Bitdefender

SOLUTION DESCRIPTION

Managed Detection & Response (MDR+SOC)

Trusted. Always.

Contents

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 significant 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 and at a fraction of the cost.

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 owns 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 eliminate or 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 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 guide. 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 guide 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.

Bitdefender MDR Services

Bitdefender MDR delivers the people, processes and technology to completely address your security needs and outcomes. Modern EDR/XDR solutions require skilled analysts to continually monitor the environment, with an ever-increasing number of alerts, and ownership of time-critical response workflows. Bitdefender MDR takes responsibility for these challenges so that your IT and Security teams can focus on helping your organization grow.

Key Benefits

- **Analysts, not alerts –** Bitdefender MDR service manages the entire alert lifecycle, analyzing thousands of alerts down to a handful of responses and recommendations. See everything transparently in your MDR portal and get notified of only what matters to you.
- **Quick, decisive response –** Our security analysts quickly assess security incidents and take decisive actions to contain and mitigate threats, leveraging a comprehensive set of pre-approved actions.
- **Best-in-class security platform –** Bitdefender MDR include our industry-leading security platform, consistently placing #1 in independent tests by MITRE®, AV-Test©, and AV-Comparatives©. Moreover, Bitdefender owns the platform, giving our customers one security technology stack to consolidate on.

Services Overview

Service Component	Bitdefender MDR	Bitdefender MDR PLUS
Industry leading security platform	✓	✓
24x7 SOC	✓	✓
Pre-approved Actions (PAAs)	✓	✓
Threat Hunting	✓	✓
Expert Recommendations	✓	✓
Incident Root Cause & Impact Analysis	✓	✓
MDR Portal & Reporting	✓	✓
Professional Services On-boarding	✓	✓
Cybersecurity Breach Warranty	✓	✓
24x7 Security Account Manager (Customer Success)		✓
Global Threat Intelligence Feeds and Analysis		✓
Dark Web Monitoring		✓
Security Baselining and Tailored Threat Modeling		✓
Brand & IP Protection		✓
High Priority Target Monitoring		✓
XDR Sensors	Add-ons	Add-ons

Bitdefender MDR Features

Leading security platform – Bitdefender MDR includes our industry leading security platform, enhanced by additional SOC tools and AI

- **24x7 security coverage –** Our global network of SOCs work when you work and cover you around the world and around the clock. If a security incident occurs, our SOC will take action and a security account manager will call your emergency contact within 30 minutes and be in constant communications throughout the incident.
- **Pre-Approved Actions (PAA) –** A comprehensive array of PAAs provide quick and decisive response actions to mitigate security incidents. Our analysts evaluate, investigate and take actions faster than any teams.
- **Threat Hunting –** Hundreds of millions of total covered endpoints allows Bitdefender security researchers, Bitdefender Labs, and the MDR Threat Intelligence team to compile a massive amount of threat intelligence, attacker research and threat analyses to continuously support threat hunts and update and protect our customers
- **Expert Recommendations –** In addition to providing complete security coverage, we elevate your security team. Our team of security experts provides recommendations to improve your security knowledge and posture as well as corrective actions to prevent possible incidents.
- **Incident Root Cause & Impact Analysis –** We identify the original threat vectors and potential impacts during incidents, offering comprehensive analyses and documentation in after-action reports. We initiate enhanced monitoring for 72 hours to ensure similar or related incidents don't occur.
- **MDR Portal & Reporting –** Your MDR portal provides dashboards and monthly, actionable reporting on your service. The report provides meaningful insights into security incidents, highlight cybersecurity trends, and guide remediation efforts, offering unparalleled transparency into the MDR service.
- **Cybersecurity Breach Warranty:** MDR customers are covered up to $100,000 in the event of a ransomware incident.

Bitdefender MDR PLUS Features

All the benefits of Bitdefender MDR included

- **24x7 Security Account Manager –** Dedicated SAM is your single point-of-contact, there to address your questions or concerns and provide a quarterly business review (QBR).
- **Professional Service On-boarding –** Professional services team provides detailed support and guidance to quickly and accurately on-board your organization onto the service.
- **Global Threat Intelligence Feeds & Analysis –** Cyber Intelligence Fusion Cell (CIFC) utilizes the threat intelligence lifecycle to research cyber threats, geopolitical activity, and industry-specific data trends and then apply this knowledge to your organization.
- **Dark Web Monitoring –** Continuously monitor the dark web, including popular criminal forums and marketplaces, as well as ransomware blogs, to detect leaked or stolen organizational data, including domains, credentials, intellectual property (IP), brand references and typo-squatting, technology stack, and industry and geography concerns.
- **Security Baselining and Tailored Threat Modelling –** Collect and process information about your organization, including your business, users, and known threats, to model and monitor your specific threat landscape.
- **Brand and IP Protection –** Continuously monitor your most valuable assets to detect and notify you of what is being shared or sold on the dark web.
- **High Priority Target Monitoring –** Continuously monitor high-value employees for information that may have been stolen or leaked.
- **Comprehensive reporting –** intelligence hunts, Tippers (industry-specific research and recommendations), and Requests for Information (customer requested)
- **Cybersecurity Breach Warranty:** MDR customers are covered up to $1,000,000 in the event of a security incident.

Bitdefender MDR for MSPs

Bitdefender MDR for MSPs delivers robust security capabilities to their clients without the need for extensive in-house resources. MSP's clients are provided continuous protection against current and emerging cyber threats removing much of the security burden from the MSP. This allows the MSP to focus their resources on strategic business growth, customer relationship management, and enhancing their core service offerings.

MSP Benefits

- **Revenue growth –** MDR service provides additional revenue opportunities and more stickiness with your customers.
- **Automated billing –** provides a streamlined experience for MSPs and customers alike.
- **Streamlined onboarding –** allows for sequential onboarding of multiple customers in a straightforward, repeatable process.
- **Communications –** multiple means of communications and notifications supports customer level interactions.

Customer Benefits

- **24x7 security coverage –** Our global network of SOCs work when you work and cover you around the world and around the clock. If a security incident occurs, our SOC will take action and a security account manager will call your emergency contact within 30 minutes.
- **Pre-Approved Actions (PAA) –** A comprehensive array of PAAs provide quick and decisive response actions to mitigate security incidents. Our analysts evaluate, investigate and take actions faster than any teams.
- **Threat Hunting –** Hundreds of millions of total covered endpoints allows Bitdefender to compile a massive amount of threat intelligence, attacker research and threat analyses to support threat hunts and continuously update and protect your customers
- **MDR Portal & Reporting –** Your MDR portal provides dashboards and monthly, actionable reporting on your customers' service.

Detailed Description of Bitdefender MDR Services

24x7 Monitoring and Support

Bitdefender MDR provides a comprehensive cybersecurity service operating 24x7 from three global Security Operations Centers (SOC), with one in the North America (US- Texas), one in Europe (Romania), and one in Asia Pacific (Singapore). Each of our SOCs is fully staffed with the same level of credentialled staff, processes, and technologies to ensure we are providing uninterrupted 24x7, 365 days a year coverage to our customers around the globe. Our global SOCs also ensure that customers in a particular region are being supported by a SOC in their same region during their working hours.

The cornerstone of our MDR service is its capacity for rapid response. In the event of a detected security incident, we will execute pre-approved actions (see below). 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. 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.

