DATASHEET

WatchGuard Endpoint for Servers

Purpose-built protection for critical infrastructure

Protecting the Core of Modern Infrastructure

Servers are the backbone of every organization, storing sensitive data and powering critical business applications. Yet, they are also prime targets for ransomware, lateral movement, and privilege escalation attacks. Traditional endpoint protection isn't optimized for server workloads that require continuous uptime, minimal latency, and resource-efficient security. Organizations need dedicated, always-on protection designed specifically to secure their infrastructure without sacrificing performance.

Keeping Critical Infrastructure Secure

As organizations evolve their IT environments, the complexity of protecting them grows exponentially more complex. Hybrid and multi-cloud architectures often leave security teams juggling disparate tools, limited visibility, and inconsistent protection. But legacy solutions can't keep pace, creating performance bottlenecks, gaps in coverage, and missed ROI on infrastructure investments.

WatchGuard Endpoint Security for Servers addresses these challenges head-on, providing unified visibility, intelligent protection, and simplified management across all workloads. WatchGuard Endpoint Security Platform, delivers a single pane view into your entire infrastructure, spanning virtual machines, endpoints, and workloads.

Agents deploy seamlessly across physical and virtual servers (on-premises or in AWS, Azure, and Google Cloud), acting as enforcement points managed from the same multi-tenant console as workstations and mobile devices. Flexible, role-based administration aligns with your organization's structure for streamlined, secure management.

Powered by self-learning AI and context-based behavioral analytics, Endpoint Security for Servers combines the broadest range of endpoint protection technologies with automated detection and response. This enables faster identification of emerging attacks and smarter, automated remediation – without sacrificing performance or user experience.

Endpoint Security for Servers integrates next-gen AV with self-learning, AI-powered analytics, and advanced EDR technologies in a single solution, allowing IT teams to deal with advanced cyber threats:

Next-Gen AV and Hardening Technologies

- Firewall, IDS, and device control
- AI-powered behavioral analytics against ransomware, phishing, fileless, and malwareless attacks
- Collective Intelligence and pre-execution heuristics
- Multi-vector anti-malware with on-demand scanning
- Anti-tampering, web/URL filtering, and anti-phishing
- Automatic remediation and rollback
- Encrypted file recovery (shadow copies)
- Vulnerability assessment

Advanced Security Technologies

- Continuous endpoint monitoring with EDR
- Self-learning AI with contextual behavioral analytics to detect and block fileless and living-off-the-land attacks (LotL)
- Cloud-based AI that classifies 100% of processes (APTs, ransomware, rootkits, etc.) and blocks hidden threats in real time
- Cloud-sandboxing in real environments
- Anti-exploit protection
- Network attack protection against vulnerabilities in Internet-exposed services
- Threat hunting with behavioral analysis and detection of indicators of attack (IoAs) for LotL attacks, with IoAs mapped to the MITRE ATT&CK framework
- Continuous evaluation of connections among endpoints to block lateral movement with Endpoint Access Enforcement
- Detection and prevention of RDP attacks
- Containment and remediation capabilities such as computer isolation and program blocking

Advanced Detection and Response, Built for Servers

WatchGuard Endpoint Security for Servers delivers the same advanced threat detection and response capabilities as our workstation protection, with added intelligence for server workloads. AI-driven behavioral analysis monitors every process, connection, and file in real time to detect and block threats before they can spread or escalate.

Exploit Prevention and Vulnerability Management

Unpatched or outdated software often makes servers easy targets. WatchGuard's exploit prevention engine identifies and blocks exploit attempts, while the dynamic attack surface reduction tools, including built-in firewall, integrated vulnerability assessment, and device control, help administrators prioritize and remediate security gaps quickly.

Smarter Protection, Stronger Performance

Server workloads demand both speed and resilience. WatchGuard's lightweight, resource-aware agents are optimized to minimize latency and preserve application performance while maintaining powerful, AI-driven protection. Each agent continuously learns from global telemetry, using cloud-trained models to analyze behavior and detect threats in milliseconds – even offline. This continuous self-learning loop ensures faster detection, smarter response, and evolving protection that gets stronger every day – without compromising uptime or user experience.

A Layered Approach

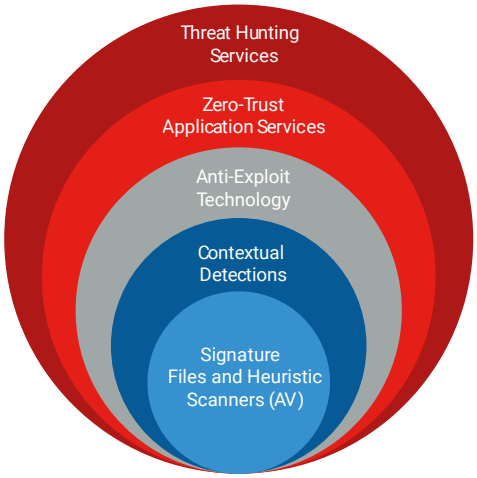
WatchGuard's Endpoint Security for Servers doesn't just rely on a single technology. It combines several together to reduce the opportunity for a threat actor to succeed and minimizes the risk of a breach. This includes our unique Zero-Trust Application Service, which automatically classifies 100% of applications and processes before they run.

Endpoint Layers:

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



Cloud Native Layers:

Layer 4 / Zero-Trust Application Service
Provides detection if a previous layer is a breach, stops attacks on already infected computers and stops lateral movement attacks inside the network

Layer 5 / Threat Hunting Service
Detect compromised endpoints, early stage attacks, and suspicious activities, and identify IoAs that minimize detection and response time (MTTD and MTTR)

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases business scale and velocity while improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect over 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com

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