All Rights Reserved. © 2023 Bitdefender.
All trademarks, trade names, and products referenced herein are the property of their respective owners.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Bitdefender

SOLUTIONS DESCRIPTION

Bitdefender Managed Detection & Response

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Contents

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Introduction to Managed Detection & Response

The Need for MDR

In today's rapidly evolving cyber-threat landscape, organizations face increasingly complex and sophisticated security challenges. Traditional security measures alone are no longer sufficient to safeguard against the ever-changing tactics employed by cybercriminals. To effectively detect, respond to, and mitigate these threats, businesses require extensive expertise in the fields of security analysis and threat hunting, but are faced with several challenges in staffing for these positions.

Building an in-house Security Operations Center (SOC) and hiring qualified analysts can be a daunting and resource-intensive task. Cybersecurity expertise is scarce and highly in-demand and it's often cost prohibitive or simply not available for many organizations, especially those that are mid-sized or SMBs. Managed Detection & Response (MDR) services, on the other hand, provide organizations with a team of experienced security analysts who possess in-depth knowledge of the threat landscape, attack methodologies, and incident response techniques. This expertise ensures that businesses can benefit from the latest insights and guidance without the burden of internal recruitment and training.

Defining MDR

With cybercriminals constantly devising new attack vectors and exploiting vulnerabilities, MDR services are equipped with cutting-edge technologies such as machine learning, artificial intelligence, and behavioral analytics. These powerful tools enable MDR services to proactively detect and respond to both known and unknown threats in real time, providing businesses with a robust defense against emerging cyber risks.

Furthermore, MDR services offer continuous monitoring and detection capabilities, with dedicated security teams operating 24x7. By constantly analyzing network traffic, system logs, and endpoint data, MDR services can promptly identify anomalies, suspicious activities, or signs of a potential breach. This proactive monitoring ensures that security incidents are swiftly detected and addressed, minimizing the dwell time of attackers and reducing the potential damage caused.

MDR services also offer a comprehensive approach to cybersecurity. In addition to advanced threat detection, they provide organizations with end-to-end incident response and remediation services. In the event of a security incident, the MDR team leads the incident response process. MDR services investigate the security events from the first moment they are identified, determining the root cause, taking action by containing and eradicating the threat, and providing recommendations to the customer on how to prevent attacks in the future. The goal of MDR is to deal with a security event or incident and reduce business impact to customers quickly and effectively.

The best MDR services also benefit from having a dedicated threat intelligence team, which plays a pivotal role in enhancing the effectiveness and efficiency of the overall service. The threat intelligence team continuously monitors the evolving threat landscape, analyzes emerging attack techniques, and gathers actionable intelligence to identify potential threats and vulnerabilities. By leveraging this comprehensive threat intelligence, an MDR service can proactively identify and prioritize security incidents, provide timely and relevant alerts to clients, and offer proactive guidance to enhance their security posture.

By outsourcing the responsibilities of threat detection, monitoring, and incident response to MDR service providers, organizations can focus on their core business operations. This allows internal teams to concentrate on their primary objectives while relying on the expertise and technologies provided by MDR services to handle the day-to-day security operations. MDR services can also aid large organizations that already have an in-house security operations team, by augmenting their existing capabilities with the those provided by the MDR services.

Offering MDR services can be highly advantageous for a managed service provider (MSP) as well. MSPs seeking to expand their portfolio and deliver comprehensive cybersecurity solutions and expertise to its customers benefit greatly by procuring an MDR partnership. By incorporating MDR services into their offerings, MSPs can provide their customers with many of the benefits described in this brief. This enables MSPs to enhance their customers' security posture, strengthen their partnership by being a trusted adviser in cybersecurity matters, and differentiate themselves in the market by providing a comprehensive and proactive approach to cybersecurity. Additionally, MDR services offer recurring revenue streams for MSPs, as they often involve ongoing monitoring and support, resulting in long-term customer relationships and increased business growth opportunities.

This solutions brief will delve further into the details of the Bitdefender MDR services, outlining the benefits, features, and considerations for businesses seeking to enhance their cybersecurity posture and mitigate the risks associated with the ever-changing threat landscape.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

The Bitdefender MDR Services

Bitdefender offers several MDR services tailored to address the needs of organizations of all sizes and budgets. Below we will outline what those services are, their features, and benefits.

Services Overview

Features	MDR Foundations	MDR Premium	MDR Enterprise
24x7 Security Operations	✔	✔	✔
↳ Threat Management	✔	✔	✔
↳ Customized Notifications & Expert Recommendations	✔	✔	✔
↳ Pre-Approved Actions (PAAs)	✔	✔	✔
↳ Incident Root Cause & Impact Analysis	✔	✔	✔
↳ MDR Portal	✔	✔	✔
↳ Monthly Service Reports	✔	✔	✔
Threat Intel-Based Hunting	✔	✔	✔
Targeted Threat Hunting		✔	✔
↳ Security Baseline		✔	✔
↳ Tailored Threat Modeling		✔	✔
Professional Services		✔	✔
Dedicated Security Account Manager		✔	✔
↳ Quarterly Business/Security Reviews			✔
Dark Web Monitoring			✔
Brand & IP Protection			✔
Priority Target Monitoring			✔
XDR Sensors	**(add-on)**	**(add-on)**	**(add-on)**

MDR Foundations

The endpoint security needs of small and midsize businesses (SMBs) have escalated. Due to the rise in digital transformation and remote work, organizations have become more digitally dependent, and their attack surfaces have increased, opening them up to new threats. At the same time, threat actors have become both more sophisticated and more frequent in their attacks. MSPs, too, face unique risks because they manage networks and IT infrastructures for hundreds of small businesses. MSPs not only want to be cyber resilient themselves, but they want cyber resiliency for their customers.

The answer for SMBs and MSPs is Bitdefender MDR Foundations. MDR Foundations is a Managed Detection & Response service that provides SMBs/MSPs 24x7 monitoring and response, threat intel-based hunting, and expert recommendations – at an affordable price.

MDR Premium

For organizations looking for a more feature-rich managed detection and response service, Bitdefender offers MDR Premium. Like Foundations, Premium includes our 24x7 monitoring and response, threat intel-based hunting, expert recommendations, but also adds a dedicated security account manager, targeted threat hunting, and a tailored threat model.

The dedicated Security Account Manager (SAM) will be the organization's primary point of contact with our Bitdefender MDR specialists. They play a pivotal role helping build a strong relationship with the customer and are focused on understanding the customer's security needs. The SAM acts as a trusted advisor, aligning the MDR service to meet the customer requirements, coordinating communication, providing proactive guidance, and serving as an advocate on behalf of the customer within the Bitdefender MDR team. They offer consultation, assist in onboarding and incident response efforts, and ensure a successful partnership, enabling customers to maximize the value of the MDR service and enhance their overall security resilience.

Using the threat intelligence gathered by the Bitdefender Labs team and our in-depth Customer Questionnaire, our threat hunting specialists create a customized threat model specific to the threats targeting the customer's organization. They then use this threat

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

model to conduct periodic threat hunts across the customer's systems. This helps proactively identify potential threats and assists in hardening the customer's security posture.

MDR Enterprise

Bitdefender MDR Enterprise offers significant benefits to enterprise-sized companies. Even if the organization has their own security operations center, MDR Enterprise provides unique services that help guard the organizations from targeted attacks, while protecting their reputation. MDR Enterprise includes all of the features available with MDR Premium, while adding Priority Target Monitoring, Brand/IP Reputation monitoring, and Dark Web Monitoring.

Priority Target monitoring is crucial for enterprises that may be attractive targets for cybercriminals due to their industry, market position, or high-value assets. Bitdefender MDR employs advanced threat intelligence and tailored detection techniques to proactively identify potential threats specifically targeting the enterprise. This allows the company to allocate appropriate resources to enhance security measures and implement additional safeguards to counteract the specific risk they face.

Brand/IP reputation monitoring ensures the company's reputation remains intact within the digital realm. Our Cyber Intelligence Fusion Cell (CIFC) team of security specialists monitor online platforms, social media, and other digital channels to identify instances of brand impersonation, phishing attempts, or unauthorized usage of intellectual property. By promptly detecting and addressing these issues, the enterprise can protect its brand and image, maintain customer trust, and preserve their intellectual property from infringement or misuse.

Finally, Dark Web monitoring provides essential visibility into the hidden corners of the internet where cybercriminals operate. By actively monitoring the dark web, our MDR services can detect potential threats related to the company's sensitive data, credentials, or intellectual property that may have been compromised or are being sold illicitly. This early warning system allows enterprises to proactively respond, mitigate risks, and prevent potential breaches before they cause significant harm.

Key Features

With Bitdefender MDR, you benefit from GravityZone® Business Security Enterprise's comprehensive feature set for endpoints and hybrid cloud workloads, with dedicated support and managed onboarding, plus all the security expertise in Bitdefender›s security operations center (SOC), to get you up and running quickly.

Service	Short Description	FOUNDATIONS	PREMIUM	ENTERPRISE
24x7 Security Operations	We eliminate the operational overhead of managing security alerts and events. Our proactive, highly skilled, and certified security analysts with experience from the U.S. Air Force, U.S. Navy, British Intelligence, and the NSA, partner with you on the frontlines of your cyber defenses.	✔	✔	✔
Threat Management	Using tailored analytics and tooling, our SOC analysts triage and asses the output of GravityZone threat detection analytics and data to identify incidents and security events that require action.	✔	✔	✔
Expert Recommendations	At all stages of the service – day or night – you benefit from tactical and strategic recommendations for incident mitigation, remediation, and hardening of your environments, thereby improving your resilience to attack.	✔	✔	✔
Root Cause & Impact Analysis	We work with your team to identify the original threat vectors and potential impacts during incidents, offering comprehensive after-action reports. These details help drive continual improvement to your security posture and processes.	✔	✔	✔

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Service	Short Description	FOUNDATIONS	PREMIUM	ENTERPRISE
Monthly Service Reports	Your designated Security Account Manager curates monthly reports detailing your MDR status, including service outcomes, detections, and actions taken.	✔	✔	✔
Threat Hunting Services	Threat hunting is critical for reducing compromise risk and keeping dwell time to a minimum. 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. The SOC uses the output of threat hunting to keep the threat model current and up-to-date, ensuring the accuracy of detections and threat discovery.	✔	✔	✔
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. Our SOC analysts and threat researchers continuously identify industry trends, system anomalies, and new adversary techniques that inform and drive comprehensive threat hunting in your environment.	✔	✔	✔
Threat Intelligence Services	Threat intelligence services delivered by our Cyber Intelligence Fusion Cell (CIFC) utilize the threat intelligence lifecycle to research cyber threats, geopolitical activity, and vertical-specific data trends and apply this knowledge to your environment.		✔	✔
Tailored Threat Modeling	Our continuous analysis, combined with ongoing research of adversary groups and industry trends, provides you with detailed intelligence of potential risks from malicious actors to your business and high-value employees.		✔	✔
Priority Target Monitoring	We assess your environments through automation and with interview questions for high-value or high-risk assets. We put separate processes in place for these assets to provide a higher priority and level of monitoring.			✔
Brand & IP Protection	Our CIFC performs extensive monitoring activities to identify company information or high-value employee information that may have been stolen or otherwise leaked.			✔

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Service	Short Description	FOUNDATIONS	PREMIUM	ENTERPRISE
Dark Web Monitoring	Our CIFC continuously monitors the dark web to discover various customer or brand information, including customer credentials, intellectual property, holdings and subsidiaries, and other customer-specific information.			✔
Domain Registration Monitoring	The CIFC monitors your domain properties for newly created domains that could indicate “typo-squatting” or URL hijacking behavior by bad actors.			✔
Digital Asset Monitoring	We monitor for brand/company information to ensure customer data or code is not being leaked or distributed on public forums such as code repositories or paste sites.			✔

Benefits of our MDR Services

The Customer Questionnaire

The first thing Bitdefender MDR does when onboarding a customer is to gather information. This comes in the form of an in-depth Customer Questionnaire (available to MDR Premium/Enterprise customers via our MDR Portal), where we learn about domains, key users who might be targeted in a phishing campaign, brand information, industry verticals, geographies in which our customers operate, and more. This initial questionnaire helps us tailor our services to each and every customer and allows us to address their specific security risks and needs.

