

Bitdefender®

Bitdefender GravityZone XDR

Nuria Galvez

Sr Sales Engineer, Iberia

Introduction by:

Massimo Lucarelli

Director, Sales Engineering EMEA



Agenda

- Defender's Challenges
- What is XDR?
- Reducing Dwell Time to fight off Attacks
- How Bitdefender helps

Defender's Challenges

The attack surface
is expanding



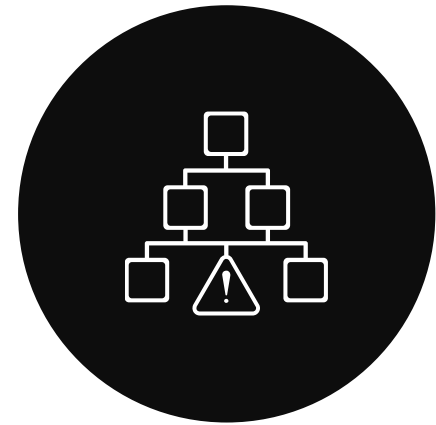
Security teams need comprehensive visibility from endpoint to cloud, across identities, application and network

Attackers are becoming
more sophisticated



Preventative controls are key, but must be augmented with detection & response

Too many alerts overwhelm
under-resourced teams



Skilled analysts are in short supply, and teams struggle to effectively combat threats

The Flood of Data Can Be **Overwhelming**

The need for visibility drives organizations to add more security tools



Identity - IAM



Email Security



Endpoint - EPP/EDR

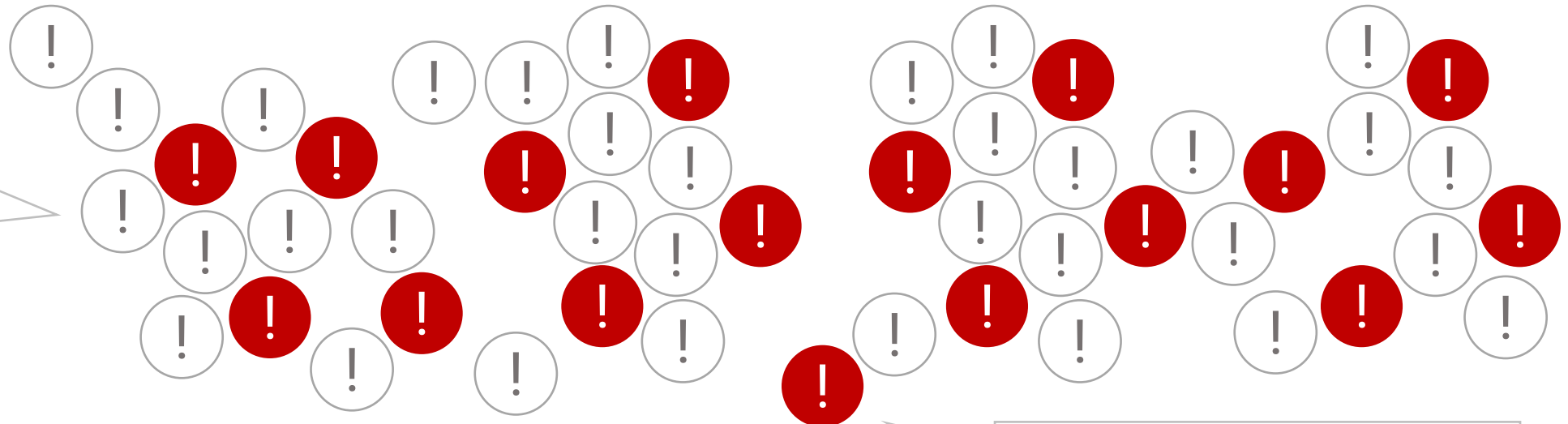


Cloud Security



Network - NDR

But too much data from disparate sources can obfuscate real threats



Manual correlation and analysis make it **NEARLY IMPOSSIBLE** to respond in time and prevent breaches

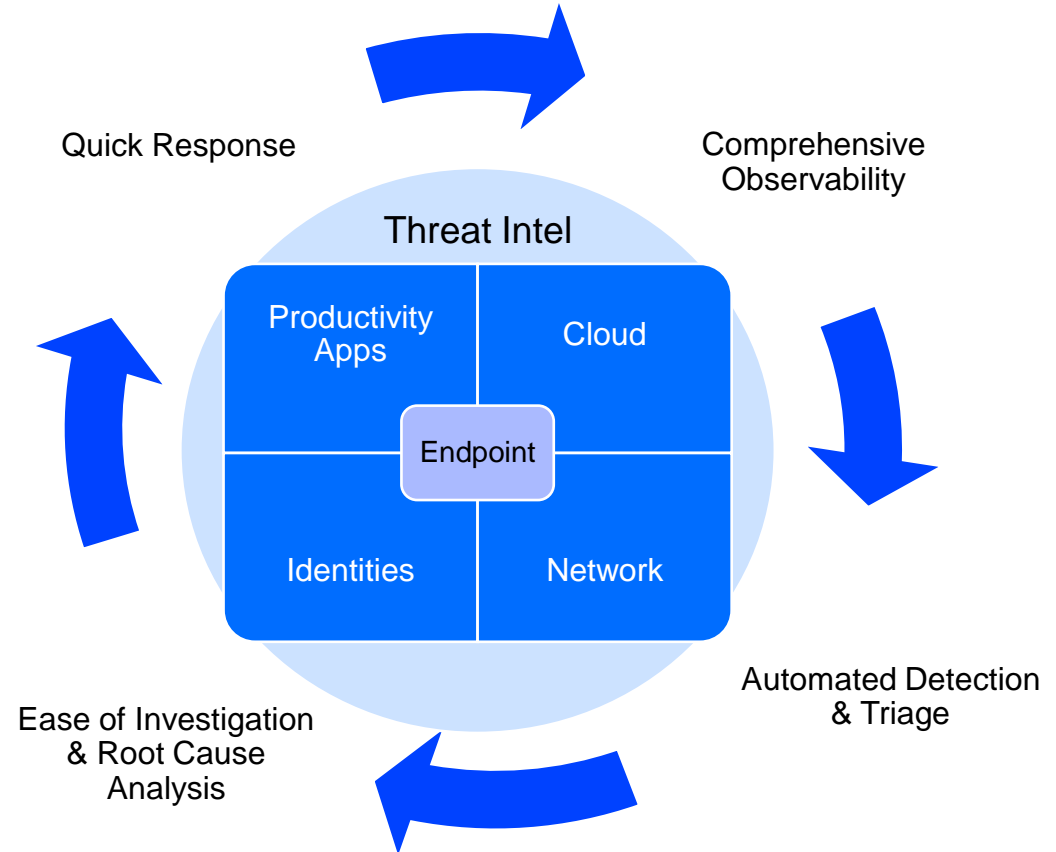
Reduce Risk with Prevention, Detection & Response



