DATASHEET

WatchGuard EDR

Endpoint Detection and Response

AI-Powered Defense Against Advanced Threats

Traditional endpoint protection and antivirus solutions, while essential for defending against known malware, fall short in providing the visibility and advanced technologies required for early detection and automated response to sophisticated attacks. Cyber threats are becoming more frequent and complex as attackers continuously refine their methods.

Single point endpoint security solutions often generate low-priority alerts that burden IT and security administrators, forcing them to manually manage and classify threats. This not only increases stress but also means critical alerts may be overlooked.

Enhance Your Security – Step up to Automated EDR

WatchGuard EDR is a Cloud-based cybersecurity solution for multiple devices. It automates prevention, detection, containment, and response to advanced threats like zero-day malware, ransomware, phishing, in-memory exploits, and fileless attacks. With full endpoint visibility, WatchGuard EDR identifies and stops cyber attacks missed by traditional security solutions.

WatchGuard EDR seamlessly integrates with existing antivirus solutions, enhancing your security framework with a full stack of EDR capabilities and managed services:

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

Key Features

- AI-driven Threat Detection: uses Cloud-based AI and machine learning technologies to classify 100% processes and applications.
- Physical Sandboxing: applications behavioral analysis in secure environments to identify threats.
- Anti-Exploit Protection: guards against exploit-based attacks.
- Network Attack Protection: prevent attacks exploiting vulnerabilities in Internet-exposed service.
- IoAs Detection: analytics based on the MITRE ATT&CK™ Framework provide indicators of attack to mitigate ongoing threats and prevent future attacks.
- RDP Attack Detection & Prevention: ensures security against remote desktop protocol attacks.
- Containment & Remediation: includes capabilities like program blocking and device isolation.
- File Recovery: recovers encrypted files using shadow copies.

Benefits

Simplifies & Minimizes Security Costs

- Managed services reduce the need for expert personnel and eliminate false alerts, ensuring no responsibility is delegated.
- Cross-platform endpoint management from a single pane of glass.
- Lightweight agent and Cloud-native architecture ensure no impact on endpoint performance.

Automates & Reduces Detection Time

- Blocks risky applications by hash or name.
- Prevents the execution of zero-day malware, fileless attacks, ransomware, and phishing.
- Detects and blocks hacking techniques, tactics, and procedures.

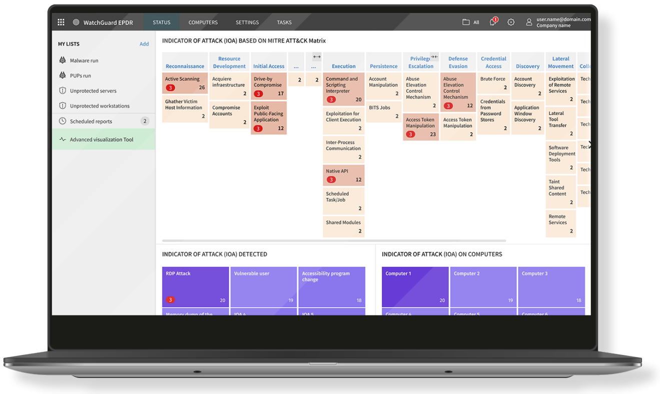
Reduces Response & Investigation Time

- Provides forensic information for thorough investigation and mitigation of attack effects (disinfection).
- Offers actionable visibility into attacker activities and advanced IoA investigations.
- Enables improvements to security policies based on forensic analysis conclusions.

Zero Trust & Threat Hunting

WatchGuard's endpoint security 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 manual intervention, leveraging AI technologies and Cloud processing for scalability and adaptability.



INDICATOR OF ATTACK (IOA) BASED ON MITRE ATT&CK Matrix

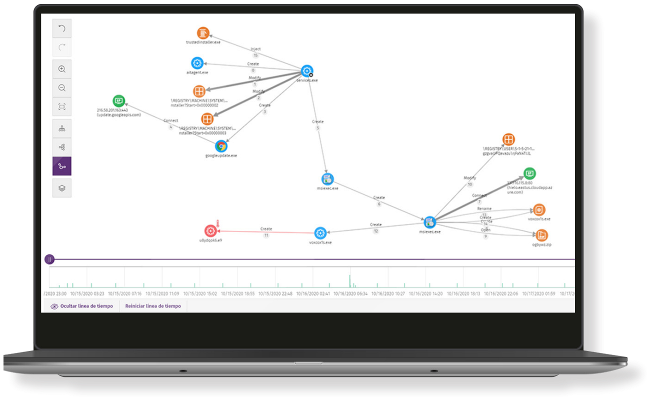
Reconnaissance	Resource Development	Initial Access	...	...	Execution	Persistence	Privileg Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Coll
Active Scanning 3 26	Acquiere infraestructure 2	Drive-by Compromise 3 17	2	2	Command and Scripting Interpreter 3 20	Account Manipulation 2	Abuse Elevation Control Mechanism 2	Abuse Elevation Control Mechanism 3 12	Brute Force 2	Account Discovery 2	Exploitation of Remote Services 2	Tech
Ghather Victim Host Information 2	Compromise Accounts 2	Exploit Public-Facing Application 3 12			Exploitation for Client Execution 2	BITS Jobs 2	Access Token Manipulation 3 23	Access Token Manipulation 2	Credentials from Password Stores 2	Application Window Discovery 2	Lateral Tool Transfer 2	Tech
					Inter-Process Communication 2						Software Deployment Tools 2	Tech
					Native API 3 12						Taint Shared Content 2	Tech
					Scheduled Task/Job 2						Remote Services 2	Tech
					Shared Modules 2							Tech

