DATASHEET

WATCHGUARD EPDR

Endpoint Protection, Detection and Response.

ORGANIZATIONAL CYBERSECURITY

Mobility, processing, and remote work have all revolutionized the business environment. Endpoints are the primary target for most cyber attacks. This is why endpoint security solutions need to be advanced, adaptive, and automatic, with the highest possible levels of prevention and detection and response.

Organizations receive thousands of weekly malware alerts, of which only 19 percent are considered trustworthy, and only 4 percent of which are ever investigated. Two-thirds of cybersecurity administrators' time is dedicated to managing malware alerts.

SOPHISTICATION OF CYBER ATTACKS

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 protection platforms (EPPs) are insufficient. This is because they 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 administrators' workloads by delegating the responsibility for managing alerts and forcing them to manually classify threats.

WATCHGUARD EPDR

Proactive Detection and Threat Hunting

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

Unlike other solutions, it combines the widest range of protection technologies (EPP) with automated detection and response 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

Thanks to its Cloud-based architecture, its agent is lightweight and has minimum impact on endpoints, which are managed via WatchGuard Cloud. WatchGuard Cloud allows you to manage the whole portfolio from a single pane of glass, reduces infrastructure costs and minimizes time spent on reporting and operational tasks.

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.
- The managed services automatically learn from threats. No time wasted on manual settings.
- 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.

Automates & Reduces Detection Time

- Blocks applications that pose a security risk (by hash or process name).
- Blocks the execution of threats, zero day malware, fileless/malwareless attacks, ransomware and phishing.
- Detects and blocks malicious in-memory activity (exploits) before it can cause damage.
- 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 of the attacker and their activity, facilitating forensic investigation.
- Improvement and adjustments to security policies thanks to the conclusions of the forensic analysis.

ADVANCED AND AUTOMATED ENDPOINT SECURITY

Traditional protection technologies (EPPs) focused on prevention are low-cost measures, valid for known threats and malicious behaviors, but they are not enough. Successfully defending an organization and putting an end to cyber threats forces a shift away from traditional prevention to continuous prevention, detection and response, assuming at all times that the organization has been compromised, and that all endpoints are continually being threatened by attackers.

WatchGuard EPDR integrates traditional preventive technologies with innovative, adaptive prevention, detection and response technologies in a single solution, to deal with advanced cyber threats, both present and future:

Traditional Preventive Technologies

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

Advanced Security Technologies

- Continuous endpoint monitoring with EDR
- Prevention of execution of unknown processes
- Cloud-based machine that learns to classify 100% of processes (APTs, ransomware, rootkits, etc.)
- Sandboxing in real environments
- Behavioral analysis and detection of IoAs (indicators of attack) such as scripts, macros, etc.
- Threat hunting
- Computer isolation
- Program blocking by hash or name
- Attack activity graph view

ZERO-TRUST MODEL

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 managed Threat Hunting Service is operated by a team of experts who use profiling analysis and event correlation tools to proactively discover new hacking and evasion techniques. The hunters at WatchGuard work on the premise that organizations are constantly being compromised.

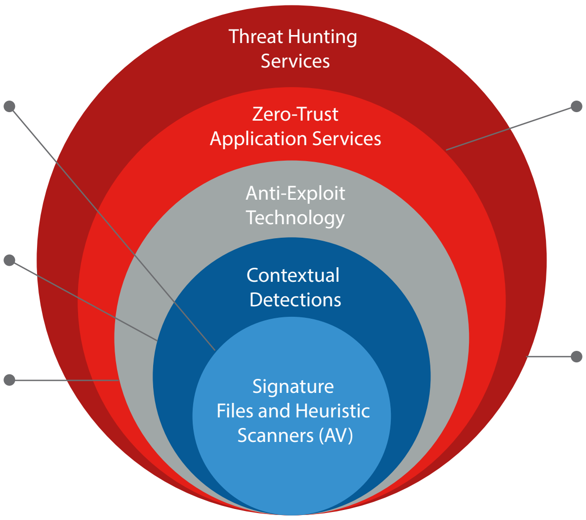
Zero-Trust Model: A layered protection

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


Threat Hunting Services
Zero-Trust Application Services
Anti-Exploit Technology
Contextual Detections
Signature Files and Heuristic Scanners (AV)

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 and suspicious activities

Supported platforms and systems requirements of Watchguard EPDR

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