THREATDOWN™

Managed Detection & Response (MDR)

Evaluation Guide

Key requirements and models for MSPs to choose the right MDR service

Contents

Executive Summary

Delivering cybersecurity for clients is no longer optional for MSPs—it's a core service that defines credibility, competitiveness, and growth. Every client expects 24×7 protection against advanced threats, and for MSPs this means always providing managed detection and response (MDR)—whether fulfilled through an in-house security operations center (SOC) team built on EDR tools, or by partnering with a vendor to deliver MDR-as-a-service.

The challenge is scale. Running a SOC demands budget, skilled analysts, and around-the-clock coverage—resources that many MSPs struggle to sustain across dozens of tenants. At the same time, outsourcing MDR entirely to a vendor raises questions of margin, differentiation, and integration with the MSP's existing service stack.

This evaluation guide is designed to help MSPs navigate those choices. Choosing how to offer MDR isn't just about comparing products, **it's a decision between operating models:**

- **Self-delivered MDR:** MSP builds and runs its own SOC on top of EDR.
- **Vendor-delivered MDR:** MSP leverages a vendor's SOC and threat hunters to fulfill its MDR promise.
- **Hybrid MDR:** MSP combines vendor coverage with selective in-house monitoring.

Selecting the right MDR path is critical to ensuring clients remain secure and productive while MSPs maintain profitability, efficiency, and scalability. Whether you are exploring SOC build-out or evaluating vendor MDR partnerships, this guide provides practical criteria and a framework to identify the MDR approach that best supports your business goals today and as you grow.

[1] Gartner, Definition of small and Midsize Business

Trends and Inhibitors in Managing Threat Detection and Response, In-House

Undoubtedly, cybersecurity is hard. Threats and adversary techniques are evolving in ways that make them harder to predict and even harder to stop.

A recent ThreatDown survey showed that organizations with fewer than 1,000 employees have on average 450 devices to maintain and just three IT staff.[2] For them, security is one task among many, and they don't have time to waste.

Security staff resources and skills shortage

Hiring and retaining seasoned cybersecurity practitioners is a challenge that continues to increase year after year. In fact, the gap between supply and demand for skilled cybersecurity professionals is estimated at 4.8 million.[4]

Detecting advanced attacks

For MSPs, detecting advanced attacks across multiple client environments is a constant challenge. Cybercriminals innovate quickly, using "low and slow" tactics that look like normal activity. Even with strong EDR tools in place, alerts often lack the full context needed to uncover sophisticated threats. To make sense of them, MSPs either need access to external threat intelligence or highly skilled analyst resources that are expensive and difficult to scale. EDR also limits MSPs to reactive investigations, requiring in-house staff to perform proactive threat hunting based on indicators of compromise (IOCs). For most MSPs, building that level of staffing is neither cost-effective nor sustainable.

68%

of SMBs say the biggest security challenge is lack of time and resources[3]

Time-consuming alert management and triage

Industry data shows it still takes an average of 292 days to identify and contain a breach5—an unacceptable delay for MSPs tasked with protecting dozens of clients simultaneously.[5]

Disconnected, complex toolsets

The average organization relies on 50 different security tools, creating integration headaches and wasted cycles.[6] For MSPs, this fragmented approach not only adds operational overhead, but it also risks eroding service quality and undermining client trust.

MSPs serving clients with limited IT budgets face the talent shortage in several ways:

- **Alert Overload** – Lean teams struggle to keep pace with the constant flood of alerts across multiple tenants.
- **Skills Gap** – Junior staff often lack the training and experience to confidently investigate and prioritize threats.
- **Retention Challenges** – Recruiting and holding on to seasoned security talent is costly, leaving gaps that slow growth and limit service expansion.

[2] ThreatDown, The Cost of Complexity
[3] ThreatDown, The Cost of Complexity
[4] (ISC)2, Cybersecurity Workforce Study, 2024
[5] IBM, Cost of a Data Breach Report 2024
[6] IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?, Doc Document number:# US51973524, Mar 2024

The Rise and Value of MDR Services

Given the complexity of managing detection and response across multiple clients, MSPs are adopting new strategies to close gaps in coverage, skills, and scalability. At the center of these strategies is Managed Detection and Response (MDR)—a service that combines advanced EDR technology with human-led threat hunting and response.

