Accessing the XDR Realm

A Guide for MSPs to Unleash Modern Security

TABLE OF CONTENTS

WatchGuard

01 XDR Is the Future of Cybersecurity

Cyber threats aren't just a problem for big corporations; they're devastating smaller organizations, too. Attackers are getting smarter, faster, and more aggressive.

Access-for-hire schemes, ransomware-as-a-service, and new AI tools have inflamed the threat landscape.

The old security playbook doesn't cut it anymore.

Businesses expect their managed service providers (MSPs) to deliver security that evolves just as fast as the threats do. If your cybersecurity strategy isn't built for adaptability, you're already behind.

02 Today's Top Cybersecurity Challenges

To overcome these challenges, you need an integrated approach that provides context and telemetry data correlation across multiple security layers and IT domains.

> With more tightly integrated security solutions, you get a comprehensive view of your security status.

A modern, integrated approach to cybersecurity should include extended detection and response (XDR) capabilities with automation and AI technologies, which can dramatically improve security efficacy against advanced threats while simplifying security operations.

Siloed Security

MSPs manage security across networks, endpoints, and identities, dealing with multiple tools to cover different attack surfaces. But more tools don't always mean better security. When solutions don't communicate, you're left with gaps that attackers can exploit.

Limited Visibility

Disconnected tools mean security teams get only fragments of the bigger picture. In a cyberattack, wasting time piecing data from multiple sources gives attackers the upper hand. If your team is juggling six different dashboards just to diagnose an issue, you're losing valuable response time.

Too Much Data

Every security tool generates its own logs, alerts, and telemetry, often in different formats. The result? A flood of data that's difficult to analyze. Important threats get buried in noise, false positives drain resources, and real attacks slip through. Integrating multiple vendors' solutions is complex, and even when it works, managing them is a challenge.

Lack of Security Automation

Without automation, security teams rely on manual processes that slow down threat detection and increase the chances of mistakes.

1. **Slow Detection**
   Manual detection extends response times, allowing threats to escalate before they're identified. Your team wastes time chasing false alarms while real threats go unnoticed.

2. **Unclear Response Actions**
   When an attack happens, every second counts. How do security admins know what response action they should take first? Without automated response capabilities, security admins must guess the best course of action, increasing the risk of prolonged downtime and data loss.

Overloaded Security Teams

Businesses rely on more systems, applications, and devices than ever, and each one needs constant monitoring. MSPs looking for new levels of security telemetry aggregation, correlation, and analysis add to the already massive workloads of their teams.

This is compounded by:

1. **Cybersecurity Talent Shortage**
   Finding and retaining skilled security professionals is harder than ever. Demand is skyrocketing, but experienced talent is scarce. Short-staffed teams are left juggling multiple security tools while trying to keep up with an expanding attack surface.

2. **Alert Fatigue**
   Security teams are flooded with thousands of alerts every week. But only 19% are worth investigating, and just 4% get checked. Instead of solving problems, many security tools add to the workload, forcing teams to manually sift through false alarms while real threats go undetected.

Security teams are flooded with thousands of alerts every week.