For a full breakdown of the Bitdefender MDR Onboarding process, please review section 4 of this guide.

Security Baseline

Bitdefender MDR next establishes a security baseline for our customers. This provides organizations with several key benefits. First it enables a comprehensive risk assessment and identifies gaps in the organization’s security posture, allowing for effective resource allocation and prioritization. This helps the organization understand the current risk landscape and align security measures accordingly.

Second, a security baseline enhances incident detection and response capabilities. By establishing a benchmark for normal activities and behaviors within the organization’s IT infrastructure, deviations from this baseline trigger alerts, enabling swift response and investigation of potential threats. This proactive approach minimizes the time it takes to identify and mitigate security incidents, reducing the potential damages and enabling rapid response.

Establishing a security baseline allows our MDR team to create a unique threat model for each customer. Threat modeling is a crucial piece of baselining and ensures an accurate threat landscape understanding for the monitored environment is developed and maintained.

The threat modeling process begins with building intelligence requirements that support the business’ strategic goals, matching the dynamic pace of the cyber threat landscape and new threats observed. Continuous research provides detailed intelligence to customers of who, what, where, and why cyber actors would potentially target their business. In conjunction with the details gleaned from the Customer Questionnaire, a threat model is created in our Security Orchestration, Automation, & Response Platform (SOAR) and the Threat Intelligence Platform (TIP). The model includes a handwritten landscape summary including industry trends, recent and related incidents, and key attack vectors that must be monitored.

The research conducted and intelligence gained will lead to threat hunts and advisory reports to the customer, both of which can provide:

- Specific risk and threat findings
- Situational awareness
- Mitigation recommendations

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

This approach enhances the accuracy and efficiency of the threat detection, allowing for proactive protection and effective response to security incidents.

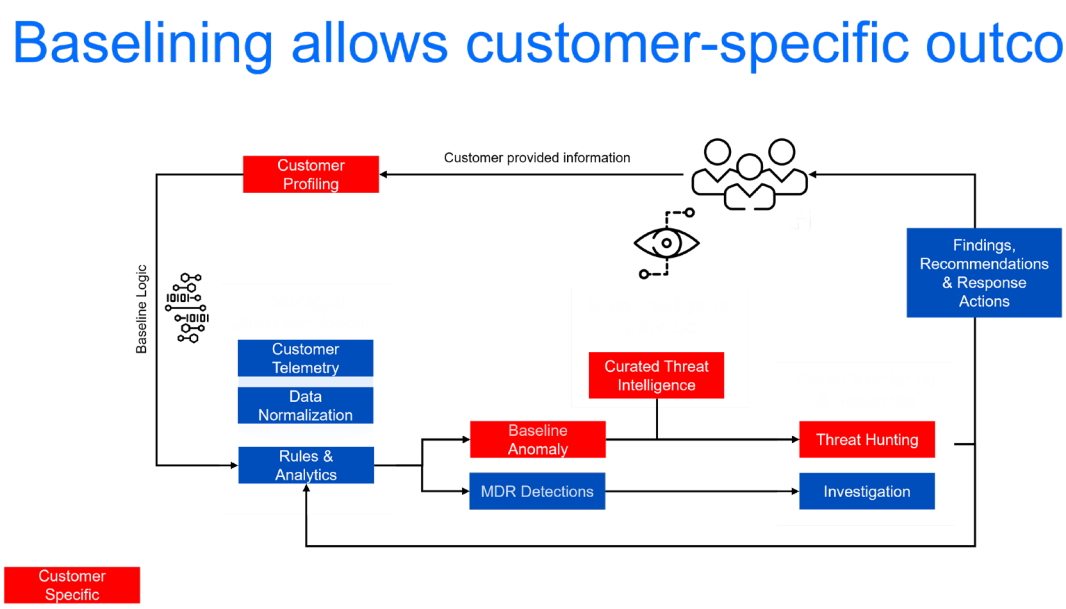


Figure 1: Custom environmental baselines are created for each Bitdefender MDR Premium/Enterprise customer unique to their environment, users, and behavior.

Risk-based Threat Hunting

A Risk-Based threat hunt begins by thoroughly assessing the unique risks and vulnerabilities of your organization. The Bitdefender security analyst conducts a comprehensive evaluation of your assets, such as systems, applications, data, and network infrastructure, to understand potential threats and their impact on your organization. This risk assessment provides the foundation for the subsequent steps of the threat hunt.

With the risk assessment in mind, we gather threat intelligence from various sources including cybersecurity feeds, industry reports, and internal incident data. By understanding the tactics, techniques, and procedures (TTPs) employed by potential attackers, we can better anticipate and detect threats.

Based on the risk assessment and threat intelligence, the analyst develops hypotheses or educated assumptions about potential threats targeting your organization. These hypotheses act as guiding principles for the subsequent investigation. We collect relevant data from multiple sources within your organization, such as security logs, network traffic, endpoint activity, and user behavior. Advanced analytics and threat detection techniques are then applied to analyze this data, searching for patterns, anomalies, and indicators of compromise (IOCs). By comparing the data against known attack signatures and behavioral baselines, we can identify suspicious activities that might indicate a potential threat or ongoing attack.

Detected threats are then triaged and prioritized based on their severity and potential impact on your organization. This prioritization allows the analysts to focus their resources and attention on the most critical threats first, ensuring efficient response and mitigation efforts. Investigations are conducted to gather additional information and determine the nature and scope of the threats. The Bitdefender MDR team takes appropriate steps to mitigate the threats, such as isolating affected systems, blocking malicious traffic, or initiating incident response procedures.

Throughout the entire process, we emphasize continuous monitoring and improvement. We continuously assess your organization's security posture, analyze new threats, and refine their detection and response capabilities. Each incident becomes a learning opportunity to strengthen your overall cybersecurity defenses. In addition, we provide regular updates, incident reports, and recommendations, ensuring you remain informed and actively involved in the threat hunt process.

Targeted Threat Hunting

Targeted threat hunting helps identify and address advanced threats, zero-day exploits, and insider threats that pose significant risks to the organization. It allows the MDR team to stay ahead of emerging attack techniques, enhance incident response capabilities, and fortify the organization's security posture. Through targeted threat hunting, the MDR team can minimize dwell time of advanced persistent threats and ensure a more resilient and proactive defense against sophisticated cyber attacks.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Every 15 days, our Active Monitoring and Response (AMR) team will do a targeted hunt against each customer's environment. The main driver is to find anomalies in the data such as: a process running on a single machine with a suspicious name, or connections over a port that shouldn't be open.

During a targeted hunt, an analyst might sort the number of processes across a customer environment and look for an anomaly, for instance, software that has been installed on a small number of endpoints. In this scenario, the analyst will review the following data:

- SHA256 and md5 hashes
- Information on the host like hostname and OS version
- Process information like process path and the commands that launched a process
- Parent process information
- Which version of the software was running

If such a process is identified, those hash values can then be run through internal and external tools, to see if they were flagged by any antimalware programs.

Bitdefender's hunting capabilities don't stop at the endpoint. Bitdefender MDR can also monitor network connections for suspicious activity or a misconfigured application.

Rapid Incident Response

Rapid incident response is a key capability of the Bitdefender MDR team offered in all of our tiers. Our security analysts swiftly assess security incidents and take decisive actions to contain and mitigate the threat. Collaborating with the organization's internal stakeholders, they provide regular updates and guidance throughout the security event. Thorough investigations help identify the root cause of the incident and collect forensic evidence, while recovery and remediation efforts focus on restoring affected systems.

The MDR team stays in constant communication with a pre-approved list of emergency contacts within the organization throughout the security incident, providing guidance and informing them of any pre-approved actions taken within the service level agreement. The pre-approved actions include:

- **Kill a process**: Our experts will terminate a process that they have determined is malicious.
- **Blocking a file**: Our experts will block a malicious executable from running on the host.
- **Exclude a safe file**: Our experts will add a safe file to an exclusion list to prevent false-alarms
- **Add a file to the Sandbox**: Our experts will upload a file to the GravityZone sandbox for detonation and analysis.
- **Search for file information**: Our experts will search for available file information on VirusTotal and search engines to determine what available information there already exists on the file.
- **Patch applications**: If the customer has the GravityZone Patch Management add-on, our experts will patch an application that was identified in an incident to have a vulnerability.
- **Collect Investigation Package**: Our experts will collect a GravityZone investigation package from the endpoint for further analysis.
- **Response shell**: Our experts may have access to run commands on the endpoint in order to investigate or mitigate malicious activity.
- **Blocking a port**: Our experts will block the host from exchanging network traffic on one or more network ports they have determined present a risk. Such as port 80 or 443.
- **Blocking an IP**: Our experts will block the host from exchanging network traffic with one or more IP addresses that they have determined are malicious.
- **Isolating a host**: Our experts will disconnect the host from the network so that it may no longer make or receive connections with other systems.
- **Deleting a file**: Our experts will delete a file that they have determined is malicious.
- **Quarantine a file**: Our experts will move a suspicious file into a quarantine folder so that it cannot be used accidentally. The file will not be deleted.
- **Disable a compromised User account**: Our experts will disable the account of a compromised user across Active Directory, Azure, Office 365, and AWS IAM.
- **Force a password reset on a compromised User account**: Our experts will force a password reset on a compromised user account across Active Directory, Azure, and Office 365.
- **Mark a User account as compromised**: Our experts will mark any account identified as compromised in an incident as such.
- **Delete a malicious email**: Our experts will delete an email identified as malicious in an incident across Exchange Online/Office 365.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

After Action reports are generated for completed incident investigations. They contain the details of the attack, a summary of the actions taken by the SOC and any recommendations on changes in the environment to help prevent similar incidents in the future.

Through the Bitdefender MDR team's expertise, the advanced technology offered through the GravityZone platform, and structured incident response, organizations are able to minimize the impact of security incidents.