For MSPs, MDR is no longer optional. It's the foundation of delivering 24×7 protection to every client. The question is how to fulfill it:

- **Build and run MDR in-house,** staffing a SOC to monitor client environments around the clock.
- **Leverage vendor-delivered MDR,** where a trusted provider (like ThreatDown) supplies the SOC, analysts, and playbooks, while the MSP focuses on client relationships and business growth.

Notably, MDR security services are growing rapidly, with the market projected to hit $11.8 billion by 2029—a 23.5% CAGR from 2024.[7] According to Gartner, "By 2025, 50% of organizations will be using MDR services for threat monitoring, detection, and response functions that offer threat containment capabilities." Proof that clients will expect their MSP to deliver it.

At a high level, MDR is the always-on cybersecurity layer MSPs must deliver to clients—ensuring protection even when advanced threats slip past standard EDR detection. MDR combines technology and human expertise to provide:

- **24×7 monitoring across all client environments**, ensuring attacks are spotted at any time
- **Expert-led detection, alerting, and response**, with seasoned analysts investigating and containing threats
- **Correlation of endpoint alerts with broader data sources**, turning noise into actionable insights
- **Proactive threat hunting based on indicators of compromise (IOCs)** to identify threats before they escalate

[7] Markets and Markets . Managed Detection and Response Market Forecast to 2029

The Rise and Value of MDR Services (continued)

Why MDR Matters for MSPs and Their Clients

When an MSP partners with an MDR provider, they gain the ability to seamlessly scale MDR across all tenants, while alleviating the staffing and cost pressures of building a SOC. Beyond coverage, MDR delivers measurable business benefits:

Client benefits

- Reduce breach risk and potential financial loss (average breach = $4.88M).[8]
- Maintain uptime and employee productivity with faster threat containment.

MSP benefits

- Improve service margins by shifting from staffing costs to predictable subscription models.
- Free technical staff from chasing alerts so they can focus on billable projects and client expansion.
- Elevate skills by learning from vendor SOC workflows and incorporating advanced threat hunting practices.

Key Evaluation Areas for MSPs

Before deciding how to fulfill MDR, MSPs should evaluate three critical areas:

1. **Essential MDR capabilities** – What features are non-negotiable for protecting clients?
2. **Delivery model** – Build MDR in-house with EDR + SOC, or outsource to a vendor service?
3. **Vendor selection** – If outsourcing, which provider offers multi-tenant support, integrations, and scalable pricing?

Let's review the criteria for each of these core areas.

[8] IBM, Cost of a Data Breach Report 2024

Essential MDR Capabilities for Managed Services

MDR services often come with a long list of features and "nice-to-haves," but for MSPs, the essentials boil down to one thing: quick, accurate detection and remediation of IOCs across all client environments.

To deliver on this promise, MSPs need to evaluate MDR offerings across both the technology stack and the human expertise that powers them. Below are the critical capabilities to consider when selecting an MDR service for your clients:

Requirement #1: 24x7 real-time threat detection

Attackers don't follow business hours—and most ransomware attacks occur between 1–5am, when IT teams are offline.[9] MSPs must ensure their MDR partner provides true 24×7 SOC coverage to deliver uninterrupted monitoring and response across all tenants.

Requirement #2: Powered by EDR and SIEM technologies

MDR is only as strong as the tools underneath it. Look for services that combine:

- **EDR** for prevention, detection, and automated response at the endpoint.
- **SIEM** for correlating endpoint alerts with logs and network data, creating actionable insights and reducing noise.

An MDR service is only as strong as the technology that powers it . There are a range of approaches, so it's important to dig into the behind-the-scenes details when evaluating MDR providers. Good security hygiene is about "defense-in-depth" to counter the many possible attack vectors, so your MDR offering should include two, essential technologies: security information and event management (SIEM), as well as endpoint detection and response (EDR).

A managed SIEM solution enriches threat analytics with endpoint alerts, correlated with log events and network flow, providing greater context that enables an MDR team to efficiently identify critical threats and IOCs. A robust EDR system is the go-to tool to deal with attacks that land on an endpoint. A high-caliber EDR solution should provide advanced threat prevention, detection, and automated response actions.

Requirement #3: Effective threat response

Speed matters. The right MDR service combines automation with experienced analysts who can contain and remediate threats quickly—reducing mean time to respond (MTTR) and minimizing client impact.

Responding to incidents has been a challenging area for Managed Service Providers, often taking teams days to weeks to contain and remediate a threat. One of the biggest values from an MDR service that you can fortify your clients's security with fast and efficient incident investigation and response.

