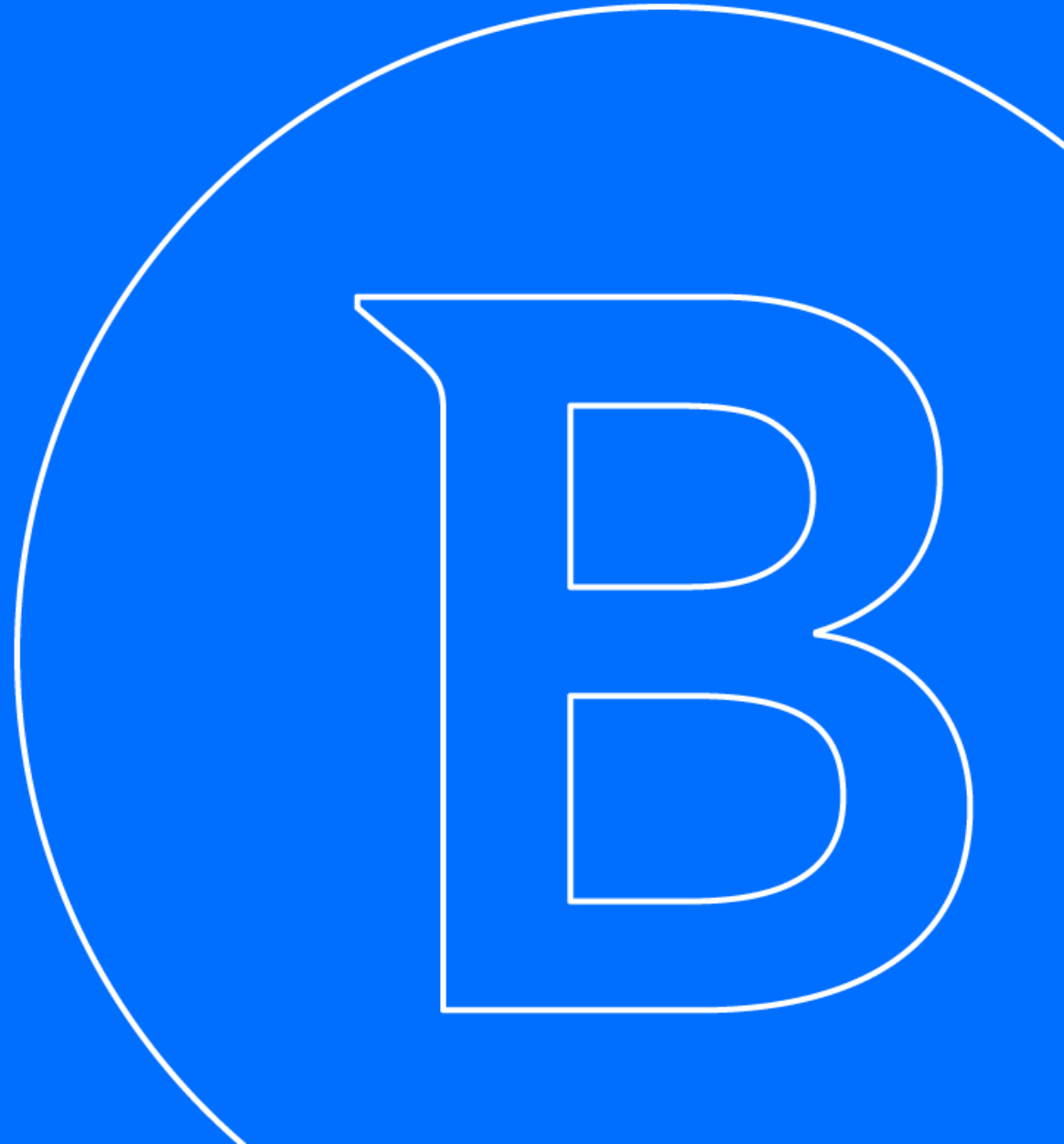


Global Leader In
Cybersecurity

Bitdefender®

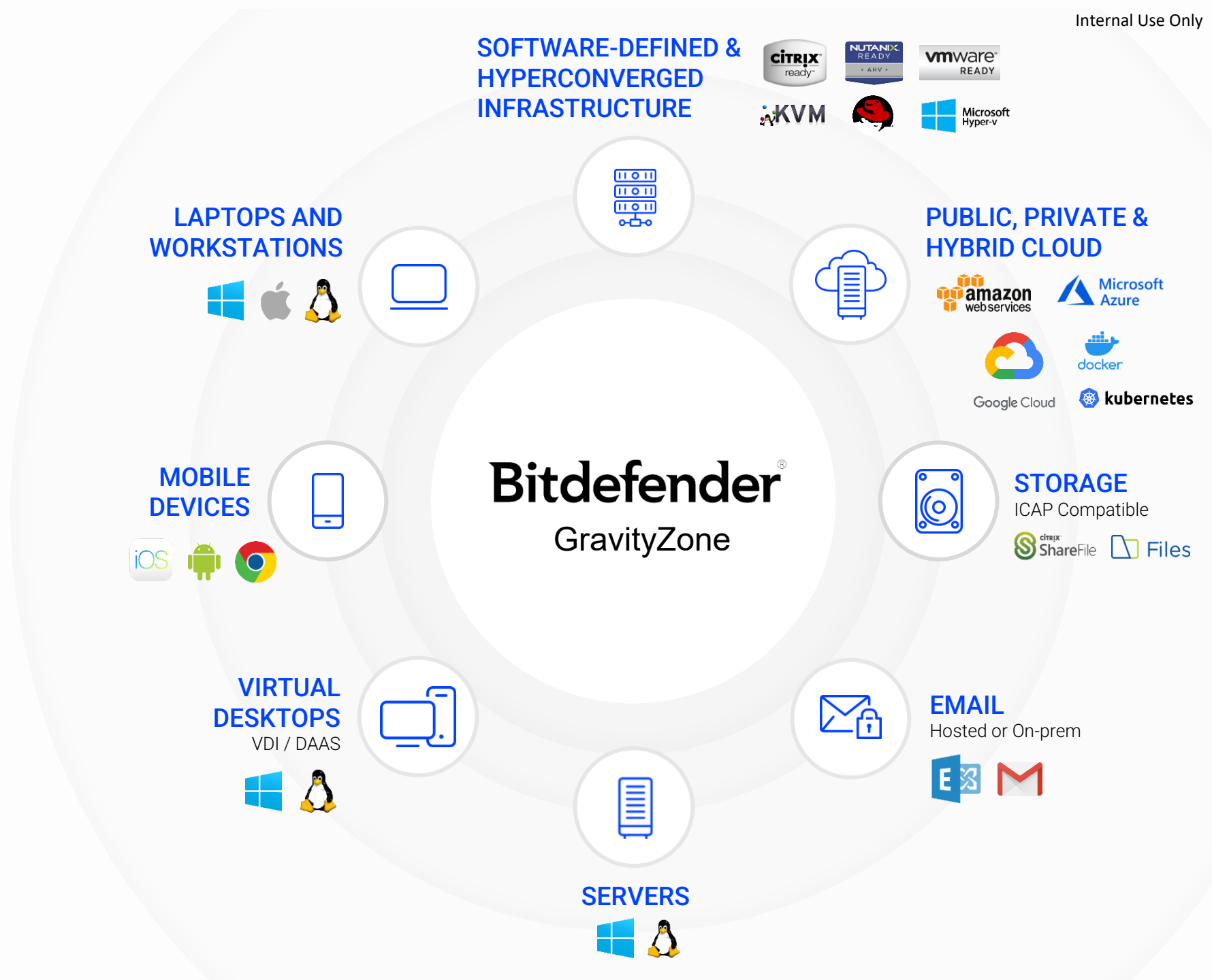
GRAVITYZONE

- **MSP Protection Models**
- **Risk & Compliance Management**
- **MDR**



GravityZone

