Managed Services Buyer's Guide

Executive insights to select the optimal managed detection and response (MDR) services partner for your organization



paloalto NETWORKS | UNIT 42

Table of Contents

3 The MDR Imperative

4 MDR Must-Haves

6 Pitfalls to Avoid When Evaluating MDR Providers

7 Questions to Ask an MDR Provider

8 The Unit 42 Difference

10 Unit 42 MDR Success Stories

12 How to Choose the Right MDR Provider

13 Conclusion

Reporting MDR Value to your Board

Choose MDR That Moves at the Speed of Threats

15 Appendix: What to Look For in an MDR Provider

paloalto NETWORKS | UNIT 42

Managed Services Buyer's Guide

THE MDR IMPERATIVE

If your security team feels like it is constantly defending against a rising tide of threats, you are not alone. Most organizations now operate in a landscape defined by machine-speed attackers, expanding attack surfaces, and internal teams stretched thin.

According to the 2026 Unit 42 Global Incident Response Report, **end-to-end attacks now unfold in under an hour, and 87% of intrusions span multiple attack surfaces**.[1] Even well-resourced teams struggle to detect, investigate, and contain attacks before damage occurs.

As adversaries increasingly automate reconnaissance, phishing, and lateral movement with AI, the challenge becomes even more daunting. Without continuous monitoring and the ability to act decisively the moment something happens, security teams cannot keep pace with attacks that unfold in minutes.

In response, many organizations are turning to MDR services to extend their security operations center (SOC). The most effective providers now go beyond basic monitoring and alert triage, delivering capabilities that reduce noise, improve detection fidelity, and provide the SOC engineering expertise required to sustain modern, complex environments.

This guide will help you evaluate MDR providers through a modern lens, accounting for investigation, response, posture, and the engineering foundations required to achieve faster detection and response at scale.

87% of intrusions span multiple attack surfaces

- cloud
- identity
- endpoint



1. 2026 Unit 42 Global Incident Response Report

MDR MUST-HAVES

Five Essentials of High-Performing MDR Providers

Modern MDR requires more than alert triage. It should combine platform-native operations, elite expertise, threat intelligence, posture improvement, and automation into a unified solution capable of keeping pace with attackers.

These five essentials define what an MDR partner must deliver to protect your organization at scale.

paloalto NETWORKS | UNIT 42

1 Platform-Native Visibility and Control

Attackers move across endpoints, identities, cloud workloads, and networks in minutes. Your MDR provider must natively ingest and correlate telemetry across all these surfaces in one system, not by stitching together partial logs after the fact. Detection, investigation, and response must happen in one place. If a provider cannot correlate your telemetry natively, attacker movement might be missed.

With the right partner: You gain complete context instead of fragmented signals. Your MDR analysts can isolate endpoints, terminate sessions, remove files, reverse malicious changes, and take action directly in the platform without delay. The provider can also ensure telemetry health and ingestion quality—distinct from hygiene—so detections remain accurate over time.

2 Actionable, High-Fidelity Threat Intelligence

Many MDR providers rely on commodity or third-party threat feeds. The best providers integrate original, proprietary threat intelligence based on real attacker campaigns observed in the wild. This level of intelligence should continuously inform detection logic, enrich investigations, and shape response playbooks.

With the right partner: Detections are enriched with relevant attacker techniques, enabling faster and more accurate investigations. You benefit from earlier identification of threats targeting your industry, region, or technology stack, and your provider can quickly update detection logic and correlation rules as new behaviors emerge to keep your defenses aligned with evolving adversaries.

MDR MUST-HAVES

3 Threat Expertise That Extends Beyond Detection and Response

Coverage must be continuous and extend beyond alert review. Proactive threat hunting helps identify emerging and evasive threats that automated detections alone may miss. The most advanced MDR providers may even offer SOC engineering capabilities, including detection tuning, noise reduction, and automation readiness.

With the right partner: Organizations can gain proactive hunters who identify early-stage signals using in-environment telemetry informed by curated, high-confidence threat intelligence. Analysts can continuously refine detection logic to improve fidelity and reduce noise. SOC engineers can write and maintain correlation rules and response playbooks. Together, these capabilities meaningfully strengthen detection quality and SOC maturity.

4 Continuous Posture and Hygiene Management

MDR must improve overall resilience, not only respond to threats. Posture and hygiene management—configuration validation, vulnerability awareness, policy tuning, and continuous validation of detections and correlation logic—are foundational to strong outcomes.

With the right partner: Posture gaps are identified and resolved before they escalate, alert noise declines as detection accuracy improves, telemetry or configuration issues are surfaced early, and correlation rules (including those written by internal teams) are incorporated into a holistic posture strategy.