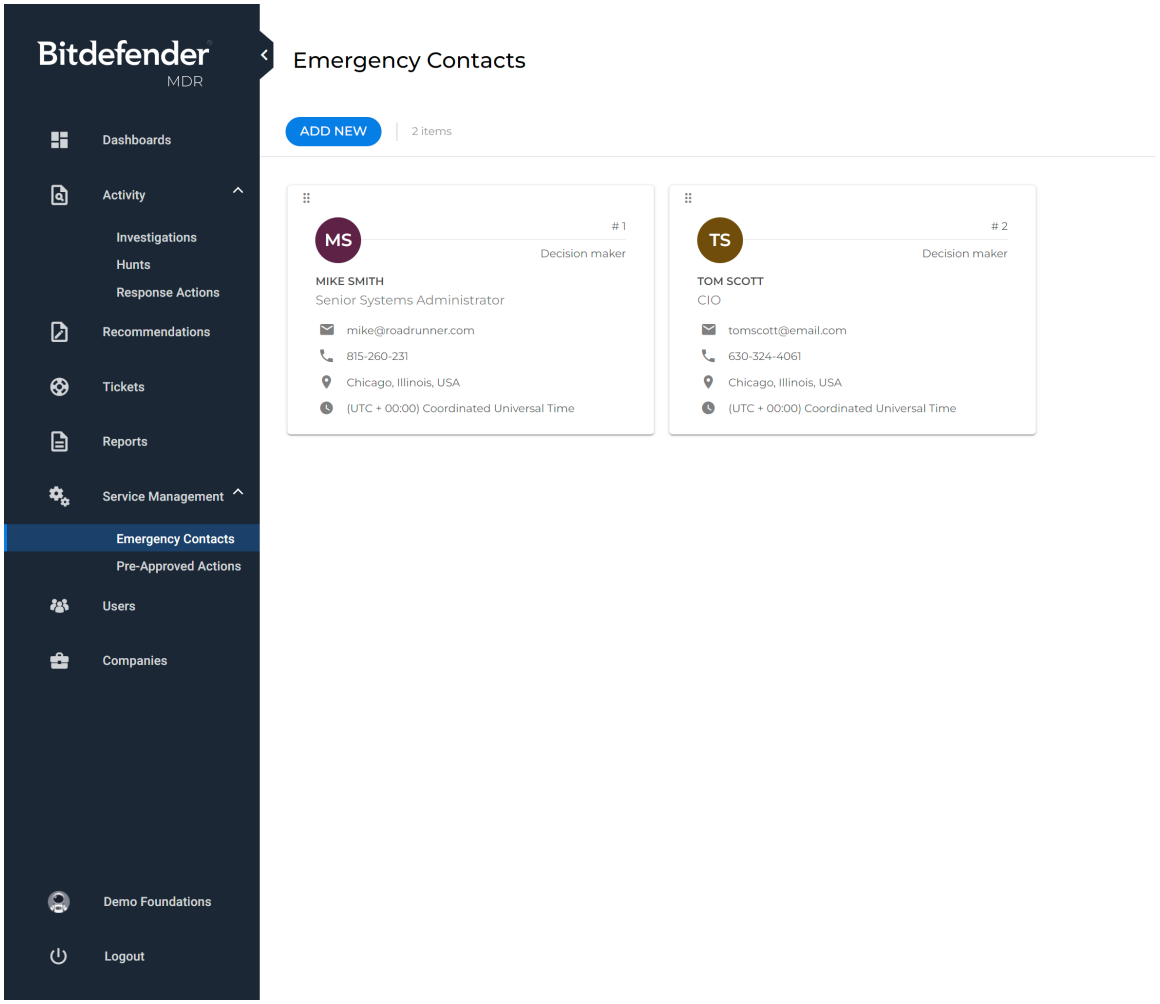


Figure 2: Through the Bitdefender MDR portal, organizations can easily configure emergency contacts as well as pre-approved actions during a security incident.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Comprehensive Reporting and Visibility

Bitdefender recognizes the importance of its MDR services to communicate intricate details and insights into the services we are providing to our customers. To that end, we have developed robust, actionable reporting within our MDR service offerings. These reports are powered by big data analytics, artificial intelligence, and human expertise. They provide meaningful insights into security incidents, highlight cybersecurity trends, and guide remediation efforts, offering unparalleled transparency into the MDR processes.

Our reporting capabilities facilitate regulatory compliance, aid in the identification and mitigation of vulnerabilities, and provide a platform for continuous security improvement. By serving as an indispensable communications tool between stakeholders, our reports enable informed decision-making and strategic planning.

In the following section we will outline the different report types offered by the Bitdefender MDR service. The reports are accessible via the Bitdefender MDR Portal.

Monthly Report

Our Monthly MDR Report provides a detailed snapshot of your security landscape. It offers a comprehensive review of baseline activity on hosts and the network, along with environmental and user growth over the last month. The report begins with an overview of general activities, including agent and network activity, EDR alerts, and discovered threats. It expands on this information by providing crucial context for understanding your organization's cybersecurity posture.

The case management section provides a detailed overview of all ongoing and closed security cases, outlining the nature of the threats, and steps taking for mitigation. The report closes with a thorough analysis of monthly security activity showcasing vital statistics on threat detections, hunting endeavors, intelligence alerts, and case activities. The Monthly Report serves as a critical tool to ensure consistent, proactive security management.

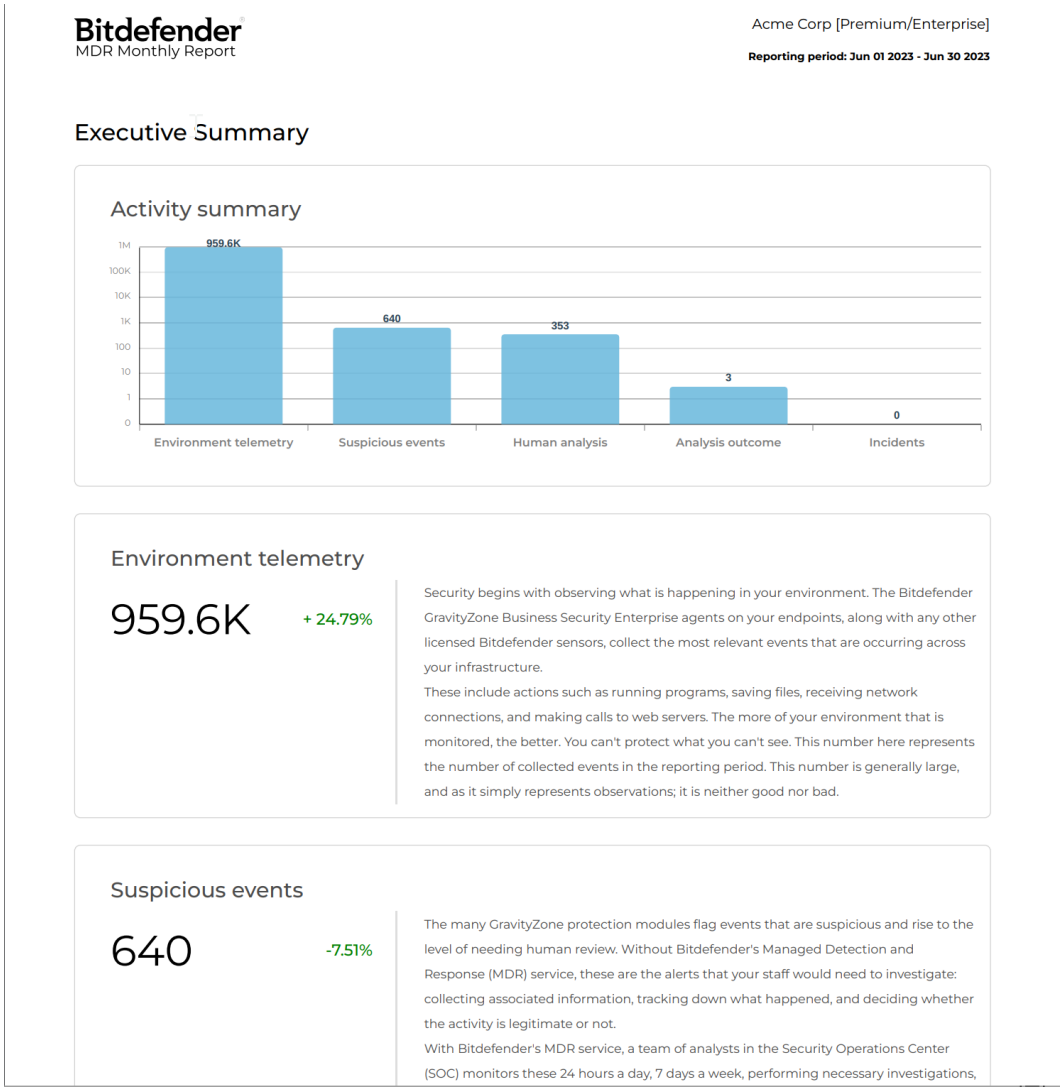


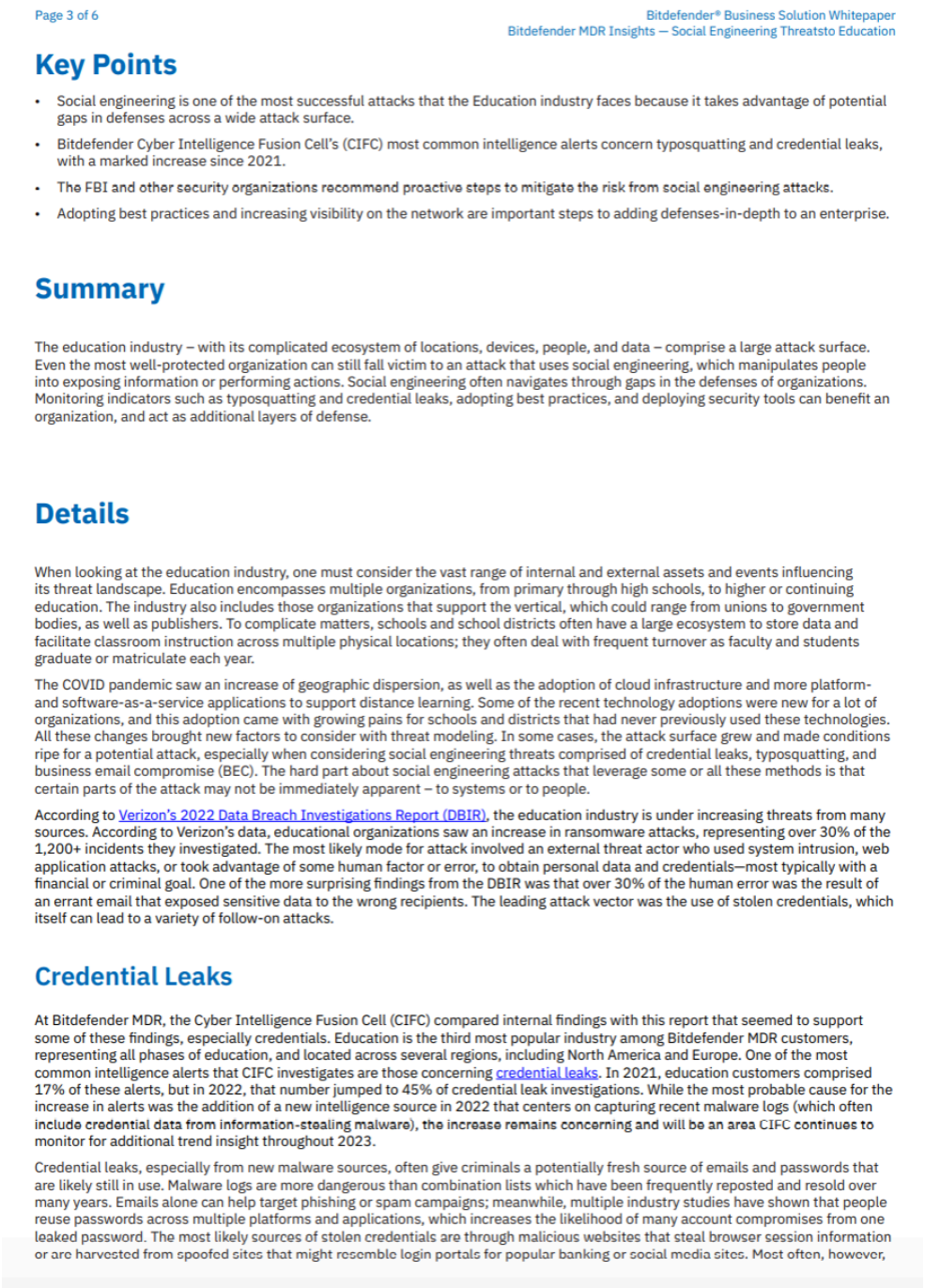
Figure 3: An example of a section of the Bitdefender MDR Monthly Report.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Tipper Report

The Bitdefender MDR Tipper Report is a crucial intelligence tool specifically designed to provide up-to-date information on specific threat actors, emerging cybersecurity trends, or information on the customer's industry vertical and how it is being targeted by threat actors. Based on comprehensive threat intelligence gathering, these reports act as an early warning system for potentially harmful cyber-attacks, enabling organizations to stay ahead of the evolving threat landscape. The Tipper Reports are generated through a combination of AI and human expertise from our Cyber Intelligence Fusion Cell (CIFC) team. The information is gathered from global cybersecurity feeds, dark web activities, as well as trends and patterns derived from within your organizational data.