Pre-Approved Actions

Pre-approved, or proactive, incident response is a key capability of the Bitdefender MDR team. 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.

Threat Hunting

Bitdefender monitors, compiles, and analyzes a massive amount of threat intelligence, attacker research, and endpoint and sensor data to continuously update threat landscapes, support threat hunts, and protect our customer environments.

By understanding the tactics, techniques, and procedures (TTPs) employed by potential attackers, we can better anticipate and detect threats.

Advanced analytics and threat detection techniques are then applied to analyze this data, searching for patterns,

anomalies, indicators of compromise (IOCs), zero-day exploits, and insider threats that pose significant risks to the organization. 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.

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.

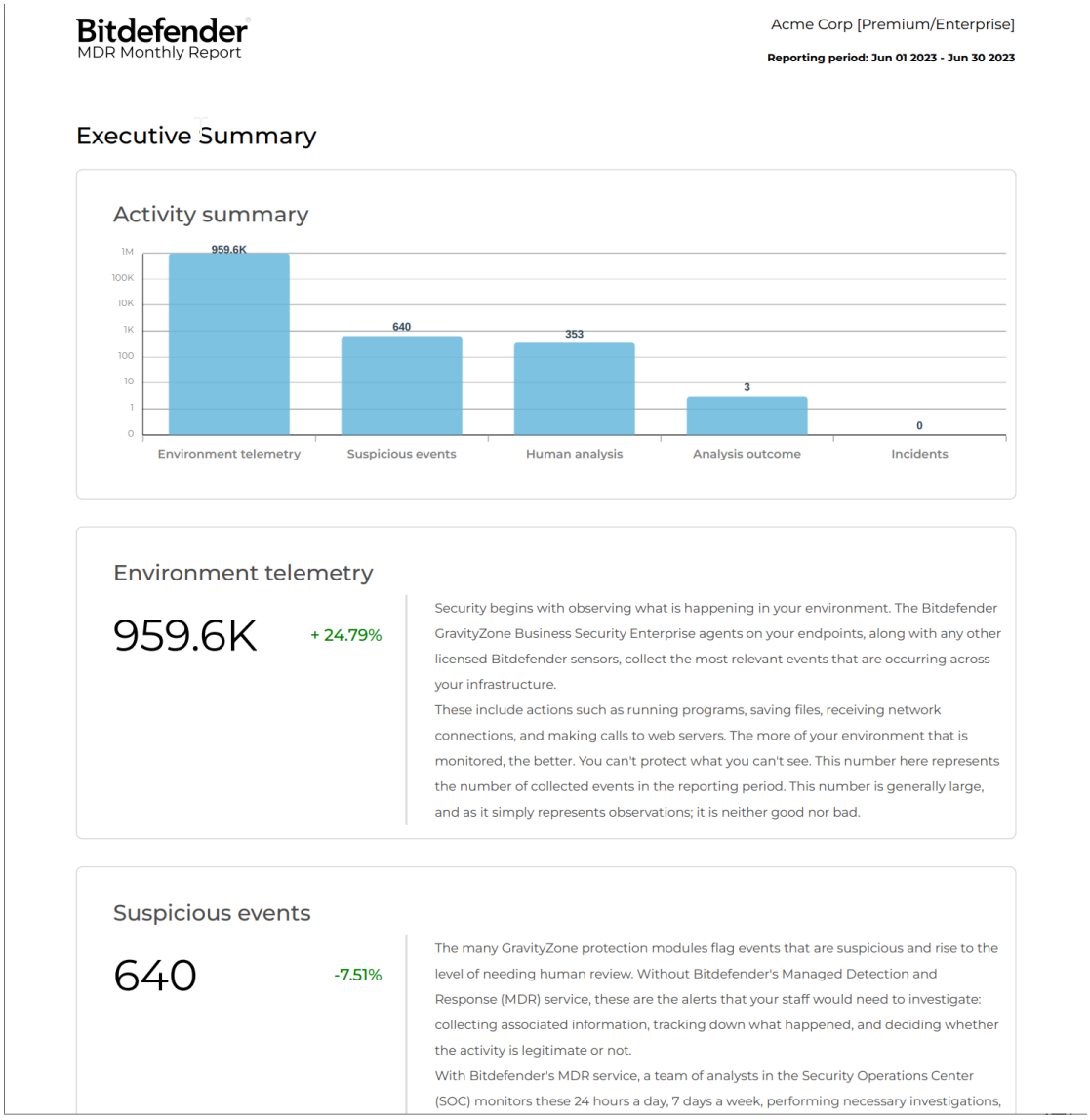
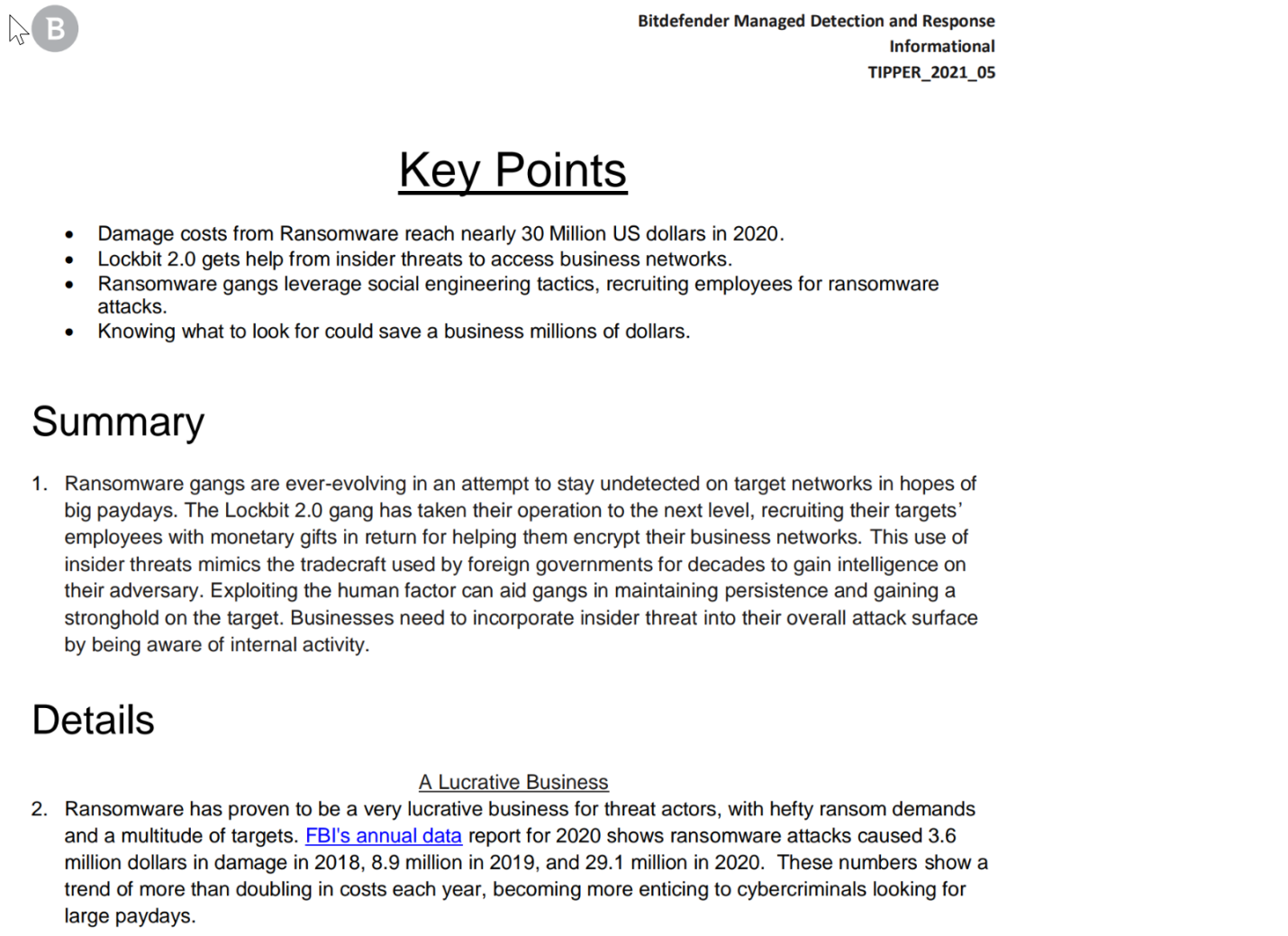


