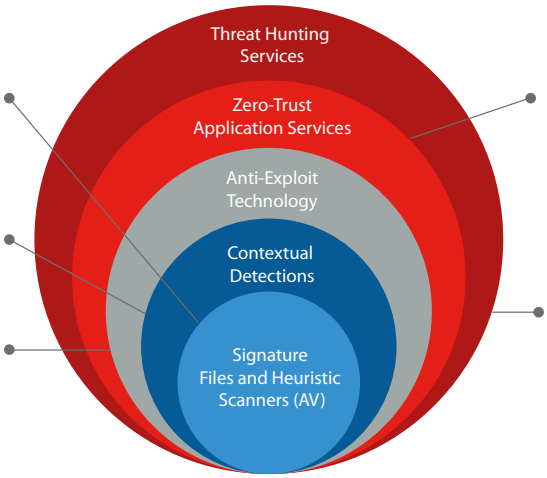
Zero-Trust Model: A layered protection

ENDPOINT LAYERS:

Layer 1/ Signature Files and Heuristic Technologies
Effective, optimized technology to detect known attacks

Layer 2 / Contextual Detections
They enable us to detect malwareless and fileless attacks

Layer 3 / Anti-Exploit Technology
It enables us to detect fileless attacks designed to exploit vulnerabilities



CLOUD-NATIVE LAYERS

Layer 4 / Zero-Trust Application Service
Provides detection if a previous layer is a breach, stops attacks on already infected computers and stops lateral movement attacks inside the network

Layer 5 / Threat Hunting Service
It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs

Signature files and heuristic technologies, known as traditional endpoint protection (EPP), make up a next-generation antivirus technology layer that is proven effective against many common, low-level threats. It's optimized to detect known attacks, based on specific signatures, generic and heuristic detection, and malicious URL blocking.

Contextual detection is key for detecting malwareless and fileless attacks as it looks for abnormal resource and application utilization. It is very effective against script-based attacks, attacks using goodware OS tools such as PowerShell, WMI, etc., web browser vulnerabilities and other commonly targeted applications such as Java, Adobe, and more.

Anti-exploit technology detects fileless attacks that are designed to exploit vulnerabilities. It searches for and detects anomalous behavior – a surefire signal of exploited processes. Anti-exploit technology is mission-critical on unpatched/waiting-to-be-patched endpoints, and on endpoints with operating systems that are no longer supported.

Our **Zero-Trust Application Service** classifies 100% of processes, monitors endpoint activity, and blocks the execution of applications and malicious processes. For each execution, it sends out a real-time classification verdict, malicious or legitimate, with no uncertainty and without delegating decisions to the user, avoiding manual processes.

The **Threat Hunting Service** is based on a set of threat hunting rules created by cybersecurity 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).

Supported platforms and systems requirements of Watchguard EPDR

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux 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, Internet Explorer, Microsoft Edge and Opera.

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