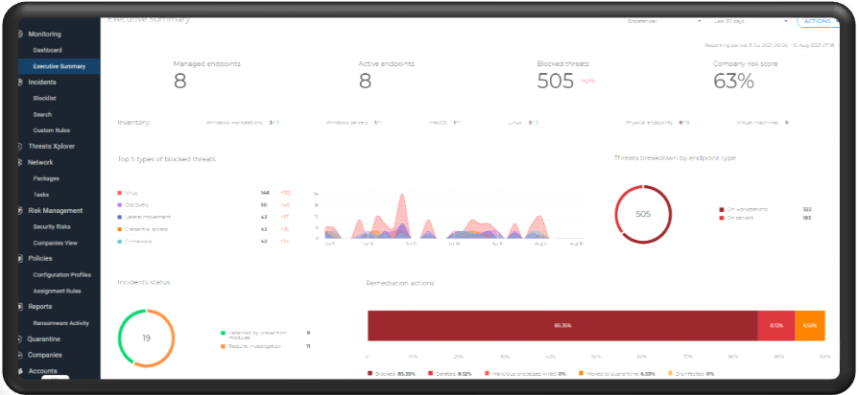
- **THE ENTERPRISE SECURITY PLATFORM FOR THE BEST BREACH AVOIDANCE**
- Unified Prevention, Cross-Endpoint Correlation, Detection, Response and Risk Analytics across Endpoint, Network and Cloud