Figure 1: An example of a section of the Bitdefender MDR Monthly Report.

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.



Bitdefender Managed Detection and Response
Informational
TIPPER_2021_05

Key Points

- Damage costs from Ransomware reach nearly 30 Million US dollars in 2020.
- Lockbit 2.0 gets help from insider threats to access business networks.
- Ransomware gangs leverage social engineering tactics, recruiting employees for ransomware attacks.
- Knowing what to look for could save a business millions of dollars.

Summary

1. Ransomware gangs are ever-evolving in an attempt to stay undetected on target networks in hopes of big paydays. The Lockbit 2.0 gang has taken their operation to the next level, recruiting their targets' employees with monetary gifts in return for helping them encrypt their business networks. This use of insider threats mimics the tradecraft used by foreign governments for decades to gain intelligence on their adversary. Exploiting the human factor can aid gangs in maintaining persistence and gaining a stronghold on the target. Businesses need to incorporate insider threat into their overall attack surface by being aware of internal activity.

Details

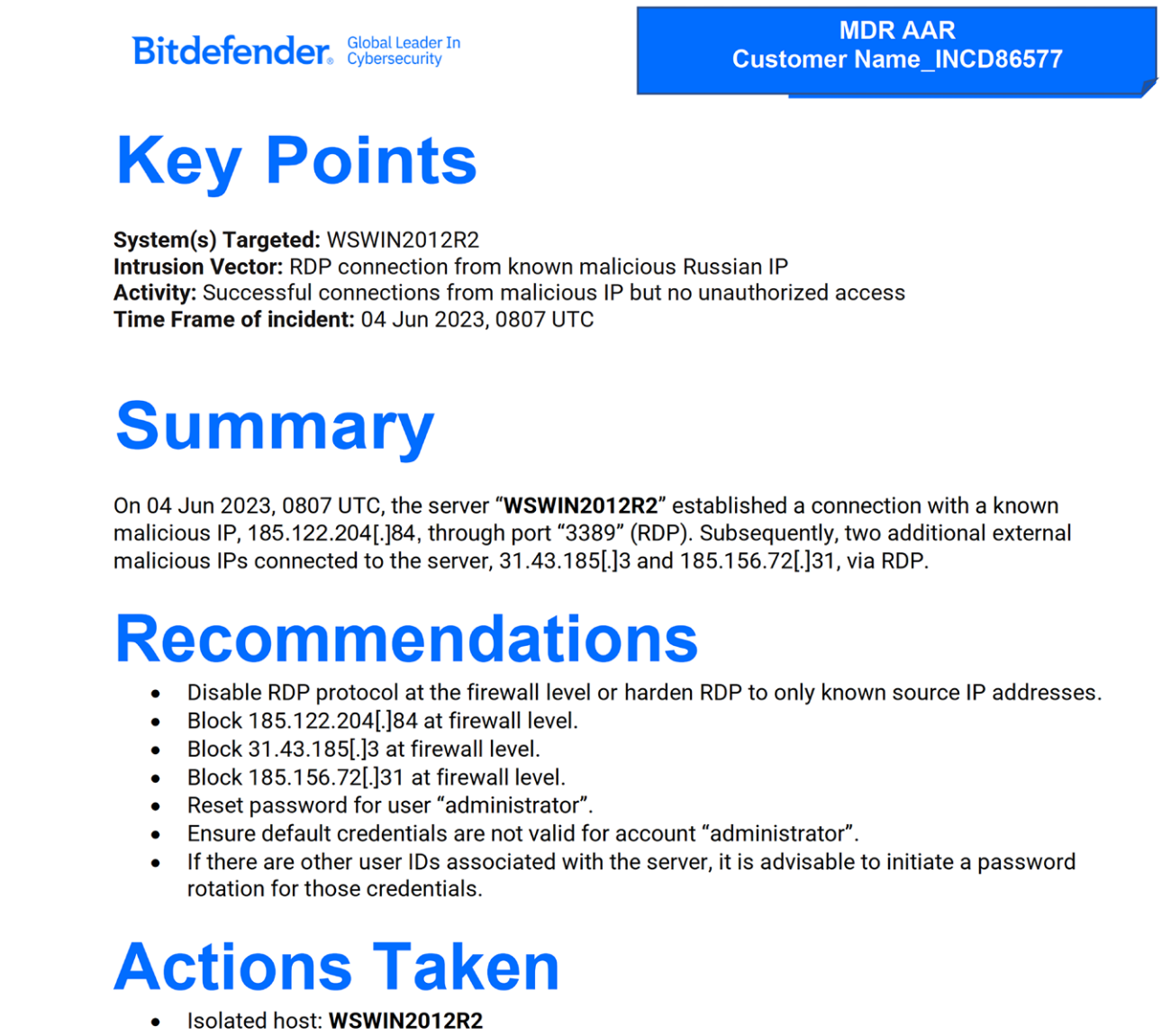
A Lucrative Business

2. Ransomware has proven to be a very lucrative business for threat actors, with hefty ransom demands and a multitude of targets. FBI's annual data report for 2020 shows ransomware attacks caused 3.6 million dollars in damage in 2018, 8.9 million in 2019, and 29.1 million in 2020. These numbers show a trend of more than doubling in costs each year, becoming more enticing to cybercriminals looking for large paydays.

Figure 2: An example of a section from the Bitdefender MDR Tipper Report

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.



Bitdefender Global Leader In Cybersecurity

MDR AAR
Customer Name_INCD86577

Key Points

System(s) Targeted: WSWIN2012R2
Intrusion Vector: RDP connection from known malicious Russian IP
Activity: Successful connections from malicious IP but no unauthorized access
Time Frame of incident: 04 Jun 2023, 0807 UTC

Summary

On 04 Jun 2023, 0807 UTC, the server "**WSWIN2012R2**" established a connection with a known malicious IP, 185.122.204[.]84, through port "3389" (RDP). Subsequently, two additional external malicious IPs connected to the server, 31.43.185[.]3 and 185.156.72[.]31, via RDP.