Each Tipper Report consists of four main sections. The 'Summary' provides a high-level overview of the identified threat or trend, offering a succinct briefing of the potential impact and affected domains. The 'Details' section delves into the specifics, including the modus operandi of the threat actor, or the technical attributes of a particular cyber threat or trend. This section helps organizations understand the nature of the issue at hand. The 'Recommendations' segment offers actionable insights on how to mitigate or guard against the identified threat, customized to the technical environment of your organization. This could include patching recommendations, system configuration changes, or enhanced monitoring of certain activities. Finally, the 'References' section provides additional resources for further information or guidance, such as bulletins from cybersecurity agencies, white papers, or links to relevant industry research. These components come together to create a report that provides a comprehensive, actionable view of the threat landscape.



Page 3 of 6

Bitdefender® Business Solution Whitepaper
Bitdefender MDR Insights — Social Engineering Threatsto Education

Key Points

- Social engineering is one of the most successful attacks that the Education industry faces because it takes advantage of potential gaps in defenses across a wide attack surface.
- Bitdefender Cyber Intelligence Fusion Cell's (CIFC) most common intelligence alerts concern typosquatting and credential leaks, with a marked increase since 2021.
- The FBI and other security organizations recommend proactive steps to mitigate the risk from social engineering attacks.
- Adopting best practices and increasing visibility on the network are important steps to adding defenses-in-depth to an enterprise.

Summary

The education industry – with its complicated ecosystem of locations, devices, people, and data – comprise a large attack surface. Even the most well-protected organization can still fall victim to an attack that uses social engineering, which manipulates people into exposing information or performing actions. Social engineering often navigates through gaps in the defenses of organizations. Monitoring indicators such as typosquatting and credential leaks, adopting best practices, and deploying security tools can benefit an organization, and act as additional layers of defense.

Details

When looking at the education industry, one must consider the vast range of internal and external assets and events influencing its threat landscape. Education encompasses multiple organizations, from primary through high schools, to higher or continuing education. The industry also includes those organizations that support the vertical, which could range from unions to government bodies, as well as publishers. To complicate matters, schools and school districts often have a large ecosystem to store data and facilitate classroom instruction across multiple physical locations; they often deal with frequent turnover as faculty and students graduate or matriculate each year.

The COVID pandemic saw an increase of geographic dispersion, as well as the adoption of cloud infrastructure and more platform- and software-as-a-service applications to support distance learning. Some of the recent technology adoptions were new for a lot of organizations, and this adoption came with growing pains for schools and districts that had never previously used these technologies. All these changes brought new factors to consider with threat modeling. In some cases, the attack surface grew and made conditions ripe for a potential attack, especially when considering social engineering threats comprised of credential leaks, typosquatting, and business email compromise (BEC). The hard part about social engineering attacks that leverage some or all these methods is that certain parts of the attack may not be immediately apparent – to systems or to people.

According to Verizon's 2022 Data Breach Investigations Report (DBIR), the education industry is under increasing threats from many sources. According to Verizon's data, educational organizations saw an increase in ransomware attacks, representing over 30% of the 1,200+ incidents they investigated. The most likely mode for attack involved an external threat actor who used system intrusion, web application attacks, or took advantage of some human factor or error, to obtain personal data and credentials—most typically with a financial or criminal goal. One of the more surprising findings from the DBIR was that over 30% of the human error was the result of an errant email that exposed sensitive data to the wrong recipients. The leading attack vector was the use of stolen credentials, which itself can lead to a variety of follow-on attacks.

Credential Leaks

At Bitdefender MDR, the Cyber Intelligence Fusion Cell (CIFC) compared internal findings with this report that seemed to support some of these findings, especially credentials. Education is the third most popular industry among Bitdefender MDR customers, representing all phases of education, and located across several regions, including North America and Europe. One of the most common intelligence alerts that CIFC investigates are those concerning credential leaks. In 2021, education customers comprised 17% of these alerts, but in 2022, that number jumped to 45% of credential leak investigations. While the most probable cause for the increase in alerts was the addition of a new intelligence source in 2022 that centers on capturing recent malware logs (which often include credential data from information-stealing malware), the increase remains concerning and will be an area CIFC continues to monitor for additional trend insight throughout 2023.

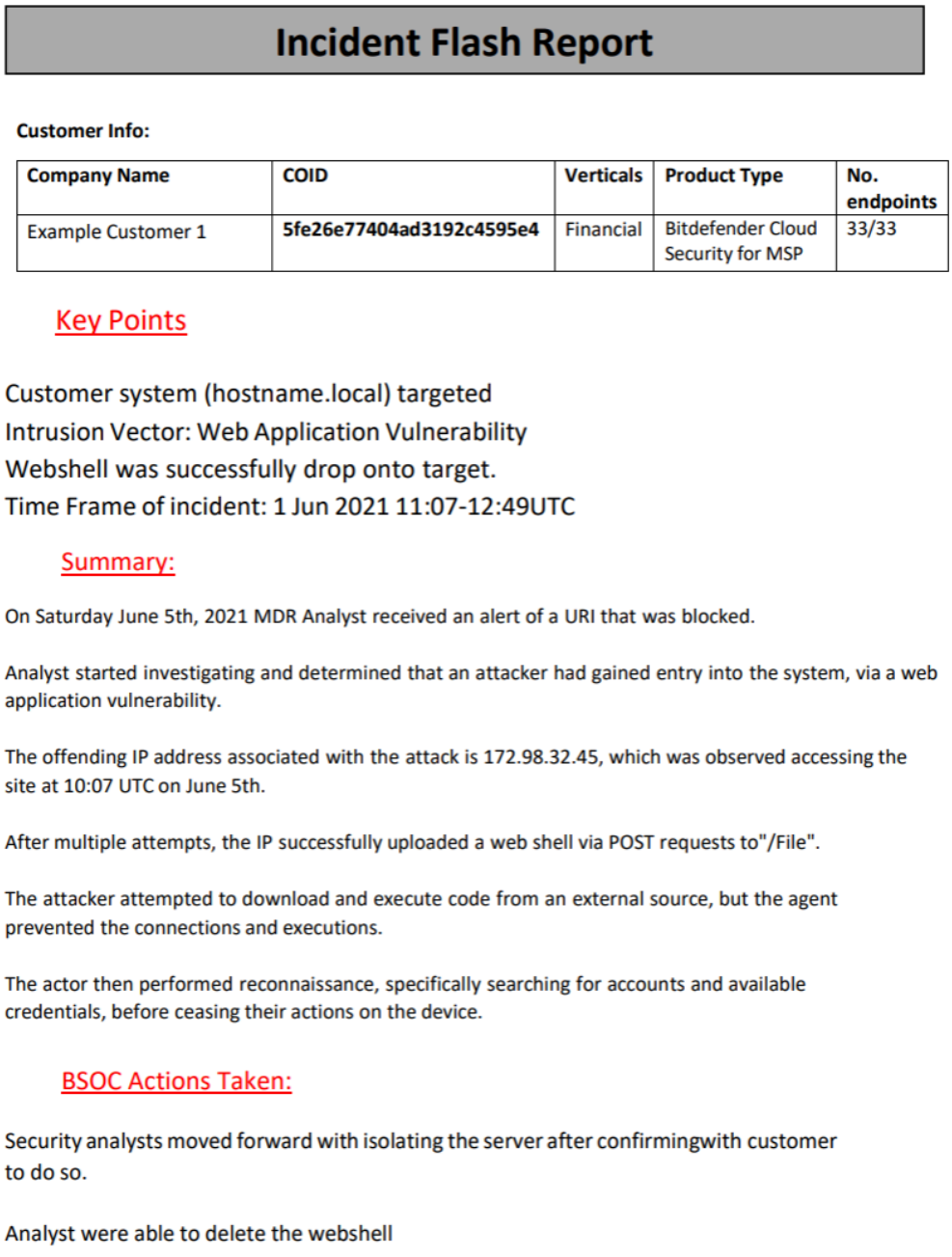
Credential leaks, especially from new malware sources, often give criminals a potentially fresh source of emails and passwords that are likely still in use. Malware logs are more dangerous than combination lists which have been frequently reposted and resold over many years. Emails alone can help target phishing or spam campaigns; meanwhile, multiple industry studies have shown that people reuse passwords across multiple platforms and applications, which increases the likelihood of many account compromises from one leaked password. The most likely sources of stolen credentials are through malicious websites that steal browser session information or are harvested from spoofed sites that might resemble login portals for popular banking or social media sites. Most often, however,

Figure 4: An example of a section from the Bitdefender MDR Tipper Report

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Flash Report

When a security incident is first detected, it's important to notify the organization of what the MDR team knows before the full investigation is concluded. This is where the Flash Report comes in. The report is one of the methods used to communicate concise information on suspicious activity detected in the customer's environment. It includes the key points, which highlights initially affected systems, timeframe of the incident, a summary of what was detected, and actions taken by the Bitdefender security team. Once the full investigation is concluded, the customer is provided with the aforementioned After Actions reports which provides greater detail.



Incident Flash Report

Customer Info:

Company Name	COID	Verticals	Product Type	No. endpoints
Example Customer 1	**5fe26e77404ad3192c4595e4**	Financial	Bitdefender Cloud Security for MSP	33/33

Key Points

Customer system (hostname.local) targeted
Intrusion Vector: Web Application Vulnerability
Webshell was successfully drop onto target.
Time Frame of incident: 1 Jun 2021 11:07-12:49UTC

Summary:

On Saturday June 5th, 2021 MDR Analyst received an alert of a URI that was blocked.

Analyst started investigating and determined that an attacker had gained entry into the system, via a web application vulnerability.

The offending IP address associated with the attack is 172.98.32.45, which was observed accessing the site at 10:07 UTC on June 5th.

After multiple attempts, the IP successfully uploaded a web shell via POST requests to"/File".

The attacker attempted to download and execute code from an external source, but the agent prevented the connections and executions.

The actor then performed reconnaissance, specifically searching for accounts and available credentials, before ceasing their actions on the device.

BSOC Actions Taken:

Security analysts moved forward with isolating the server after confirmingwith customer to do so.

