Bitdefender Managed Detection & Response

For Laptops & Desktops

With many of our customer struggling to protect their businesses in the face of increasingly complex and mutable technology environments and more sophisticated attacks the Bitdefender Managed Detection and Response offer pairs our award-winning detection and prevention engines with a modern 24x7 security operation staffed by world class expertise to hunt, find and eradicate adversaries.

Bridge your skills gap with managed detection and response

Security continues to increase in risk and importance for business. According to the 2019 Accenture "Cost of Cybercrime" study, the average cost of cyber-incidents for businesses has increased 72% over the last 5 years to $13M USD while the number of breaches has increased 67% over the same timeframe.

In the 2019 Data Breach Investigations Report (DBIR) from Verizon, laptops and desktops accounted for about 25% of assets in data breaches. The users of those devices are the direct targets of adversaries with social engineering attacks like phishing which accounted for 33% of breaches up 18 points from the 2017 numbers. As a result, it is critical that Detection and Response services focus on employees and their personal devices as they are a common first step in a compromise chain.

While customers increasingly recognize the importance of security to their business and the vulnerability of their systems, most lack the resources to mount an operation capable of detecting and responding to sophisticated and commodity threats. From the Verizon 2019 DBIR, 56% of breaches took months or longer to detect while the attackers' Compromise and Exfiltration phases measure in minutes to days.

Bitdefender's Managed Detection & Response service starts with our award-winning technology platform we call the triple stack – endpoint, network and security analytics. For network and endpoint visibility, we use Bitdefender's GravityZone Ultra protection platform paired with Bitdefender Network Security Traffic Analytics. This data is fed in to our security analytics platform.

This telemetry is used to generate alerts through direct tool detections, machine learning and threat hunting. Our proactive threat hunting uses tactical and strategic threat intelligence to generate hunting missions which are executed by our analysts to detect sophisticated adversaries or attackers that tooling may miss.

Our security operations team will investigate and respond to any incidents generated by tooling or found during our threat hunting operations through a set of pre-approved actions. These actions are detailed and approved by your team during onboarding so we can execute them quickly to interdict and adversary before they can cause damage to your business.

	Bronze	Silver	Gold
Endpoint Detection	Yes	Yes	Yes
Threat Intel	Yes	Yes	Yes
Endpoint Prevention	Recommended	Recommended	Recommended
Network Traffic Analytics	No	Yes	Yes
Pre-Approved Actions	Endpoint Only	Standard*	Standard + Custom**
Dashboards	Endpoint Only	Standard*	Standard + Custom**
Technical Account Manager	Ticket Only	Pool	Named
Quarterly Business Review	No	Yes	Yes
Policy Tuning	Yes	Yes	Yes
SLA (incident response time)	2 hours	1 hour	30 min
Threat Hunting	No	Yes	Yes
Malware Analysis	No	Automated	Automated + Custom***

* Custom dashboards are available for an additional fee.
** Gold package includes a set number of custom items with more items available for an additional fee.
*** Customer malware analyses (above and beyond malware sandbox reports) limited to a set number per contact term.

For the best protection including both network and endpoint visibility, we recommend the Silver tier for most customers. If your organizations needs to integrate with non-standard systems (internal APIs, etc) or has an existing security operation that Bitdefender would need to integrate with, Gold may be a better fit.

Many customers have existing anti-virus or anti-malware platforms that would be difficult to replace immediately. In that case, we offer an EDR only offering for Windows that simplifies deployment and can co-exist with existing platforms. However, for best protection, we recommend enabling Bitdefender's protection platform as it is the most effective according to third party testing.

Contact Bitdefender to talk about Managed Detection & Response services today.

More information available at www.bitdefender.com/managed-services

Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business