Bitdefender[®]

What is XDR?

The **evolution of EDR**, which provides more efficient and effective threat **detection, investigation and response** in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools to enable organization to **identify threats, understand the full impact, find the root cause and take immediate response to minimize business damage.**

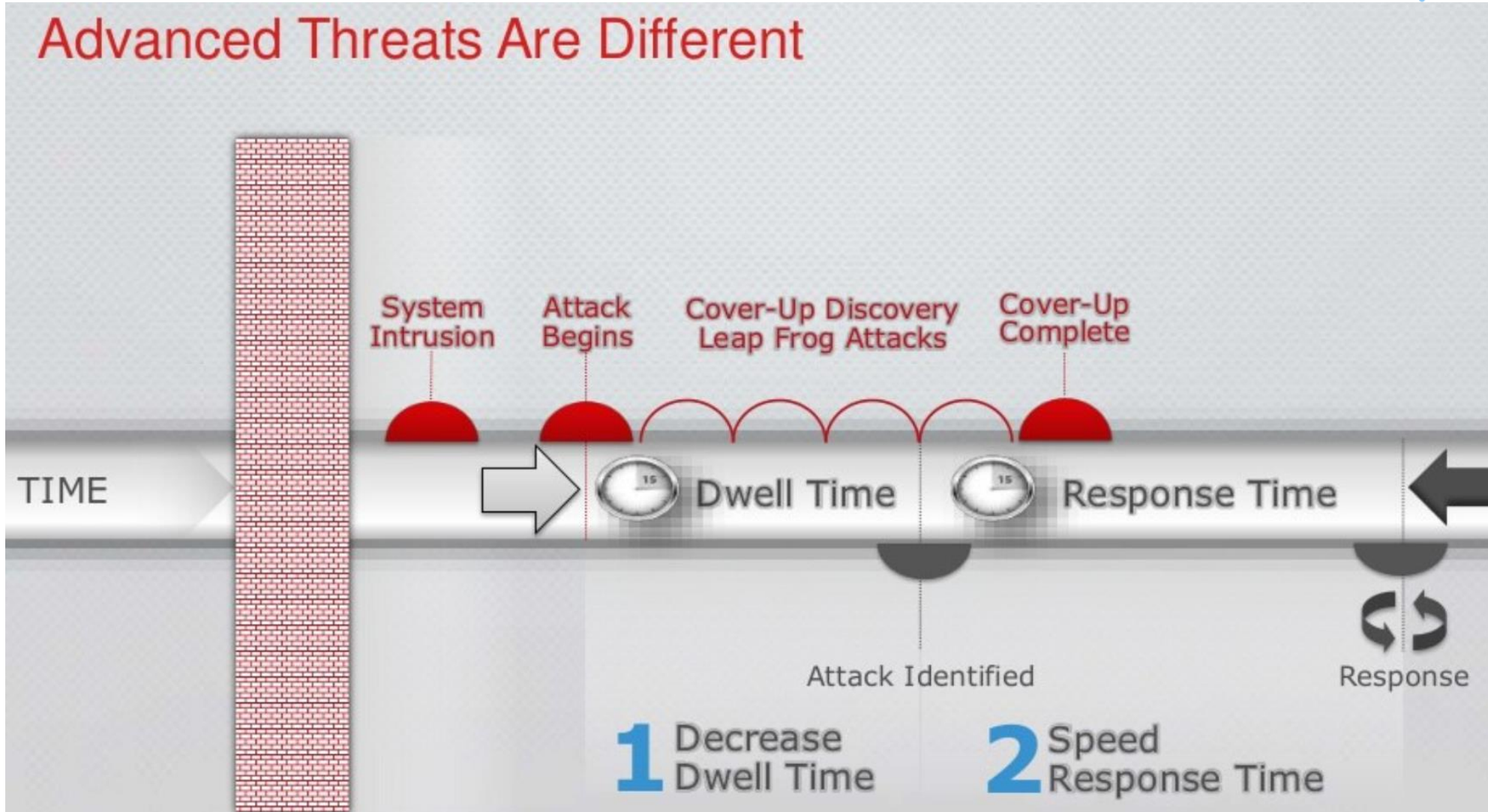


In a hyperconnected world where cyber attackers seek to do harm 24x7 and organizations face unpredictable risk, becoming resilient is the goal. This is where XDR comes in.