Recommendations

- Disable RDP protocol at the firewall level or harden RDP to only known source IP addresses.
- Block 185.122.204[.]84 at firewall level.
- Block 31.43.185[.]3 at firewall level.
- Block 185.156.72[.]31 at firewall level.
- Reset password for user "administrator".
- Ensure default credentials are not valid for account "administrator".
- If there are other user IDs associated with the server, it is advisable to initiate a password rotation for those credentials.

Actions Taken

- Isolated host: **WSWIN2012R2**

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

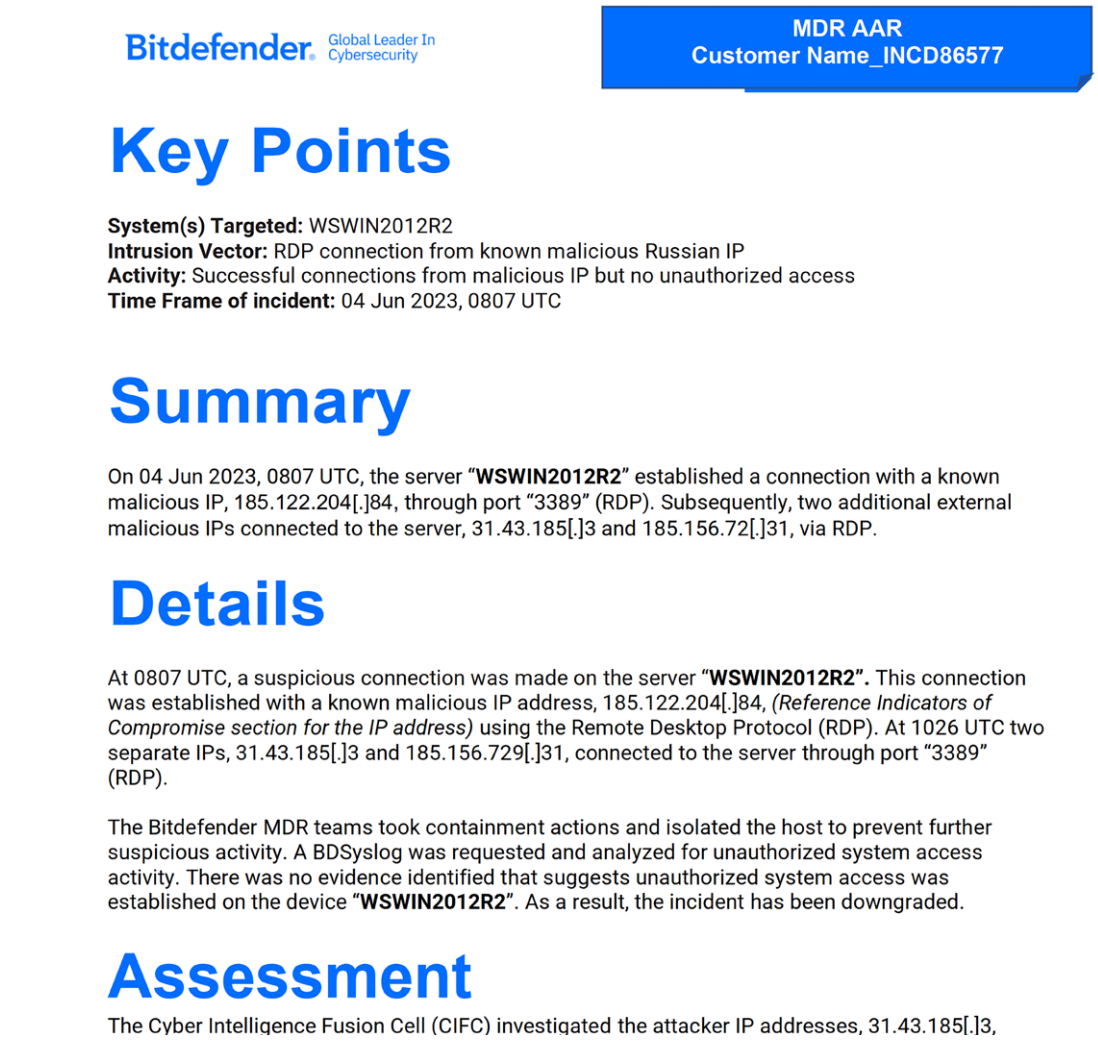
After Action Report

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.



Bitdefender Global Leader In Cybersecurity

MDR AAR
Customer Name_INCD86577

Key Points

System(s) Targeted: WSWIN2012R2
Intrusion Vector: RDP connection from known malicious Russian IP
Activity: Successful connections from malicious IP but no unauthorized access
Time Frame of incident: 04 Jun 2023, 0807 UTC

Summary

On 04 Jun 2023, 0807 UTC, the server "**WSWIN2012R2**" established a connection with a known malicious IP, 185.122.204[.]84, through port "3389" (RDP). Subsequently, two additional external malicious IPs connected to the server, 31.43.185[.]3 and 185.156.72[.]31, via RDP.

Details

At 0807 UTC, a suspicious connection was made on the server "**WSWIN2012R2".** This connection was established with a known malicious IP address, 185.122.204[.]84, *(Reference Indicators of Compromise section for the IP address)* using the Remote Desktop Protocol (RDP). At 1026 UTC two separate IPs, 31.43.185[.]3 and 185.156.729[.]31, connected to the server through port "3389" (RDP).

The Bitdefender MDR teams took containment actions and isolated the host to prevent further suspicious activity. A BDSyslog was requested and analyzed for unauthorized system access activity. There was no evidence identified that suggests unauthorized system access was established on the device "**WSWIN2012R2**". As a result, the incident has been downgraded.

Assessment

The Cyber Intelligence Fusion Cell (CIFC) investigated the attacker IP addresses, 31.43.185[.]3,

Figure 4: An example of a small section from the Bitdefender MDR After Actions Report

Incident Root Cause & Impact Analysis

We identify the original threat vectors and potential impacts during incidents, offering comprehensive analyses and documentation in after-action reports. We initiate enhanced monitoring for 72 hours to ensure similar or related incidents don't occur.

Expert Recommendations

In addition to providing complete security coverage, we elevate your security team. Our team of security experts provides recommendations to improve your security knowledge and posture as well as corrective actions to prevent possible incidents.

Bitdefender MDR PLUS-specific Services

Dedicated Security Account Manager

Your dedicated Security Account Manager (SAM) is your single point-of-contact into all of Bitdefender. The SAM is there to address your questions or concerns and provide a quarterly business review (QBR) to clearly communicate the state of your security and outstanding issues and recommendations. If a security incident occurs, our SOC will take action and your SAM will call your emergency contact within 30 minutes and be in constant communications throughout the incident.

Tailored Threat Modeling

Beginning with onboarding and an initial period of developing a security baseline, we then continuously collect and process information about your organization, including your business, users, and known threats, to model and monitor your specific threat landscape.

A core component of tailored threat modeling is having additional, comprehensive context into the customer's unique environment, which is first gathered in the form of an in-depth Customer Questionnaire, 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.

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

Global Intelligence Analysis

Our Intelligence Analysts are organized into a Cyber Intelligence Fusion Cell (CIFC), which utilizes the threat intelligence lifecycle to research cyber threats, geopolitical activity, and industry-specific data trends and then apply this knowledge to your organization. Unlike other vendors, that may incorporate a single external intelligence source into an add-on service, Bitdefender leverages multiple sources, including our own, into the core service.