Analyst were able to delete the webshell

Figure 5: An example of a section of the Bitdefender MDR Flash Report

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

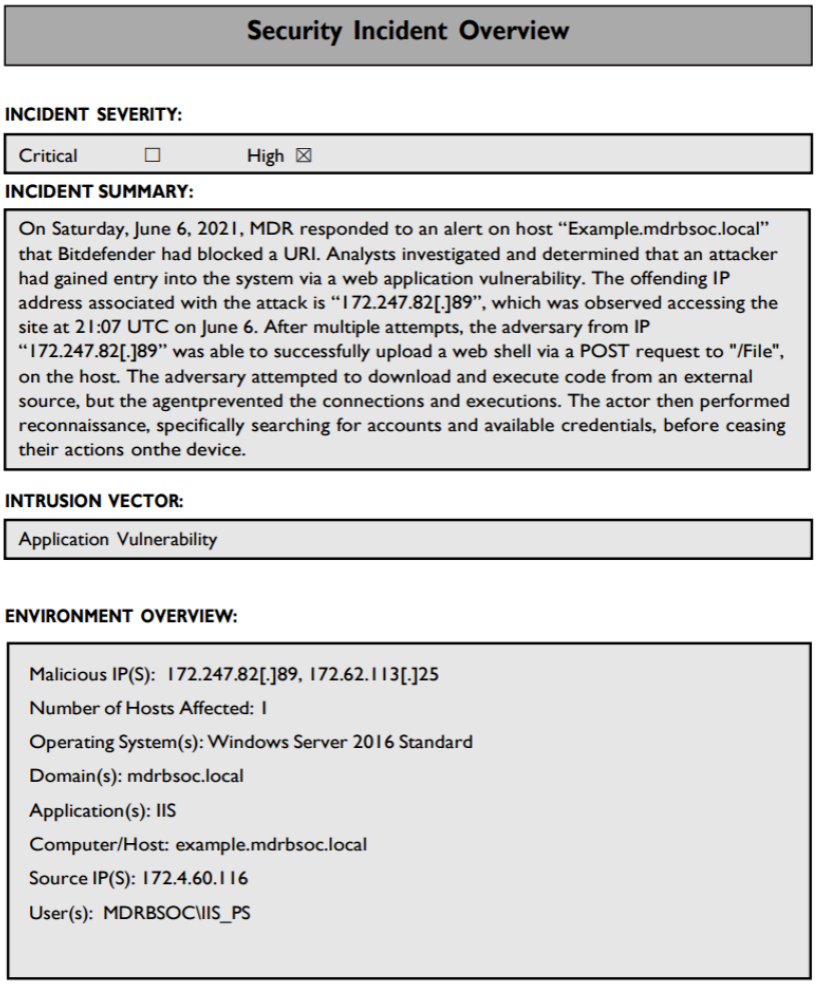
After Actions Report

The After Actions report is an all-inclusive document that provides a comprehensive analysis of a cybersecurity incident that has transpired within a customer's environment. This report is crucial for understanding the complete lifecycle of an attempted security breach, starting from its inception to its eventual containment and remediation. The report details the severity of the incident, with a summary of what transpired, the intrusion vectors, environment overview, the analyst summary and details of the incident and the actions the Bitdefender MDR team took to mitigate the threat.

The report details the precise sequence of events that unfolded during the breach attempt. This includes initial detection, subsequent actions taken, the response and recovery process, files, networks, and systems involved in the attack. The report elaborates on the specific actions that were undertaken to identify, contain, and eradicate the threat. This includes steps like the isolation of infected systems, patching of vulnerabilities, removal of malware, and any other measures taken to neutralize the threat and minimize its impact.

Provided after a 72-hour period of high priority monitoring post-incident, the report concludes with an in-depth list of recommendations to prevent such incidents from happening in the future. These suggestions could range from strengthening security controls and improving incident response procedures, to employee training and awareness programs.

By providing a thorough account of the incident and actionable steps for future prevention, an 'After Actions' report serves as a learning tool, helping organizations to enhance their cybersecurity posture and resilience against future attacks.



Security Incident Overview

INCIDENT SEVERITY:

Critical ☐ High ☒

INCIDENT SUMMARY:

On Saturday, June 6, 2021, MDR responded to an alert on host "Example.mdrbsoc.local" that Bitdefender had blocked a URI. Analysts investigated and determined that an attacker had gained entry into the system via a web application vulnerability. The offending IP address associated with the attack is "172.247.82[.]89", which was observed accessing the site at 21:07 UTC on June 6. After multiple attempts, the adversary from IP "172.247.82[.]89" was able to successfully upload a web shell via a POST request to "/File", on the host. The adversary attempted to download and execute code from an external source, but the agentprevented the connections and executions. The actor then performed reconnaissance, specifically searching for accounts and available credentials, before ceasing their actions onthe device.

INTRUSION VECTOR:

Application Vulnerability

ENVIRONMENT OVERVIEW:

Malicious IP(S): 172.247.82[.]89, 172.62.113[.]25
Number of Hosts Affected: 1
Operating System(s): Windows Server 2016 Standard
Domain(s): mdrbsoc.local
Application(s): IIS
Computer/Host: example.mdrbsoc.local
Source IP(S): 172.4.60.116
User(s): MDRBSOC\IIS_PS

Figure 6: An example of a small section from the Bitdefender MDR After Actions Report

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

24x7 Monitoring and Support

Bitdefender MDR provides a comprehensive cybersecurity service operating 24x7 from two global Security Operations Centers (SOC). One of our SOCs is located in Texas, United States, while the other is in Romania, in the European Union. Both of our SOCs use the same level of knowledgeable staff, processes, and technology to ensure we are providing unsurpassed 24x7, 365 days a year coverage to our customers around the globe. We are committed to ensure the highest level of security for an organization's digital assets. With our constant vigilance, we seek to detect, contain, and eradicate any potential threats as swiftly as possible.

The cornerstone of our MDR service is its capacity for rapid response. In the event of a detected security incident, we can execute pre-approved actions agreed upon by the customer. These could range from simply notifying the client's security team to isolating infected systems or temporarily blocking network traffic. This enables our MDR service to act immediately, potentially averting damage before it can occur and buying valuable time for further investigation and remediation.

Bitdefender MDR provides clients with detailed remediation recommendations tailored to the specific incident across all of our service tiers. These recommendations can involve a variety of measures like patching software vulnerabilities, adjusting security settings, improving user access controls, and/or taking action on specific files and processes. This comprehensive approach not only helps to resolve the current incident but also contributes to strengthening the organization's overall security posture against future threats.

By providing round-the-clock monitoring, instant response, and remediation guidance, Bitdefender MDR offers an end-to-end solution for managing and responding to cyber threats, freeing organizations to focus on their core business operations.

Compliance and Regulatory Support

Compliance and regulatory support are crucial aspects of any Managed Detection & Response (MDR) service. Given the increasing complexity and stringency of data protection regulations across industries, organizations need to ensure their cybersecurity practices align with all applicable legal requirements and industry standards. An MDR service that provides compliance and regulatory support can guide organizations in managing and documenting their cybersecurity efforts effectively. This includes ensuring that security controls are adequate and align with regulatory frameworks, such as NIS2, GDPR, HIPAA, or PCI DSS. Moreover, in case of a security incident, an MDR service can help in providing necessary incident response documentation, showing that the organization took all reasonable precautions to prevent and mitigate the breach. This kind of support is invaluable in minimizing the risk of non-compliance, which can lead to hefty fines, damage to reputation, and potential loss of customer trust.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Deployment Process & Onboarding

A smooth deployment and onboarding process is crucial when engaging with an MDR service provider. This process sets the tone for the ongoing relationship and can significantly influence the efficiency and effectiveness of the MDR service. A well-structured onboarding plan ensures that the service is integrated seamlessly into the existing IT environment, minimizing disruption to the organization's operations.

With Bitdefender MDR, customers experience a transparent and comprehensive onboarding process that fosters trust and communication between the organization and Bitdefender security operations team, setting the foundation for a successful, long-term partnership. In the following section, we will describe our onboarding process and what customers can expect in detail.

Deployment Timeline

Deployment of the Bitdefender GravityZone technology can easily be done by the partner or customer, using the GravityZone console, or they can procure the services of our Bitdefender Enterprise Professional Services team. The specifics of the Enterprise Professional Services deployment can be found below. Before deployment, the customer must first perform the onboarding steps outlined here.

Onboarding Steps

Once the customer receives access to the Bitdefender MDR portal, they can sign in and begin the onboarding process by filling out our onboarding questionnaire. The questionnaire gives us an initial starting point to building out a baseline for our customers through establishment of precise datapoints. Some of the specific datapoints we look for are:

- High-level corporate user (C-suite users, for example) information, including names, emails, usernames, hostnames for their workstations, the physical locations they primarily work from
- Which industry vertical or verticals the organization belongs to
- Users who have privileged access to systems, like system administrators
- The type of products and/or services the organization offers, including what kinds of sensitive and classified data they store
- Third-party suppliers who have access to sensitive data
- IP address and domain names of public-facing infrastructure
- A network map

Bitdefender MDR uses the Bitdefender GravityZone Business Security Enterprise product as the foundation of our threat detection technology. All MDR customers should begin by creating their GravityZone account. MDR Premium and Enterprise customers can utilize Bitdefender Enterprise Professional Services to assist in their MDR deployment, as ProServe is included in these MDR service tiers. MDR Foundations customers can choose to add-on Professional Services to save time and ensure that all necessary configuration is correct.

If the customer chooses to leverage the Professional Services, the customer will receive an email from the Professional Services team within 2 Business Days of purchasing MDR Premium or MDR Enterprise with information on how to begin the engagement.

Enterprise Professional Services Delivery Process

Every Enterprise Professional Services delivery consists of five sessions:

1. Kick-off call

- Meet the customer
- Discuss needs and expectations
- Assess infrastructure focusing on
  - Number of locations
  - Number of endpoints per location
  - Number of virtual servers per location/data center
  - Virtualization technology
  - Previous security vendor

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

- Provide information about relays and security servers
- Discuss Statement of Work
  - Inform the customer about the SOW
  - Explain the parts that need to be filled in
- Provide the delivery plan:
  - GravityZone configuration (2-4h)
  - Deployment start and validation(1-2h)
  - Finish deployment and verify failed installations(2-3h)
  - Health check and acceptance(1-2h)
- Provide hardware, software, and connectivity requirements
  - Don’t forget to highlight ingestors-eu.bmdr.bitdefender.com and ingestors-us.bmdr.bitdefender.com for MDR traffic to be submittedProvide GravityZone Documentation

2. GravityZone Configuration Session

During the GravityZone initial setup the following steps should be followed:

- Cloud Console setup:
  - Create the GravityZone cloud account
  - Change the partner to MDR
- **If inside the EU:** 76cbfb09b35f316dccc73c3cde11c794
- **If outside the EU (US)**: 8874a0b092a98842184c5feb45599570
  - Create Installation packages (be sure to enable EDR Sensor in all created packages)
  - Create security policies
- Do not configure Splunk server in Security Telemetry Tab
- Be sure to enable EDR Sensor in all policies
  - Create integrations
  - Create Assignment rules and apply policies on Active Directory OUs if needed
  - Create users
  - Create reports
  - Configure Notifications
  - Create Offline machines cleanup rule
- Deployment of relays and security servers
- GravityZone Walkthrough
  - Explain GravityZone Features
  - Explain security best practices
  - Give tips for exclusions
  - Give tips for maintenance

3. Deployment start and validation Session

- Deploy a test batch of endpoints
- Assign security policy for them
- Verify endpoints for issues
  - Check communication
  - Check update

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

- Check cloud services connectivity
- MDR Telemetry (Check if Security Telemetry Status is Established and Transport type is Bitdefender MDR)

↳ Ask the customer to test and validate if BEST is not interfering with the installed software