Bitdefender® Global Leader
In Cybersecurity

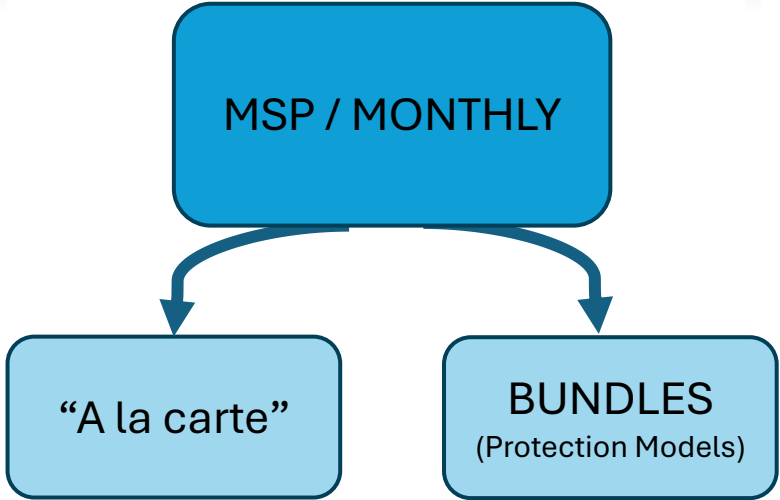


GRAVITYZONE



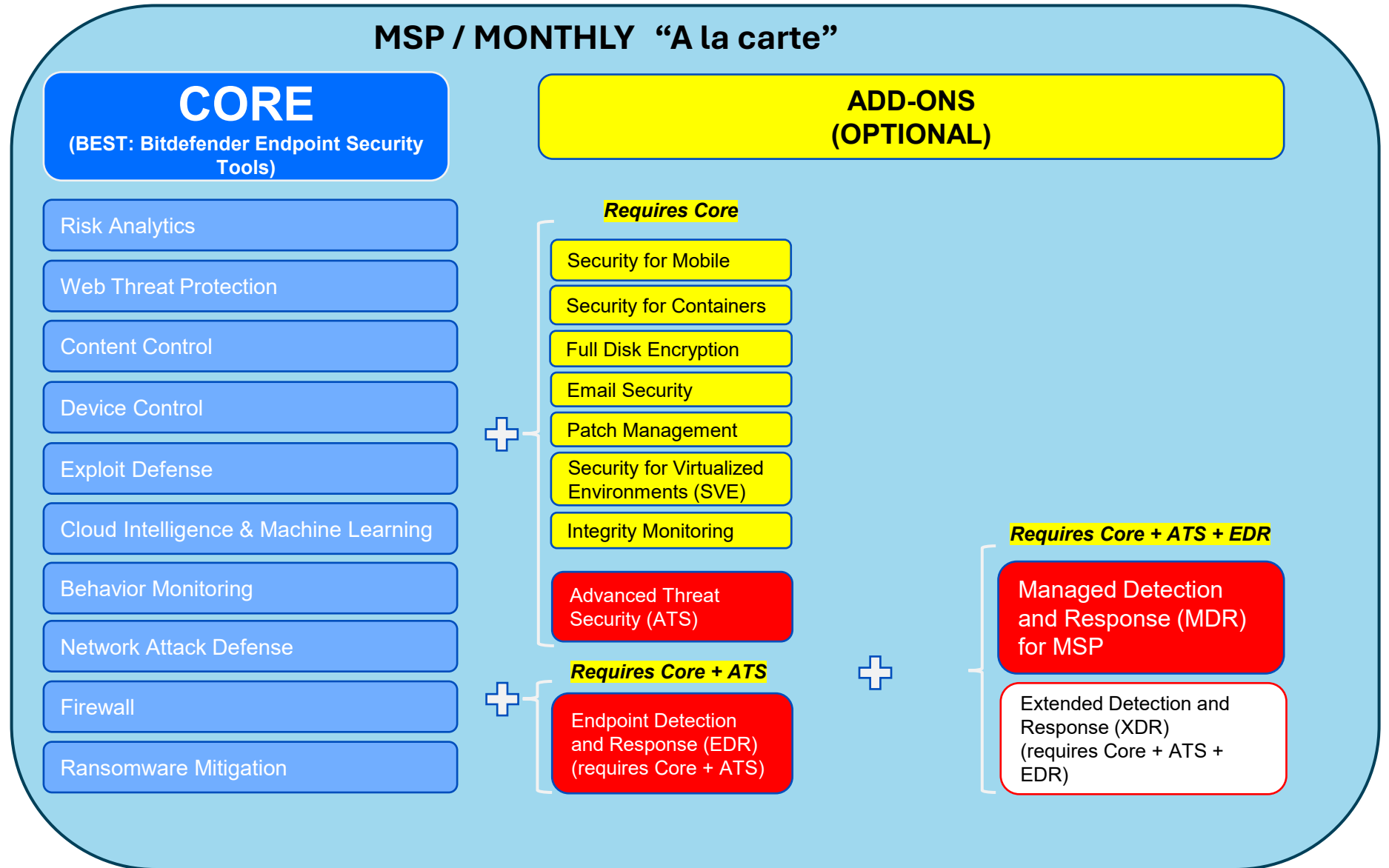
NOTE:
If a device is registered into the Gravity Zone even for just 1 sec it gets billed for the whole month.

