SERVICE BRIEF

WatchGuard Open MDR

WatchGuard Open MDR delivers enterprise-grade Managed Detection and Response that works with existing security investments. The MDR service integrates with supported third-party and WatchGuard security tools to extend protection across endpoint, identity, network, and cloud environments.

Extend the Power of MDR to Existing Tools

By combining automation, human threat hunting, and 24/7 SOC oversight, Open MDR quickly identifies threats, validates suspicious activity, and takes immediate action to contain them. Continuous monitoring and coordinated response strengthen defenses and streamline security management without disrupting existing systems.

Key Partner Benefits

Faster Time to Protection

Deployment takes hours, not weeks, allowing organizations to see value quickly and strengthen defenses immediately.

New Revenue Stream

Open MDR creates a managed service opportunity through predictable, usage-based pricing that aligns with existing contracts and business models.

Built-In 24/7 SOC

Deliver around-the-clock detection and response without the need to build or staff a security operations center. Live experts monitor the environment continuously to stop threats as they occur, giving partners the power to say they have a SOC.

Automation That Scales

AI and machine learning filter alerts, isolate threats, and trigger containment actions automatically. By reducing manual triage and false positives, organizations can expand coverage and efficiency without increasing headcount.

Unified Operations

A single, cloud-based portal brings together activity from existing tools, including endpoint, identity, and cloud into one view for streamlined oversight and reporting.

Dedicated Partner Support

Technical Account Managers (TAMs) provide ongoing guidance, threat insights, and escalation assistance that strengthen customer confidence and retention.

Supported Third-Party Tools

> **Endpoints:**
WatchGuard Endpoint, Microsoft Defender, CrowdStrike

> **Network:**
WatchGuard Firebox, ThreatSync NDR, select third-party firewalls

> **Identity:**
WatchGuard AuthPoint, Okta

> **Cloud & CSPM:**
Microsoft 365 (Azure), AWS, and Google Workspace, with CSPM capabilities specifically for Azure and AWS environments

Features and Capabilities

> Flexible Integration and Coverage

Works across WatchGuard and third-party tools, including Microsoft Defender, CrowdStrike, Okta, and leading firewalls, to meet partners where they are without requiring a tool migration.

> Coordinated Incident Response

24/7 SOC analysts take direct action to contain and remediate incidents, providing detailed notifications and follow-up reporting.

> Continuous Monitoring

Around-the-clock oversight by AI systems and security analysts to detect and assess threats in real time.

> Cloud and CSPM Integration

Identifies misconfigurations, compliance gaps, and cloud security risks across multi-cloud environments.

> Proactive Threat Hunting

Expert threat hunters investigate unusual patterns and emerging tactics to uncover hidden or evolving threats.

> Unified Portal and Reporting

Consolidates detections, response actions, and performance metrics in one dashboard for simplified oversight.

> Automated Threat Containment

Automation isolates endpoints, blocks malicious traffic, and disables compromised accounts to stop attacks early.

> AI-Powered Efficiency

Machine learning reduces alert noise and prioritizes high-fidelity threats, improving accuracy and speed of response.

Open MDR at a Glance