DATASHEET

WatchGuard Endpoint Security Elite

Advanced EDR for Security Teams

Deep Visibility and Advanced Threat Investigation

For organizations with mature security programs or partners delivering advanced security services, deep visibility and investigation capabilities are critical. Security teams need prevention, detection, and response solutions to investigate and respond to threats in their environments, elevating the security stack to the next level and minimizing adversaries' dwell time.

WatchGuard Endpoint Security Elite provides a full-featured EDR (Endpoint Detection and Response) platform with enriched telemetry, advanced query tools, and AI-assisted investigation capabilities, so security teams can quickly understand complex attacks, correlate events across endpoints, and respond with precision. By combining powerful analytics with automated response and extended data visibility, Endpoint Security Elite gives security teams the tools they need to detect, investigate, and stop sophisticated threats at enterprise scale.

Advanced EDR Built for Security Operations

WatchGuard Endpoint Security Elite is designed for organizations and managed security service providers (MSSP) that require deeper security visibility and advanced investigative capabilities. Building on WatchGuard's AI-powered EDR foundation, it provides enriched telemetry, extended historical visibility, and advanced threat detection tools that enable security teams to detect, investigate, and respond to sophisticated attacks more effectively.

With detailed endpoint telemetry and contextual incident data, analysts can view attack timelines, identify root causes, and understand how adversaries move across systems. Integrated MITRE ATT&CK mapping and automated behavioral correlation provide clear insight into attacker tactics, techniques, and procedures, helping security teams quickly prioritize threats and respond with confidence.

Advanced investigation tools include STIX and YARA-based threat detection and a built-in generative AI assistant that allows analysts to query security data using natural language. These capabilities dramatically accelerate investigation workflows, enabling security teams to identify hidden threats, reduce dwell time, and strengthen overall security posture.

For MSPs and organizations delivering advanced security services, WatchGuard Endpoint Security Elite provides the depth of visibility and analytical power needed to support modern security operations without the complexity of fragmented tools.

Advanced Investigation Tools

- GenAI Assistant to query telemetry
- STIX indicators of attack (IoCs) and YARA rules searches
- CAPA tool to analyze file information (behaviors, strings, imports, exports)
- Remote shell for reduced MTTR and dwell time

WatchGuard Endpoint Security Elite brings together advanced investigation and response capabilities for Security Operations teams.

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
- URL and web filtering
- Detection via network traffic analysis
- 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)
- Deep context and real-time computer forensics telemetry to speed investigations
- Integrations with ThreatSync (XDR) for visibility and remediations
- Real-time computer and network isolation, scan, and restart
- Encrypted file recovery (shadow copies)

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

Strategic Benefits

Deep Telemetry for Faster Investigations
Endpoint Security Elite provides access to enriched and forensic telemetry as well as extended data retention, allowing analysts to analyze attack activity over time and reconstruct attacker behavior across endpoints.

Advanced Threat Detection
Security teams can proactively search for emerging threats with advanced tools that analyze endpoint telemetry for indicators of compromise and suspicious behavior. With support for structured detection frameworks such as STIX and YARA, security teams can uncover hidden threats and investigate activity across the environment.

Rich Visual Attack Context
Interactive timelines, process trees, and lateral movement maps provide a clear visual context for understanding how attacks unfold across endpoints. This enables security teams to quickly identify the root cause, understand attacker behavior, and accelerate investigations.

AI-Assisted Security Analysis
A built-in generative AI assistant allows analysts to query security data using natural language, accelerating investigations and reducing the time required to understand incidents – no complex queries required.

Granular Policy Controls
Endpoint Security Elite enables administrators to enforce detailed security policies that control application execution, device access, and system behavior across endpoints. These granular controls reduce the attack surface while ensuring consistent security enforcement across users, devices, and environments.

Built for Managed Security Services
Endpoint Security Elite provides the deep telemetry, investigation tools, and automation needed for MSPs to deliver high-value security services. With centralized multi-tenant management and advanced investigative capabilities, partners can efficiently monitor, investigate, and respond to threats across multiple customer environments.

Zero Trust Model: A Layered Protection

WatchGuard's Endpoint Security platform doesn't rely on just one single technology. We implement layers of tools together to reduce the opportunity for a threat actor to succeed. Working in concert, these technologies utilize resources at the endpoint to minimize the risk of a breach.

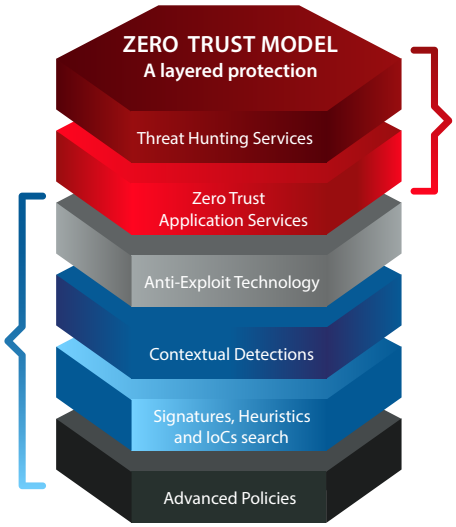
Endpoint Layers:

Layer 1/ / Enhanced Security Policies
Detect or block the execution of common attack techniques

Layer 2 / Signature Files, Heuristic Technologies, and STIX IoCs Search Engine
Hunt for recently disclosed attacks by hash, filename, path, C2 domain, IP, and YARA Rules

Layer 3 / Contectual Detections
Identify malwareless attacks that abuse legitimate tools like PowerShell, WMI, and web browsers

Layer 4 / Anti-Exploit Technology
Detect fileless attacks designed to exploit vulnerabilities



Endpoint Layers:

Layer 5 / Zero-Trust Application Service
Classifies 100% of processes before they run, denying any execution until it is certified as trusted

Layer 6 / Integrated Threat Hunting Service
Detect compromised endpoints, IoAs, early-stage attacks, and suspicious activities. IoAs are contextualized in the cloud-based console with the associated telemetry, enabling security analysts to investigate potential attack attempts

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.