5 Smart Automation and Response Orchestration

Attackers now use automation and AI to scale reconnaissance and lateral movement; MDR must match this speed. Automated correlation, prioritization, and pre-approved response actions dramatically reduce mean time to respond (MTTR).

With the right partner: Analysts spend less time triaging noise and more time on high-impact threats, while automated workflows accelerate containment. Some providers also identify where playbooks, automations, or correlation rules need refinement, helping your response processes become faster and more consistent.

PITFALLS TO AVOID WHEN EVALUATING MDR PROVIDERS

Selecting an MDR provider is not just about comparing feature lists. It is about avoiding partnerships that leave your organization exposed.
These are the eight most common (and costly) traps:

The "Alert-only" model

Some providers only notify you when an incident occurs but stop short of taking action. They do not investigate deeply or assist with containment, forcing your internal team to scramble and handle critical tasks during a crisis.

Business-hours-only coverage

Attackers don't keep office hours. Providers without 24/7/365 staffed analysts inevitably introduce delays that translate directly into business risk.

Patchwork visibility

If a provider cannot natively ingest and correlate telemetry from endpoint, identity, cloud, and network sources in one system, they will miss attacker movement. Even small blind spots can lead to disproportionately large impacts.

Third-party threat intelligence

Generic feeds produce generic detections. Without proprietary intelligence and frontline research, providers cannot stay ahead of emerging campaigns or industry-specific threats.

Outsourced incident response

If MDR teams cannot take direct action—such as isolating a host, terminating a process, or reversing malicious changes—remediation slows to a crawl. Worse, you may still be responsible for the heaviest lift of manual labor.

No hygiene support

Successful MDR services should harden your environment against future risk. Effective MDR should include continuous hygiene reviews, misconfiguration detection, and support for enforcement of baseline controls.

Limited automation capabilities

Modern attacks move too quickly for manual workflows. If automation is not deeply integrated into the provider's processes, investigations will lag behind attacker speed.

Static detection fidelity

Monitoring alone is insufficient. A provider should actively assist with writing, tuning, and validating correlation rules and playbooks, not just reviewing alerts.

QUESTIONS TO ASK

Questions to Ask an MDR Provider

A strong provider should be able to clearly answer these questions.

1. Scope of Actions
2. Defined Speed
3. Analyst Workflow
4. Response Capabilities
5. Telemetry
6. Hygiene
7. Threat Intel
8. Tuning & Fidelity
9. Threat Hunting
10. Reporting

paloalto NETWORKS | UNIT 42

- [ ] **Scope of Actions**

  Do you provide real-time containment and remediation actions, or only alert triage?

- [ ] **Analyst Workflow**

  How do your analysts investigate threats directly within the platform?

- [ ] **Telemetry**

  What data sources do you natively ingest and correlate?

- [ ] **Threat Intel**

  How is your threat intelligence produced and operationalized?

- [ ] **Threat Hunting**

  Is proactive threat hunting included as part of the service, and how frequently is it performed?

- [ ] **Define Speed**

  How do you define and measure MTTR?

- [ ] **Response Capabilities**

  What actions can you take on my behalf (e.g., host isolation, file quarantine, session termination, scripted remediation)?

- [ ] **Hygiene**

  How do you support ongoing posture improvement or identify hygiene gaps?

- [ ] **Tuning & Fidelity**

  Can you assist with detection-quality enhancements—such as tuning correlation rules, validating playbooks, or advising on automation improvements?

- [ ] **Reporting**

  How do you demonstrate ROI to executives or the board?

These questions help determine whether the provider can support both today's threats and the operational maturity your SOC needs.

While the five essentials outlined earlier offer a universal framework for evaluating any MDR providers, Unit 42 stands out through deep platform integration and frontline expertise.

Our flexible operating model allows you to move from core MDR into more advanced managed services, including full SOC engineering, as your needs evolve.

Unlike providers that monitor dozens of platforms at arm's length, Unit 42 teams focus exclusively on the Cortex platform—Cortex XDR and Cortex XSIAM—ensuring unmatched depth because we operate and defend the same platform we help build and secure.

THE UNIT 42 DIFFERENCE

Here's what sets Unit 42 MDR apart:

- Platform-Native Operations
- Elite Expertise Integrated With the Platform
- Proactive Threat Hunting by Design
- High-Fidelity Proprietary Threat Intelligence
- Integrated End-to-End Response and Remediation
- Continuous Posture Improvement
- Built for AI-Enabled Attacks

paloalto NETWORKS | UNIT 42

Platform-Native Operations

Unit 42 analysts work directly inside Cortex XDR and Cortex XSIAM, unifying endpoint, cloud, network, and identity telemetry within a single platform. This eliminates data silos, speeds up investigations, improves response accuracy, and builds a strong foundation for adding deeper engineering or automation support as your SOC matures.

