SERVICE BRIEF

WatchGuard Total MDR

WatchGuard Total MDR is a fully managed, 24/7 threat detection and response service that unifies the WatchGuard security stack – endpoint, firewall, identity, and network – plus select third-party cloud environments like Microsoft 365, Azure, AWS CloudTrail, and Google Workspace.

How Partners Win with Total MDR

Accelerated Onboarding: Activate full-stack protection without complex deployments. Fast onboarding means faster revenue.

Built for WatchGuard Stack: Partners who already sell Firebox, AuthPoint, or WatchGuard EDR can expand coverage and value without adding tools.

Unified Portal = Sales Enablement: Show customers how you're protecting them – endpoints, network, identity, and cloud – all from one place.

Low Noise, High Confidences: Fewer false positive mean less busywork and more time to focus on delivering value and building customer confidence.

Total MDR Threat Detection and Response Includes:

> **Endpoints:**
WatchGuard EDR, EPDR, AEPDR

> **Firewall:**
WatchGuard Firebox

> **Identity:**
AuthPoint

> **Network:**
ThreatSync+ NDR

> **Cloud:**
Microsoft 365/Azure, AWS CloudTrail, Google Workspace

Key Features & Benefits

Unified Threat Visibility

> Get a complete view of your security posture in one place. WatchGuard Total MDR brings together data from endpoint, firewall, identity, network, and cloud environments into a single, easy-to-use portal. No more jumping between tools or missing the bigger picture – just clear, centralized insight to detect and act on threats faster.

24/7 SOC Coverage

> Our expert security analysts monitor, investigate, and respond to threats around the clock, so you don't have to. Whether it's 2 p.m. or 2 a.m., the WatchGuard SOC is actively working to protect organizations without the cost or complexity of building a SOC in-house.

AI-Driven Detection

> Machine learning is constantly analyzing thousands of signals to detect suspicious activity in real time. It cuts through alert noise, flags anomalies, and adapts to new threats faster than traditional rules-based tools, giving better protection with less manual effort.

Quick Active Response

> With average response times under six minutes, threats are stopped before they spread. WatchGuard Total MDR isolates compromised devices, contains malicious files, and escalates incidents only when necessary so teams stay focused on what matters, not buried in alerts.

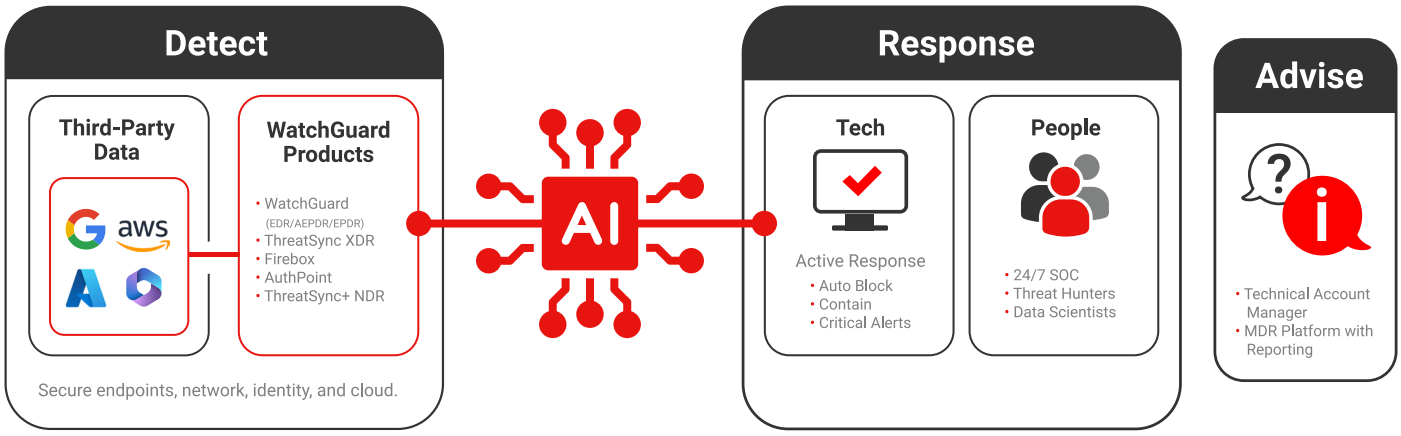
High Fidelity, Low Noise

> WatchGuard Total MDR delivers fewer than one false positive per month on average. That means you get high-confidence alerts with clear action plans – reducing alert fatigue, building trust, and helping you respond decisively when it counts.

Expert Support Team

> Technical account managers (TAMs) provide ongoing security guidance, threat insights, and escalation support. They help make sense of complex activity, surface trends, and recommend improvements to strengthen protection over time.

Total MDR Service Overview



Secure the Full Attack Surface

Endpoint Protection

> Endpoints are a primary target for ransomware, phishing, and fileless attacks. Total MDR uses WatchGuard EDR, EPDR, AEPDR to detect behaviors like credential theft and privilege escalation, then isolates compromised devices, stops malicious processes, and enables live analyst response before malware can spread laterally and escalate.*

Identity Protection

> Total MDR integrates with WatchGuard's AuthPoint to detect and respond to suspicious activity, such as login anomalies, failed login storms, or rogue account creation. By disabling compromised accounts in real time, it blocks attackers from impersonating users or accessing cloud platforms undetected.

Network Protection

> Attacks that bypass endpoints, such as lateral movement, port scans, or C2 traffic, are identified through Firebox and NDR. Total MDR responds instantly by blocking malicious IPs, closing ports, or stopping data exfiltration, protecting internal systems from stealthy threats.

Cloud Protection

> Total MDR monitors Microsoft 365 and other cloud platforms for signs of compromise, including suspicious sign-ins, permission changes, and mailbox access. It responds through API integrations to revoke access, reset credentials, and contain threats before email fraud or data loss occurs.

*Partners already using WatchGuard Core MDR can upgrade to Total MDR to unlock additional features for Firebox, AuthPoint, and NDR.

Metrics That Matter

<1 False Positive
per month

Average 6 Alerts
per month

6 Minutes
mean time to first response

10 Milliseconds
to auto-contain threats

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