Dark Web Monitoring

Our Intelligence Analysts continuously monitor the dark web on key sources like forums, marketplaces, and ransomware blogs to detect leaked or stolen organizational data, including domains, credentials, intellectual property (IP), brand references and typo-squatting, technology stack, and industry and geography concerns. We can also monitor key vendors and strategic partners to notify you of issues we find with them.

Brand and IP Protection

While monitoring the dark web, our Intelligence Analysts continuously look for information about your organization, its brand, and your IP. These are among your most valuable assets so detecting what is being shared or sold on the dark web is critical to protecting them. We monitor domain registrations to detect newly created domains that could indicate typo-squatting or URL hijacking behavior by bad actors. In addition to looking for malicious activity across the internet, the team also monitors for exposed sensitive information, such as passwords or access keys on code repositories.

High Priority Target Monitoring

It's no secret that that executives and Board of Directors have access to very sensitive data but don't necessarily follow security policies and procedures. Our intelligence Analysts can monitor high-value employees for information that may have been stolen or leaked.

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.

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. Customers can utilize Bitdefender Enterprise Professional Services to assist in their MDR deployment. Professional Services is included in Bitdefender MDR PLUS. Bitdefender MDR core 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 with information on how to begin the engagement.

Enterprise Professional Services Delivery Process

Every Enterprise Professional Services delivery consists of five sessions:

- **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

- 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 submitted
- Provide GravityZone Documentation

GravityZone Configuration Session

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

- Cloud Console setup:
- Create the GravityZone cloud account
- 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

Deployment start and validation Session

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

- Check update
- 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

Finish Deployment and verify failed installations Session

- Check endpoints with issues
- Check failed installations and perform initial troubleshooting
- Create support tickets for discovered issues

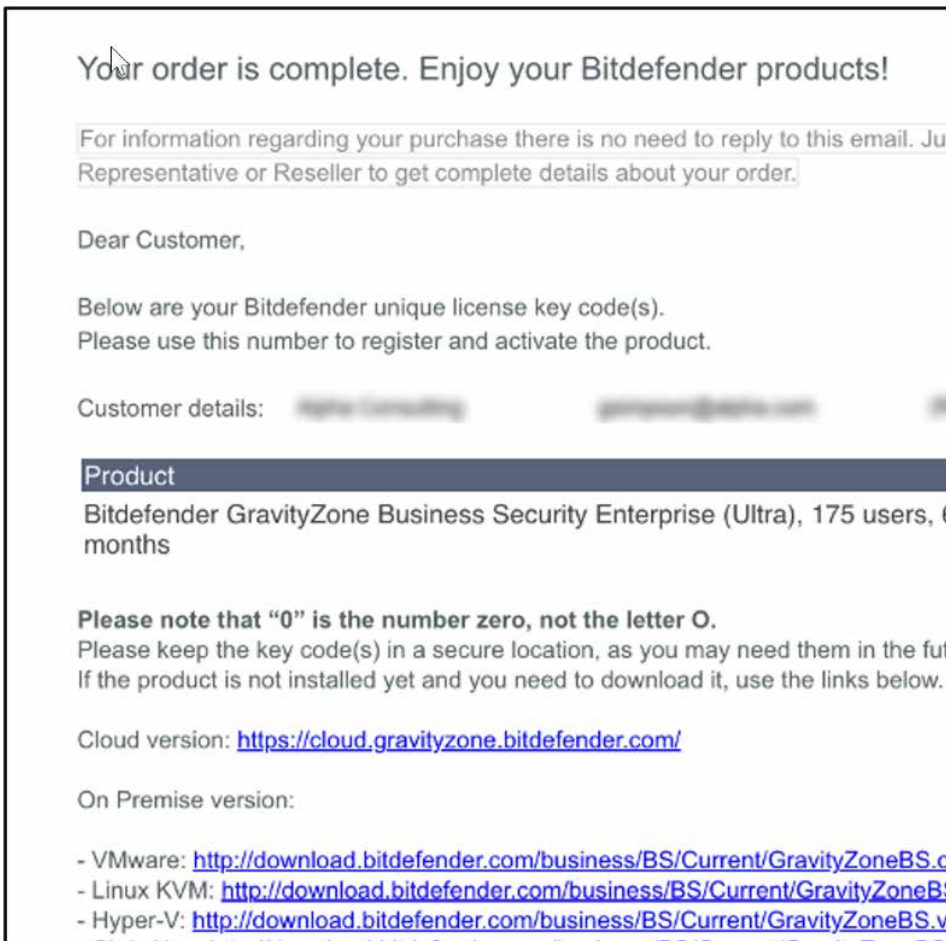
Health check and acceptance Session

- 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.

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. Ju
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:

Product
Bitdefender GravityZone Business Security Enterprise (Ultra), 175 users, (months

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 fut
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.c
- Linux KVM: http://download.bitdefender.com/business/BS/Current/GravityZoneB
- Hyper-V: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.v

Figure 5: 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 Bitdefender MDR PLUS customers to contact their assigned Security Account Manager. Bitdefender MDR 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.

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

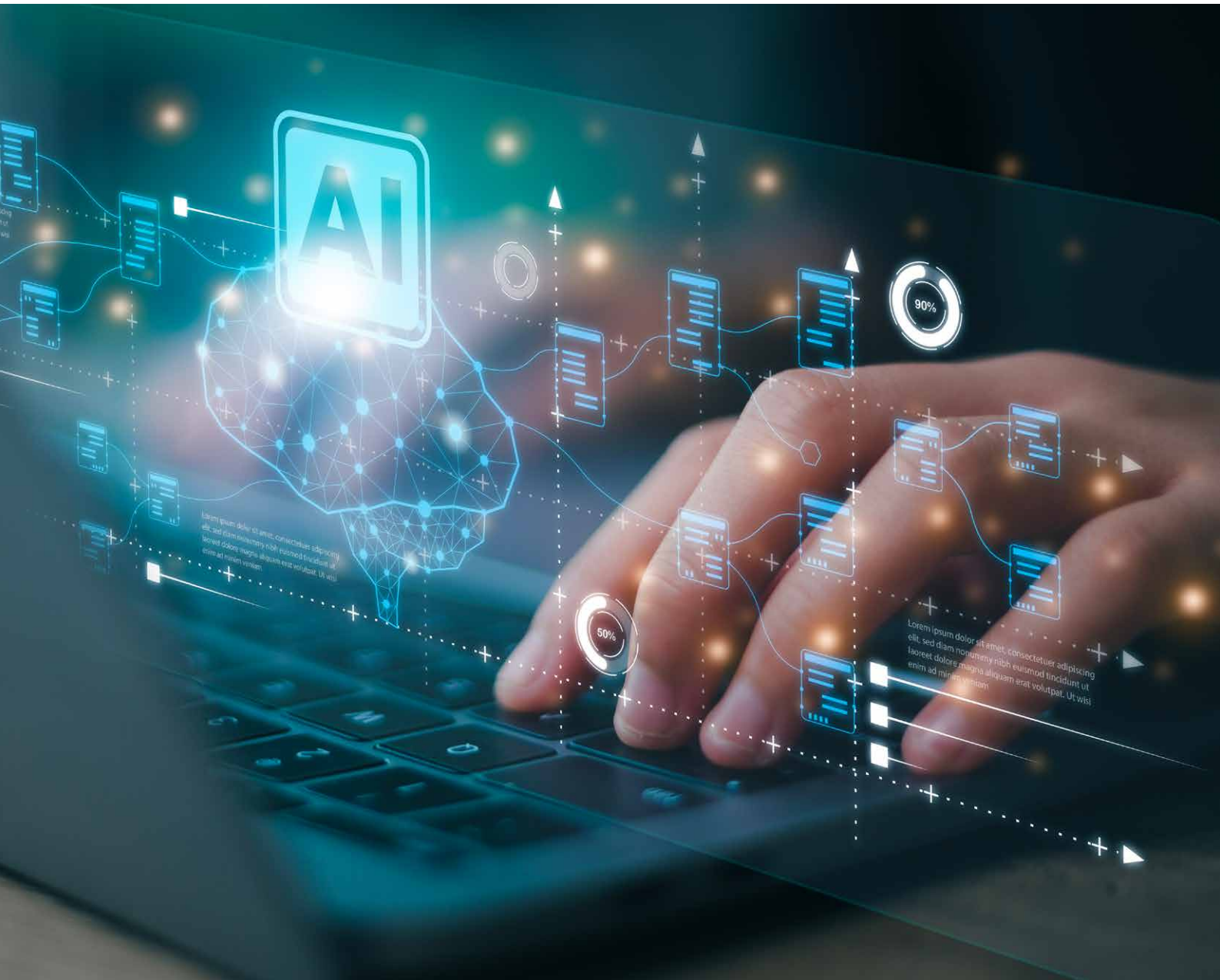
Once the customer receives access to the Bitdefender MDR portal, they can sign in and begin For MDR PLUS customers, the onboarding process by filling out our onboarding questionnaire. The questionnaire gives us an initial starting point to building out a baseline for our customers through establishment 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