Two types of licensing models



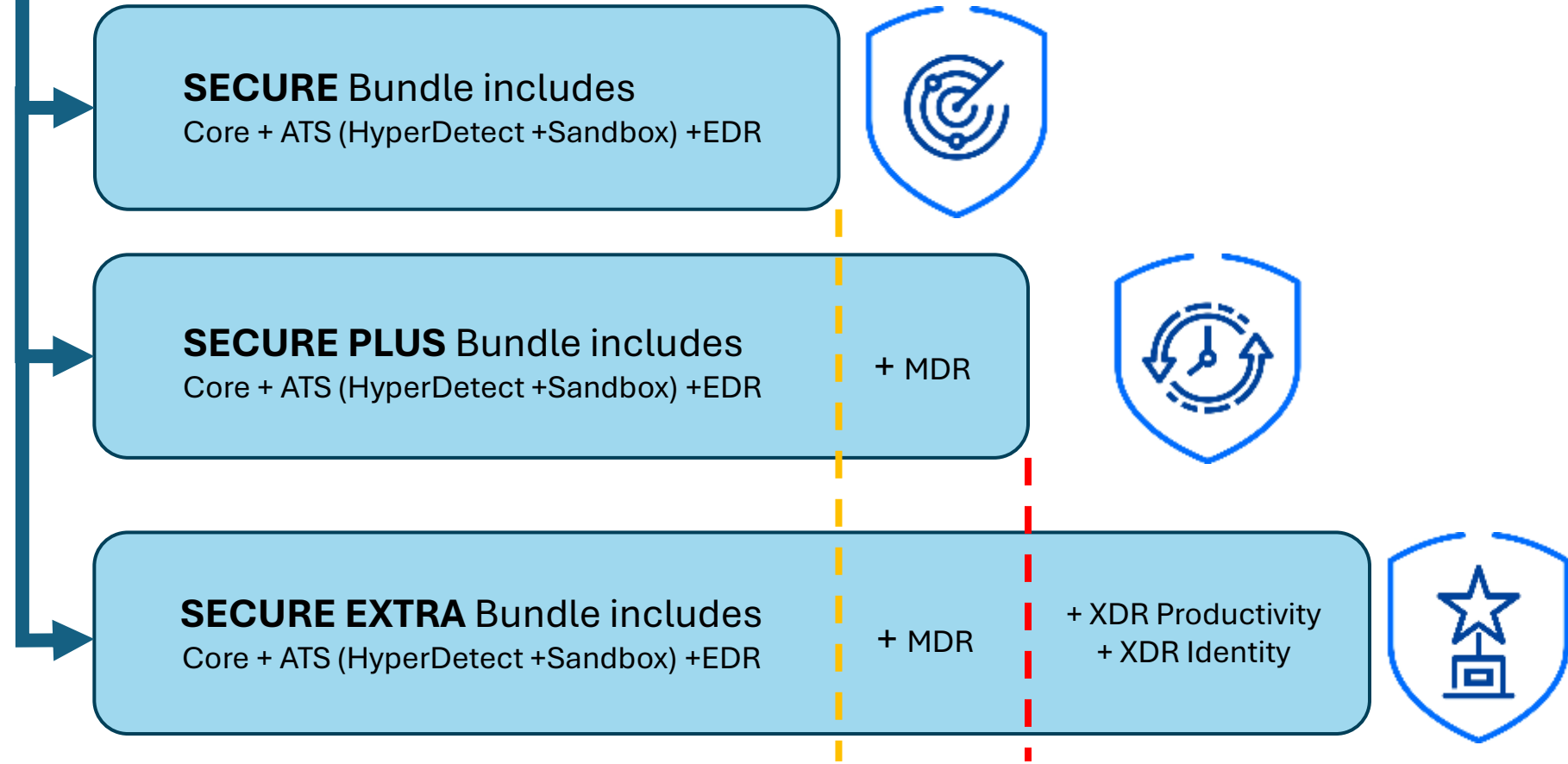
“A-la carte”

Build your
customized
security offer
from the basics



Two types of licensing models

MSP / MONTHLY Protection models / BUNDLES



ADD-ONS common to all the BUNDLES

- Patch Management
- Full Disk Encryption
- XDR Sensors (Cloud | Network | Business Apps)
- Integrity Monitoring
- Email Security
- Security for Mobile
- Security for Virtual Environments (SVE)
- Security for Containers

MSP Protection Models
- BLUEPRINT

GRAVITYZONE Cloud MSP Security Protection models

UNIFIED PREVENTION, PROTECTION, EXTENDED DETECTION AND RESPONSE

GRAVITYZONE CLOUD MSP SECURITY - SECURE EXTRA

GRAVITYZONE CLOUD MSP SECURITY - SECURE PLUS

GRAVITYZONE CLOUD MSP SECURITY - SECURE

PRODUCT PACKAGES

CAPABILITIES AND PRODUCTS

DEVICE & APPLICATION CONTROL	EXPLOIT DEFENSE	RANSOMWARE MITIGATION	INCIDENT ADVISOR	MANAGED DETECTION AND RESPONSE	EXTENDED DETECTION AND RESPONSE
ENDPOINT & USER RISK ANALYSIS	PROCESS PROTECTION	TUNABLE MACHINE LEARNING	INCIDENT VISUALIZATION	ADVISORY AND DEPLOYMENT SERVICES	XDR SENSORS • IDENTITY • PRODUCTIVITY
WEB AND CONTENT CONTROL & FILTERING	FILELESS ATTACK DEFENSE	ATTACK FORENSICS	GUIDED RESPONSE	ANOMALY DEFENSE	
	NETWORK ATTACK DEFENSE	SANDBOX ANALYSIS	LIVE SEARCH		