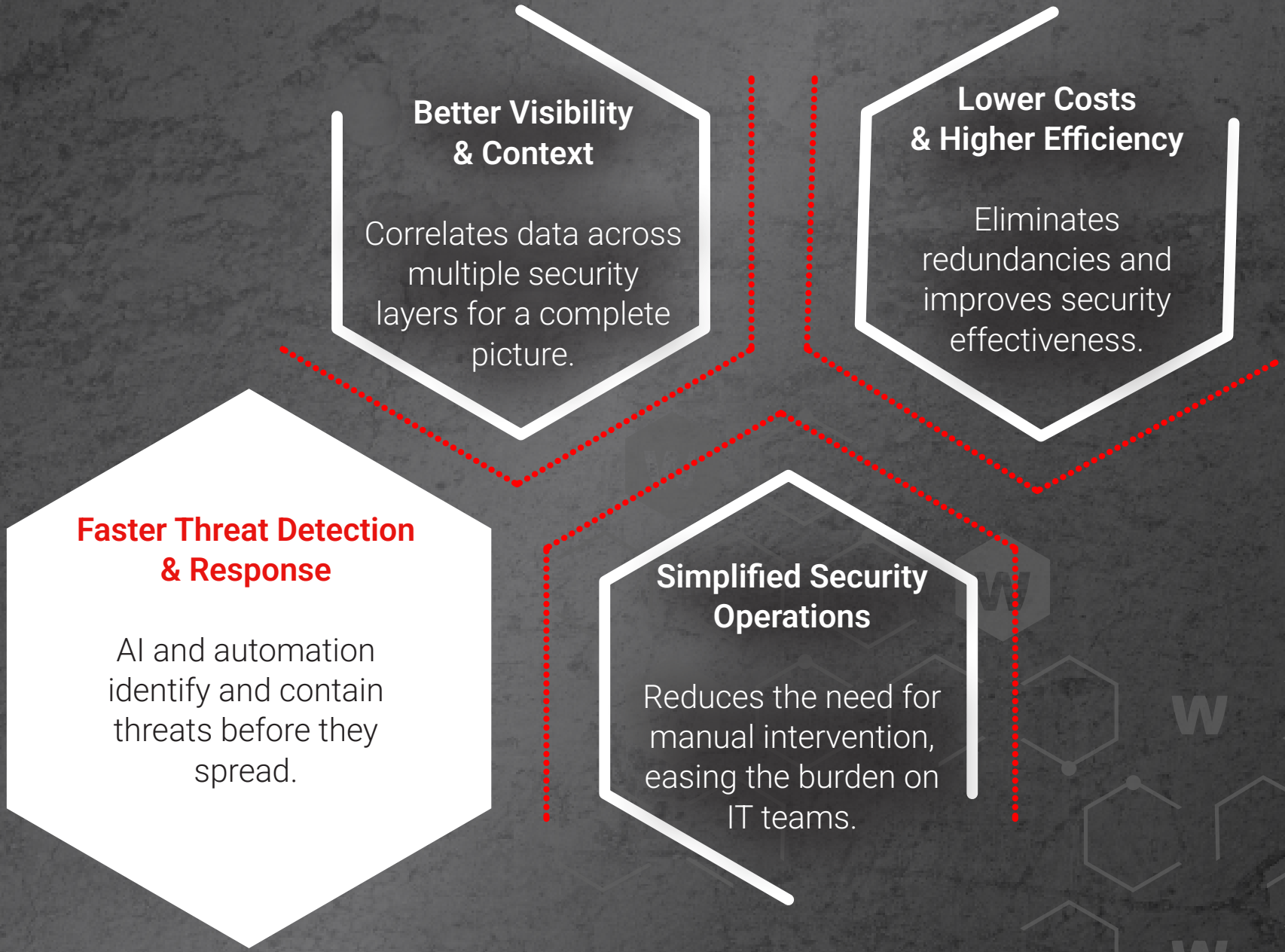
But only **19%** are worth investigating, and just **4%** get checked.

03 A Smarter Approach to Modern Cybersecurity

To stay ahead of threats, you need an integrated approach that connects the dots across your entire IT environment. That means using security solutions that work together providing real-time visibility, context, and correlation across multiple layers.

XDR consolidates data from **firewalls, servers, workstations, and devices** to detect and stop attacks faster. With AI-driven automation, it cuts through the noise, reducing false alarms and helping security teams focus on real threats.

WatchGuard


Better Visibility & Context
Correlates data across multiple security layers for a complete picture.
Lower Costs & Higher Efficiency
Eliminates redundancies and improves security effectiveness.
Faster Threat Detection & Response
AI and automation identify and contain threats before they spread.
Simplified Security Operations
Reduces the need for manual intervention, easing the burden on IT teams.

04 MSPs Can't Afford to Ignore XDR

As an MSP, your clients trust you to protect them from increasingly sophisticated attacks. **If you want to provide your clients with stronger, smarter security without adding complexity, XDR is the way forward.** MSPs can't afford to juggle disconnected security tools anymore.

XDR provides a scalable way for MSPs to offer advanced cybersecurity without requiring an expensive security operations center (SOC) or costly SIEM. XDR delivers a unified, AI-driven security approach to detecting and responding to threats to your clients from a single platform.

With XDR, MSPs can:

1. **Eliminate Security Gaps & Blind Spots**
   Relying on a patchwork of independent security tools leads to fragmented visibility and delayed threat response. XDR integrates all security layers into a single, intelligent system, reducing blind spots and improving threat detection.