To make that a reality, a high quality MDR service should provide incident response that is supported by both security analysts and the EDR platform. An MDR service provider with top tier security analysts will have the skills to tackle complex threats. This will reduce your clients's mean time to response (MTTR) and ensure they receive appropriate response actions for each type of incident.

[9] ThreatDown, 2024 State of Ransomware Report

Essential MDR Capabilities for Managed Service (continued)

Requirement #4: Threat intelligence

MDR should integrate curated, multi-source threat intelligence to reduce false positives and focus only on the threats most relevant to your clients. This context helps analysts act faster and with greater accuracy.

To keep data safe from zero-day attacks and advanced persistent threats (APTs), your MDR solution should include threat intelligence that applies specific tools and practices. Threat intelligence, or cyber threat intelligence, is information security experts use to understand the threats that have, will, or are currently targeting your clients. This provides insights into who attackers are, where they can access the network, and specific actions that can be taken to strengthen defenses against a future attack.

Your MDR solution should use curated threat intelligence from multiple sources. This important feature reduces false positive alerts and ensures that your service is focusing on the threats that are most relevant and likely to be launched against your clients.

Requirement #5: Threat hunting

Look for both:

- **Research-based hunting** for past IOCs and vulnerabilities that may still be exploitable.
- **Active hunting** for live suspicious activity in client environments. Best-in-class MDR delivers both, not just reactive hunting.

Threat hunting typically includes two, essential functions in the delivery of MDR services. The first one is research-based threat hunting where security analysts look, or "hunt," for past IOCs and vulnerabilities that can pose a risk to your environment. When an analyst identifies a potential exploit, this information drives the team's priorities to provide related detection and response functions.

The second approach is active threat hunting where the security analysts systematically reviews your organization's environment to uncover any current suspicious activity or newly emerging IOCs that are in progress. Of course, when an IOC is detected, your MDR provider's response efforts should kick into action.

Requirement #6: Reporting

MSPs need clear, consistent communication. MDR reports should be accessible via dashboards or email, showing not just detected threats and responses, but also the overall health of client environments. This allows MSPs to prove value to clients and track provider performance.

Requirement #7: Multi-Tenancy

MSPs must manage dozens of client environments efficiently. A true MDR solution should provide a single pane of glass for all tenants—consolidating alerts, reporting, and remediation in one console.

A multi-tenant architecture eliminates the need to log into separate dashboards for each customer, reduces overhead, and ensures consistent service delivery. This capability is critical to scaling MDR profitably while maintaining visibility across the client base.

Essential MDR Capabilities for Managed Service (continued)

Requirement #8: Automation & Scalability

MDR must reduce the manual burden of alert triage across multiple tenants. Look for services that automate correlation, prioritization, and remediation so analysts don't drown in low-value alerts.

Effective automation allows MSPs to deliver enterprise-grade outcomes with lean teams. Scalable MDR means alert fatigue is reduced, response is faster, and teams can focus on higher-value client projects instead of repetitive tasks.

Requirement #9: Service Margin

For MSPs, MDR is about coverage as well as profitability. Outsourcing MDR to a vendor can stabilize margins by replacing unpredictable staffing costs with subscription-based pricing.

By contrast, self-delivered MDR can erode margin if analyst time is consumed by 24×7 monitoring and manual response. The right MDR partner should enable MSPs to expand service offerings while preserving profitability.

Requirement #10: Integration

An MDR solution should plug seamlessly into an MSP's existing ecosystem—including PSA and RMM tools, billing workflows, and compliance reporting.

Tight integration reduces swivel-chair management, accelerates service delivery, and makes it easier to package MDR into existing offerings. Without this, MDR becomes siloed and adds operational friction rather than removing it.

Requirement #11: Differentiation

MDR should give MSPs a competitive edge. While many providers simply resell EDR, offering MDR-as-a-service positions an MSP as a trusted security partner with true 24×7 coverage.

Differentiated MDR allows MSPs to stand out in crowded markets, strengthen client retention, and command higher-value contracts by delivering services that go beyond commodity endpoint protection.

Requirement #12: Cost Transparency

Predictable, transparent pricing is essential for MSP business models. MDR should be priced per endpoint or per client, with no hidden SOC or staffing costs.

This enables MSPs to forecast margins accurately, scale services without financial surprises, and avoid the capital expense of building and maintaining their own SOC. Clear cost models protect both the MSP's profitability and the client's budget expectations.