ADD-ON

PATCH MANAGEMENT	FULL DISK ENCRYPTION	SECURITY FOR CONTAINERS	SECURITY FOR MOBILE	EMAIL SECURITY	PREMIUM SUPPORT SERVICES	INTEGRITY MONITORING	XDR SENSORS • NETWORK • CLOUD
------------------	----------------------	-------------------------	---------------------	----------------	--------------------------	----------------------	-------------------------------------

SECURITY FUNCTIONS

PREVENTION	PROTECTION	DETECTION AND RESPONSE					
------------	------------	------------------------	--	--	--	--	--

PLATFORM AND SERVICES FUNCTIONS

DATA ANALYTICS & RETENTION	LOCAL & CLOUD MACHINE LEARNING	ANOMALY DETECTIONS	THREAT INTELLIGENCE	CONFIGURATION MANAGEMENT	VULNERABILITY IDENTIFICATION	AUTOMATION & ORCHESTRATION	DASHBOARDS & REPORTING	INTEGRATION APIs
----------------------------	--------------------------------	--------------------	---------------------	--------------------------	------------------------------	----------------------------	------------------------	------------------

SECURED ENVIRONMENTS

GRAVITYZONE PLATFORM ENDPOINT CLOUD NETWORK MOBILE IDENTITY PRODUCTIVITY								
--	--	--	--	--	--	--	--	--

Bitdefender®

ASM – Risk & Compliance Management

Compliance Manager Available Standards

Basic Standard Available at Launch

- Bitdefender Cyber Hygiene Baseline for Windows

Advanced Standards Available *

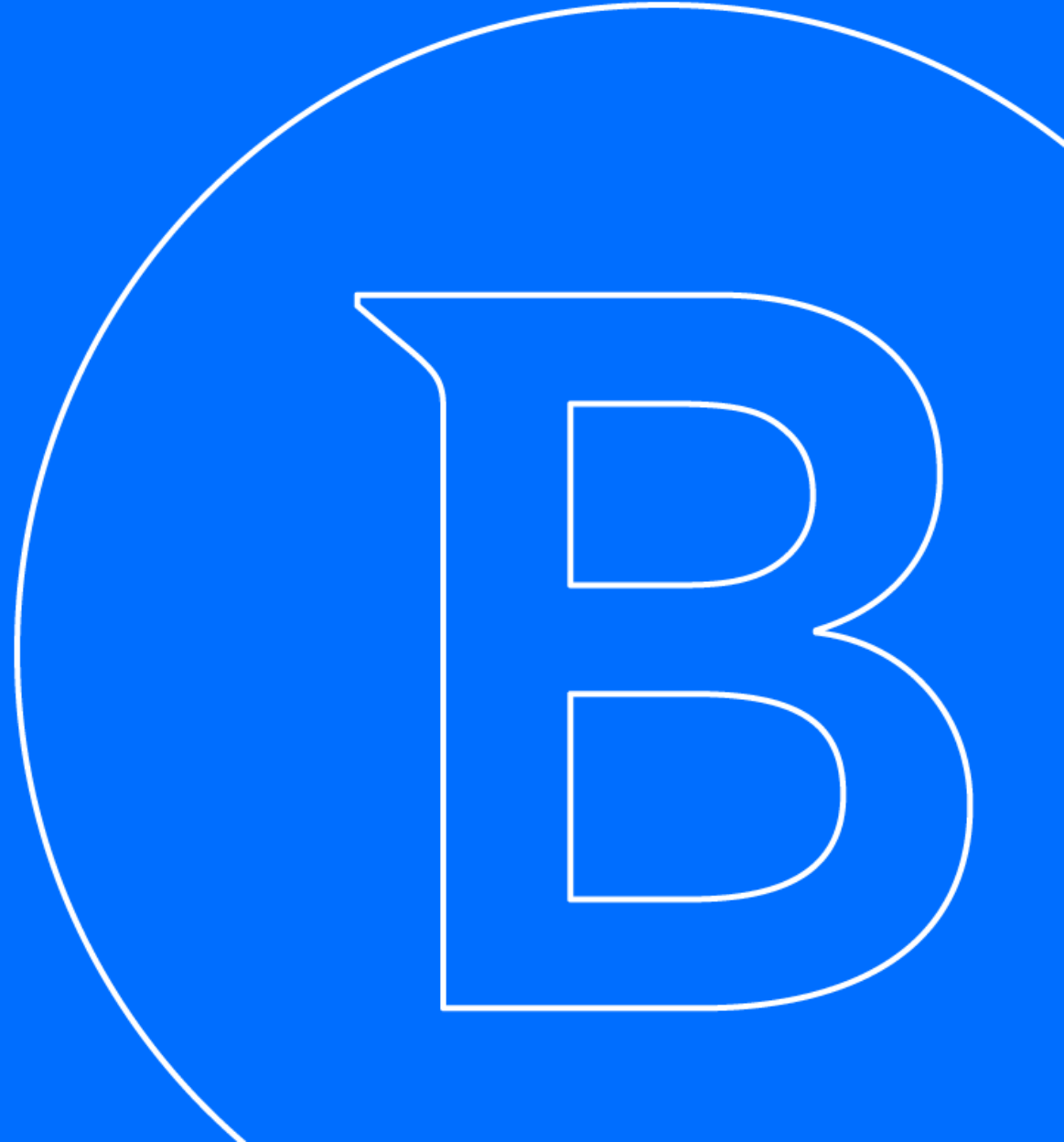
- GDPR (EU)
- DORA (EU)
- NIS 2 Directive (EU)
- CMMC 2.0 (US)
- HIPAA (US)
- CISv8
- SOC 2
- PCI DSS v4.0.1
- ISO 27001
- CyberEssential v3.2 (UK)
- Essential Eight 2023.11 (AU)