2. **Boost Operational Efficiency & Reduce Costs**
   With XDR, automation and AI handle complex threat analysis, reducing manual workloads and increasing efficiency. This means your team spends less time managing multiple disconnected security tools and more time focusing on business growth.

3. **Offer Stronger Security to Happier Clients**
   Adopting XDR provides your clients with a proactive, AI-driven security solution that offers real-time detection and response. This strengthens their overall cybersecurity posture – making you an indispensable security partner.

4. **Solve More Complex Security Problems**
   Cybersecurity is no longer just about staying safe. XDR can help your clients save on compliance, adhere to industry controls, apply for cyber insurance, and demonstrate security to their supply chain partners.

5. **Tap Into a High-Growth Market**
   XDR is one of the fastest-growing segments in cybersecurity, with a CAGR of nearly 40%. XDR is a prime opportunity for MSPs to increase revenue, enhance service offerings, and stay ahead of competitors.

WatchGuard

05 XDR for the MSP

What to Look For:

1 **Comprehensive threat surface coverage**
Unifying detection and response across your entire threat surface is the goal of XDR, but many vendors only cover a small portion of what's required. Moreover, many XDR solutions are extensions of EDR tools and lack network and Cloud coverage. Look for an XDR partner that pairs strong endpoint coverage with ingest data across your entire environment, including on-premises networks, data centers, firewalls, VM/Containers, users, and the Cloud.

2 **Easy to deploy and integrate**
XDR solutions that are difficult to deploy, integrate, and tune are doomed to fail. Security vendors often encumber their customers and partners with complex integration and tuning processes that inhibit the XDR promise. Look for solutions that are 100% Cloud-native for easy integration and deployment, with minimal configuration required to start seeing detections.

3 **Unifies AI analysis**
XDR solutions typically only apply AI analysis (supervised machine learning) at the endpoint. All other threat detection, including in-network and Cloud, is policy-based. Look for solutions that unify threat data from the endpoint, networks, Cloud platforms, SaaS applications, and VPN logs for deeper analysis by AI tools.

4 **Designed for the MSP**
Because they were designed for large SOCs, many XDR offerings focus on fancy analytical and visualization tools, with limited consideration for smaller teams. As a result, they produce an overwhelming number of alerts and false positives. If an XDR solution overwhelms your team, it is ineffective.

XDR solutions also shouldn't require hiring new experts or having your team undergo extensive retraining. Look for vendors prioritizing alert minimization with clear workflow, threat scoring, and response automation capabilities that make your team more effective.

WatchGuard

> Look for vendors prioritizing alert minimization with clear workflow, threat scoring, and response automation capabilities that make your team more effective.

06 XDR with ThreatSync Core

ThreatSync Core is a native XDR solution that equips MSPs with a centralized intelligence and incident response console for responding to security incidents.

ThreatSync is simple to use and deploy. It's also powerful. In just a matter of clicks, you can unify detection across WatchGuard security layers, enabling faster threat response from a single interface.

Centralizes WatchGuard Alerts

Unifies Incident Workflows

Enables Auto and Manual Response Actions

WatchGuard

ThreatSync provides XDR capabilities by correlating indicators of compromise (IoCs) from all WatchGuard security products. Individual security events are distilled into scored incidents, providing more insights and cross-domain context to speed threat detection. There's no complex orchestration; security teams deploy and manage simple policies to immediately improve visibility and control.

ThreatSync allows responders to automatically target response actions where they will most effectively prevent damage and limit an attack from spreading. Threats are scored so teams understand the threat's risk level, know precisely where to start, and make the most accurate decisions faster.