Elite Expertise Integrated With the Platform

Our teams—comprising MDR analysts, threat hunters, incident responders, and SOC engineers—collaborate directly with Cortex R&D, enabling quick updates to detection logic and rapid correction of false positives or gaps. Unit 42 MDR customers get immediate protection, and access to experts who can support advanced tuning, engineering, and full-cycle incident response as environments grow.

Proactive Threat Hunting by Design

Threat hunting is continuous and intentional. Analysts actively look for early-stage behaviors and industry/geography-specific techniques. This provides visibility beyond automated alerts and helps organizations prioritize long-term security improvements.

High-Fidelity Proprietary Threat Intelligence

Derived from frontline incidents and global research, Unit 42 threat intelligence directly shapes detection logic and offers early insight into relevant attacker campaigns. This enriches MDR investigations and supports organizations looking to strengthen detection engineering beyond traditional monitoring.

Integrated End-to-End Response and Remediation

Unit 42 performs real containment across native and third-party EDR. By isolating hosts, terminating processes, removing files, and driving full remediation through eradication and recovery, we can reduce MTTR by 90% or more.[2] These capabilities also provide a solid foundation for organizations looking to build more automated and orchestrated response workflows.

Continuous Posture Improvement

Unit 42 actively uncovers vulnerabilities, configuration issues, and hygiene gaps that impact detection quality. For Cortex XSIAM users, optional SOC engineering support is available to author new correlation rules for emerging threats, refine playbooks, and optimize automation as attacker techniques evolve.

Built for AI-Enabled Attacks

With over 10,000 behavioral detectors and 2,500 machine-learning models, Cortex analytics enables Unit 42 MDR experts to stay ahead of threats. Automation speeds containment decisions, and customers seeking deeper SOC transformation can build on these capabilities through additional managed SOC engineering and orchestration support.

2. Mercan Properties tackles cyberthreats 90% faster using Unit 42 MDR Case Study

What Better Looks Like

Here is how organizations are using Unit 42 MDR to transform their security operations, reduce risk, and achieve speed at scale.

- Green Bay Packers
- Global business process outsourcing company
- Mercan Properties
- Oneida Nation
- Rovensa Group

paloalto NETWORKS | UNIT 42

Green Bay Packers

Protecting a high-visibility environment with a lean team, the Packers increased data ingestion by 490% while reducing alert noise by 95%. This 250% efficiency gain provided the confidence needed to secure a complex attack surface.

They saved up to **120** labor hours per week

READ THE FULL STORY

Global business process outsourcing company

When global cybercriminal group Muddled Libra attempted a second brute-force attack, Cortex XDR blocked it immediately. Within 16 minutes, Unit 42 analysts had already investigated the incident and provided actionable defensive recommendations, delivering a full, coordinated response rather than simply triaging the alerts.

16 minutes to actionable response following brute-force attempt

READ THE FULL STORY

UNIT 42 SUCCESS STORIES

Mercan Properties

Faced with a distributed environment and limited resources, Mercan achieved what internal staffing could not: 24/7 monitoring and proactive hunting. They now detect threats 90% faster without the overhead of building a full-scale SOC.

Threats detected **90%** faster than before.

READ THE FULL STORY

Oneida Nation

Securing 17,000+ members across government services, healthcare, hospitality and gaming, Oneida reduced MTTR to just 43 seconds after implementing Unit 42 MDR and Cortex XSIAM. They now ingest 7x more data at 20% lower cost, enabling rapid, accurate response across a highly complex environment.

MTTR reduced to just **43** seconds.

READ THE FULL STORY

Rovensa Group

Managing 2,500 users across 40 countries, Rovensa Group relied on Unit 42 MDR to overcome a critical skills shortage. The result was a 90% reduction in MTTD and MTTR, freeing up two full-time equivalents (FTEs) to focus on strategic security initiatives rather than daily administration.

90% reduction in MTTD and MTTR.

READ THE FULL STORY

ONBOARDING

How to Choose the Right MDR Provider

Use this framework to compare providers objectively:

- Assess coverage and capabilities
- Evaluate expertise and intelligence
- Validate response action
- Examine posture and prevention support
- Confirm integration and scalability
- Evaluate operational impact

paloalto NETWORKS | UNIT 42

Step 1 | Assess coverage and capabilities

- Do they deliver 24/7 staffed monitoring?
- Can they investigate and remediate directly within the platform?
- Do they ingest telemetry across endpoint, identity, cloud, SaaS, and network?
- Do they offer options that support more advanced SOC engineering needs as your environment matures?

Step 2 | Evaluate expertise and intelligence

- Is their threat intelligence proprietary?
- Do hunters and analysts specialize in your industry and are experts on your platform?
- How do they evolve detection logic over time, and can they assist with tuning or improving it when needed? How do your analysts investigate threats directly within the platform?