Bitdefender[®]

Reducing Dwell Time to fight off Attacks

Reducing Dwell Time matters



Tackling the Pyramid of Pain

- ATT&CK Reflects tactics and techniques observed in the real world
- Why is this important?
 - Industry historically focused on methodology that is low on the pyramid
 - Forces adversary to change tools and behavior to avoid detection
 - Lowers their ROI
 - For the Defender:
 - Behavior focused detection > artifact focused detection
 - ATT&CK based hunting

What to search? David Bianco's pyramid of pain



<http://detect-respond.blogspot.mx/2013/03/the-pyramid-of-pain.html>

MITRE ATT&CK: Sample Threat Model

about
Sample Threat Model

filters
Windows, Linux, macOS
act

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Internal Spearphishing	Clipboard Data	Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Destruction
Exploit Public-Facing Application	PowerShell	Registry Run Keys / Startup Folder	Bypass User Access Control	Bypass User Access Control	Password Cracking	Local Account	Remote Services	Input Capture	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Data Encrypted for Impact
Phishing	Windows Command Shell	Boot or Logon Initialization Scripts	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Domain Account	Remote Desktop Protocol	Keylogging	DNS	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Disk Wipe
Spearphishing Attachment	Unix Shell	Logon Script (Windows)	Token Impersonation/Theft	Token Impersonation/Theft	Credentials from Web Browsers	Email Account	SSH	Screen Capture	Dynamic Resolution	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Disk Content Wipe
Spearphishing Link	Visual Basic	Create or Modify System Process	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Hide Artifacts	Application Window Discovery	VNC	Video Capture	Fast Flux DNS	Exfiltration Over C2 Channel	Disk Structure Wipe
Valid Accounts	JavaScript/JScript	Windows Service	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Hidden Files and Directories	Browser Bookmark Discovery	Software Deployment Tools		Encrypted Channel		Inhibit System Recovery
Default Accounts	Exploitation for Client Execution	Hijack Execution Flow	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	OS Credential Dumping	File and Directory Discovery	Use Alternate Authentication Material		Asymmetric Cryptography		Resource Hijacking
Domain Accounts	Inter-Process Communication	DLL Search Order Hijacking	Logon Script (Windows)	Logon Script (Windows)	Input Capture	Network Service Scanning	Pass the Hash		Ingress Tool Transfer		Service Stop
Local Accounts	Dynamic Data Exchange	Scheduled Task/Job	Create or Modify System Process	Create or Modify System Process	Keylogging	Network Share Discovery	Pass the Ticket		Non-Standard Port		System Shutdown/Reboot
	Native API	Scheduled Task	Windows Service	Disable or Modify System Firewall	Network Sniffing	Network Sniffing			Protocol Tunneling		
	Scheduled Task/Job	Valid Accounts	Exploitation for Privilege Escalation	Indicator Removal on Host	LSASS Memory	Permission Groups Discovery			Proxy		
	Scheduled Task	Default Accounts	Hijack Execution Flow	Clear Windows Event Logs	LSA Secrets	Domain Groups			External Proxy		
	Software Deployment Tools	Domain Accounts	DLL Search Order Hijacking	Clear Command History	Unsecured Credentials	Local Groups			Remote Access Software		
	System Services	Local Accounts	Process Injection	File Deletion	Credentials in Files	Process Discovery			Web Service		
	Service Execution		Dynamic-link Library Injection	Masquerading		Query Registry			Dead Drop Resolver		
	User Execution		Portable Executable Injection	Masquerade Task or Service		Remote System Discovery			Bidirectional Communication		
	Malicious Link		Scheduled Task/Job	Match Legitimate Name or Location		Software Discovery					
	Malicious File		Scheduled Task	Modify Registry		System Information Discovery					
			Valid Accounts	Obfuscated Files or Information		System Network Configuration Discovery					
			Default Accounts	Software Packing		System Network Connections Discovery					
			Domain Accounts	Process Injection		System Owner/User Discovery					
			Local Accounts	Dynamic-link Library Injection		Virtualization/Sandbox Evasion					
				Portable Executable Injection		System Checks					
				Signed Binary Proxy Execution		User Activity Based Checks					
				Rundll32		Time Based Evasion					
				Compiled HTML File							
				CMSTP							
				Regsvr32							
				Msiexec							
				Odbcconf							
				Subvert Trust Controls							
				Code Signing							
				Use Alternate Authentication Material							
				Pass the Hash							
				Pass the Ticket							
				Valid Accounts							
				Default Accounts							
				Domain Accounts							
				Local Accounts							
				Virtualization/Sandbox Evasion							
				System Checks							
				User Activity Based Checks							
				Time Based Evasion							
				XSL Script Processing							

Bitdefender[®]