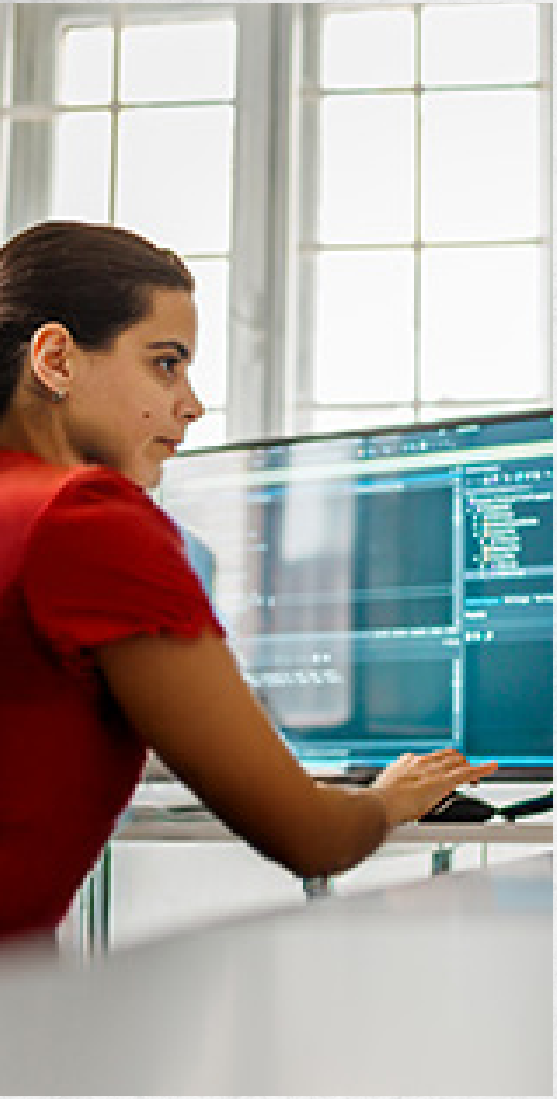
ThreatSync allows responders to automatically target response actions where they will most effectively prevent damage and limit an attack from spreading. Threats are scored so teams understand the threat's risk level, know precisely where to start, and make the most accurate decisions faster.

ThreatSync correlates detection and response across:

1. **WatchGuard's Firebox and Unified Security Platform®**
2. **Wi-Fi**
3. **WatchGuard EDR/EPDR**
4. **WatchGuard AuthPoint**

No Added Costs to Unlock XDR

WatchGuard believes XDR capabilities are now critical cybersecurity protection for all businesses. That's why we built ThreatSync, our native XDR solution, into the WatchGuard Unified Security Platform for no additional cost.



07 Deeper Detections with ThreatSync+

ThreatSync+ is WatchGuard's advanced AI engine for XDR. It leverages a neural network of over 95 learning models trained to baseline and search out signs of attack. Operating securely from the Cloud, ThreatSync+ is the centralized source of truth for identifying ongoing threats, providing 24/7 overwatch for your client's entire threat surface.

ThreatSync+ makes it easy for security teams to uncover evidence of threats as they progress across the cyber kill chain, from network reconnaissance, command and control, privilege escalations, lateral movement, data staging, backup disruption, and mass encryption to data exfiltration.

How it works:

Intelligent Baselining
ThreatSync+ undertakes an intensive learning process starting with a baseline of normal behaviors correlated to your network, users, services, and associated assets. This context also enables ThreatSync+ to identify and classify previously unknown assets and devices, helping you understand their role and gauge their importance.

Data Breadth
ThreatSync+ leverages multiple data sources to build context around the behaviors in your environment. ThreatSync+ collects telemetry from traffic logs, NetFlow, DHCP, VPN, Entr ID/ AD, M365 and Azure Cloud workloads/workspaces, application activity, and WatchGuard Endpoint solutions.

Smart Alerts
Smart Alert details include charts and maps, providing information on the behavior by historical activity and timeline. These include a behavior map showing the links between the major actor and the different behavior types. You can point to each behavior type and IP address to view details about the device type, organization, or location of the behavior.

AI-Powered XDR Delivered from the Cloud
ThreatSync+ extends WatchGuard's coverage to overlay and manage disparate environments of 3rd-party security and network tools from a single pane of glass. Offering an Open XDR solution, MPSs can leverage their vendor ecosystem of third-party firewalls, routers, and switches while enhancing security visibility and control with ThreatSync+.

WatchGuard

08 How It Works: Delivering XDR Services with WatchGuard

Unified Threats Dashboard

The threats dashboard gives MSPs an aggregated view of their clients entire XDR deployment, starting with open threat alerts, correlated into "Incidents," each ranked in order of severity. This provides a simple way for teams to know where to prioritize. Each Incident allows the security team to drill in for more information and, in most cases, take a response action to stop the threat.

Response Actions

ThreatSync enables automatic detection and response to threats detected on the network, endpoint devices, or identity infrastructure.