Requirement #13: Delivery Model

MSPs must decide how MDR will be fulfilled for their customers. There are three primary models:

- **Self-delivered MDR** – The MSP builds and operates its own SOC, using EDR as the foundation. This provides control but demands heavy staffing and 24×7 coverage.
- **Vendor-delivered MDR** – The MSP leverages a vendor's SOC, analysts, and playbooks (e.g., ThreatDown MDR) to deliver MDR as a managed service. This accelerates time-to-market and preserves margins.
- **Hybrid MDR** – The MSP blends both approaches, handling certain monitoring or response functions internally while relying on the vendor SOC for after-hours or advanced threat coverage.

Choosing the right delivery model is a strategic decision that balances control, cost, scalability, and differentiation. The best option depends on the MSP's size, available talent, and growth ambitions.

Essential MDR Capabilities for Managed Service (continued)

Here is a comparison between the described delivery models:

Criteria	Self-Delivered MDR (MSP SOC + EDR)	Vendor-Delivered MDR (ThreatDown)	Hybrid Model
Coverage	Business hours or limited 24×7 (depends on MSP staff)	True 24×7×365 monitoring, triage, and response by vendor SOC	MSP covers daytime, vendor provides overnight/weekend coverage
Staffing	Requires SOC analysts, threat hunters, and on-call rotation	Vendor supplies expert analysts, hunters, and playbooks	Shared staffing burden between MSP and vendor
Cost Model	High fixed costs (analysts, tools, training, SOC infrastructure)	Predictable per-endpoint/per-customer pricing	Mix of fixed cost and variable vendor cost
Scalability	Limited by hiring and training capacity	Instantly scalable across all tenants with no new hires	Flexible—can add vendor coverage as MSP grows
Alert Handling	MSP team triages all alerts, high risk of burnout	Vendor delivers prioritized, actionable incidents	Alerts filtered by vendor, escalations handled by MSP
Multi-Tenant Management	Depends on EDR console capabilities; often siloed	Single pane of glass (ThreatDown OneView) across all clients	Split view: MSP EDR console + vendor MDR portal
Margin Impact	Thin margins due to staffing costs and slow onboarding	Higher margins through subscription resale + cross-sell opportunities (e.g., DNS Filtering, Email Security, Patch Management)	Moderate margins, balance of vendor subscription + internal labor
Time-to-Value	Weeks/months to stand up SOC, tune EDR, and train staff	Minutes to onboard endpoints with MDR already active	Faster than self-delivery, slower than full vendor MDR
Differentiation	"We built our own SOC" story may appeal to select clients	Vendor MDR provides enterprise-grade coverage that MSPs can white-label	Blend of both stories, but messaging is complex
Risk & Liability	High—MSP responsible for missed alerts or gaps in 24×7 coverage	Vendor shares responsibility; backed by SLAs and expert SOC	Risk partially offset by vendor support

Choosing Your MDR Delivery Path

For MSPs, the critical decision is not whether to provide MDR—every client now expects it—but how to deliver it. You have three options: build MDR in-house, outsource MDR to a vendor, or adopt a hybrid model.

Market trends show that most providers are moving toward vendor-delivered MDR, because it removes the heavy cost, staffing, and infrastructure burden of building a SOC, while accelerating time-to-market and profitability. Still considering building MDR in-house? Here are the realities:

MDR staffing requirements

- Hire a minimum of five, full-time employees to provide 24/7 coverage
- Identify effective avenues to find, hire, and replenish high-caliber security talent
- Invest into an employee loyalty and retention program

MDR facilities requirements

- Build out SOC facilities
- Purchase, implement, and maintain the hardware and software for your SOC
- Project manage day-to-day SOC operations and incident response
- Provide ongoing security training, certifications, and red team exercises to expand staff expertise
- Purchase and manage third-party security intelligence feeds
- Engage periodic outside consultation to assess the caliber of your detection and response services and invest in appropriate items to make any recommended improvements

In short, self-delivered MDR is the equivalent of launching an entirely new business unit inside your MSP—high cost, high effort, and high risk. By contrast, partnering with a vendor-delivered MDR service provides immediate advantages:

- Fast time-to-market across your client base.
- Access to the latest MDR technology and tools without upfront capital investment
- No need to carry staffing costs for a 24×7 SOC.
- Predictable pricing aligned to per-endpoint or per-customer billing.
- Expertise from seasoned threat hunters and analysts working attacks every day.

This choice defines how well you can scale MDR profitably while meeting client expectations for round-the-clock protection.

