THREATDOWN™ | MSP Program

ThreatDown Managed Detection & Response (MDR)

Unlocking 24×7 threat monitoring and remediation for Managed Service Providers (MSPs)

How it works

ThreatDown MDR empowers MSPs to deliver always-on security protection to their clients—without the cost and complexity of building a SOC. Through a combination of advanced ThreatDown technology and expert human analysis, MSPs can provide 24×7 monitoring, rapid incident investigation, and precise threat remediation across all client environments.

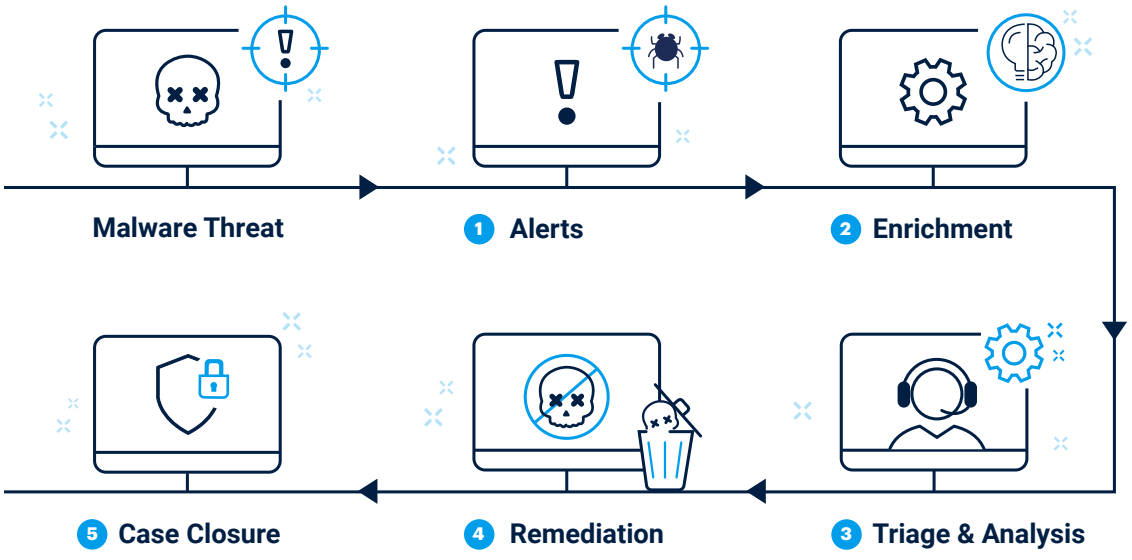
Purpose-Built MDR for MSPs

ThreatDown MDR empowers MSPs to deliver always-on security protection to their clients—without the cost and complexity of building a SOC. Through a combination of advanced ThreatDown technology and expert human analysis, MSPs can provide 24×7 monitoring, rapid incident investigation, and precise threat remediation across all client environments.

ThreatDown MDR gives partners a scalable, profitable way to deliver enterprise-grade security outcomes. Whether you operate a self-delivered, vendor-delivered, or hybrid MDR model, ThreatDown adapts to your service strategy while keeping clients secure and your operations efficient.

Key benefits for MSPs:

- 24×7 monitoring and human-led investigation across all tenants.
- Flexible remediation options to fit your delivery model.
- Predictable per-endpoint pricing that protects margins.
- Transparent reporting for compliance and client visibility.



1 Alerts

With ThreatDown Endpoint Detection and Response (EDR) deployed in customer environments, MSPs gain a powerful first line of defense. The solution includes multiple protection layers, multi-mode isolation, and the industry's only 7-day ransomware rollback.

Our SOC analysts continuously monitor endpoint data to detect suspicious activity or indicators of compromise (IOCs) and immediately initiate analysis.

Leveraging ThreatDown EDR, our team of security experts provides 24x7 monitoring of customer endpoints for threats to the organization. We'll consistently assess the EDR data to look for alerts that indicate suspicious activity, a detected threat, or an indicator of compromise (IOC).

2 Enrichment

ThreatDown's backend security orchestration, automation, and response (SOAR) platform enriches EDR telemetry with curated threat intelligence from multiple global feeds. This correlation provides full context to help analysts quickly assess the scope, severity, and intent of every detection—enabling faster, smarter decisions.

This adds powerful SOAR capabilities, maintained by our MDR team, and equips the MDR Analysts with additional information and insights about what is happening in the environment, enabling them to understand the threat and its potential impact quickly and easily. Armed with this information, the MDR Analysts can swiftly make informed decisions on the best way to respond.

3 Triage & analysis

Unlike providers that rely solely on automation, ThreatDown analysts perform human-in-the-loop validation to ensure accuracy. They examine artifacts, open cases, and collaborate across tiers—including senior analysts—to confirm whether alerts are legitimate threats or false positives. This combination of automation and expertise delivers a higher detection rate and fewer misses.

Our approach provides a higher degree of accuracy and catches more threats, which includes the following steps:

- During the alert analysis, the MDR Analysts review specific artifacts to find those that require a deeper examination.
- A case is opened on each artifact that requires triage.
- The Analysts will collaborate to analyze and assess the artifacts, as well as include a Tier 3 Analyst, if needed.
- The Analysts will decide on the artifact and share that information.

4 Remediation

We understand your MSP business has unique considerations for your MDR service, and there is no 'one size fits all' model for remediating threats. That's why our MDR service gives you options for remediation so you can choose the model that works best for your MSP business. The choice is yours.

- **ThreatDown managed:** The MDR Analysts remediate the threat in your customer environments.
- **MSP managed:** Our analysts provide actionable guidance so your team can complete remediation. This model ensures each partner can align MDR delivery with their service design and client SLAs.

5 Case closure & reporting

After each incident, ThreatDown documents every step—from alert to resolution—within comprehensive SOC reports. These reports are accessible through ThreatDown OneView, providing MSPs and clients with audit-ready visibility for compliance and performance tracking.

Why MSPs Choose ThreatDown MDR

- Fast time-to-market: Launch MDR within days, not month
- Integrated platform: Manage MDR, EDR, and additional services from a single console.
- Scalable delivery: Expand across clients without adding headcount.
- Trusted expertise: Backed by ThreatDown's 24×7 global SOC and proven threat researchers.

Grow Profitably with ThreatDown MDR

By partnering with ThreatDown, MSPs can offload the cost and complexity of continuous threat monitoring while providing premium, always-on protection to their clients.

Learn More

Learn more how the ThreatDown MSP partner program works:

threatdown.com/partner-program/msp/