Response actions include:

- Block Threat Origin IP
- Delete File
- Isolate Device
- Kill Malicious Process
- Block User

Policy Alerts and Framework Mapping

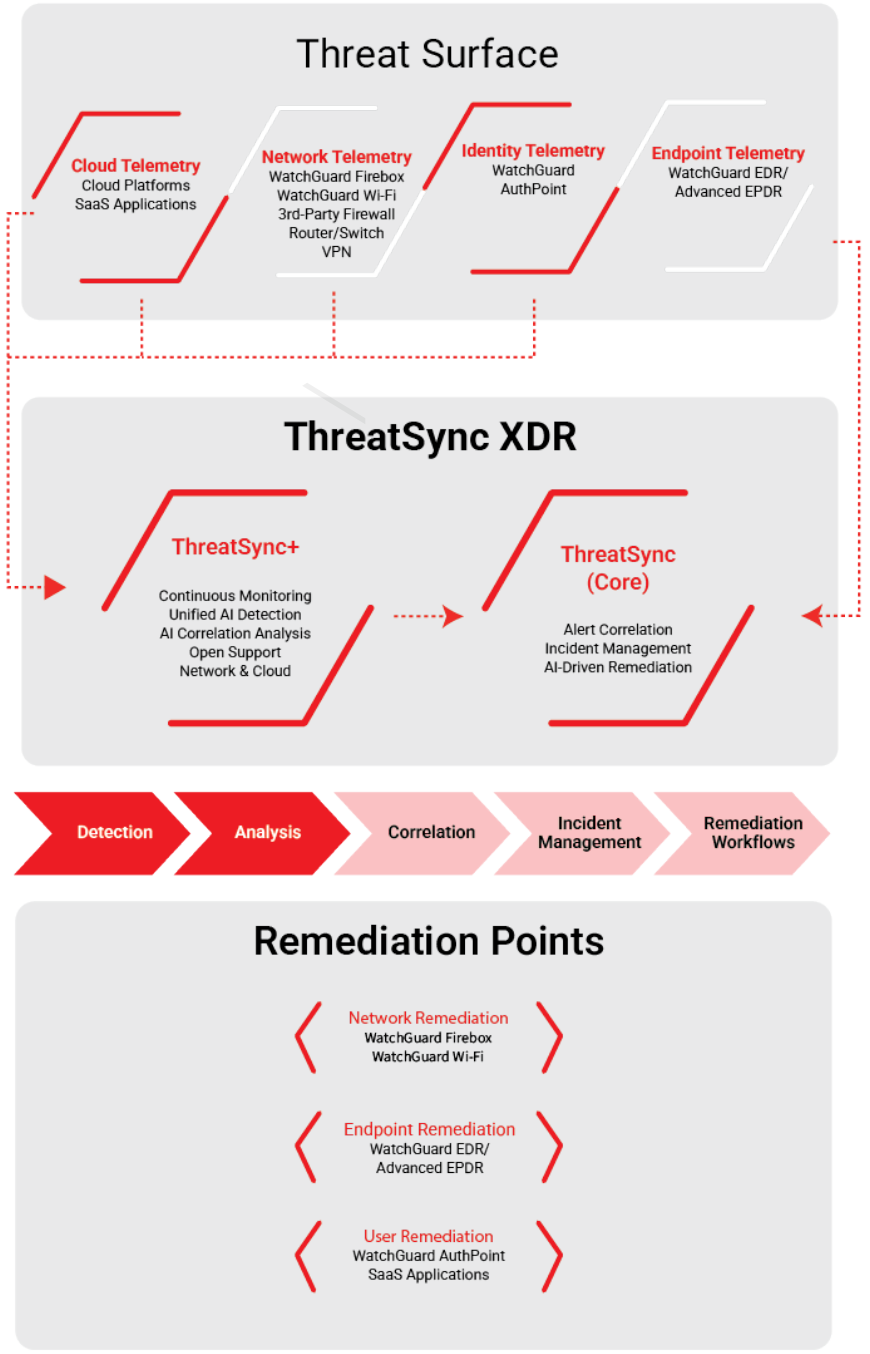
Relying on a patchwork of independent security tools leads to fragmented visibility and delayed threat response. XDR integrates all security layers into a single, intelligent system, reducing blind spots and improving threat detection.

Continuous Compliance with Reporting

No more manual assessments and building reports in Excel. ThreatSync combines hundreds of pre-built policy controls with WatchGuard's continuous automated compliance reporting engine to automate compliance reporting.