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, however, most important is the quality of our MDR team which 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.

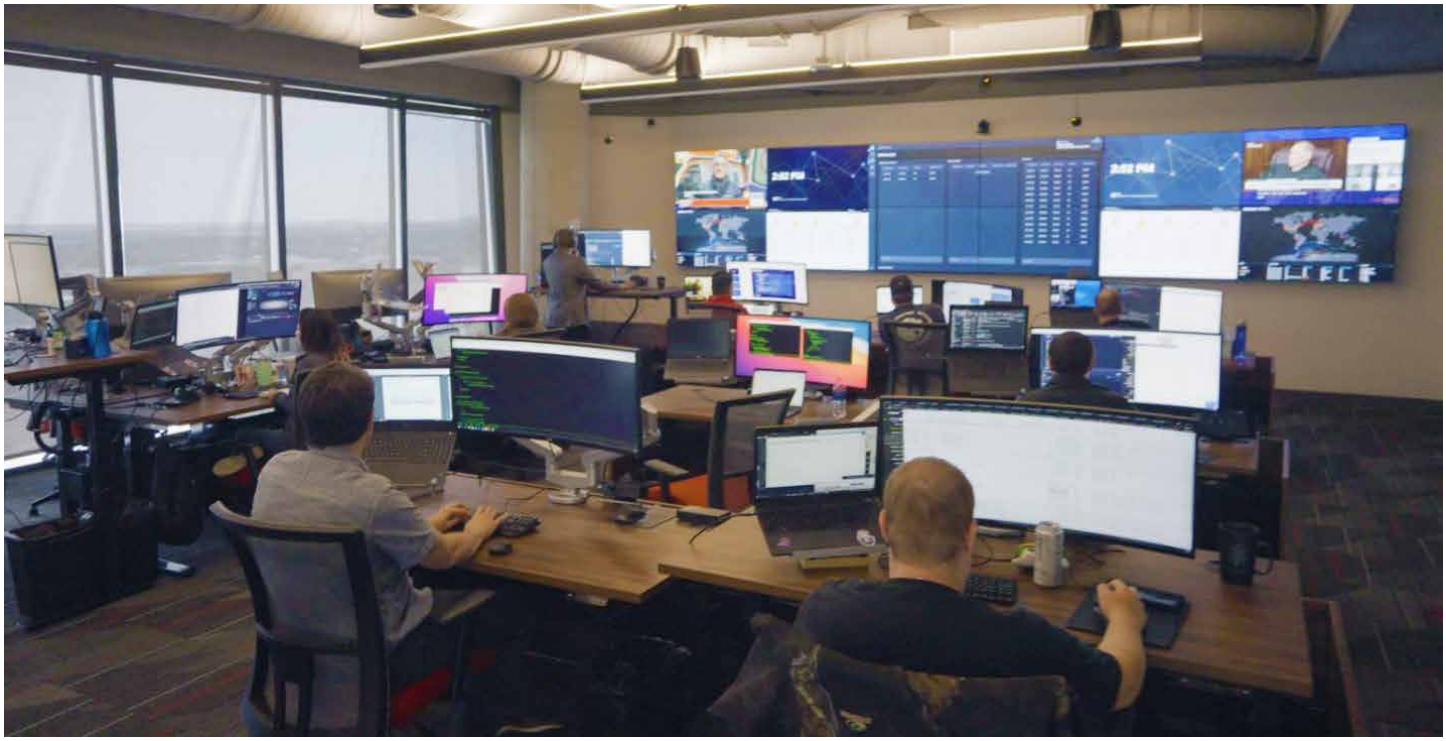


Figure 6: Hosted out of San Antonio, Texas, Bitdefender's NA SOC boasts a staff with a wealth of cybersecurity expertise.

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 analysts' experience isn't limited to cyberthreats, as many of the staff have years of experience in military intelligence or data science. 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 information sources throughout the security community, such as law enforcement, other security researchers, and intelligence vendors around the world, fusing 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 and actionable 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 have cybersecurity impact.

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 for MDR PLUS customers and help eliminate false positives, ambiguity, and duplication of efforts Threat intelligence analysts develop intelligence hunts for MDR PLUS customers, which are tailored to customers based on the environment, trending threats, or potential attacker methods. Finally, during a security incident, the threat intelligence team also supports Bitdefender MDR SOC analysts to develop additional threat hunting and to investigate attack indicators to ensure the environment stays secure.

Our Advanced Technology

Bitdefender's Managed Detection & Response (MDR) service leverages the power of the award-winning GravityZone EDR and XDR platform1. 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/.

