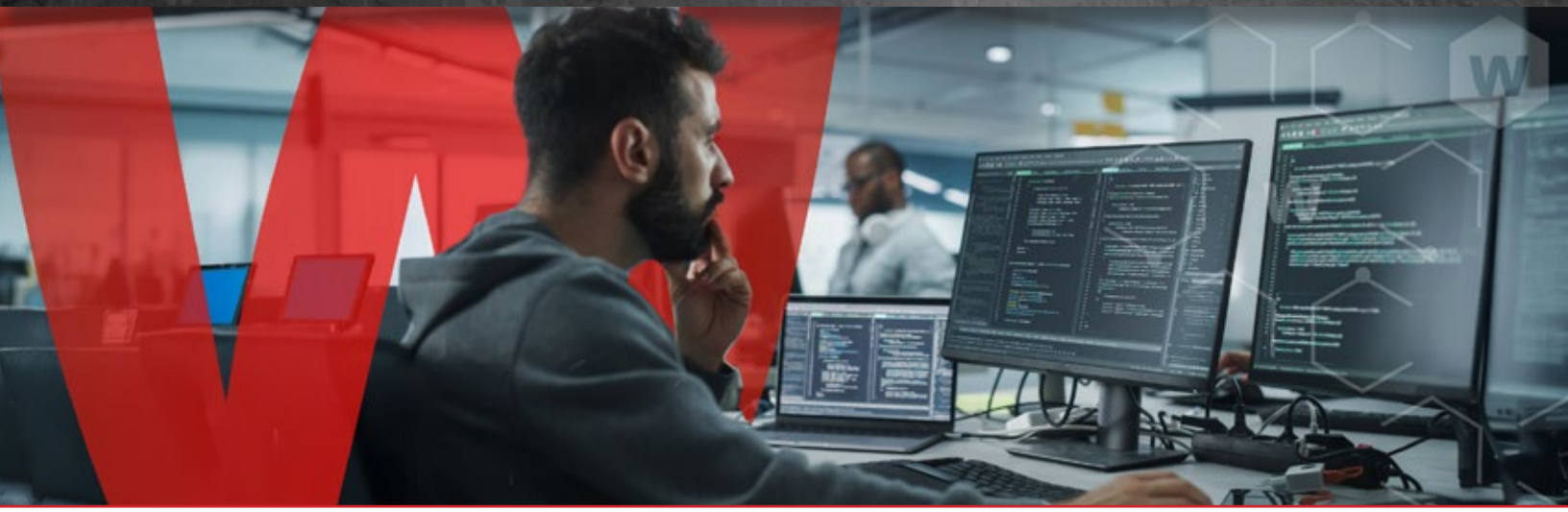
WatchGuard DUXBURY CYBERSECURITY

WatchGuard MDR



24/7 Threat Detection and Response Across Your Security Stack

WatchGuard MDR is a fully managed 24/7 service that doesn't just alert you to threats – we act on them. Cutting through the noise, our team helps you focus on what matters, and respond fast to threats across your laptops, servers, user identities, network, and cloud.

Your business doesn't stop and neither should your security. WatchGuard MDR gives you full visibility and expert protection around the clock. Whether it's a risky login, a suspicious email, or a hidden threat in your network, we detect it fast and stop it before damage is done, all without adding work to your team.

What You Get with WatchGuard MDR

- Detect real threats 24/7 across your entire environment – endpoint, identity, network, and cloud.
- Cut through the noise to deliver only high-fidelity alerts.
- Respond automatically or escalate to experts based on severity.
- Reduce risk by identifying root causes and closing gaps.
- Provide real-time visibility and reporting into threat activity, response actions, and SOC performance.

Key Capabilities

Single View Across Your Security Stack
Get a unified view of threat activity across endpoint, identity, network, and cloud activity from one place, saving time and reducing complexity.

24/7 Monitoring and Response
Our global SOC is always on. Real people and powerful automation work together to detect and stop threats. You'll have access to live threat hunters when it matters most, with security operations based across four locations for built-in redundancy and true around-the-clock coverage.

Smarter Detection with AI/ML
AI and machine learning scan thousands of signals in real time, spotting patterns humans might miss and learning how to stop new threats. The system learns from every incident and gets smarter each day to detect and respond faster.

Proactive Threat Hunting
Our analysts look for hidden threats that automated tools can miss, so you're protected even when attackers try to get clever.

Fast-Acting Automation
We automate the manual review and action, filtering noise, escalating only what matters, and acting quickly to contain threats before they spread.

Precise Threat Response
We act quickly to contain threats, isolate endpoints, block malicious files, and investigate activity across your environment.

Flexible Response Options
You decide how the response is handled: do it yourself, let us take over, or share the responsibility. It's your call.

Real-Time Visibility
The MDR portal gives a live view across your environment into alerts, actions taken, and metrics that show how you're protected, all in one place.

Low Noise, High Signal
You'll receive only high-confidence alerts, with fewer than one false positive per month, keeping your team focused.