Cost savings

100% Cloud-native, ThreatSync eliminates the need for new hardware and automates manual processes such as threat monitoring, threat hunting, and compliance reporting – all within an easy-to-deploy, user-friendly, enterprise-grade XDR solution.



09 MDR: WatchGuard as an Extension of Your Team

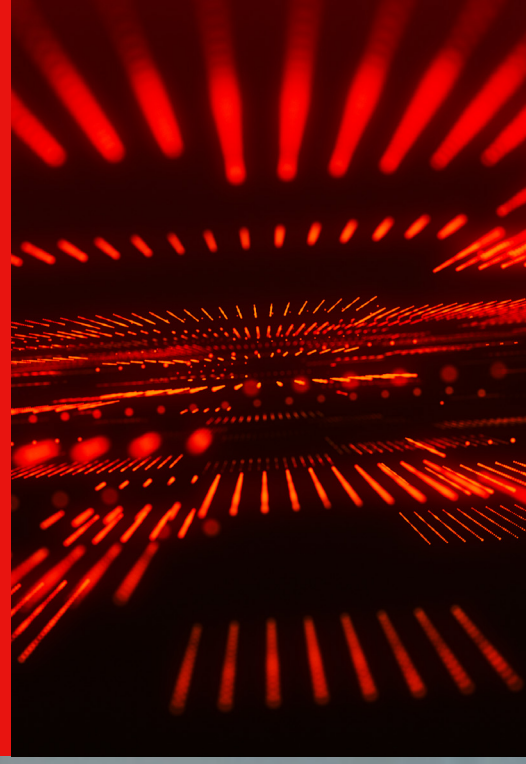
Not ready to offer 24/7 coverage to support your XDR program? Team up with our cyber experts using our top-notch Managed Detection and Response (MDR) service. A skilled team of WatchGuard cybersecurity experts provides 24/7 activity monitoring, threat hunting, detection, investigation, and optional, selective, and tailored containment for each client. WatchGuard MDR gives you the coverage you need and enables you to expand your managed security service portfolio with your own branded MDR offering.

How it works:

- Our team of experts from WatchGuard SOC transforms endpoint monitoring and 365-day telemetry into actionable security analytics, augmented by industry-leading, trusted security machine learning/AI and up-to-the-minute threat intelligence operated around the clock.
- WatchGuard MDR supports you with automatically delivered periodic service activity and security health status reports that help you to provide preventive and attack surface reduction services.
- As part of onboarding the service, our team assesses the attack surface at the endpoints to strengthen their security posture, improving their overall resiliency to cyber threats immediately.
- In the event of a cyberattack, the team guides you through the response process to stop and remediate threats. For added convenience and to minimize response time, you can delegate containment to the SOC by default – 24/7 or during your after-business hours.

WatchGuard

> A skilled team of WatchGuard cybersecurity experts provides 24/7 activity monitoring, threat hunting, detection, investigation, and optional, selective, and tailored containment for each client.



WatchGuard Portfolio

PROTECT ENVIRONMENTS

Network Security

WatchGuard's firewalls and network security services combine essential protection with advanced threat prevention, including high-performance deep packet inspection and integrated SD-WAN. Our secure, Cloud-managed Wi-Fi solutions create a protected airspace for wireless networks, with expansive engagement features that enhance connectivity without compromising security.

PROTECT USERS

Multi-Factor Authentication

WatchGuard AuthPoint® delivers strong, user-friendly authentication through a powerful Cloud-native platform. The AuthPoint mobile app enables users to approve or deny login attempts via simple push notifications, making every sign-in attempt visible and verifiable in real time.

PROTECT DEVICES

Endpoint Security

Preventing breaches, data loss, and cyberattacks is simple with WatchGuard's comprehensive Endpoint Security suite. Lightweight and Cloud-managed, these solutions integrate best-in-class technology, threat intelligence, and expert-driven controls to provide advanced prevention, detection, containment, and response capabilities.

PROTECT THE ENTIRE BUSINESS

Managed Detection and Response

WatchGuard MDR extends your team with 24/7 expert-led monitoring and response, without the cost of building an internal SOC. Delivered through trusted WatchGuard partners, this service monitors endpoints, networks and Microsoft environments to detect suspicious activity, correlate events, investigate threats, and respond quickly and effectively to sophisticated attacks.

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.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com