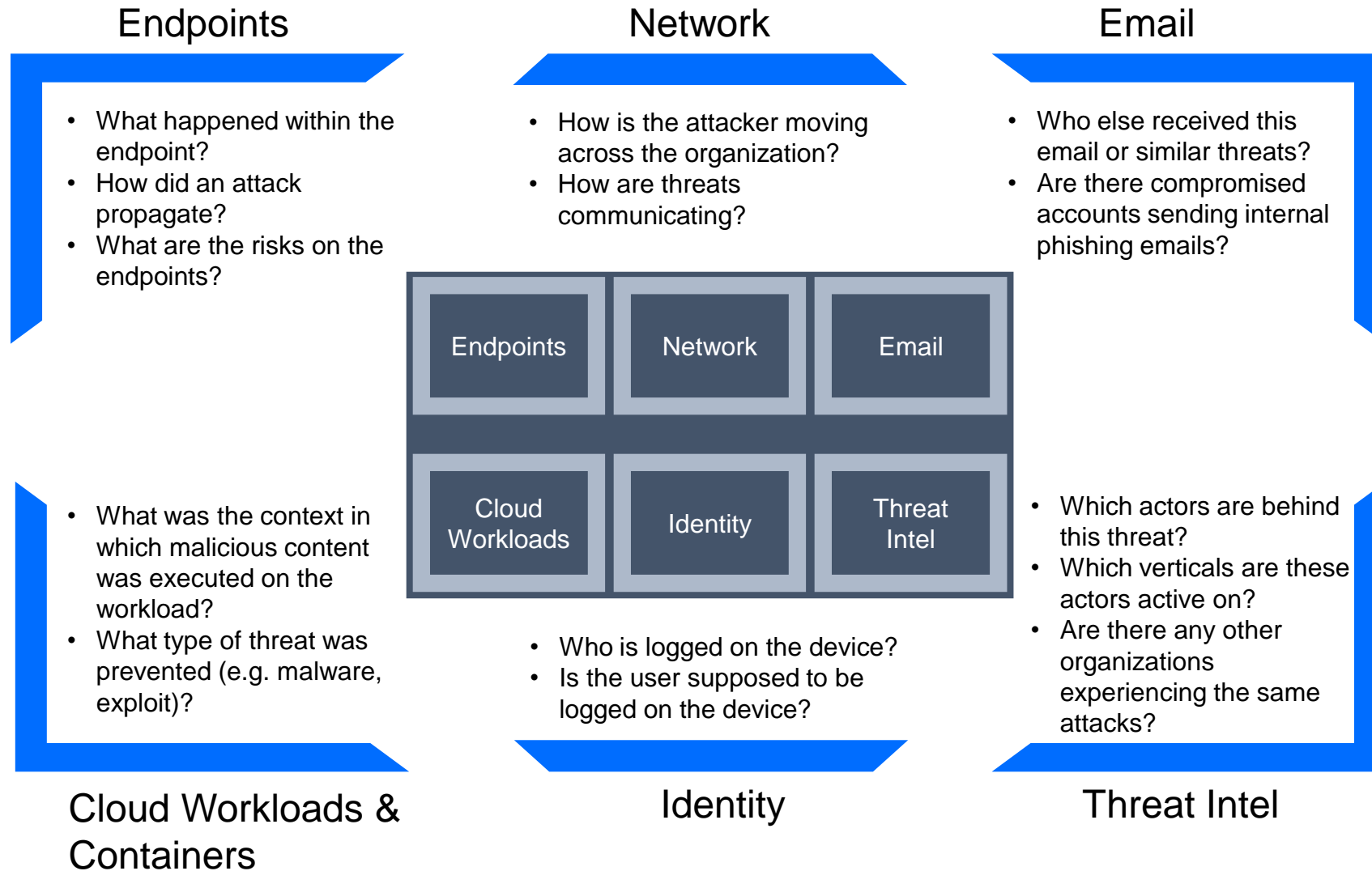
Bitdefender

How Bitdefender helps

XDR Concepts

eXtended Detection and Response

Bitdefender®



Bitdefender[®]

Bitdefender XDR Core Capabilities

Executive Summary

Bitdefender®

XDR evolves EDR cybersecurity capabilities and out-of-the-box fulfills the incident responders' needs to integrate additional telemetry sources, deliver contextualized security incidents and more comprehensive response capabilities.

Customer problems solved with XDR

Efficacy of detections

XDR detections are based around the endpoint and correlated with other telemetry sources where business data is stored and accessed

Speed of investigation

XDR extends investigation capabilities by building an automate root cause analysis across integrated telemetry sources within the entire organization

Completeness of response

XDR extends response capabilities outside of EDR to provide both endpoint and non-endpoint response recommendations and swift response actions

XDR CORE CAPABILITIES

Collect

Detect

Correlate

Visualize

Investigate

Respond

GA Features

- Endpoint
- Network
- Identity
- Cloud

- Endpoint
- Non-endpoint
- Anomalies

- Extended Root-cause analysis
- Multiple sources within the organization

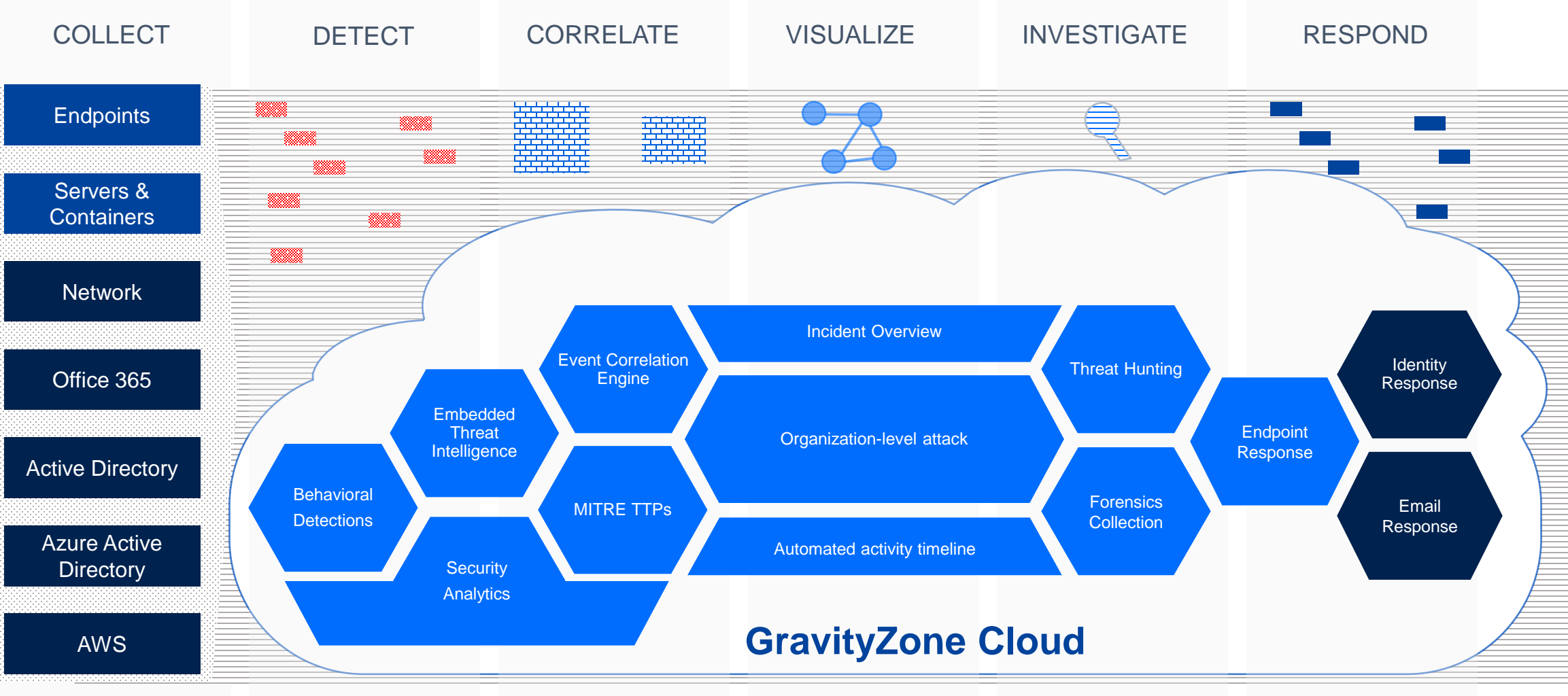
- Extended Incident Overview
- Extended Incident Graph

