DATASHEET

WatchGuard EDR

Endpoint Detection and Response

Cyber Defense Against Advanced Threats

State-of-the-art cyber attacks are designed to get around the protection provided by traditional security solutions. These attacks are becoming more frequent and more sophisticated as hackers become more professionalized. It is also a result of a lack of focus on correcting security vulnerabilities in systems.

In light of this scenario, traditional endpoint protection platforms (EPPs) do not provide detailed enough visibility into the processes and applications running on corporate networks. What's more, some EDR solutions, far from solving anything, create greater stress and increase security administrator workloads by delegating the responsibility for managing alerts and forcing them to manually classify threats.

Enhance Your Security – Step up to Automated EDR

WatchGuard EDR 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 malwareless attacks, both present and future, inside and outside the corporate network.

WatchGuard EDR was built to provide complete visibility into your endpoints by monitoring and spotting malicious activity that bypasses traditional solutions. WatchGuard EDR installs on top of existing antivirus solutions to add a full stack of EDR capabilities including the following automated services:

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

WatchGuard EDR provides the means to effectively combat threats and respond to malicious attacks by enabling the following 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
- Network attack protection: prevent attacks exploiting vulnerabilities in Internet-exposed service
- Threat hunting: behavioral analysis and detection of indicators of attack (IoAs) to detect living off the land attacks (LotL)
- Twelve-month data retention and real-time physical sandboxing to avoid unnoticed hacker actions
- 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
- Recover encrypted files with shadow copies

Benefits

Simplifies & Minimizes Security Costs

- Its managed services reduce the costs of expert personnel. There are no false alerts to manage and no responsibility is delegated.
- Cross-platform endpoint management from a single pane of glass.
- Endpoint performance is not impacted, since it is based on a lightweight agent and Cloud-native architecture.

Automates & Reduces Detection Time

- Applications that pose a security risk can be blocked (by hash or name).
- Blocks the execution of threats, zero day malware, fileless/malwareless attacks, ransomware and phishing.
- Detects and blocks hacking techniques, tactics and procedures.

Automates & Reduces Response & Investigation Time

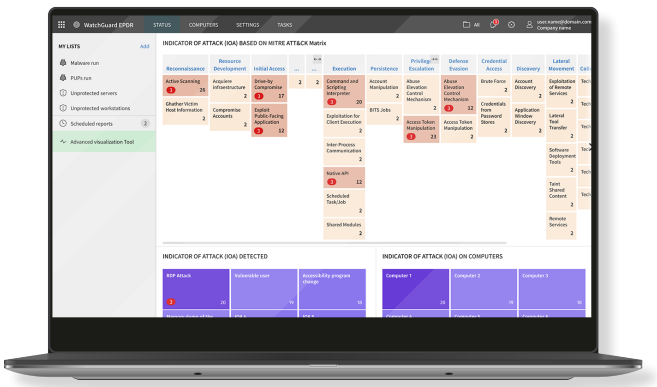
- Resolution and response: forensic information to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each action: actionable visibility into the attacker and their activity. Advanced indicators of attack (IoAs) investigations.
- Improvements and adjustments to security policies thanks to forensic analysis conclusions.

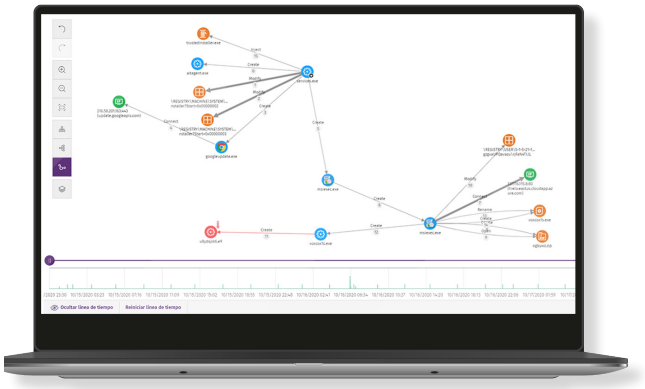
Zero Trust & Threat Hunting

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.

The **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 decision to the client, avoiding manual processes. All of this is possible thanks to the capacity, speed, adaptability and scalability of AI and Cloud processing.

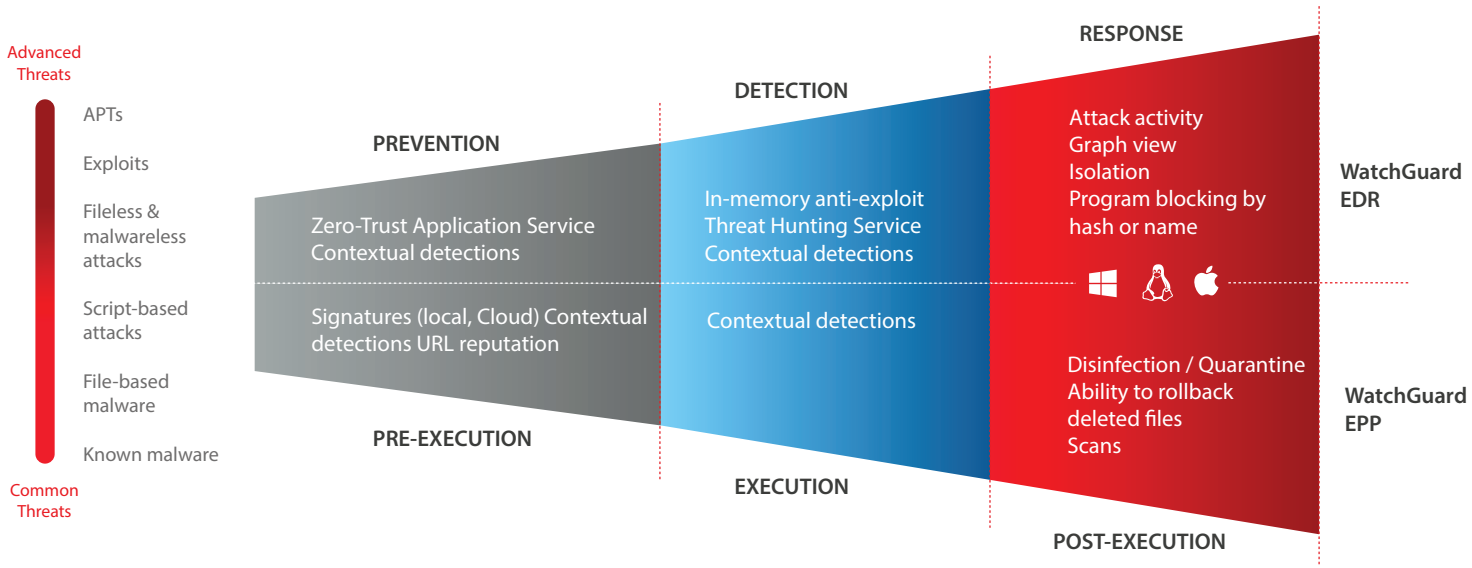
The service unifies big data technologies and multi-level machine-learning techniques, including deep learning, the results of continuous supervision and the automation of the experience and knowledge accumulated by WatchGuard's threat team.





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).

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. The hunters at WatchGuard work on the premise that organizations are constantly being compromised.



Supported platforms and systems requirements of Watchguard EDR

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

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, Microsoft Edge and Safari.

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