4. Finish Deployment and verify failed installations Session

↳ Check endpoints with issues

↳ Check failed installations and perform initial troubleshooting

↳ Create support tickets for discovered issues

5. Health check and acceptance Session

↳ Check endpoints

- Update status
- Connectivity issues
- Performance issues

↳ Check Relays and SVAs for update and connectivity issues

↳ Review policies and look for poorly created exclusions

↳ Check endpoints module status

- Validate if all endpoints are having the EDR module installed and turned on
- Verify what other modules are installed

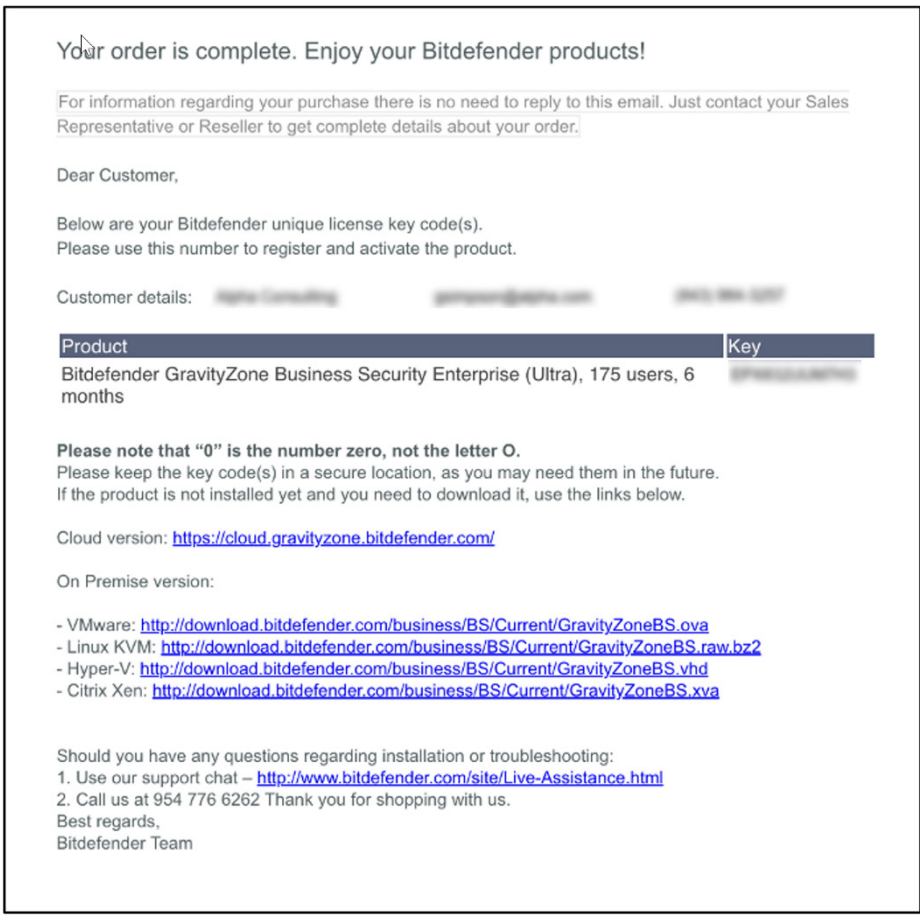
↳ Discuss the acceptance letter

↳ Create a snapshot of the customer environment as per our confluence procedure and send it to the Customer Success Team (CST)
Once those steps are completed, the MDR Enterprise Professional Services delivery is concluded.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Creating your GravityZone Account and Accessing the GravityZone Console

The next step in the onboarding process is to log into the Bitdefender GravityZone console. Your partner should provide you with a license key and credentials to log into the GravityZone console. Otherwise, you may have received an email from noreply-partnerlink@info.bitdefender.com like this one.



Your order is complete. Enjoy your Bitdefender products!

For information regarding your purchase there is no need to reply to this email. Just contact your Sales Representative or Reseller to get complete details about your order.

Dear Customer,

Below are your Bitdefender unique license key code(s).
Please use this number to register and activate the product.

Customer details: [redacted]

Product	Key
Bitdefender GravityZone Business Security Enterprise (Ultra), 175 users, 6 months	[redacted]

Please note that "0" is the number zero, not the letter O.
Please keep the key code(s) in a secure location, as you may need them in the future.
If the product is not installed yet and you need to download it, use the links below.

Cloud version: https://cloud.gravityzone.bitdefender.com/

On Premise version:

- VMware: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.ova
- Linux KVM: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.raw.bz2
- Hyper-V: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.vhd
- Citrix Xen: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.xva

Should you have any questions regarding installation or troubleshooting:
1. Use our support chat – http://www.bitdefender.com/site/Live-Assistance.html
2. Call us at 954 776 6262 Thank you for shopping with us.
Best regards,
Bitdefender Team

Figure 7: After creating your GravityZone account, look for a welcome letter like this one.

If you've only received a product code but no login credentials, you can set up your account in GravityZone by following these steps.

Post-Onboarding Support

Once customers have completed the onboarding process, if they need assistance from the MDR team, we encourage Premium and Enterprise customers to contact their assigned Security Account Manager. Foundations customers can open a support case from the MDR Customer Portal, or reach out via one of the support channels covered later in this document.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Why Choose Our MDR Service?

There are many reasons organizations should choose Bitdefender MDR as their cybersecurity solutions provider, many of which are already outlined in this document:

- **The Bitdefender MDR Onboarding Process:**Bitdefender offers a thorough onboarding process thru our comprehensive 50-question onboarding questionnaire that helps us to create a better baseline for customers.
- **Why this is important:** Being able to have a better baseline about our customers allows us to provide superior anomaly detection. This allows us to identify unusual behavior that could be associated with or lead to an attack.
- **Bitdefender GravityZone's Native XDR:** Bitdefender doesn't rely on partner integrations, that can sometimes compromise data fidelity. These integrations can often lead to mismatched data, and sometimes missing data because of non-concurrent product updates or compatibility issues. With GravityZone XDR, we have a unified language across our technology, threat intelligence, and human expertise. This gives us the best-in-breed data dependability.
- **Why this is important:** This allows for a more cohesive story to be told for each incident, leading to more efficient results and quicker actions for security events.
- **Human-Driven Analysis with All Tiers:** Our most affordable offering, MDR Foundations, is more than just an automated email alerting system, it includes 24x7 monitoring, threat-intel based hunting, and pre-approved remediation actions.
- **Why this is important:** We have human beings engaged at all levels, providing valuable insight and expertise to all of our customers without compromise.
- **Bitdefender MDR includes Threat Response in all of our tiers:** 24x7 monitoring is offered by all of our competitors, but for their low-cost tiers this typically doesn't include response actions, only notifications and sometimes recommendations.
- **Why this is important:** All Bitdefender MDR customers benefit with not only 24x7 monitoring, but actionable responses to identified security events. This reduces threat dwell time, and curbs the cybersecurity skills gap for organizations.
- **Bitdefender MDR Enterprise offers more features such as** priority target monitoring, dark web monitoring, domain registration monitoring, asset monitoring, brand and IP protection, tailored threat monitoring and targeted threat hunting.
- **Why this is important:** Many of these services are not available at all with most of our competitors. Most importantly, the quality of our MDR team spans across our security analysts, our threat intelligence experts, and our operations team. The next section will provide insights as to what makes our MDR team so special.

Our Experience and Expertise

When it comes to cybersecurity, experience matters, and our Managed Detection & Response (MDR) operations team brings to the table an impressive collective expertise of over 100 years. This seasoned team comprises professionals who have honed their skills in various sectors, dealing with an array of cyber threats and incidents. They bring a depth and breadth of understanding that allows them to swiftly identify, analyze, and respond to security incidents, keeping our client's digital assets safe.

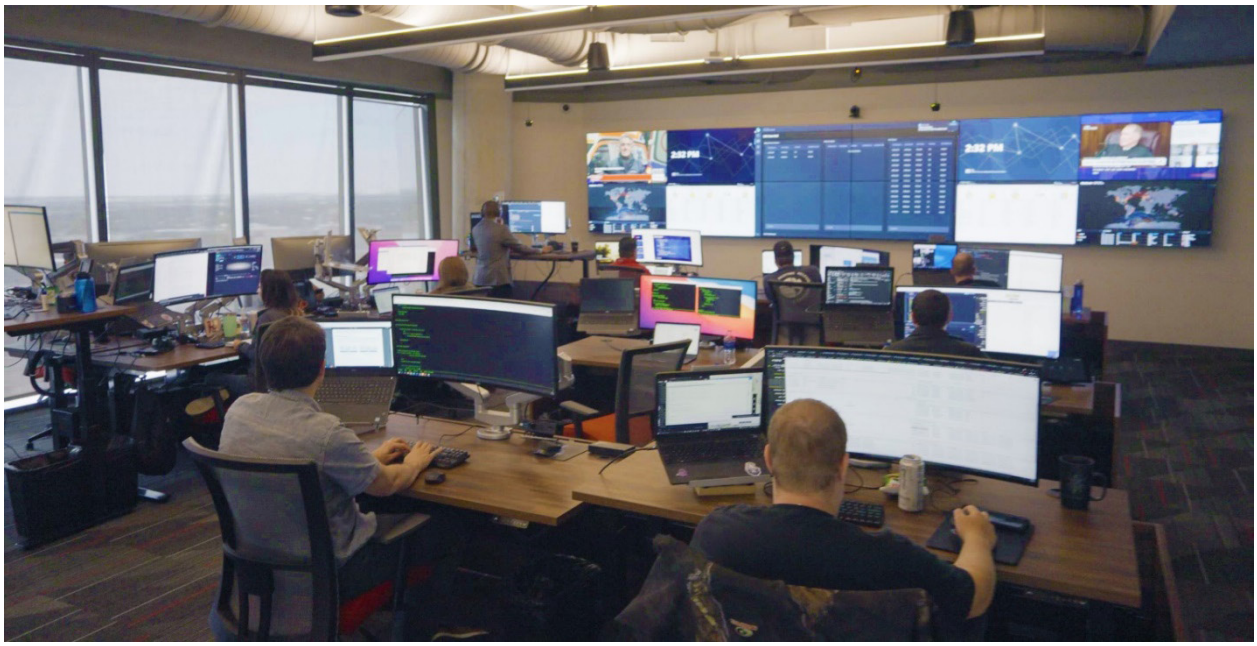


Figure 8: Hosted out of the famous Frost Tower in San Antonio, Texas, Bitdefender's main Security Operations Center boasts a staff with a wealth of cybersecurity expertise.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

The Bitdefender MDR Operations Team

Leveraging their vast experience, our MDR operations team continually navigates the evolving threat landscape, delivering effective and efficient solutions that bolster our clients' cybersecurity posture.

Security Analysts

Bitdefender's Managed Detection & Response (MDR) team is a cohort of seasoned security analysts with rich expertise in both cybersecurity and broader aspects of Information Technology. Each team member holds a host of certifications that testify to their skills and knowledge. These include a diverse array of SANS accreditations, such as GCFA, GFIH, GCDA, GDAT, and GISP, among others. Furthermore, they possess internationally recognized certifications such as CISSP, CEH, CCNA, OCSP, as well as CompTIA's suite including A+, Net+, Security+, and Pentest+.

Our analysts bring to the table not just their technological prowess, but also a wealth of diverse experiences. This includes stints in military intelligence, systems and cloud administration roles, and even in national security spheres. This multifaceted background gives them a unique perspective, enabling them to offer unparalleled cybersecurity insights and solutions.

Dedicated Cyber-Intelligence

We have a dedicated threat intelligence team we call our Cyber Intelligence Fusion Cell (CIFC). The threat intelligence personnel's experience isn't limited to cyberthreats, as many of the staff have years of experience as military intelligence personnel. The CIFC team assesses information gathered from a wide variety of sources including various cyber intelligence gathering tools, scouring the dark and deep web, gathering data from various law enforcement organizations around the world, gathering threat information from the Bitdefender Labs team, and reviewing information from various reliable news authorities.

