DATA SHEET

THREATDOWN™
Powered by Malwarebytes

ThreatDown Managed Detection & Response

Extend your team with expert-led 24x7x365 threat monitoring, investigation, and remediation

Overview

For security teams 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.

92% **report skills gaps in their organizations[2]**

ThreatDown, powered by Malwarebytes, alleviates these challenges with a purpose-built managed detection and response (MDR) offering. Your business will gain a posture of cyber resilience with expert services that accelerate threat detection and response with precision. ThreatDown MDR and MDR Plus 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 and identities.

ThreatDown MDR Advantages

- **24x7x365 monitoring**: We monitor endpoints and identities to perform expert investigations day and night. We're always watching.
- **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.
- **Service Level Objectives**: We deliver rapid response backed by defined performance targets to speed detection and reduce impact:
  - **Customer Notification: <10 minutes** from confirmed threat detection
  - **Analyst Engagement: <30 minutes** for investigation and response initiation

Challenges

- Limited resources to address security needs – 57% reported cybersecurity staff shortages[1]
- Organizations lack needed security expertise – 92% report skills gaps in their organizations[2]
- Slow response allows attackers more time on your endpoints – 292 days average number of days to identify and contain a breach[3]

Benefits

Protect your organization's workstations and servers with ThreatDown MDR

- Continuous Detection and Response – Extend security with 24/7 expert monitoring, delivering prioritized insights without playbooks or manual case management
- Faster Expert Analysis – Expert teams speed analysis and triage, dramatically lowering remediation costs compared organizations handling alerts internally
- Expert Remediation and Guidance – Enables faster threat containment and incident response while minimizing human error and attack impact

[1] State of Cybersecurity 2024, ISACA. [2] 2023 Cybersecurity Workforce Study, ISC2. [3] Cost of a Data Breach Report 2024, Ponemon Institute.

- **Award winning EDR**: Powered by our ThreatDown Endpoint Detection and Response (EDR) platform and enriched from multiple threat intelligence feeds, including MITRE and others.
- **Identity Threat Detection & Response (ITDR)**: We stop identity-based attacks by continuously monitoring behavior associated with credentials, privileges, and access across Active Directory, Entra ID, and Okta*
- **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 and ITDR is known for ease of set-up, allowing your security team to rapidly onboard new endpoints and identities in a matter of minutes.

ThreatDown MDR Plus Advantages

- **Malware Removal Service**: Hands-on analyst support to fully remove complex, persistent threats from your environment.
- **Root Cause Analysis**: Post-incident investigation to identify how an attacker got in, what happened and what needs to change.
- **Threat Intelligence Feeds**: ThreatDown MDR Plus enriches detection with credential exposure intelligence, giving analysts earlier warning, before attackers can use them.
- **Contractual SLAs**: Contract guaranteed response and containment times.

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 SIEM and 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

ThreatDown consistently earns the top ranking of Level 1 certification in MRG Effitas' quarterly 360 degree testing. In addition, G2 badges of #1 Endpoint Security Suite and MDR Grid Leader validate ThreatDown's effective and easy-to-use solution.

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

THREATDOWN™
Powered by Malwarebytes

threatdown.com/mdr

sales@threatdown.com