

Overview of Offerings

Contents

- [Overview of Offerings](#)
- [Key Benefits & Differentiators](#)
- [Versus Top Competitors](#)
- [Questions & Answers](#)
- [Latest Awards & Use Cases](#)

Bitdefender MDR Features Matrix

SERVICE COMPONENT	MDR	MDR PLUS
Industry Leading Security Platform	✓	✓
24x7 Security Operations Center	✓	✓
Pre-Approved Actions (PAAs)	✓	✓
Threat Hunting	✓	✓
Expert Recommendations	✓	✓
Incident Root Cause & Impact Analysis	✓	✓
MDR Portal & Reporting	✓	✓
24x7 Security Account Manager (Customer Success)		✓
Professional Services Onboarding		✓
Global Threat Intelligence Feeds & Analysis		✓
Dark Web Monitoring		✓
Security Baselineing & Tailored Threat Modeling		✓
Brand & IP Protection		✓
High Priority Target Monitoring		✓
XDR Sensors	(add-on)	(add-on)

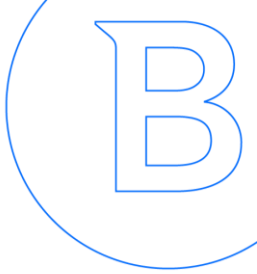
Who is Bitdefender MDR For?

- ↳ **Orgs with Cybersecurity Skills Gap:** Companies lacking resources to cover 24x7 monitoring or can't find or afford security expertise.
- ↳ **Increasing Cyber-attack Sophistication & Alert Fatigue:** Orgs. that are struggling to keep up with increasing attack surface and sophistication of attacks and are challenged with prioritizing alerts.
- ↳ **Compliance Requirements:** Orgs. looking to obtain or renew cyber insurance, or who have to meet security compliance, are often required to have MDR.
- ↳ **Cybersecurity Tools Complexity:** Orgs. looking to move away from SIEM and simplify their security stack to improve incident response time.
- ↳ **Enterprises looking to Strengthen their Security Posture:** Large organizations with in-house security teams may want to augment existing capabilities by procuring the services of a dedicated MDR team.

*Available as add-ons

All product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners
Copyright © 2023 Bitdefender, All rights reserved.

Professional Services is included for MDR Plus tier for onboarding and deployment. For MDR, Professional Services **should** be offered to prospects as a paid add-on.



Key Benefits & Differentiators

Contents

[Overview of Offerings](#)

[Key Benefits & Differentiators](#)

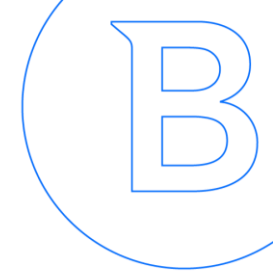
[Versus Top Competitors](#)

[Questions & Answers](#)

[Latest Awards & Use Cases](#)

Key Benefits & Differentiators

- ↳ **Bitdefender MDR Customer Baselineing:** Bitdefender offers a thorough onboarding process not offered by other MDR providers. Our comprehensive 50-question Customer Questionnaire helps us create customized threat models specific to each customer. Many MDR providers use a “one size fits all” threat model. Bitdefender tailors individual threat models for each customer with our baselining. Being able to construct better customer baselines allow us to provide superior anomaly detection and provide first-rate protection from emerging threats that could be targeting customers.
- ↳ **Bitdefender Native XDR Unified Platform:** Unlike other MDR providers, Bitdefender doesn’t rely on partner integrations that can sometimes compromise data fidelity. With GravityZone XDR we have best-in-breed. This allows for a more cohesive story to be told for each incident. The details of the incident are well-defined across services, research teams, and the technology. This leads to more efficient results and quicker actions for security events.
- ↳ **Human-Driven Analysis with All Tiers:** Our most affordable offering, Bitdefender MDR, is more than just an automated email alerting system, which is what most similar MDR services offer with their lowest-cost offering. We have human beings engaged at all service levels, providing valuable insight and expertise to all our customer without compromise.
- ↳ **Dedicated Cyber-Intelligence team brings value to all Bitdefender MDR customers:** Our CIFC team provides advanced monitoring services to our Bitdefender MDR Plus customers, but their findings trickle down to benefit all Bitdefender MDR customers. When a threat is identified by our CIFC team that has broad implications, we will take actions to protect every single MDR customer.
- ↳ **Bitdefender MDR includes threat response in all tiers:** 24x7 monitoring is offered by MDR providers, but often, their base tier typically doesn’t include response actions. With our pre-approved actions, customers can define the responses we can take on their behalf. All Bitdefender MDR customers benefit with not only 24x7 monitoring, but actionable responses to identified security events. This reduces threat dwell time and also curbs the cybersecurity skills gap for organizations.
- ↳ **Bitdefender MDR offers more features than comparable competitor tiers:** We offer more features with each of our tiers than similar services. Bitdefender MDR is comparable with other MDR providers' top tiers, but at a fraction of the cost.. Bitdefender MDR Plus offers even more value.
- ↳ **Bitdefender gathers threat intelligence across several product lines including consumer, OEM, and business.** There is more threat data fed to us every minute than there are Google queries. This positioning gives us a distinct advantage over our similar solutions - so much so that many of our competitors use some of our technologies in their own solutions.
- ↳ **Our tamper-proof ransomware mitigation technology is unique in the industry.** Unlike many similar solutions, we don’t rely on VSS Shadow Copies, which is easily compromised by ransomware. Instead, we developed our own proprietary solution that ransomware can’t corrupt or destroy.
- ↳ **No other cybersecurity vendor has been consistently rated as high as Bitdefender in independent testing for prevention, protection and detection and response.** For two consecutive years, AV-Comparatives has labeled us a “Strategic Leader” in their Endpoint Prevention and Response report showing we had the highest return on investment of any of the vendor evaluated.
- ↳ **The MDR Portal** provides features that allow customers a better way to keep track of the MDR investigations, threat hunts, and cases, while also providing a forum for cross-communication between our customers and MDR Security Specialists.



