DATASHEET

WatchGuard Endpoint Security 360

Autonomous Zero Trust Endpoint Protection

Maximum Protection with Minimal Operational Effort

Modern cyberattacks move faster than traditional endpoint security tools can detect them. Attackers increasingly rely on fileless techniques, the use of legitimate software to perform malious actions, compromised trusted applications, and lateral movement to bypass traditional defenses. WatchGuard Endpoint Security 360 is designed to automatically stop these advanced threats. Delivering autonomous zero trust EDR that blocks unknown applications by default, it detects compromised trusted software and prevents lateral movement across the network. By combining AI-powered detection with automated investigation and response, Endpoint Security 360 dramatically reduces attacker dwell time while minimizing operational workload.

Designed for organizations that want maximum protection efficiency, it delivers stronger protection, faster response, and significantly lower security management overhead.

Autonomous Protection Removes Risks

WatchGuard Endpoint Security 360 provides advanced endpoint detection and response (EDR) capabilities with zero trust execution controls, ensuring only trusted and verified applications can run. This enables organizations to reduce risk and stop attacks early, without relying on constant human intervention.

By automatically blocking unknown activity and continuously validating trusted software, Endpoint Security 360 eliminates many of the attack techniques used in modern breaches, including fileless attacks, living-off-the-land techniques, and malicious scripts.

Endpoint Security 360 adds additional protection layers, including detection of compromised trusted applications, lateral movement containment, automated threat hunting, and incident-level Investigations, to further reduce risk and prevent advanced attack techniques.

For MSPs, this means they can operate more efficiently, protecting more customers without growing headcount. And for end customers, this means better protection with less worry.

WatchGuard Endpoint Security 360 includes the full capabilities of WatchGuard's AI-powered EDR platform plus autonomous zero trust protection.

Attack Surface Reduction

- Customizable endpoint risk dashboard
- Unmanaged endpoint detection
- Vulnerability assessment

Built-In Prevention Technologies

- Firewall, IDS, and device control
- Protection for multiple attack vectors (web, email, network, devices)
- Signature files, pre-execution heuristics, and collective intelligence
- AI-powered detections that identify and block malicious installers and scripts
- Anti-phishing protection
- Multi-vector anti-malware & on-demand scans
- URL filtering and web browsing
- Deny-by-default execution

Detection and Response Capabilities

- Continuous endpoint monitoring
- Self-learning AI with contextual behavioral analytics to detect and block fileless and living-off-the-land (LotL) attacks
- Automatically blocks attempts to exploit vulnerabilities in active processes on the device
- Network attack protection against vulnerabilities in Internet-exposed services
- Automated detection and prevention of RDP attacks
- Lateral movement containment
- Automatic detection and correlation of an attack, with alerts, mapped to the MITRE ATT&CK® framework
- Interactive, multi-signal incident view for comprehensive Root Cause Analysis (RCA)
- Integrations with ThreatSync (XDR) for visibility and remediations
- Real-time computer and network isolation, scan, and restart

Autonomous Protection for Modern Threats

Block Unknown Activity by Default

Today's cybercriminals move more quickly than endpoint protection tools can keep up with. That's why WatchGuard Endpoint Security 360 includes the unique Zero-Trust Application Service, which implements deny-by-default controls, allowing only verified applications to run on endpoints. Unknown applications are automatically blocked until they are classified as trusted, eliminating a large portion of modern malware and ransomware attacks before they can execute.

Detect and Contain Sophisticated Attacks

Advanced behavioral detection continuously analyzes activity across endpoints to identify suspicious behavior patterns associated with modern cyberattacks. When malicious activity is detected, automated response actions such as isolation, containment, and remediation stop the attack before it spreads across the network.

Reduce Workload. Improve Efficiency.

WatchGuard Endpoint Security 360 offers a host of automations to improve protection and efficiency. By automatically investigating suspicious activity, correlating signals into incidents, and blocking unknown threats by default, it dramatically reduces alert noise and investigation effort. The result is stronger protection with less operational overhead.

Designed for MSP Scale and Efficiency

WatchGuard Endpoint Security 360 is built to support modern managed service providers (MSPs). Multi-tenant cloud management enables MSPs to deploy policies, monitor protection, and manage security across multiple customers from a single console. Zero trust execution controls, automated investigation, and intelligent response actions allow MSPs to protect more endpoints while dramatically reducing investigation time and alert volume.

This automation allows service providers to deliver stronger endpoint security services while improving operational efficiency and profitability. For MSPs, this means delivering strong endpoint protection efficiently while maintaining healthy service margins.

Implement powerful, simplified security with WatchGuard's Unified Security Platform

WatchGuard's Unified Security Platform architecture is a single platform for elevating modern security delivery. Our platform approach helps you deliver powerful security services across every threat vector, with increased scale and velocity while supporting operational efficiencies and greater profitability. Learn more at WatchGuard.com.

Supported platforms and systems requirements of Watchguard EPDR

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS 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, Safari, and Microsoft

About WatchGuard

WatchGuard Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers (MSPs). For more than 30 years, WatchGuard has defined how MSPs deliver security at scale, continuously innovating to stay ahead of every major shift in the threat landscape. WatchGuard's AI-powered Unified Security Platform® delivers zero trust-aligned network, endpoint, and identity protection in a single, integrated platform, enabling MSPs to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by more than 25,000 MSPs protecting over 1.5 million customers worldwide, WatchGuard enables partners to deliver strong, measurable security outcomes for customers across the globe. Learn more at WatchGuard.com.

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