

# 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.

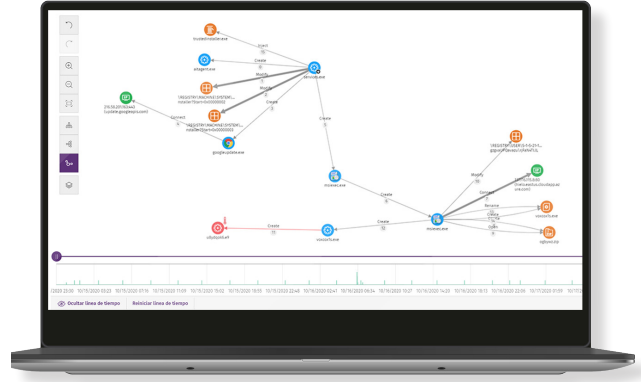
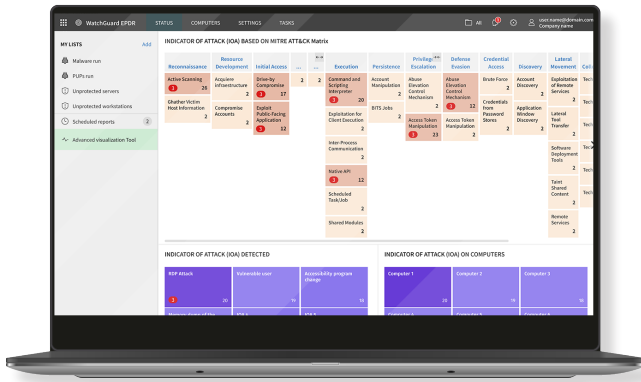
#### Reduces Response & Investigation Time

- 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.

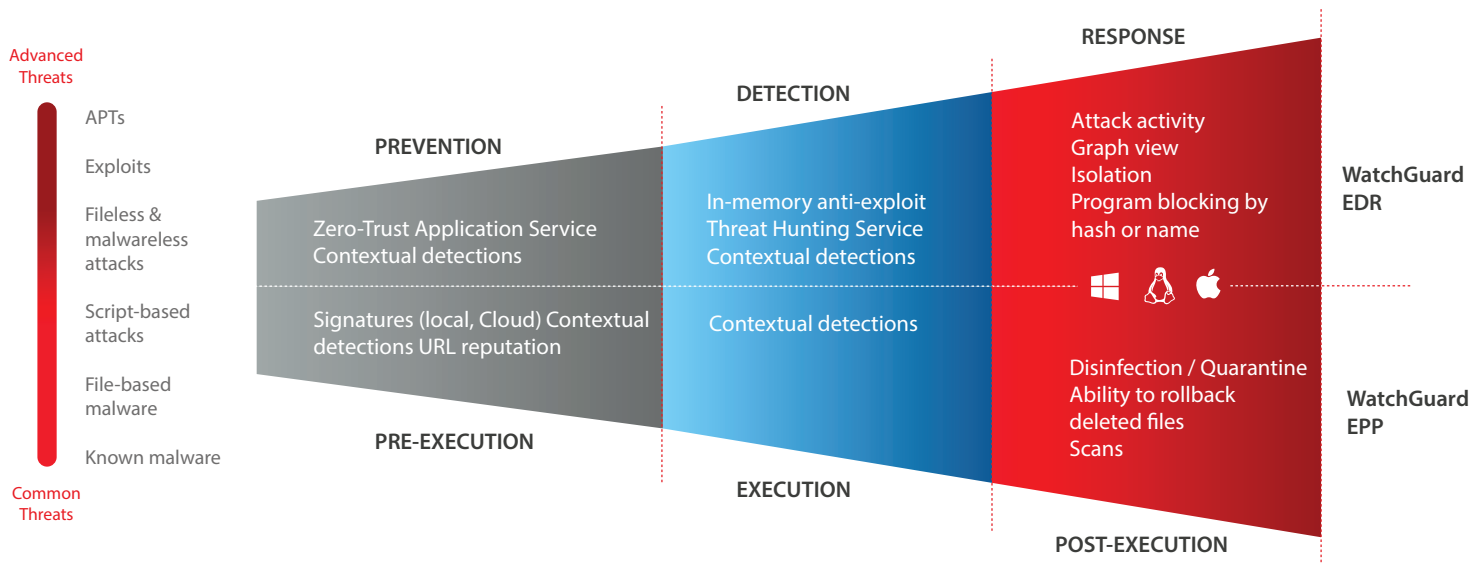
The **Zero-Trust Application Service** classifies 100% of processes, monitors endpoint activity, and blocks the execution of applications and malicious processes. For each execution, it sends out a real-time classification verdict, malicious or legitimate, with no uncertainty and without manual intervention, leveraging AI technologies and Cloud processing for scalability and adaptability.



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.



### 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](#).