- Investigation Package
- New Search

- Endpoint Response
- Full Remote Shell
- O365 Response
- AD Response

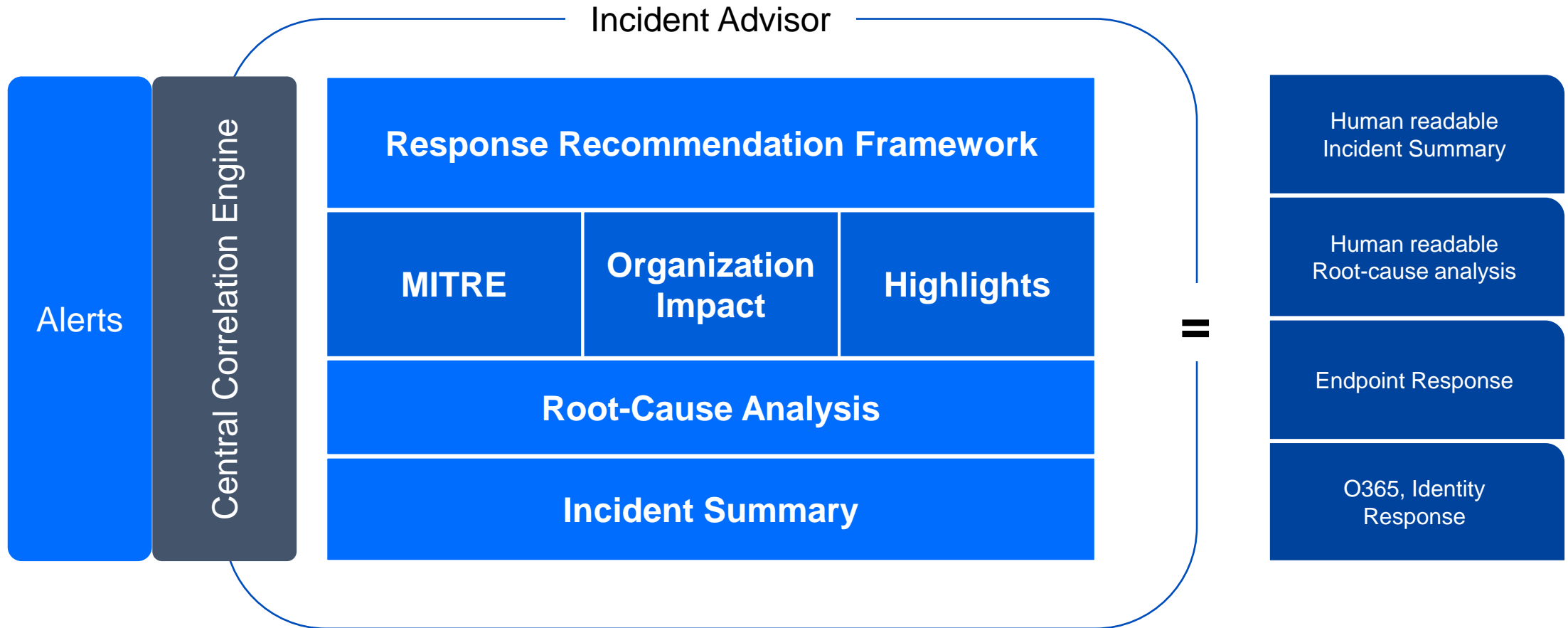
GravityZone XDR

Enabled via licensing add-on



**Visualize, Investigate,
Response**

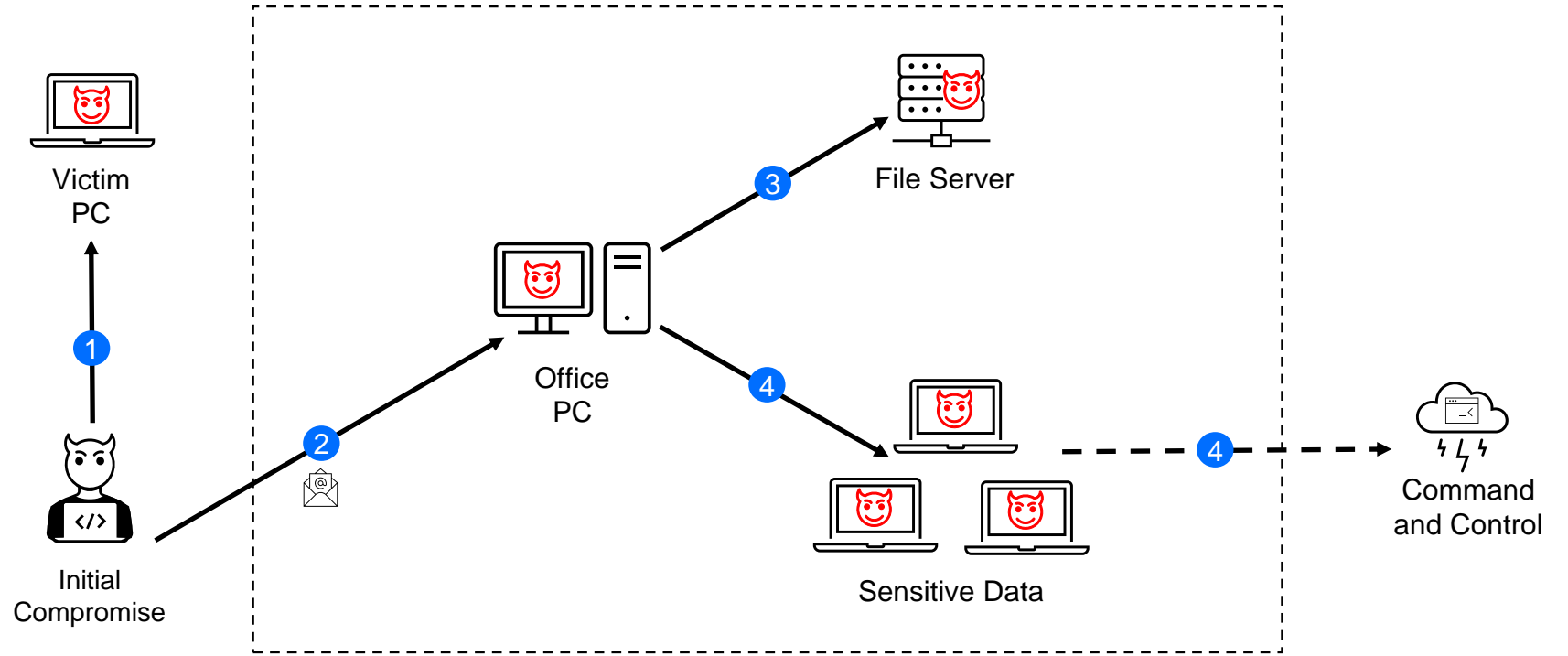
Incident Advisor



XDR Scenario

Sensors

- EDR
- Office365
- Active Directory



- 1 M365 Compromise