Bitdefender MDR

<< Managed Detection & Response >>

**Attackers work around the clock. And so do we.
Bitdefender MDR service provides 24x7 defense
against cyber threats.**



WHAT is Bitdefender MDR

Our global network of SOCs work when you work and cover you around the world and around the clock.

WHO are the experts you are relying to

Global Team: Security Operations Centers: North America (US-TX), Europe (RO), Asia Pacific (Singapore) ← **WHERE** are they located?

Expertise:

- 40+ SANS certifications; Incident Handling, Forensics, SIEM with Tactical Analysts, Cyber Threat Intelligence
- Cloud Admins, System Administrators, IT (education, government, healthcare)
- Global Military Background (USAF/USA, NSA, NATO)



Threat Intelligence

Researching cyber threats, geopolitical activity, and vertical-specific data trends and applies this knowledge to customer environments



24x7 Monitoring & Response

Eliminates the operational overhead of managing security alerts and events, providing tactical and strategic recommendations to reduce customer exposure to risk



Threat Hunting

Continuously monitoring the global threat landscape, using the knowledge gained to drive threat hunts across customer systems

"It is not quite equivalent to having someone... living in this environment 24/7, but it's the closest you're gonna get to an external entity, it's super comprehensive." Gartner

WHY MDR?

Bitdefender MDR directly addresses your single greatest security need – people. Hiring, training, and retaining security professionals to manage security technologies has never been more challenging – or expensive.

Skills Gap	Complexity	Alert Fatigue	Response
<p>"We have a team of 3 for security. No possible way we have eyes even 12 hours a day."</p> <p>"MDR is huge for partners coming off of traditional AV. This is where people tend to flop."</p>	<p>"If I can't get to 95% [understanding of an issue], I will probably reach out to support, which has a 2 – 4 day turnaround."</p>	<p>"My last \$h*tty day was when EDR flagged our RMM tool—we had thousands of alerts."</p> <p>"I have a calendar reminder to pop in every day to make sure there is not something burning down."</p>	<p>"When the \$h*t hits the fan, I need somewhere to go!"</p> <p>"We just kind of scramble... it's a mess."</p>
 <p>Cottingham & Butler</p>	 <p>Commerce STATE BANK Earning Relationships</p>	 <p>MOREFIELD communications SMART TECHNOLOGY DECISIONS</p>	

HOW we deliver MDR? - the technology

We rely on our award winning technology delivered through our Gravity Zone Business Security Enterprise (the most complete bundle, which includes EDR and incident data correlation)

The screenshot displays the Bitdefender GravityZone dashboard for a Security Analyst. The interface includes a left-hand navigation menu with options like Monitoring, Incidents, Threats Xplorer, and Risk Management. The main content area is titled 'INCIDENT #57' and shows a summary of an incident with a severity score of 83/100. The incident was created on May 12, 2022, and is categorized as 'Exfiltration Exploit SpearPhishing'. The summary describes a potential network breach originating from 2 users, detected through 6 alerts, affecting 2 managed assets and 2 users. A lateral movement was detected from managed asset FDWD04, involving 5 alerts and 5 managed assets. Sensitive data was exfiltrated to the IP 100.0.0.100. The dashboard also features sections for 'ORGANIZATION IMPACT' (5 endpoints, 3 users, 4 emails, 4 users, 87 documents), 'HIGHLIGHTS' (SuspiciousEmailsReceived, Initial Access vedInTransition), and 'RESPONSE' (4 endpoints to isolate, 2 emails to delete).

Bitdefender GravityZone

Welcome, Security Analyst

INCIDENT #57 | Status Open

Back | Overview | Graph | Alerts | Response

83/100 Incident Severity Score

Created: 12 May 2022, 07:21:35
Last updated: 12 May 2022, 08:49:35
Type of attack: Exfiltration Exploit SpearPhishing

SUMMARY

A potential network breach originating from 2 users, has been detected as part of 6 alerts, affecting the following: 2 managed assets, and 2 users.

Lateral Movement originating from managed asset: **FDWD04**, has been detected in your network as part of 5 alerts, affecting the following: 5 managed assets. Credentials may have been compromised on user: **it.admin**, based on alert **KerberosBruteForce**, originating from managed asset: **FDWD04**. Multiple attempts to gain or maintain the persistence of a possible malicious objects were detected in 3 alerts, on 3 managed assets. Sensitive data may have been exfiltrated to external ip: **100.0.0.100**, based on 5 alerts, originating from 3 managed assets.