Top Considerations for Selecting the Ideal MDR Vendor

Selecting the right MDR partner is one of the most important decisions an MSP can make. The vendor you choose will not only impact service quality but also your margins, scalability, and client satisfaction. When evaluating MDR providers, consider these areas:

✔ Breadth of threat detection and response capabilities

- How effective are they at detecting new and obfuscated malware?
- What technologies do they use to power the MDR service, such as EDR, SIEM, and threat intelligence feeds?
- How often do they update the threat definitions on their EDR software agents?
- Do they support all the threat response requirements such as network, process, and desktop isolation, as well as automated remediation and rollback of ransomware encryptions so you can restore access to their files?

✔ Trusted brand

- Do you know and trust the brand to be hands-on with their customers' endpoints?
- How is the vendor perceived in the market, and what kind of customer ratings do they receive?

✔ Ease of EDR deployment and onboarding

- What's the typical amount of time to install the EDR agents on machines? Is it a process that can be done in days, or will it take weeks?
- Once the EDR solution is set up, how much time will it take to establish a baseline profile for alerts?
- How long will it take before the MDR can enable communications with your internal IT security team?

✔ Threat hunting expertise

- How many security analysts will be supporting your organization? What are their qualifications?
- Does the MDR vendor have cyber security practitioners with well-established and seasoned pedigrees?
- Do you have strong confidence in the MDR vendor's ability to identify all levels of threats and swiftly deliver appropriate incident response efforts?

✔ Reporting and Transparency

- Do the reports provide clear visibility into detected threats, actions taken, and ongoing investigations?
- Can you easily share dashboards and summaries with clients to demonstrate value?
- Does the vendor highlight weaknesses in client environments to guide proactive improvements?

Top Considerations for Selecting the Ideal MDR Vendor (continued)

✔ Multi-Tenancy and Integration

- Can the MDR service manage multiple client environments from a single pane of glass?
- Does the offering integrate seamlessly with PSA and RMM tools for workflows, billing, and compliance reporting?
- Do the integrations reduce operational overhead instead of adding complexity?

✔ Affordable, Predictable Pricing

- Is pricing structured per endpoint or per client, and is it easy to forecast costs?
- Are all fees transparent, with no hidden SOC, setup, or escalation costs?
- Does the model support healthy margins while remaining competitive for clients?

✔ Differentiation and Growth Potential

- Does the MDR service provide features beyond basic EDR resalethat differentiate your offering?
- Does the vendor offer a broad security portfolio (e.g., DNS, Email Security, Patch, etc.) that creates cross-sell opportunities to increase ARPU?
- Can the vendor's MDR help you strengthen client retention by positioning your business as a trusted, long-term security partner?

✔ Vendor communications

- What method will the MDR team use to communicate with you and how often? What channels are available to reach the MDR team—phone, email, ticketing, live chat?
- Can your team easily connect with the MDR service provider when you need support? How about outside of business hours?
- Are you satisfied with the level of communication offered by the vendor? Does it align with your business needs?
  - How quickly can you escalate an issue to a human analyst, including outside business hours?
  - Are communication practices aligned with your service commitments to clients?

✔ Threat enrichment via SIEM

- How many and which type of security data sources does the MDR vendor use to monitor and identify threats?
- Does the vendor use MITRE data, network, and third-party threat intelligence feeds to enrich their threat intelligence telemetry data and increase their threat detection effectiveness?

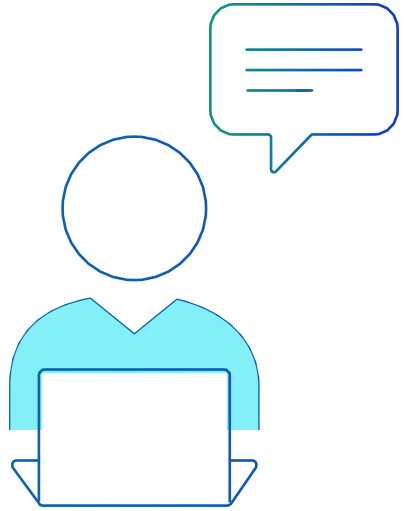
Considerations for Future Growth

MSPs face the dual challenge of protecting clients while also scaling their own business. Delivering MDR is a non-negotiable part of that equation—but how it's fulfilled will determine profitability, efficiency, and long-term growth.

Standing up an in-house SOC is costly, requiring heavy investments in staffing, infrastructure, and continuous training. That's why most MSPs turn to vendor-delivered MDR, offloading the most resource-intensive tasks while ensuring clients receive enterprise-grade protection.