Expert Guidance Built In
Technical Account Managers (TAMs) provide ongoing security guidance, helping to understand SOC activity, spot trends, and improve protection over time. With expert support always within reach, you can confidently deliver stronger outcomes for your clients.

Why WatchGuard? Competitive Advantage

Proven Security Leader
With over 25 years in the cybersecurity space, WatchGuard has built a reputation for delivering enterprise-grade protection in a way that's simple, scalable, and accessible. Today, we help secure over 10 million endpoints across 250,000 organizations worldwide.

Truly Integrated Security
Unlike MDR providers that only monitor endpoint or bolt on cloud support, we bring together endpoint, identity, firewall, and network detection.

Partner-First Design
We're built for MSPs and smaller organizations, without retrofitting enterprise tools. You stay in control of customer relationships and service delivery.

Less Alert Fatigue, More Action
We average fewer than one false positive per month compared to the 15+/day some vendors generate. That means fewer distractions and faster response.

Faster Time to Protection
Quick-start onboarding, pre-built integrations, and strong partner support get you up and running fast without the heavy lifting.

Built for the Modern Stack
With native support for Microsoft 365, Azure, AWS, and Google Workspace, we help secure hybrid and cloud-first environments out of the box.

Proven Tech, Trusted Team
Our SOC combines deep security expertise with powerful AI to detect and stop threats fast. WatchGuard's MDR platform has been tested in industry evaluations like MITRE and built on decades of delivering reliable, high-performance protection to businesses worldwide.

Secure the Full Attack Surface

Endpoint Protection
Endpoints are a primary target for ransomware, phishing, and fileless attacks. WatchGuard MDR integrates with WatchGuard Endpoint or supported third-party endpoint products 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
WatchGuard MDR integrates with WatchGuard AuthPoint or Okta 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 the Firebox and ThreatSync NDR. Total MDR responds instantly by blocking malicious IPs, closing ports, or stopping data exfiltration, protecting internal systems from stealthy threats.

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

<6-minute mean time to respond

"We need solutions that are easy to deploy and maintain. We can't afford heavy, complicated tools. It frees up time so we can focus on strategic support. We no longer have to juggle multiple consoles, which would be unmanageable with a small team."
~ Julien Perret, Eiffie

AI-driven threat hunting + automation

Built-in support for both WatchGuard and third-party security tools.

Support for Microsoft 365, Azure, AWS CloudTrail, Google Workspace

Single portal for visibility, response, and reporting

Fully managed or co-managed options available

<1 false positive per month

Protect More with WatchGuard MDR

ATTACKER MOVES	WATCHGUARD MDR STOPS THEM	WHAT IS PROTECTED
Stolen Credentials	**Identity**: Blocks account takeover	Identities
Exploits and Malware	**Endpoint**: Stops malware and isolates endpoints	Data at Rest
Lateral Movement	**Network**: Detects & blocks lateral movement	Data in Motion
Cloud Access & Exfiltration	**Cloud Integration**: Revokes access, resets credentials	Applications

Which MDR Service Is Right for You?

Not every environment is the same. Some customers already use Microsoft Defender. Others want full-stack WatchGuard protection. WatchGuard MDR lets you match the right level of protection to each customer.

	WatchGuard Core MDR	WatchGuard Core MDR for MS	WatchGuard Total MDR	WatchGuard Open MDR
Ideal for Partners/Customers:	Using WatchGuard Endpoint	Using Microsoft Defender	Using WatchGuard Endpoint, NDR, Identity, Firewall	Using third-party tools
24/7 SOC Monitoring	✓	✓	✓	✓
AI/ML-based Threat Detection	✓	✓	✓	✓
Incident Response (Human and Automated Response, Root Cause Analysis)	✓	✓	✓	✓
Advanced Incident Response (Post-breach investigation, recovery, and prevention)	✓	✓	✓	✓
Threat Hunters	✓	✓	✓	✓
Defense Portal	✓	✓	✓	✓
Partner Access to Technical Account Manager	✓	✓	✓	✓
Endpoint Integration	WatchGuard Endpoint	Microsoft Defender	WatchGuard Endpoint	WatchGuard Endpoint, CrowdStrike, Microsoft Defender
Network Integration			WatchGuard Firebox ThreatSync NDR	WatchGuard Firebox, ThreatSync NDR, and most third-party firewalls
Identity Integration			WatchGuard AuthPoint	WatchGuard AuthPoint, and Okta
Microsoft 365	✓	✓	✓	✓
AWS CloudTrail Coverage			✓	✓
Google Workspace			✓	✓

About WatchGuard Technologies, Inc.

WatchGuard® Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers. Unlike others, WatchGuard delivers Real Security for Real World environments through its Unified Security Platform®, bringing networks, endpoints, and identities together with AI and zero trust advances for strong protection that scales. Trusted by more than 17,000 security resellers and managed service providers protecting over 250,000 companies, WatchGuard helps partners grow fast, eliminate operational drag, and deliver strong outcomes without added vendors, consoles, or complexity. WatchGuard is headquartered in Seattle, Washington, with offices worldwide. Learn more at WatchGuard.com.