Top Reasons to Buy WatchGuard Endpoint Security

WatchGuard EPDR offers the ultimate endpoint security package, combining next-gen antivirus with EDR capabilities. It includes the unique Zero-Trust Application Service that certifies the legitimacy and safety of all running applications thanks to a combination of automated, AI-driven processes and threat hunting services for detecting malicious actors and insiders.

WatchGuard EPDR delivers XDR capabilities, and when combined with the cross-product correlation that our Unified Security Platform architecture provides, the solution heightens deep visibility and security efficacy against sophisticated attacks.

Why Organizations Are Choosing WatchGuard EPDR

WatchGuard EPDR does not rely on just one single technology; we implement several together to reduce the opportunity for a threat actor to have success. Working in concert, the following technologies minimize the risk of a breach:

Layer 1/ Signature Files and Heuristic Technologies

Effective, optimized technology to detect known attacks

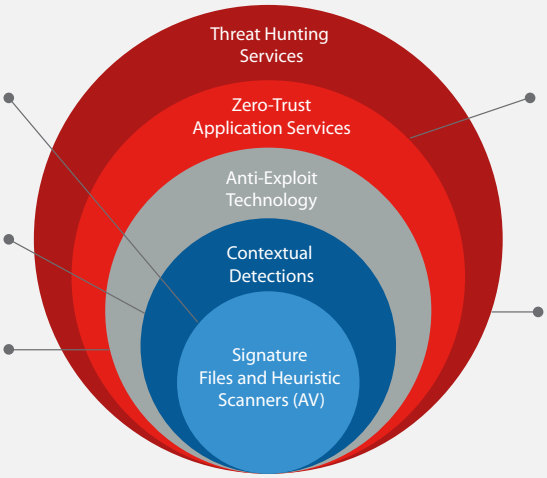
Layer 2 / Contextual Detections

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

Zero Trust Model: A layered protection



Layer 4 / Zero-Trust Application Service

Classifies 100% of processes, by default denying any execution until it is certified as trusted. No need to manually classify threats or delegate them to security admin

Layer 5 / Threat Hunting Service

Detect compromised endpoints, early stage attacks, suspicious activities, and identify IoAs that minimize detection and response time (MTTD and MTTR)

Key Endpoint Security Features

ENDPOINT SECURITY & MANAGEMENT

Protection
Protection against known and zero day malware, ransomware and exploits
Traditional protection with generic and optimized signatures
Protection against advanced persistent threats (APTs)
Zero-Trust Application Service: machine learning to classify 100% of processes
Threat hunting: behavioral analysis and detection of indicators of attack (IoAs)
Personal and managed firewall
IDS / HIPS
Network attack protection
URL filtering, web browsing and anti-phishing
Monitoring
Endpoint risk monitoring
Vulnerability assessment
Zero-Trust Application Service
Twelve months data retention for retrospective attack investigation

Detection
Detection of compromised trusted applications
Zero-Trust Application Service
Fully configurable and instant security risk alerts
Containment
Computer isolation and program blocking
Response and remediation
Ability to roll back and remediate the actions taken by attackers
Centralized quarantine
Automatic analysis and disinfection
Shadow copies
Ability to block unknown and unwanted applications
Investigation
Threat Hunting Service: Deterministic indicators attack mapped to MITRE ATT&CK
Threat Hunting Service: Non-deterministic indicators attack mapped to MITRE ATT&CK with contextual telemetry
Incident graphs and lifecycle information available from the web console
Ability to export lifecycle information for local analysis
Advanced Reporting Tool (add-on)
Advanced attack investigation (Jupyter Notebooks)

Attack surface reduction
Lock mode in the advanced protection
Anti-exploit technology
Web protection
Device control
Automatic updates & discovery of unprotected endpoints
Patch Management for OS and third-party applications
Security for VPN connections (requires WatchGuard Firebox)
Secure access to Wi-Fi network through access points
Add-ons
WatchGuard Data Control
WatchGuard Advanced Reporting
WatchGuard Patch Management
WatchGuard Full Encryption
WatchGuard SIEMFeeder
Supported Platforms
Windows Intel and Windows ARM
macOS Intel and macOS ARM (M1 & M2)
Linux
Android & iOS Devices
Virtual environments - persistent and non-persistent (VDI)

Don't Take Our Word for It

"As cyberattacks on endpoints continue to rise, customers increasingly need us to help them address their security needs. The combination of WatchGuard Cloud with the Endpoint Security portfolio not only allows us to offer this protection, but also gives us the ability to expand our security service offering, increase efficacy and efficiency, and grow the business."

– Bill Walter, Partner
Gross, Mendelsohn & Associates