INDICATOR OF ATTACK (IOA) DETECTED

RDP Attack 3 20	Vulnerable user 19	Accessibility program change 18
Memory dump of the	IOA 4	IOA 5

INDICATOR OF ATTACK (IOA) ON COMPUTERS

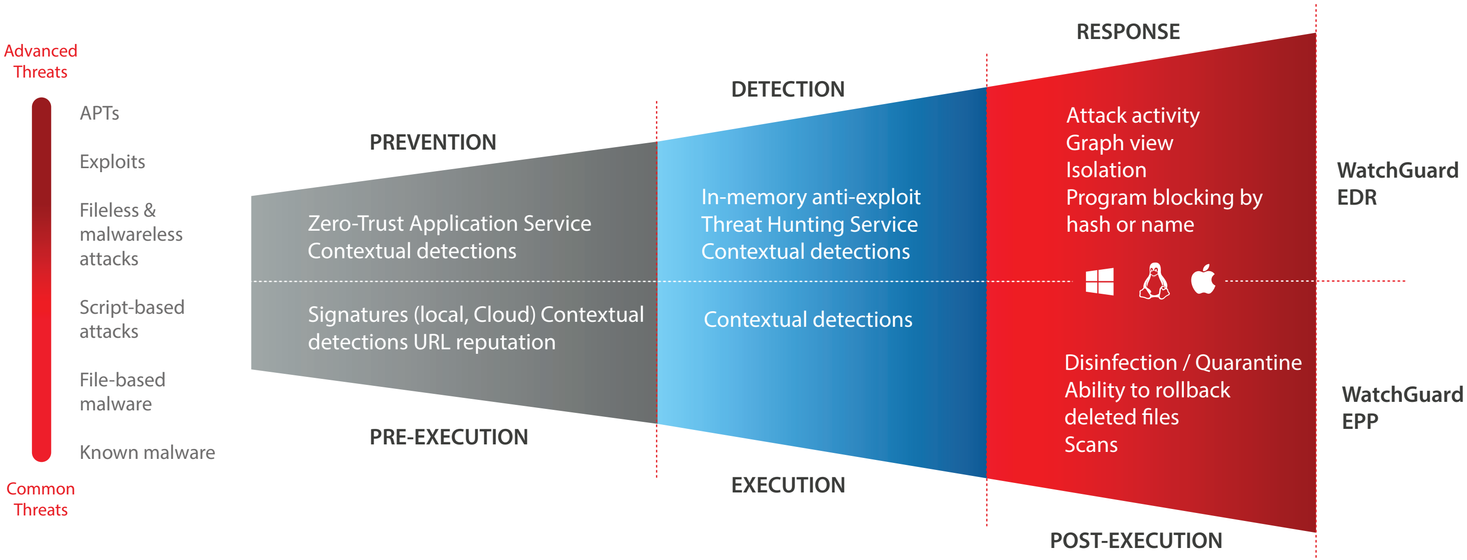
Computer 1 20	Computer 2 19	Computer 3 18
Computer 4	Computer 5	Computer 6



The **Threat Hunting Service** utilizes rules created by cybersecurity specialists, processed against all telemetry data to trigger high-confidence IoAs with minimal false positives. This continuous process employs advanced analytics, proprietary threat intelligence, and expert analysis to discover and minimize MTTD and MTTR, operating on the premise that organizations are constantly targeted.

Eliminate Missed Threats with Complete EDR Security

Upgrade your security with WatchGuard EDR. Enhance your traditional antivirus with cutting-edge EDR capabilities to stay ahead of advanced threats. With automated detection, response, and continuous monitoring, WatchGuard EDR provides comprehensive protection for your devices, users, and data. Our unique Zero-Trust Application Service and Threat Hunting Service help minimize the impact of modern cybersecurity challenges, ensuring robust and proactive security for your business. Secure your tomorrow, today.



Advanced Threats

APTs

Exploits

Fileless & malwareless attacks

Script-based attacks

File-based malware

Known malware

Common Threats

PREVENTION

Zero-Trust Application Service
Contextual detections

Signatures (local, Cloud) Contextual detections URL reputation

PRE-EXECUTION

DETECTION

In-memory anti-exploit
Threat Hunting Service
Contextual detections

Contextual detections

EXECUTION

RESPONSE

Attack activity
Graph view
Isolation
Program blocking by hash or name

Disinfection / Quarantine
Ability to rollback deleted files
Scans

POST-EXECUTION

WatchGuard EDR

WatchGuard EPP

Supported platforms and systems requirements of Watchguard EDR

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

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.

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. Part No.WGCE67475_052124