ORGANIZATION IMPACT

5 3 4 4 87

HIGHLIGHTS

- SuspiciousEmailsReceived** | Initial Access vedInTransition
Severity: Low
A chain of suspicious emails has been received. This indicates that one e-mail account might have been compromised and further used to send potentially malicious e-mails to other members of the organisation.
Detected by sensor: Endpoint on 12 May 2022 at 07:23:16
1 2
+ 6 OTHER INITIAL ACCESS ALERTS
- Exploit NRPC CVE-2020-1472 ZeroLogon** | Lateral Movement

RESPONSE

Last updated 8:43:40

ACTION NEEDED (6) EXECUTED

CONTAINMENT

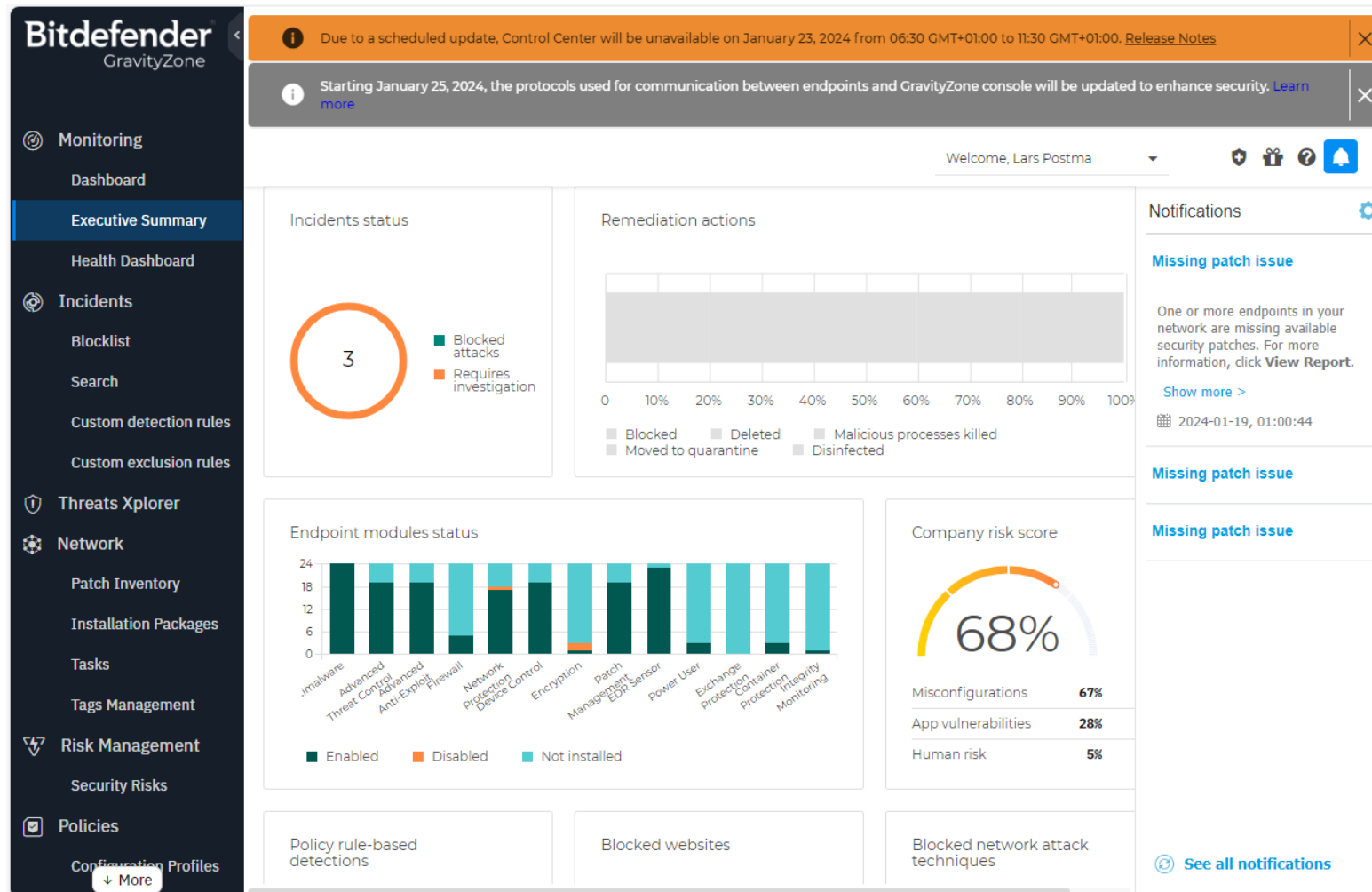
4 Endpoints to isolate
[VIEW DETAILS](#)

REMEDIATION

2 Emails to delete
[VIEW DETAILS](#)

HOW we deliver MDR? - the technology

We rely on our award winning technology delivered through our [Gravity Zone Business Security Enterprise](#) (the most complete bundle, which includes EDR and incident data correlation)



The ultimate solution for protecting your endpoints:

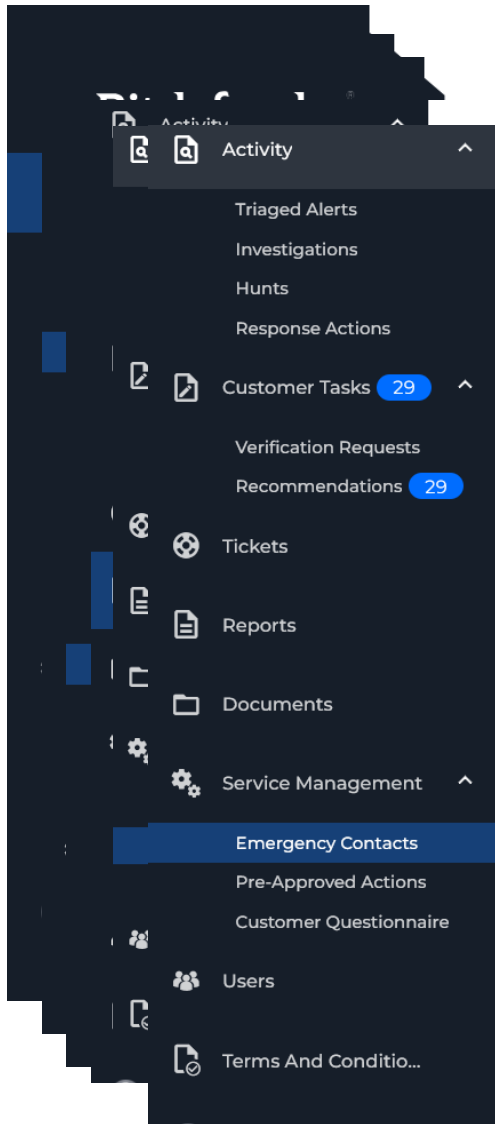
- Advanced Prevention
- Extended Detection
- Effective Response
- Risk Analytics.
- Designed to address the entire threat lifecycle.
- Combines the world's most effective endpoint protection platform with Endpoint Detection and Response (EDR)
- **(Threat Detection) Visibility to the Bitdefender MDR Team.**

HOW we deliver MDR? - the technology

We rely on our award winning technology delivered through our Gravity Zone Business Security Enterprise (the most complete bundle, which includes EDR and incident data correlation)

The screenshot displays the Bitdefender GravityZone console interface. On the left is a dark sidebar with navigation options: Monitoring, Dashboard, Executive Summary, Incidents (highlighted), Blocklist, Search, Custom Rules, Threats Xplorer, Network, Patch Inventory, Packages, Tasks, Risk Management, and Security Risks. The main content area shows an incident overview for Incident #57, which is currently 'Open'. The incident severity score is 83/100. The incident was created on May 12, 2022, at 07:21:35 and last updated at 08:49:00. The attack type is categorized as Exfiltration, Exploit, and SpearPhishing. The summary states that a potential network breach originating from 2 users was detected as part of 6 alerts, affecting 2 managed assets and 2 users. A lateral movement originating from managed asset FDWD04 was detected in 5 alerts, affecting 5 managed assets. Credentials may have been compromised on user it.admin, based on alert KerberosBruteForce, originating from managed asset FDWD04. Multiple attempts to gain or maintain the persistence of a possible malicious objects were detected in 3 alerts, on 3 managed assets. Sensitive data may have been exfiltrated to external ip: 100.0.0.100, based on 5 alerts, originating from 3 managed assets. The organization impact shows 5 endpoints, 3 users, 4 emails, 4 users, and 87 documents affected. The response section shows 6 actions needed, with 4 endpoints to isolate and 2 emails to delete. Two highlights are shown: 'SuspiciousEmailsReceivedInTransition' (Initial Access) with a severity of Low, and 'Exploit NRPC CVE-2020-1472 ZeroLogon' (Lateral Movement).

HOW we deliver MDR? - the portal to the experts



Emergency Contacts

ADD NEW | 5 items

The Emergency Contacts page displays four contact cards in a 2x2 grid. Each card includes a profile picture, name, title, email, phone number, location, and time zone.

ID	Name	Title	Email	Phone	Location	Time Zone
# 1	ROY	Decision maker	rcorrea@bitdefender.com	951-555-1515	San Diego	(UTC - 08:00) Pacific Time (US & Canada)
# 2	DAVID LEEMAN	Security Analyst	dleeman@acmecorp.com	4043585549	San Diego, CA	(UTC - 08:00) Pacific Time (US & Canada)
# 3	CHRIS MCDONALD	IT Analyst	cmcdonald@acmecorp.com	9123853647	Miami, FL	(UTC - 05:00) Eastern Time (US & Canada), Bo...
# 4	DANIEL HÂNGAN	Decision maker	dhangan+acme@bitdefender.com	0742000000	Romania, Bucuresti, Sector 3, Drumul Gur...	(UTC + 02:00) Athens, Bucharest, Amman, Cair...



We will provide you also **MDR Portal** in which you can:

- see all the activity our security analyst are conducting,
- have reports,
- share files,
- open tickets,
- see recommendations
- and also manage you predefined actions and their exceptions.
- ...



Thank you!