- 2 Lateral Movement

- 3 Ransomware Deployment
- 4 Data Exfiltration

XDR Data Sources (GA)

Bitdefender[®]

Microsoft Office365

- ✓ OneDrive
- ✓ SharePoint
- ✓ MS Teams
- ✓ Email

Active Directory

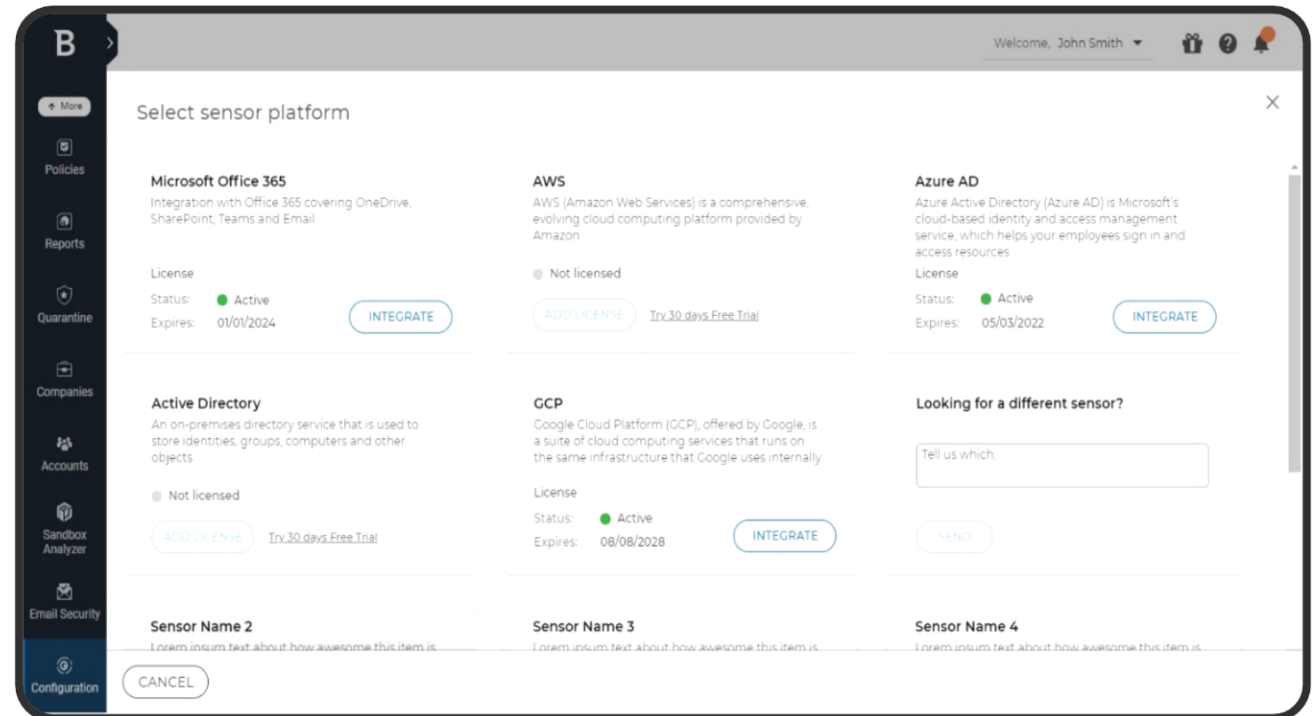
- ✓ On-premises AD
- ✓ Azure AD

Clouds

- ✓ AWS

Network

- ✓ Bitdefender Network Sensor



Detection & Response (GA)