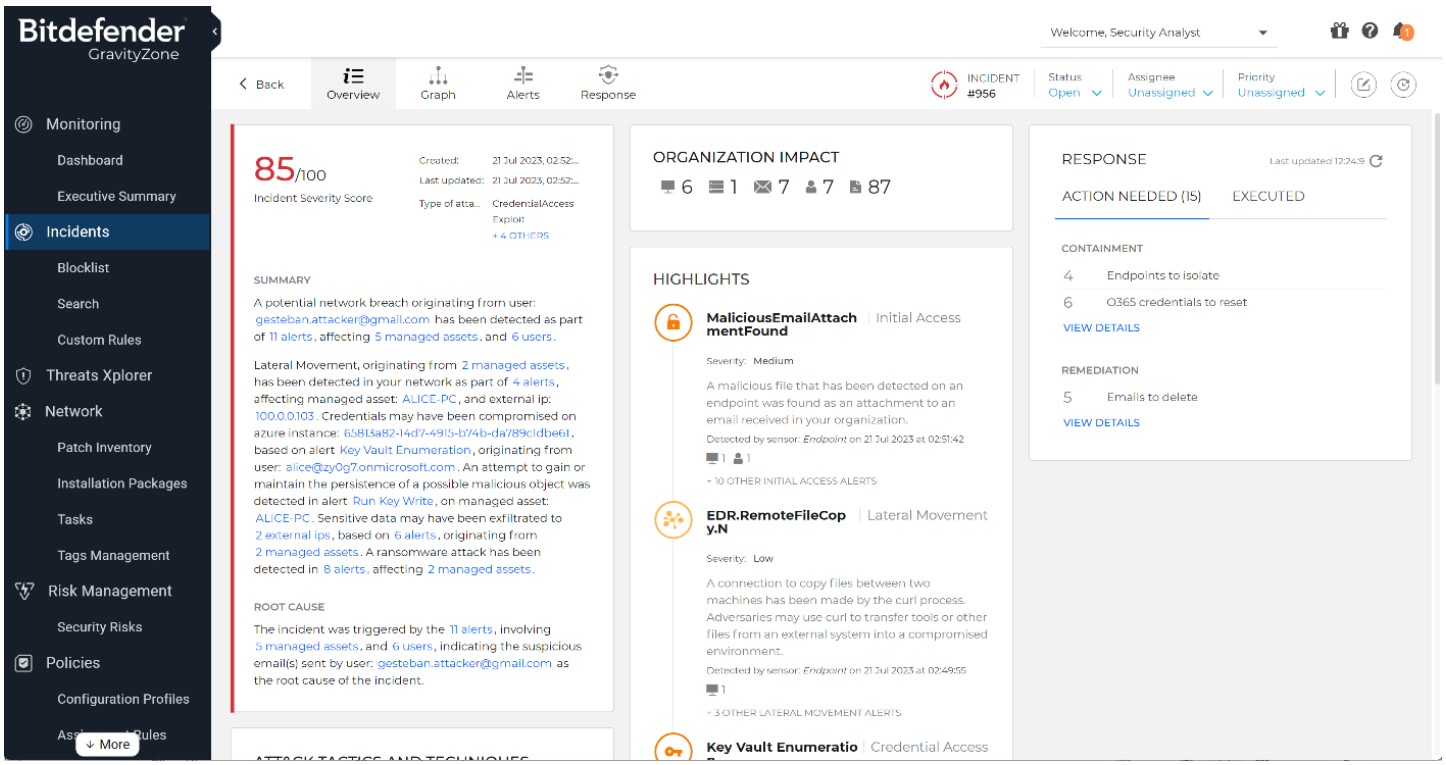


Figure 7: Using the GravityZone XDR Incident Advisor, security teams can quickly assess the important details of an incident which allows for quicker response.

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.

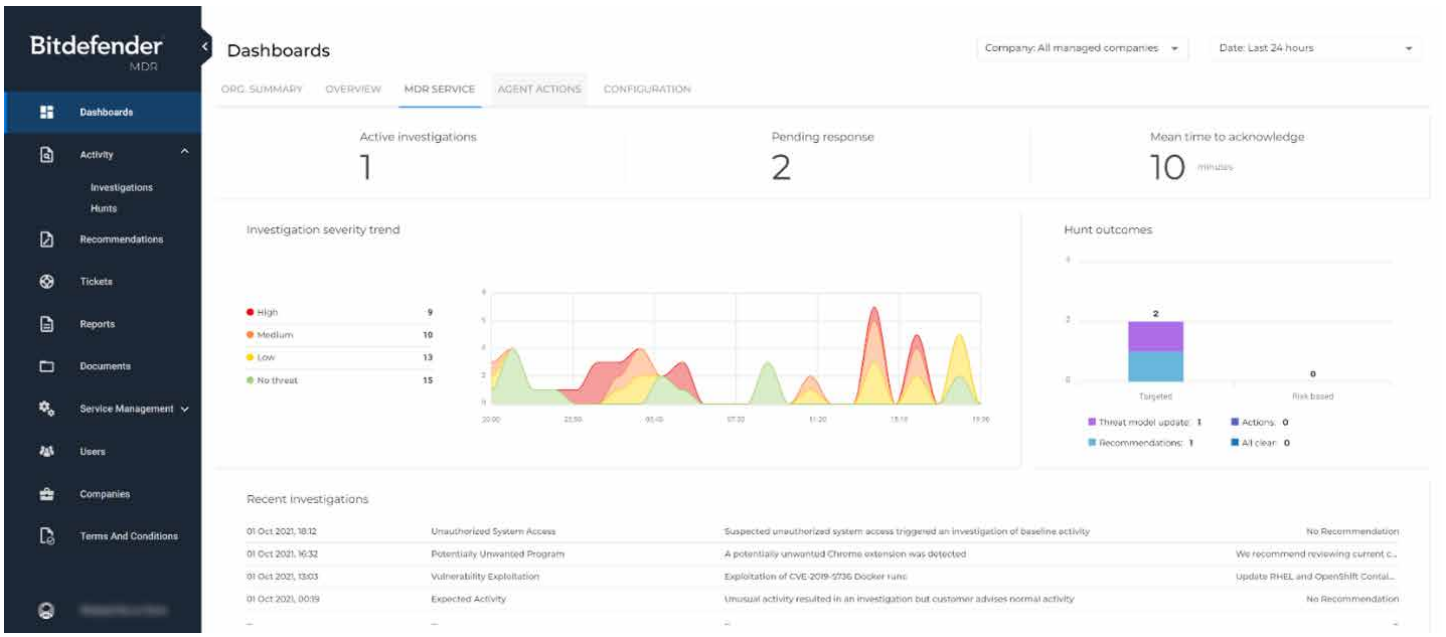


Figure 8: Using the Bitdefender MDR Portal, customers will be able to track the MDR team's cybersecurity activity, access reporting, investigation results, and more.

Our Proven Track Record

No other cybersecurity vendor has been consistently rated as high as Bitdefender in independent testing2. From 2018 to 2023, Bitdefender had 64% 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 August – November 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.

