DATASHEET

Bitdefender

MDR

Bitdefender Managed Detection & Response: Threat Hunting

www.bitdefender.com

Threat hunting is a critical component of MDR, protecting customers from compromise and keeping attacker dwell time to a minimum

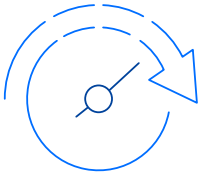
Bitdefender MDR Threat Hunting provides a comprehensive approach to reducing compromise of business systems and attacker dwell-time. Continuous and proactive assessment of risks to your business, combined with a deep understanding of your networks and systems activity, enables us to recognize any abnormalities.

Global

Bitdefender Labs, threat intelligence teams, and security researchers continuously monitor all aspects of the global threat landscape, using the knowledge gained to drive threat hunts across your systems.

Personalized

Using detailed business and technology profiling, combined with a deep system and user behavior baseline, Bitdefender's expert Threat Hunters can quickly identify potential risks to your business.



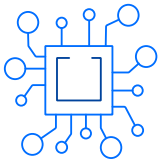
Proactive

Our team continuously identifies industry trends, system anomalies, and new adversary techniques that inform and drive comprehensive threat hunting in your environment.

With Bitdefender MDR, you can benefit from periodic threat hunting activities targeted at your business systems, as well as risk-based threat hunting triggered by expert analysis of the global threat landscape.

Targeted Threat Hunting

Our threat hunting experts use the latest threat intelligence powered by Bitdefender Labs and a continually updated threat model tailored to your organization to perform periodic threat hunts across your systems.



Risk-based Threat Hunting

Our teams compile a massive amount of organic and systematic threat intelligence, attacker research, and threat analysis that trigger proactive threat hunts in your environment.

Why We Threat Hunt

Discover: Attackers are continually advancing and improving their tools and techniques, rendering existing detections out-of-date. Without threat hunting, an attacker will inevitably breach a system using methods that cannot be detected using only technology.

Evict: Industry research shows that attacker dwell-time (the time an attacker can stay inside an organization through the deployment of command-and-control malware or using back-doors) is significantly high. Threat Hunting is a critical component in evicting attackers post-compromise.

Learn: At Bitdefender, the end of the hunt is not the end of the story. We use the knowledge, information, and data gained through the hunt to enrich each customer's risk profile to ensure continuous security improvement can be achieved for everyone.

How We Threat Hunt

We utilize multiple data sources and proactive analysis to investigate anomalies and suspicious activity that detection alone will miss. These methods provide much deeper visibility than technology alone.

Keep watch for new threat actor activity and emerging threats: Threat intelligence teams and Bitdefender Labs provide valuable external observations that can indicate a risk to one or many of our customers.

Establish the normal to recognize the abnormal: A continuous stream of telemetry from customer systems compared to detailed baselines of past activity provide critical internal observations that trigger threat hunts based on new and unusual activity.

Theorize, Understand, Search: Threat hunters understand the attacker's mindset, forming hypotheses around what they may have done and working to search in customer environments to establish and document behavior.

Take Action: While the primary goal of threat hunting is to discover attackers – or their actions within your systems – there are various outcomes. Even if a threat hunt does not result in an incident, our experts will advise you on other findings. These can include weaknesses, bad practices, or other security posture improvements they have identified, which you can then use to harden your environment.

Outcomes

Whether through threat hunting or the normal course of investigations, there are a set of outcomes that you can expect from the Bitdefender MDR service.

All-Clear

Sometimes knowing that we've looked and found nothing of concern is valuable. After each hunt and investigation, we'll be sure to communicate that everything is okay.

Pre-Approved Actions

As part of the service, you can define specific actions we can take on your behalf. These are highly customizable to give you the confidence that critical operations will not be affected.

Action Plan

Without a pre-approved action, our Security Account Manager will contact you with a plan of action, delivering reports during and after an incident for sharing with internal stakeholders and management.

Bitdefender MDR Service Offerings

Bitdefender MDR is available via two service tiers.

	Advanced	Enterprise
24/7 Security Operations	✓	✓
Threat Management	✓	✓
Tailored Response Playbooks	✓	✓
Expert Recommendations	✓	✓
Root Cause & Impact Analysis	✓	✓
Monthly Service Reports	✓	✓
Targeted Threat Hunting	✓	✓
Tailored Threat Modeling	✓	✓
Priority Target Monitoring		✓
Risk-Based Threat Hunting		✓
Brand & IP Protection		✓
Dark Web Monitoring		✓
Domain Registration Monitoring		✓
Digital Asset Monitoring		✓

What our customers are saying:

Bitdefender MDR assures me that someone is watching our entire network in real-time, including when my staff and I are not in the office. We're able to protect our information assets regardless of where employees are logging in from. MDR is an extension of my team to support the mission of the Archdiocese.

– IT Director, Archdiocese | Non-profit, USA

"The Bitdefender MDR team has been responsive, knowledgeable, and successful at protecting our valuable data. Our number one priority is providing top patient care and Bitdefender has been successful in supporting that at every turn."

– Mostafa Mabrouk, Corporate Information Security Manager | Magrabi Hospitals and Centers

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

Bitdefender-MDR-Datasheet-ThreatHunt-NoLocalization-creat5764-en_EN
15/09/213 November 2021 9:32 pm03/11/21