Bitdefender®

Incident Advisor

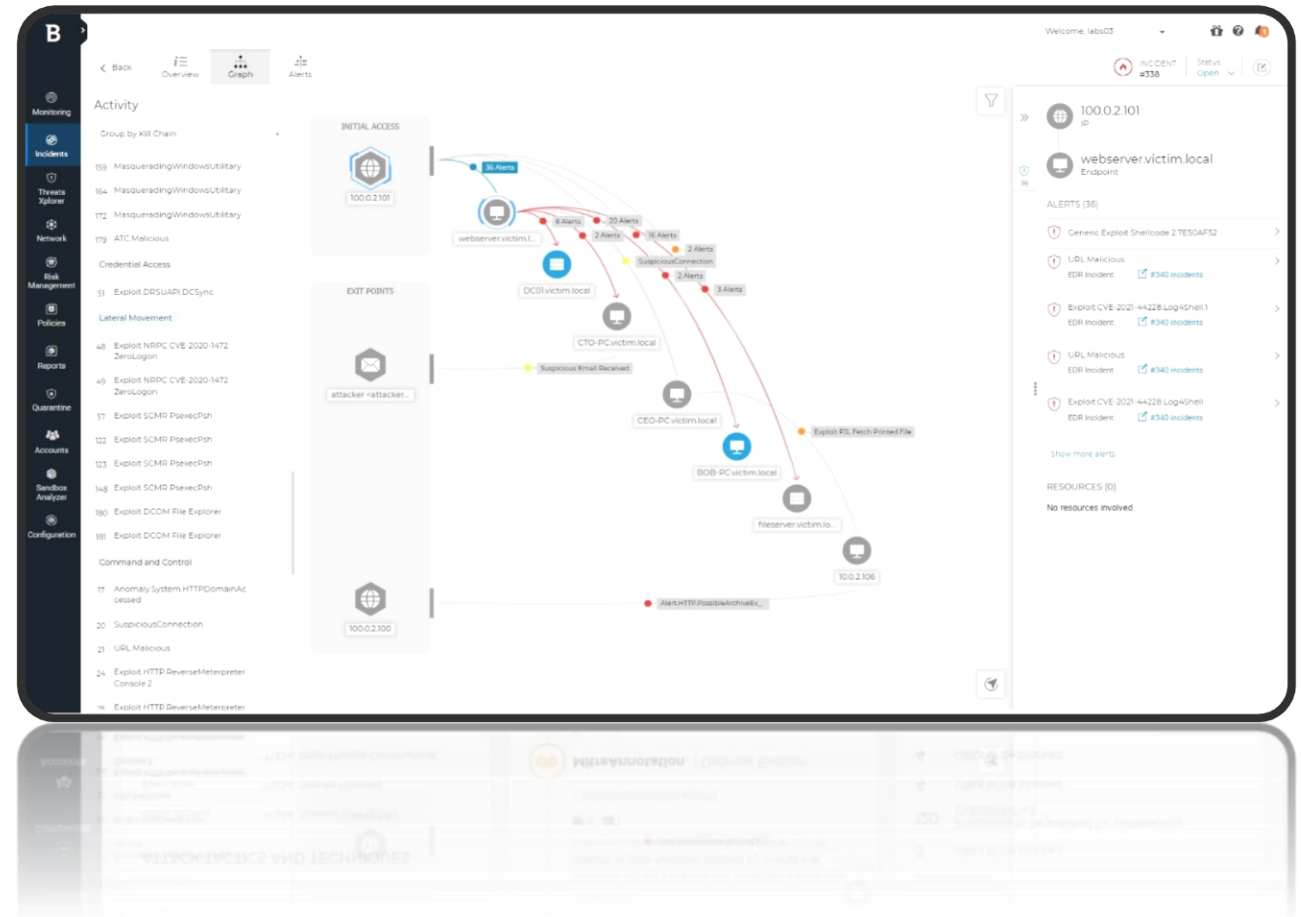
- ✓ Summary
- ✓ Root Cause
- ✓ Organization Impact
- ✓ Highlights

Response

- ✓ Recommendations
- ✓ Endpoint
- ✓ Office365
- ✓ Identity
- ✓ List of Executed actions

New Graph

- ✓ Initial Access
- ✓ Exit Points
- ✓ Multiple Resource types
- ✓ Alerts on Transitions



Investigation (GA)

Historic Search

- ✓ Advanced filtering
- ✓ Enhanced data display
- ✓ Multiple data sources
- ✓ Smart views