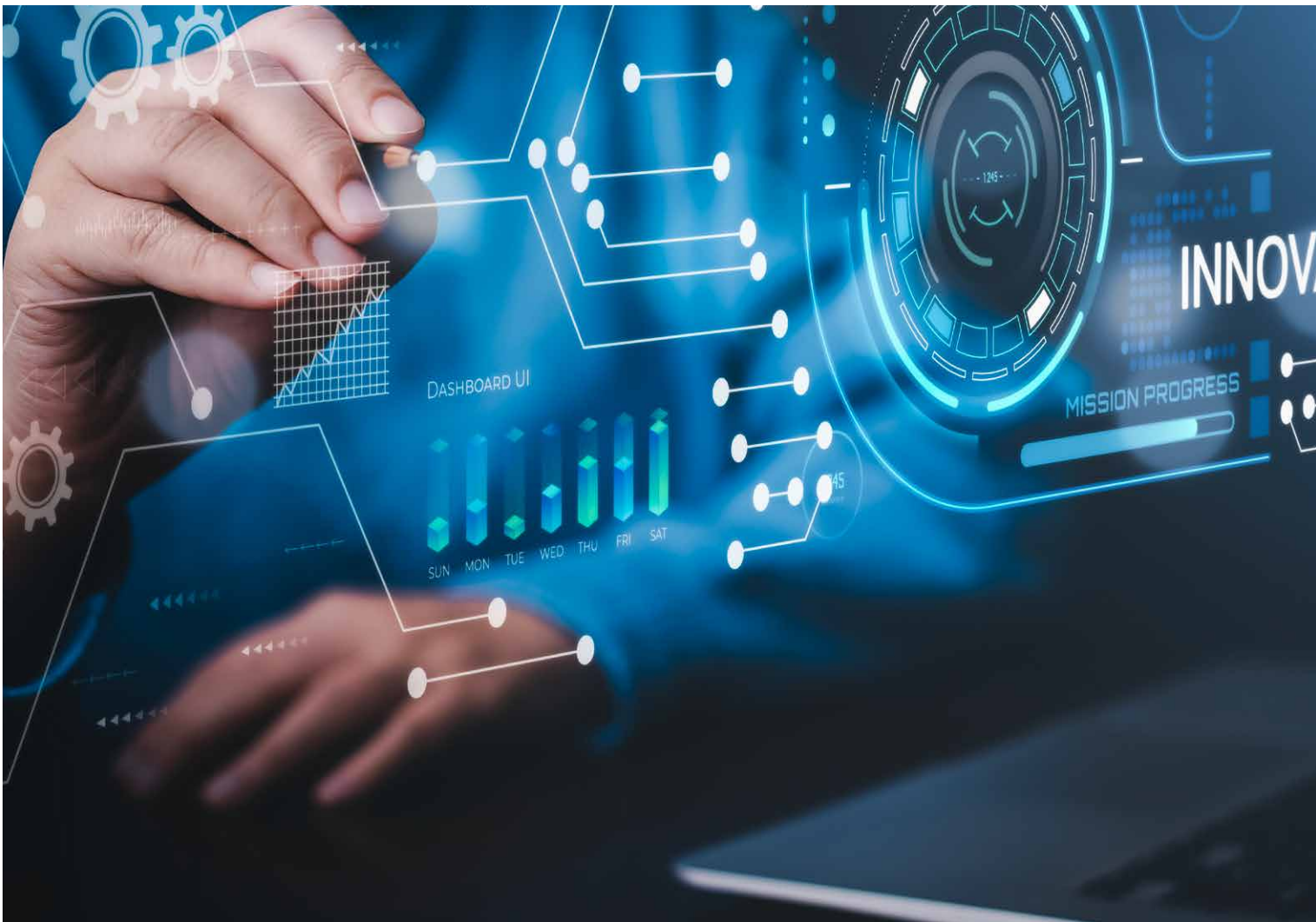
Bitdefender MDR was named a "Representative Vendor" for the second consecutive time in the 2023 Gartner® Market Guide for Managed Detection & Response Services. Forrester also recognized Bitdefender MDR as a "Notable Provider" in the Managed Detection and Response Landscape, Q1 2023 and the Managed Detection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

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/.

	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 9: 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 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.

Bitdefender MDR Cybersecurity Breach Warranty

In the never-ending fight against cyberthreats, Bitdefender aims to support our customers in all aspects of their security program while reducing their worry about the impact that cyber incidents bring. That's why we partnered with Cysurance to offer a cybersecurity breach warranty, at no additional cost, to both our MDR and MDR PLUS customers. In the event of a cybersecurity incident, MDR customers can receive financial support to help mitigate the costs of a breach.

Bitdefender MDR customers are eligible for up to $1,000,000 USD in financial assistance in the event of an incident through this agreement. Bitdefender's MDR Cybersecurity Breach Warranty is available at the start of a new MDR subscription or for existing MDR customers till the end of their contract after reviewing and accepting additional terms and conditions. For additional information check out the FAQ.

Coverage	MDR
Ransomware (Inclusive of costs/penalties associated with event)	$100,000

Coverage	MDR PLUS or MDR (1000+ endpoints)
Total	$1,000,000
Ransomware and BEC Event	$200,000
Compliance Event	$200,000
Cyber Legal Liability Event	$500,000
Business Income Event*	$100,000*
**There is a $2,500 per claim deductible that applies to this Event*	

What's Covered?

Bitdefender's MDR Cybersecurity Breach Warranty, in partnership with Cysurance, provides financial support for a wide range of cybersecurity incident costs including:

- **Ransomware –** Ransomware, including remediation and ransoms
- **Business Email Compromise –** A BEC event resulting in funds transfer or invoice fraud, including remediation and lost funds
- **Compliance and Regulatory Failure –** A cyber breach that triggers HIPAA, PCI, OSHA, and/or state related violations and results in a regulatory penalty, fine, or related expenses
- **Cyber Legal Liability –** A suit arising out of a cyberattack, including loss or misuse of data, or a media peril related to your website where legal defense and settlement costs are incurred
- **Business Income Loss –** A security breach that results in the loss of business income (net profit or loss before income taxes), and/or any continuing operating expenses affected by it.

Additional Services

In addition to MDR services, Bitdefender also provides add-on offensive services that help your organization understand and target vulnerabilities in your systems, processes, and people. Bitdefender Offensive Services provides organizations

with Penetration (Pen) Testing and Red Teaming services to ensure key security weaknesses and vulnerabilities are identified in order to improve and strengthen the security of your IT environments. Detailed information on these services and more is available here.

Offensive Security Services – Pen Testing

Bitdefender Pen Testing goes beyond vulnerability assessment by identifying key security weaknesses so that they can be remediated, thus improving the security of infrastructure, and by extension, your organization.

This offering includes both internal and external penetration testing, identifying vulnerabilities in web and mobile applications; networks; thick client applications; web services and APIs; and wireless access points. Every environment is unique, so our pen testers tailor their methods and attack vectors for each engagement.

We offer a variety of pen tests including:

- Web applications
- Mobile applications
- Web Services / API
- Networks (internal or external)
- Thick client applications
- Wireless Access Points

Offensive Security Services – Red Teaming

Bitdefender Red Teaming is an intelligence-led assessment that simulates real-life threat actors to demonstrate how attackers would attempt to compromise the critical functions and underlying systems of your organization. It identifies security vulnerabilities (physical and digital) in the organization to help your security team improve detection and response capabilities.

With our Red Teaming exercises, organizations can:

- Identify attack path(s) to the critical assets that may exist in the network
- Provide a clear understanding of a Blue Team's actual visibility and detection coverage in order to identify gaps and/or prioritize the development of new detection rules
- Allow a Blue Team to gain experience and handle incidents based on an internal incident response playbook
- Drive healthy debate and discussion across the Blue Team
- Help build resilience and adaptability across security operations by exposing it to different viewpoints and scenarios
- Build a business case for deploying new solutions or other security spending

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) PLUS.

“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).

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.

Contact Information

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

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

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-BSG-MDR-SolutionGuide-creat8017-en_EN
CD-08/06/24 • MD-September 12, 2024 12:07 pm