The key is selecting a partner that aligns with your MSP business model—offering multi-tenant support, strong EDR capabilities, seasoned security analysts, and predictable pricing that scales with your customer base. A vendor purpose-built for MSPs not only fills the talent and technology gaps but also frees your team to focus on higher-margin projects and client expansion.

By choosing the right MDR delivery model and partner, MSPs can strengthen client security today while positioning themselves to grow profitably in the years ahead.



ThreatDown: MDR Purpose-Built for Resource-Constrained Managed Service Providers

MDR designed for MSP delivery

ThreatDown MDR empowers MSPs to deliver always-on threat detection, investigation, and response across all client environments—without the overhead of building a SOC. With 24×7 monitoring backed by seasoned threat hunters, analysts, and service leaders, MSPs can ensure clients stay resilient against evolving attacks while their own teams focus on growth. ThreatDown's proprietary remediation technology eliminates dynamic and hidden artifacts in real time, providing complete and precise incident response.

Affordable, scalable packaging

Built for the MSP business model, ThreatDown MDR is priced predictably and packaged to scale. It enables providers to extend enterprise-grade protection to every client while maintaining healthy margins and competitive rates.

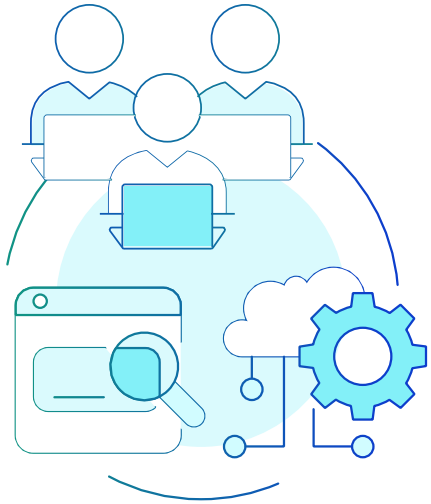
Powered by ThreatDown EDR

ThreatDown EDR provides powerful and effective threat detection, isolation, and remediation. Along with Malwarebytes' patented ransomware detection, it includes many advanced layers of protection, multi-mode isolation, and automated malware clean up . Other feature highlights include:

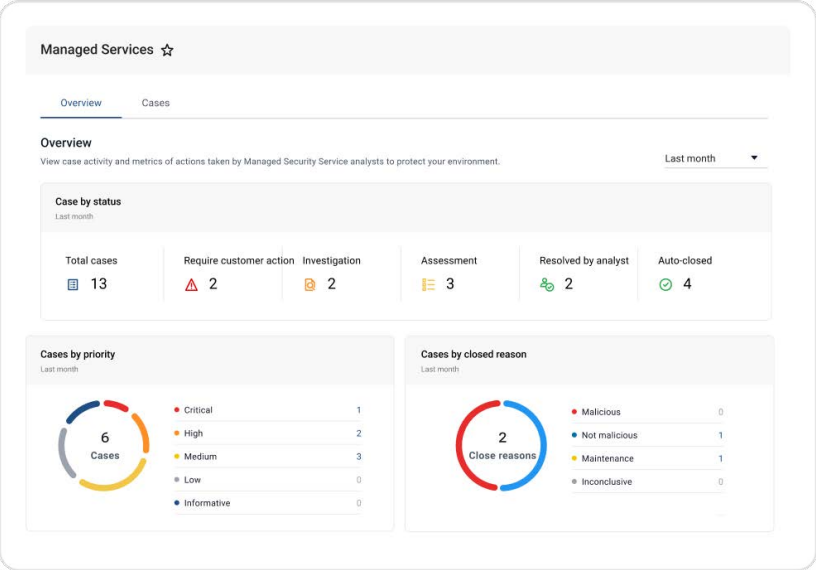
- **Provides the industry's only 7-day ransomware rollback, enabling full recovery from ransomware attacks in minutes.**
- **Applies multiple detection techniques to provide full attack chain protection.**
- **Delivers advanced remediation capabilities that uncover and remove hidden malware artifacts to provide thorough endpoint clean up.**

Backed by advanced SIEM and SOAR technology

ThreatDown MDR leverages integrated SIEM and SOAR to enrich detection data with threat intelligence and automate response actions—helping our analysts respond faster, with greater accuracy, around the clock.



Detect and Neutralize Threats 24x7 with MDR



Learn more about how ThreatDown MDR can help your business.

Speak to an MDR expert

THREATDOWN™ | threatdown.com/mdr | sales@threatdown.com