Questions & Answers

Contents

[Overview of Offerings](#)

[Key Benefits & Differentiators](#)

[Versus Top Competitors](#)

[Questions & Answers](#)

[Latest Awards & Use Cases](#)

Qualifying Questions



THE NEED FOR MANAGED DETECTION & RESPONSE

1. Does your team have a security solution to proactively search/investigate threats?
2. Do you have full visibility (XDR) on all your potential attack surfaces and know how to respond to those attacks?
3. Are you interested in being more proactive about today's sophisticated attacks, but cannot afford to hire additional security staff?



ADDRESSING THE CYBERSECURITY SKILLS GAP

1. How do you handle security issues today? (Do you have an experienced security resource on your team?)
2. Do you or your team have the expertise to recognize a sophisticated security breach/compromise in your environment?
3. Are your security teams overwhelmed by alerts?



PROTECTING BUSINESS ASSETS AND REPUTATION

1. How damaging to your company's reputation – and bottom line – would it be should it fall victim to a damaging breach or cyber attack?
2. Do the MDR services you are considering offer to monitor when the brand, IP, domain, or asset of your company has been compromised on the dark web?
3. What happens if you are breached at 4am in the morning? (Do you have a plan of action to protect the environment?)

For additional questions or objections support contact [#ent-competitive](#)

Answers to Typical Objections

OBJECTION:

Another vendor allows me to bring my own security stack to their MDR service. Why doesn't Bitdefender offer that?

ANSWER:

By using Bitdefender as our technology platform we have higher data fidelity. A unified language across our services, research teams, and technologies allows us to more effectively and quickly respond to threats, than having to parse through disparate sources of information. If you're aggregating various vendor solutions, you're subject to be impacted by the timeliness of alerts that can come with breaks or changes in the integration.

OBJECTION:

Other MDR providers offer 24x7 monitoring and threat hunting capabilities. Why do I need more than that?

ANSWER:

24x7 monitoring and threat hunting are certainly important links in your security chain, but response and proactive services that can monitor when your brand, IP, domain, or assets have been compromised can be a powerful preventative measure that can thwart an attack before it takes place.

OBJECTION:

Another vendor promises me \$1 million in breach protection. Why should I even consider Bitdefender who doesn't offer that?

ANSWER:

Read the fine print on those "breach protections," and you'll realize they are almost impossible to collect on. For example, one single application on a system being out-of-date is all it takes to nullify many of those claims. Bitdefender offers technologies and services that are singularly focused on preventing breaches.

OBJECTION:

What makes your affordable MDR service any better than what others offer?

ANSWER:

Most vendors' affordable offerings are not much more than email-alerting systems. Bitdefender MDR offers a true MDR service, including threat management, threat intel-based hunting, and root cause and impact analysis. We also include a 30-minute SLA across **ALL** of our tiers.. Most vendors only offer that with the highest-priced tier, if at all.

Awards & Recognition

Contents

- [Overview of Offerings](#)
- [Key Benefits & Differentiators](#)
- [Versus Top Competitors](#)
- [Questions & Answers](#)
- [Latest Awards & Use Cases](#)

Bitdefender is a Consistent Top Performer

Bitdefender Excelled in the 2024 MITRE Engenuity ATT&CK® Evaluations for Managed Services

MITRE Engenuity's ATT&CK® Evaluations: Managed Services—Round 2 (2024)

Company	Actionability (%)	Noise (emails + alerts)
Bitdefender	~95%	~100
SecurityHQ	~55%	~200
Field Effect	~45%	~250
SentinelOne	~65%	~250
Trend Micro	~50%	~350
Microsoft	~55%	~400
BlackBerry	~60%	~450
CrowdStrike	~85%	~600
Secureworks	~55%	~900
Sophos	~65%	~950
Palo Alto Networks	~80%	~1100

First in Actionability: We led in providing actionable insights, enabling analysts to act swiftly when an attack happens.

Minimal Alert Fatigue: We sent only 28 alerts and 54 emails, with high quality actionable information, compared to hundreds from other.

Second in Detection: We were just one detection behind CrowdStrike and we surpassed all other major competitors like Microsoft, Palo Alto, Sophos, and SentinelOne.

Fast Response Time: Our average response time was just 24 minutes, significantly faster than the vast majority of competitors

All product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners
Copyright © 2023 Bitdefender, All rights reserved.

Bitdefender Recognized by Leading Industry Analysts

THE FORRESTER WAVE™
Endpoint Security
Q4 2023

Bitdefender was named a “**Leader**” in the latest [Forrester Wave Endpoint Security](#) Evaluation for 2023.
“Bitdefender differentiates with its aggressive prevention-first mindset” - Forrester

Bitdefender was also rated as a “**Visionary**” in the **Gartner MQ**.
“Bitdefender shows strong market understanding and innovation, with an early focus on endpoint and human risk analytics, integrated tools that help identify and remediate endpoint OS weaknesses and identity attacks” - Gartner

To find more competitive assets such as battlecards, overviews and more:
[Competitive Intelligence SharePoint](#)

To ask questions, ask for assistance, or provide feedback contact us at:
[#ent-competitive Slack Channel](#)
[Competitive Intelligence Team Email](#)

Industry Recognitions