The threat intelligence team casts a wide net and parses through the information to extract reliable, relevant information. This intelligence helps the security team address and prepare for the wide variety of threats that are actively targeting or could be targeting the Bitdefender customers. They identify trends that help them make educated deductions and stay one step ahead of cybercriminals. Their analysis is not limited to cybersecurity however, as they examine business and geopolitical news that can also be a contributing factor to cybersecurity vulnerabilities.

To organize the data, the team uses security and information event management (SIEM) tools, a security orchestration, automation, and response (SOAR) platform, and the GravityZone platform to identify meaningful data. The Threat Intelligence analysts will provide context to the data and help to eliminate false positives, ambiguity, and duplication of efforts. Their findings are discussed with the Bitdefender MDR SOC analysts and actions plans are custom tailored to each individual customer based on the customer's environment, the businesses' field of activity, and details of the identified potential threat.

Our Advanced Technology

Bitdefender's Managed Detection & Response (MDR) service leverages the power of the award-winning GravityZone EDR and XDR platform[1]. The GravityZone suite, meticulously designed for a broad range of organizations, offers an all-inclusive cybersecurity shield across systems, networks, email, productivity applications, identity, and cloud workloads.

The architecture of the GravityZone suite relies on a defense-in-depth strategy, fusing visibility and control in one holistic management interface. From here, our cybersecurity professionals can efficiently maintain and manage an organization's cybersecurity threat landscape. Importantly, this management interface delivers the means to probe into and recover from potential incidents effectively.

At the heart of GravityZone's multi-faceted security approach is a sophisticated blend of Artificial Intelligence and Machine Learning technologies, purposed for safeguarding organizations from known and emerging cyber threats. To ensure a balance between precise threat detection and minimizing false positives, we constantly refine our cutting-edge algorithms. This minimizes the resource commitment required to secure the customer's systems. Optimized specifically for cloud and virtual environments, GravityZone ensures minimal impact on your cloud computing resources and virtualized assets as well. It integrates additional sensors across your hybrid and multi-cloud deployments to streamline security management, effectively thwarting security breaches.

Our Native XDR functionality offers superior data accuracy and enables quicker responses to potential threats. By using GravityZone XDR, our MDR team can swiftly comprehend the who, what, when, and how of an attack and execute remediation actions without unnecessary delay caused by deciphering disorganized data sources.

1 Claim based on data gathered from independent evaluations like https://www.av-comparatives.org/, https://av-test.org, https://www.mrg-effitas.com/, https://attackevals.mitre-engenuity.org/.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

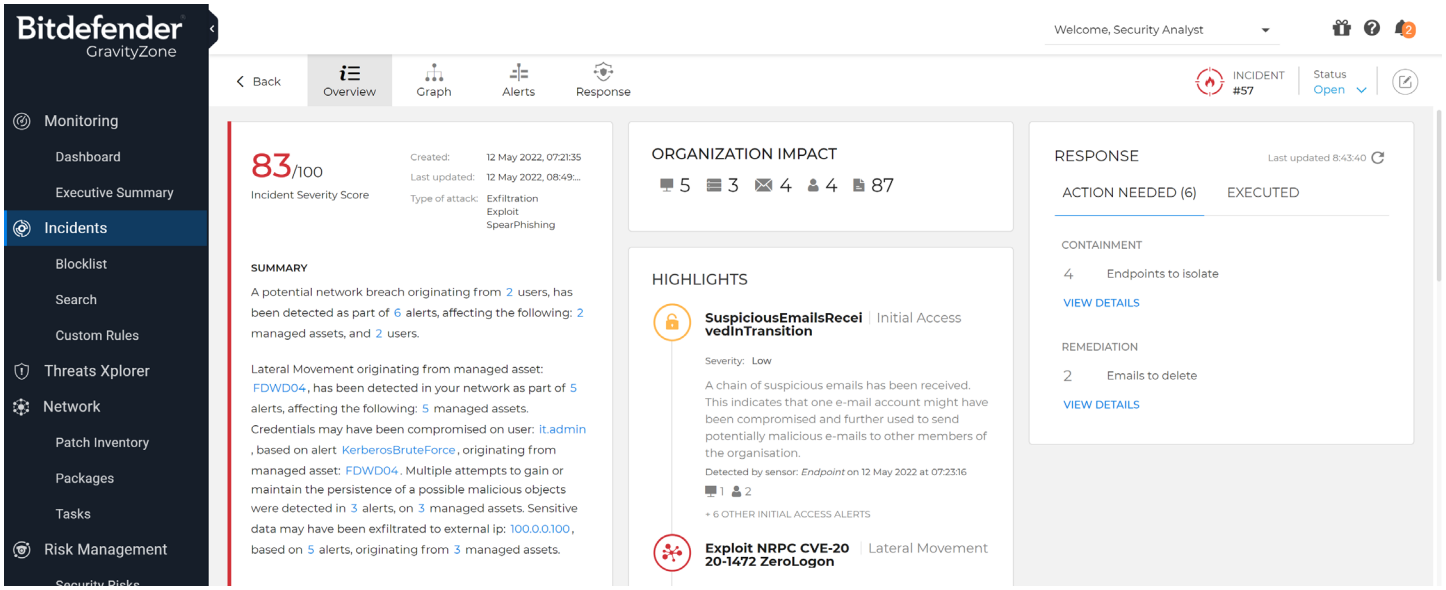


Figure 9: Using the GravityZone XDR Incident Advisor, security teams can quickly assess the important details of an incident which allows for quicker response.

Additional Tools

The Bitdefender MDR team leverages other instruments as well to perform threat hunting in the customer's environment. Within MDR operations, we use a SIEM, SOAR, and TIP to engage in the customer environment. All data that is created by our EDR/XDR alerts is retained in our SIEM platform for 180 days by default, which allows us to perform high-efficacy hunts on longer timeframes. A SIEM also allows analysts to dig deep into security events to determine the root cause of the identified activity.

A threat model is also created in our Security Orchestration, Automation, & Response Platform (SOAR) and TIP. The threat model will contain all known information about the customer and any open source intelligence gathered by the cyber intelligence team. This data also allows us to create watchlists that our cyber intelligence team uses to triage alerts daily. These alerts may then be converted into Customer Verification Requests or Threat Hunts.

Custom proprietary tools are used that allow us to gather threat information from Bitdefender sensors worldwide. Other external tools are utilized to monitor the dark web, Slack and Discord communities, threat intelligence blogs, GitHub, Pastebin, VirusTotal, Twitter, and other sources of cybersecurity/cybercrime information.

The MDR Customer Portal

The MDR Customer Portal provides features that allow customers a better way to keep track of the MDR investigations, threat hunts, reports, and cases, while also providing a tool for cross-communication with the GravityZone MDR SOC specialists. From the Bitdefender MDR Portal, customers can review the following:

- **Dashboard** – customers can quickly review graphs and statistics on everything from activity, deployment progress, investigations, top impacted users and systems, active licensing, threat hunt data and more.
- **Activity section** - where customers can track investigations and threat hunt activity including analysis results and recommendations.
- **Recommendations** – customers can review recommendations on threat activity, hunts, and investigations delivered from the Bitdefender MDR SOC.
- **Tickets** – customers can use the tickets section to open and monitor cases submitted to the MDR Security analysts.
- **Reports** – this section allows customers to access the different reports delivered by the Bitdefender MDR team.
- **Documents** - where the customer and MDR team can exchange valuable information such as screenshots, logs and more.
- **Service Management** – allows customers to easily set up emergency contact information and pre-approved actions, as well as complete or update the Customer Questionnaire. **Users** – where additional accounts can be created and managed for users who are provided access to the MDR Portal. Three different roles can be assigned to users:
  - **Admin** – Full access to the MDR Portal.
  - **User** – Can upload documents, submit tickets, and acknowledge investigations.
  - **Read-Only** – limited access to only read the data displayed in the portal, without capacity for further interaction.
  - **Companies** – allows Partners, MSPs, and MSSPs leveraging our MDR service to track their customers using our MDR service.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

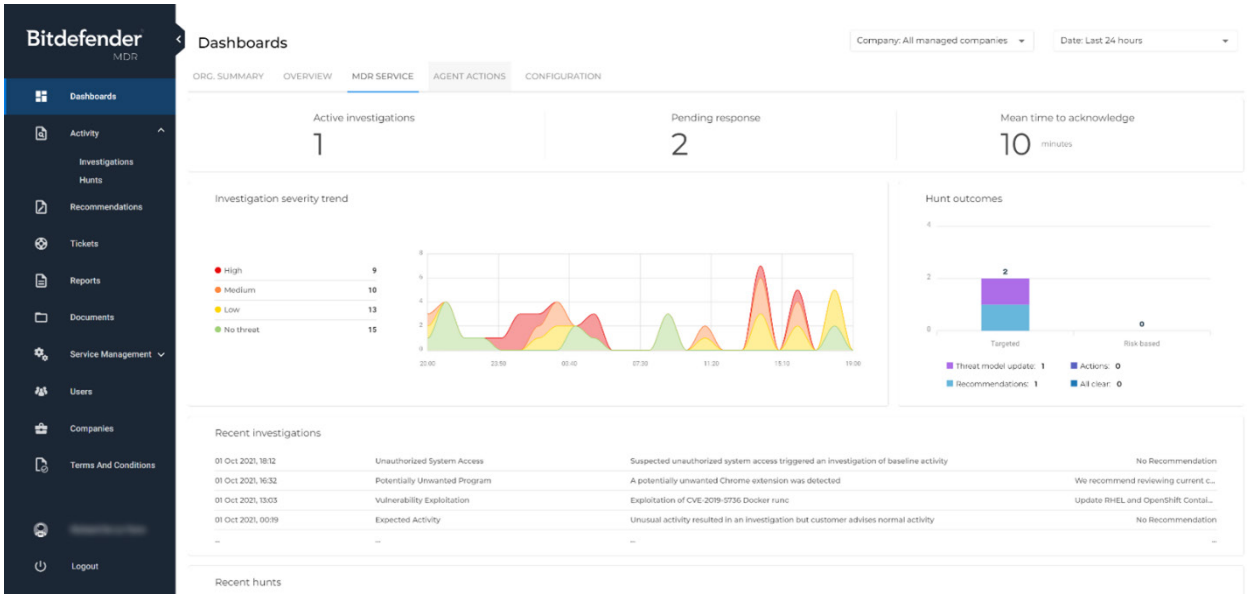


Figure 10: Using the Bitdefender MDR Portal, customers will be able to track the MDR team's cybersecurity activity, access reporting, investigation results, and more.

Our Proven Track Record

No other cybersecurity vendor has been **consistently rated** as high as Bitdefender in independent testing[2]. From 2018 to 2022, Bitdefender had 63% of the #1 rankings in AV-Comparatives attack prevention tests, prompting them to categorize us as a ***Strategic Leader*** in the industry. The AV-Comparatives Business Security Test for March – June 2023 results show Bitdefender GravityZone provides the best protection among all vendors evaluated with 100% protection rate. We excel in MITRE ATT&CK® evaluations by having among the highest analytical detections and continue to garner awards from the other independent evaluators such as Forrester, MRG Effitas, AV-Test and more.