Investigation Package

- ✓ Collect forensic endpoint data
- ✓ OS: Windows, Linux, Mac

Full Remote Shell

- ✓ Direct investigation & response across endpoints
- ✓ OS: Windows, Linux, Mac

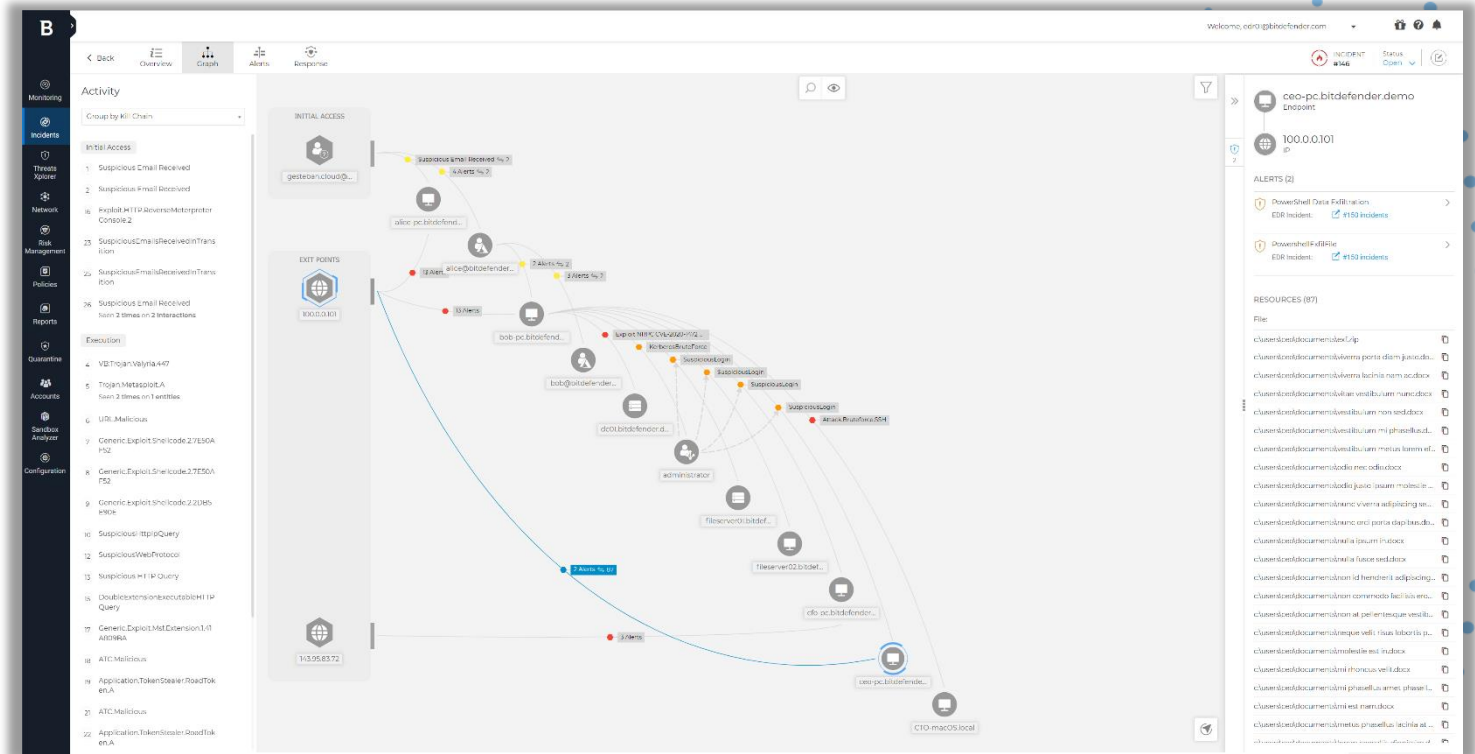
The screenshot displays the Bitdefender investigation interface. On the left is a navigation sidebar with options like Dashboard, Incidents, Threats Explorer, Network, Risk Management, Policies, Reports, Quarantine, and Companies. The main area shows a search results page for the query: `process.parent_path: *explorer.exe AND process.path: *cmd.exe`. The results are presented in a table with columns for Date, Source, Event, Detection name, Type, Score, Timestamp, MITRE tactics, and MITRE techniques. The table contains 10 rows of data, all with a score of 1 and a timestamp of 16305074... The event types are a mix of 'Raw event' and 'Alert'. The detection names are 'ctc_raw_pr...' and 'ctc_raw_proce...'. The source for all events is 'hr-ro_0987'. The table also includes a 'Back to top' link and a 'LOAD MORE 250' button.

Date	Source	Event	Detection name	Type	Score	Timestamp	MITRE tactics	MITRE techniq...
25 Aug 2021, 10:27	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
24 Aug 2021, 01:18	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Alert	1	16305074...	Execution	Command and s...
23 Aug 2021, 02:51	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
22 Aug 2021, 11:34	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Alert	1	16305074...	Execution	Command and s...
21 Aug 2021, 06:57	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
20 Aug 2021, 11:23	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
19 Aug 2021, 02:12	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
19 Aug 2021, 02:12	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...
18 Aug 2021, 16:11	hr-ro_0987	ctc_raw_pr...	ctc_raw_proce...	Raw event	1	16305074...	Execution	Command and s...

GravityZone XDR

Combines advanced threat protection with **out-of-the-box analytics** and **rich security context** for correlation of disparate alerts, **quick triage** of incidents and attack containment through **automated and guided response**.

GravityZone exposes the **full scope of the attack** by connecting incidents over time and delivering deeper context through automated evidence collection and **root cause analysis** across endpoint, cloud, identity, network and productivity application data.



GravityZone XDR is a cloud delivered product for organizations that want to run the technology in house. For organizations looking for a managed service, Bitdefender MDR, leveraging GravityZone XDR, keeps organizations safe with 24x7 security monitoring plus targeted and risk-based threat hunting by a certified team of security experts.

The image features the Bitdefender logo centered on a black background. The logo consists of the word "Bitdefender" in a white, bold, sans-serif font, with a registered trademark symbol (®) to its upper right. Below it, the tagline "BUILT FOR RESILIENCE" is written in a smaller, white, all-caps, sans-serif font. The background is decorated with a pattern of small, light blue dots arranged in a grid that appears to be slightly distorted or curved, creating a sense of depth and movement.

Bitdefender[®]
BUILT FOR RESILIENCE