ThreatDown
Powered by Malwarebytes

Data Sheet

ThreatDown Managed Detection & Response

Protect your organization with managed 24x7x365 threat monitoring, investigation, and remediation by our expert MDR analysts

Overview

For security teams of small and medium-sized organizations, delivering high quality security services and keeping business environments free from threats requires a skilled team that can provide 24x7 coverage. Yet, many organizations face constrained staff resources and lack deep cyber security expertise. In addition, they are constantly overloaded with alert triage responsibilities. Add to this the skyrocketing cost and complexity of managing multiple solutions to uncover hidden threats, which leads to inefficiency and lengthy incident response times.

Constrained security teams need an easy, efficient, cost-effective way to detect and respond to threats

ThreatDown, powered by Malwarebytes, alleviates these challenges with a purpose-built managed detection and response (MDR) offering. ThreatDown MDR provides a powerful and affordable threat detection and remediation offering with 24x7x365 monitoring and investigations by our top-tier security analysts. Your business will gain a posture of cyber resilience with expert services that accelerate threat detection and perform incident response with precision. ThreatDown MDR provides flexible threat response options that suit the needs of both your business and your security environment, ensuring you maintain full visibility and control over your endpoints.

ThreatDown MDR Advantages

- **24x7x365 monitoring**: We monitor endpoints and perform expert investigations day and night, weekdays, weekends, and holidays. We're always watching.

Challenges

- Limited resources to address security needs – 67% reported cybersecurity staff shortages[1]
- Too many alerts lead to alert fatigue – 80% of EDR alerts are being inored by IT[2]
- Slow response allows attackers more time on your endpoints – 277 days average number of days to identify and contain a breach[3]

Benefits

Protect your organization's workstations, servers and more with ThreatDown MDR

- Better Security – Proactively mitigate risk before a breach
- Less Effort – Save your team resources by relying on expert ThreatDown security analysts to help monitor, investigate, and remediate suspicious activites
- Best Value – Achieve faster response and remediation times, at significantly less cost compared to customers' own management efforts

[1] Malwarebytes State of Malware Report. [2] ThreatDown Research. [3] Cost of a Data Breach Report 2023.

- **Skilled MDR analysts**: Our team of security experts are accomplished threat hunters with deep incident response backgrounds and decades of experience triaging and mitigating complex malware threats.
- **Award winning EDR**: Powered by our ThreatDown Endpoint Detection and Response (EDR) platform and enriched from multiple threat intelligence feeds, including MITRE and others.
- **Flexible remediation options**: Our MDR Team can actively remediate threats as they are discovered or provide highly, actionable guidance for IT teams to follow in their own remediation efforts.
- **Active threat hunting**: Our MDR Team hunts unseen threats based on past indicators of compromise (IOCs) and suspicious activity observed on endpoints.
- **Rapid deployment**: ThreatDown EDR is known for ease of set-up, allowing your security team to rapidly onboard new endpoints into our 24x7 MDR service in a matter of minutes.

How Does it Work?

Once endpoint agents are deployed, the MDR service is activated within minutes and ThreatDown analysts can monitor the customer's environment. Detection data is ingested into the MDR Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform where it is enriched with internal and external threat intelligence feeds. This process speeds the identification, analysis, and triage (response prioritization and investigation) of security events. At this point, the MDR SIEM/SOAR platform verifies suspicious activity alerts as actual threats or benign detections and can escalate the severity rating of certain EDR detections based on threat intelligence. Cases that require remediation are either completed by the analyst or guidance is provided to the customer or MSP if they have opted to perform their own remediation actions.

ThreatDown's Industry Accolades

Consistent top ranking of Level 1 certification in MRG Effitas 360 degree testing and #1 Endpoint Security Suite by G2 validates ThreatDown's effective and easy-to-use solution.

Learn More

To learn more about how ThreatDown MDR can help reduce cyber risk of your organization, please visit threatdown.com/mdr.