Bitdefender MDR was named a "*Representative Vendor*" for the second consecutive time in the 2023 Gartner® Market Guide for Managed Detection & Response Services. Forrester also recognized Bitdefender MDR as a "Notable Provider" in the Managed Detection and Response Landscape, Q1 2023 and the Managed Detection and Response Landscape in Europe, Q3 2023.

	Test scenarios														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Acronis	PRE	PRE	–	PRE	–	ON	–	ON	PRE	PRE	–	ON	–	–	–
Avast	POST	PRE	–	PRE	ON	ON	ON	ON	ON	ON	–	–	–	–	ON
Bitdefender	PRE	PRE	ON	PRE	ON	ON	ON	PRE	PRE	PRE	ON	PRE	PRE	–	POST
CrowdStrike	ON	ON	ON	ON	ON	ON	ON	ON	ON	POST	ON	–	–	–	–
ESET	POST	ON	PRE	PRE	ON	PRE	ON	POST	PRE	ON	PRE	–	ON	ON	ON
G Data	PRE	PRE	ON	PRE	POST	ON	–	PRE	PRE	ON	ON	PRE	ON	–	–
Kaspersky	PRE	ON	ON	ON	–	ON	–	POST	PRE	PRE	PRE	ON	–	ON	ON
Microsoft	PRE	PRE	PRE	PRE	ON	ON	PRE	–	ON	POST	PRE	–	PRE	–	–
VMware	PRE	ON	–	ON	–	ON	–	–	ON	PRE	–	ON	PRE	–	–

Figure 11: AV-Comparatives' detailed Advanced Threat Protection Test showed Bitdefender was able to stop more attacks at the pre-execution stage than any other vendor evaluated, the results prompted the evaluator to comment, "A good burglar alarm should go off when somebody breaks into your house, not wait until they start stealing things"

At Bitdefender, we have obsessive dedication to providing the best technology and services to fight cybercrime. Our reputation for being leaders in cybersecurity has allowed us to collaborate with law enforcement agencies around the world to thwart criminal organizations responsible for some of the most damaging ransomware attacks, including Revil, Gandcrab, and many more. One of the

2 Claim based on data gathered from independent evaluations like https://www.av-comparatives.org/, https://av-test.org, https://www.mrg-effitas.com/, https://attackevals.mitre-engenuity.org/.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

ways we disrupt these Ransomware-as-a-Service groups is by releasing free ransomware decryptors anyone can download from labs.bitdefender.com. These decryptors have allowed organizations to recover their encrypted data without paying out these criminal organizations for decryption keys – and in doing so, have damaged the trusted relationships between the ransomware providers, and the cybercriminals that make use of this malware. If we show this much dedication to helping the general public against cybercriminals, consider how much more dedicated we are to protecting customers that count on us to protect their assets.

Case Studies

Home services provider raises cybersecurity bar for global businesses

The company, a U.K.-based global home repair and improvement services provider with 8.4 million residential customers, was seeking to standardize cybersecurity capabilities and centralize visibility across the infrastructure for its federated businesses in Europe, North America, and Asia.

The company's group chief information security officer explains, "We wanted to improve control of our cybersecurity risk given ever-increasing threats and shift to a more remote workforce. The distributed business model had become more of a factor we had to accommodate in our selection. In addition, we wanted to bring up the varying levels of cybersecurity expertise and solutions across our independently managed business units regardless of their size."

To address these objectives, the company standardized its cybersecurity environment on Bitdefender Managed Detection & Response (MDR) Enterprise.

"After evaluating and testing several cybersecurity solutions, we decided to consolidate all our global operations onto Bitdefender MDR," recalls the group CISO. "During the testing, we were impressed with the strong exploit prevention capabilities of Bitdefender MDR compared to the other solutions. The quality of the Bitdefender security team's expertise and the collaborative nature of how Bitdefender set up the relationship with us also were factors in our choice."

Click here to review the full case study.

Healthcare provider opts for 24x7 security monitoring service and protection at 40 percent less cost than hiring additional staff

As cybersecurity threats continue to proliferate, internal security operations departments at organizations worldwide must devote significant resources to managing and analyzing an unrelenting flow of alerts and notifications. To address this challenge, Magrabi Hospitals and Centers, a major healthcare provider in Saudi Arabia considered hiring additional security operations employees to provide 24x7 monitoring.

Instead, Magrabi determined that outsourcing to a managed endpoint detection and response service would provide more comprehensive protection and at a lower cost. Magrabi evaluated managed detection and response service offerings from Crowdstrike and Bitdefender and selected Bitdefender Managed Detection and Response (MDR) Premium.

Mostafa Mabrouk, Corporate Information Security Manager, Magrabi Hospitals and Centers, explains, "We chose Bitdefender MDR because it would provide us with comprehensive endpoint control, detection, forensics, reporting, and protection. Viewing all the security components from a single console—from malware removal to sandboxing to quarantine to logs and more—was valuable to us. We also were impressed with the in-depth expertise and knowledge of the security analysts staffing Bitdefender MDR."

Click here to review the full case study.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Frequently Asked Questions

- **Question**: In how many languages is the Bitdefender MDR service delivered?
- **Answer**: While the MDR Portal is in English, we currently provide MDR service support in English, French and German.
- **Question**: How does Bitdefender MDR provide visibility and confidence that they are making the best choices for my organization in the case of a security event?
- **Answer**: Every customer undergoes a thorough baselining process during onboarding that gives the SOC an incredible picture of what normal looks like for just that customer. The resulting threat model is the basis from which we conduct hunts on behalf of that customer in the future.
- In fact, this process is so crucial and effective that efficiency actually improves over time. As we learn more about a single customer, the less time we waste on false positives. We also provide visibility and ensure confidence through the dashboards in our MDR Portal and reporting.
- **Question**: What's the possibility for human error in the Bitdefender MDR Operations?
- **Answer**: It's inevitable that human error can occur when you place emphasis on human expertise. However, our operation is backed up by automation and first-class technology. There are also organizational controls in place (L1 to L2 to L3 analysts to Team Leads to Managers for decision making etc.).
- Lastly, in the case of incidents, we produce Flash Reports (day 0), and incident reports (at the end). Human error is accounted for and documented in all incident reports.
- **Question**: How much control does Bitdefender have over a customer's infrastructure?
- **Answer**: Outside of pre-approved actions agreed upon by the customer, Bitdefender does not touch a customer's infrastructure.
- **Question**: In the event of a security incident, how quickly will the Bitdefender MDR team respond?
- **Answer**: When a security incident takes place, the customer will be notified as soon as the incident is declared according to our Service Level Agreement outlined in the Bitdefender MDR Terms and Conditions. There is no ability to provide a specific time to resolve an incident, as the depth and specifics of the incident vary. Our aim is to continuously monitor and analyze, detect quickly, respond immediately and contain rapidly to minimize any impact on the customer environment. The customer is expected to work with the SOC analyst in the event we need actions on their end. The customer will also be given recommendations on remediation steps to take as a result of an incident.
- **Question**: Will Bitdefender MDR integrate or ingest data from my existing security solution?
- **Answer**: We do not ingest logs from other security tools that the customer has. To ensure data fidelity – while delivering the best prevention, protection, and detection and response technology – and in turn provide the quickest, most accurate response to security events, Bitdefender MDR customers are required to use Bitdefender GravityZone Business Security Enterprise across their environment.

This information is property of Bitdefender LLC. You may not publish or redistribute this document without advance permission from Bitdefender.

Support

- Business Technical Support Portal
  https://www.bitdefender.com/business/support/?lang=en
- Business Technical Support Contact
  https://www.bitdefender.com/business/support/en/71263-85158-contact.html
- Enterprise Support Policies
  https://www.bitdefender.com/site/view/enterprise-support-policies.html

Open / Track / Update / Close a Ticket

MDR customers looking to open, track, update, or close a support ticket can do so easily from the MDR Customer Portal in the Tickets section. From there they can create new tickets and include any relevant attachments, as well as track responses from the MDR team.

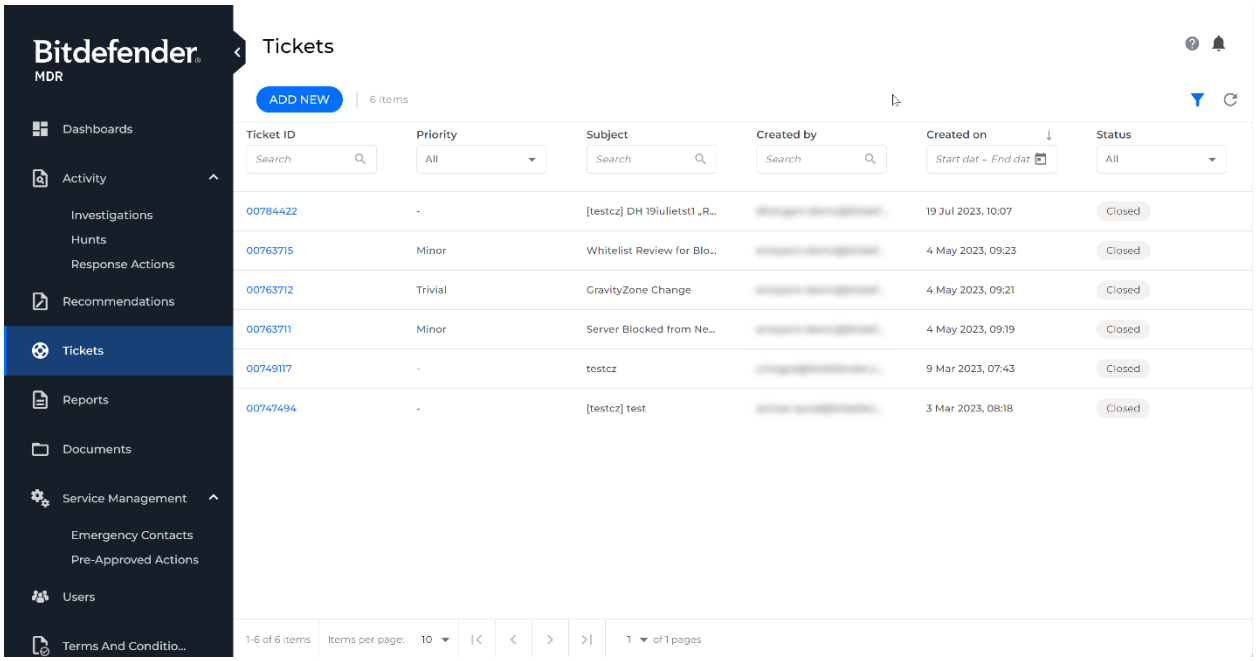


Figure 12: Customers can open, track, and update cases from the MDR Customer Portal

Bitdefender's Managed Detection & Response (MDR) is an advanced cybersecurity approach that consolidates top-notch detection, investigation, response, and threat hunting capabilities powered by award-winning GravityZone technologies. It delivers a comprehensive, multi-layered defense mechanism, designed to safeguard organizations of varied sizes across diverse infrastructures, workloads, and end-user systems.

Bitdefender MDR empowers organizations in the fight against cybercriminals with robust, agile protection against the ever-evolving cyber threat landscape. It reflects Bitdefender's unwavering commitment to delivering sophisticated, efficient, and dependable cybersecurity solutions in alignment with the rapidly advancing digital world.

Contact Information

- To learn more about Bitdefender MDR services, please contact us through the MDR Inquiry Form.

© 2023 Bitdefender, LLC. The information contained in this document is confidential and only for the use of the intended recipient. You may not publish or redistribute this document without advance permission from Bitdefender.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BGS-MDR-SolutionDescription-Confidential-Creat7181-en_EN
CD-09/06/23 • MD-September 14, 2023 10:00 pm