Step 3 | Validate response action

- What actions can they take without escalation?
- How quickly do they act?
- Can they fully remediate issues, or do they only notify?
- Do they support automation or playbook improvements to accelerate future responses?

Step 4 | Examine posture and prevention support

- Do they help harden configurations and validate vulnerabilities?
- Is posture management included or treated as an add-on?
- Can they identify telemetry or data-quality gaps that impact detection accuracy?

Step 5 | Confirm integration and scalability

- Does the service scale with your cloud, identity, SaaS, and network growth?
- Can they support new platforms or data sources without re-architecting?
- Are there optional services available if you need deeper SOC engineering support?

Step 6 | Evaluate operational impact

- How will they reduce workload for your team?
- What is their typical mean time to remediate?
- Do they provide clear reporting and metrics that demonstrate ongoing value?

DEMONSTRATING ROI

Reporting MDR Value to Your Board

Boards care about business outcomes, not raw alert counts. When reporting MDR value, emphasize clarity, risk reduction, and measurable improvements in security operations. For organizations using additional SOC engineering maturity capabilities (such as improved detection tuning or automation support), these outcomes can be even more pronounced.

› Speak in business risk:

- Reduced unauthorized access attempts by X percent
- Lowered ransomware exposure window from hours to minutes
- Improved resilience across critical business systems

› Highlight time to remediation and containment speed:

- Reduced MTTR from X hours to Y minutes
- Containment actions now initiated within minutes
- Faster triage due to higher-fidelity detections

› Show posture improvements:

- Vulnerabilities validated and remediated
- Policy misconfigurations corrected
- Discoveries of telemetry or configuration drift resolved earlier
- Reduction in repeated offenses due to better detection logic

› Demonstrate efficiency gain:

- Reduction in alert volume
- Time saved per investigation
- Automation-driven efficiencies from tuned playbooks or workflows

› Show strategic alignment:

- Cloud migrations supported securely
- Compliance initiatives advanced with improved visibility
- Security operations scaled effectively during organizational growth

CONCLUSION

Choose MDR That Moves at the Speed of Threats

Security teams must detect more, respond faster, reduce risk, and scale operations—often without enough staff. The right MDR partner should ease that burden while measurably improving security outcomes.

Unit 42 MDR delivers continuous detection, investigation, and response within the Cortex platform, correlating signals across endpoint, identity, cloud, network, and SaaS. Proactive threat hunting and intelligence-driven detections surface high-impact threats sooner, while analysts take direct containment actions that reduce MTTR and business impact. The service also improves posture by strengthening cyber hygiene and providing executive-ready reporting that shows clear risk reduction.

Unit 42 Managed XSIAM combines the Cortex XSIAM platform with Unit 42's elite analysts, threat hunters, responders, and SOC engineers to deliver a 24/7 managed SOC with continuous detection, investigation, and full-cycle remediation. Through ongoing SOC engineering, security operations improve over time—reducing operational burden while accelerating response as threats evolve.

UNIT 42®

If your organization is ready to move from overwhelmed to optimized, Unit 42 MDR can help you get there.

APPENDIX

What to Look For in an MDR Provider

Capability	Why It Matters
24/7/365 Monitoring	Threats don't follow business hours—coverage must be 24/7 to reduce risk.
Native Integration	Unified detection, triage, and remediation without context loss or delays, with a platform foundation that supports deeper SOC maturity when needed.
Proactive Threat Hunting	Surfaces emerging threats that haven't triggered alerts—based on your environment and risk profile.
Unified Detection, Investigation, and Response	Streamlined workflows accelerate MTTD and MTTR while reducing analyst burden by managing all data sources, including native and 3rd-party data sources.
High-Fidelity Threat Intelligence	Proprietary intelligence, informed by live incident response, directly shapes detection logic and investigation quality.
AI-Driven Triage and Analysis	Reduces alert noise and prioritizes the most meaningful threats in real time.
Full Visibility Across Surfaces	Endpoint, identity, network, cloud, and third-party telemetry—all correlated natively within your SecOps platform for a complete picture.
Rapid Containment and Guided Remediation	Direct in-console actions isolate and mitigate threats immediately, improving MTTR.
Executive Reporting and Dashboards	Clear, tailored reporting for both technical teams and business stakeholders.
Scalable Coverage and Embedded Expertise	Grows with your business and, when needed, provides access to deeper expertise such as SOC engineers, threat hunters, and incident responders.

About Unit 42

We believe no organization should face advanced cyberthreats alone. Unit 42® strengthens your team with the tools and expertise needed to stay ahead of threats and protect your business. With our proven strategies and insights from thousands of engagements, we'll help your team handle the toughest situations with confidence.

Interested in learning how our team can help your organization? Schedule a 30 minute discovery call.

Contact us now

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks in the United States and other jurisdictions can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.