Bitdefender

Bitdefender GravityZone XDR

Nuria Galvez
Sr Sales Engineer, Iberia

Introduction by:
Massimo Lucarelli
Director, Sales Engineering EMEA

Bitdefender

Agenda

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

Defender’s Challenges

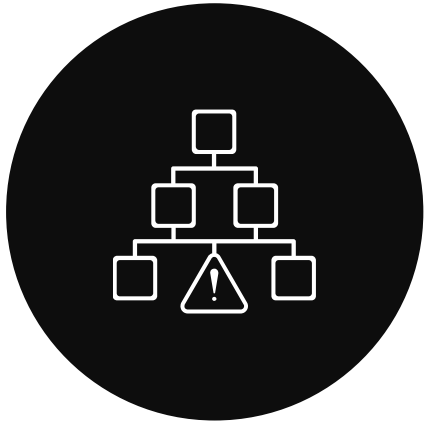
The attack surface is expanding

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

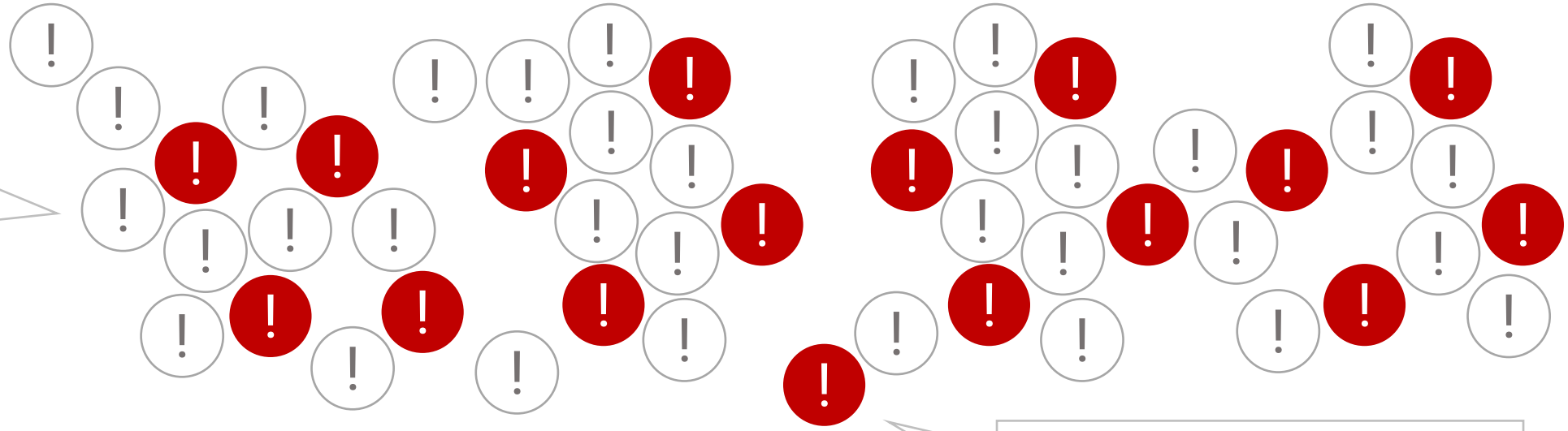
Email Security

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

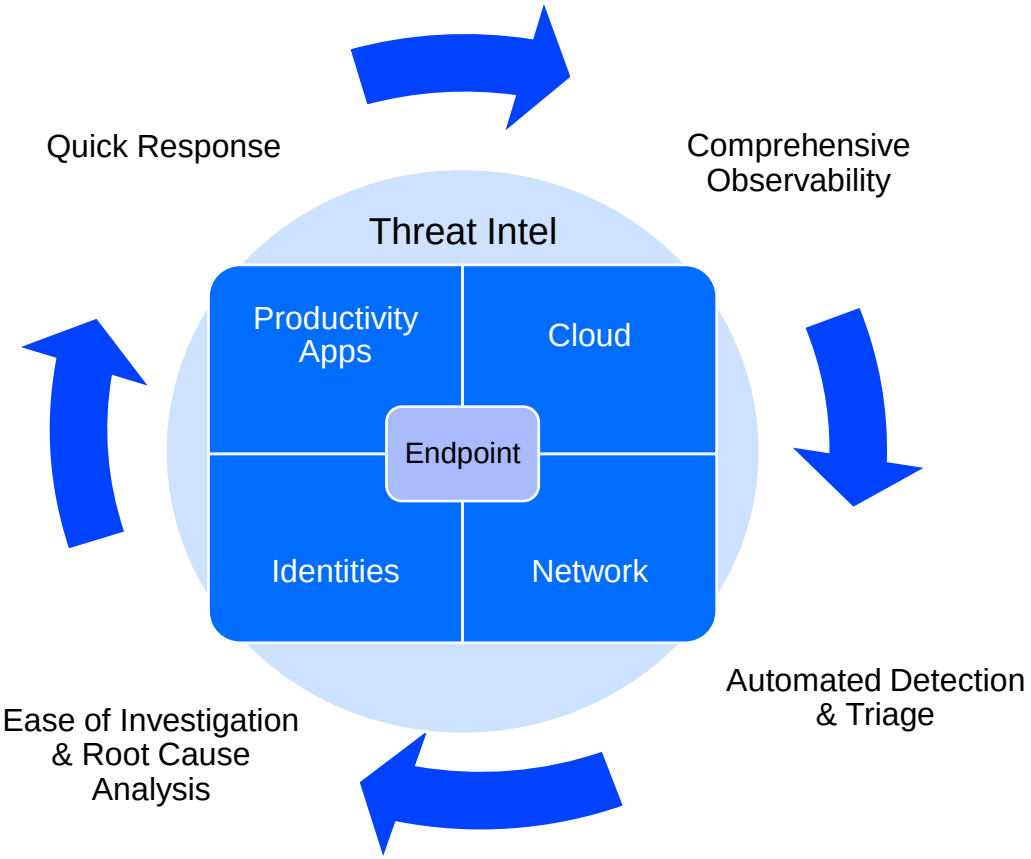
Reduce Risk with Prevention, Detection & Response

Bitdefender

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**.



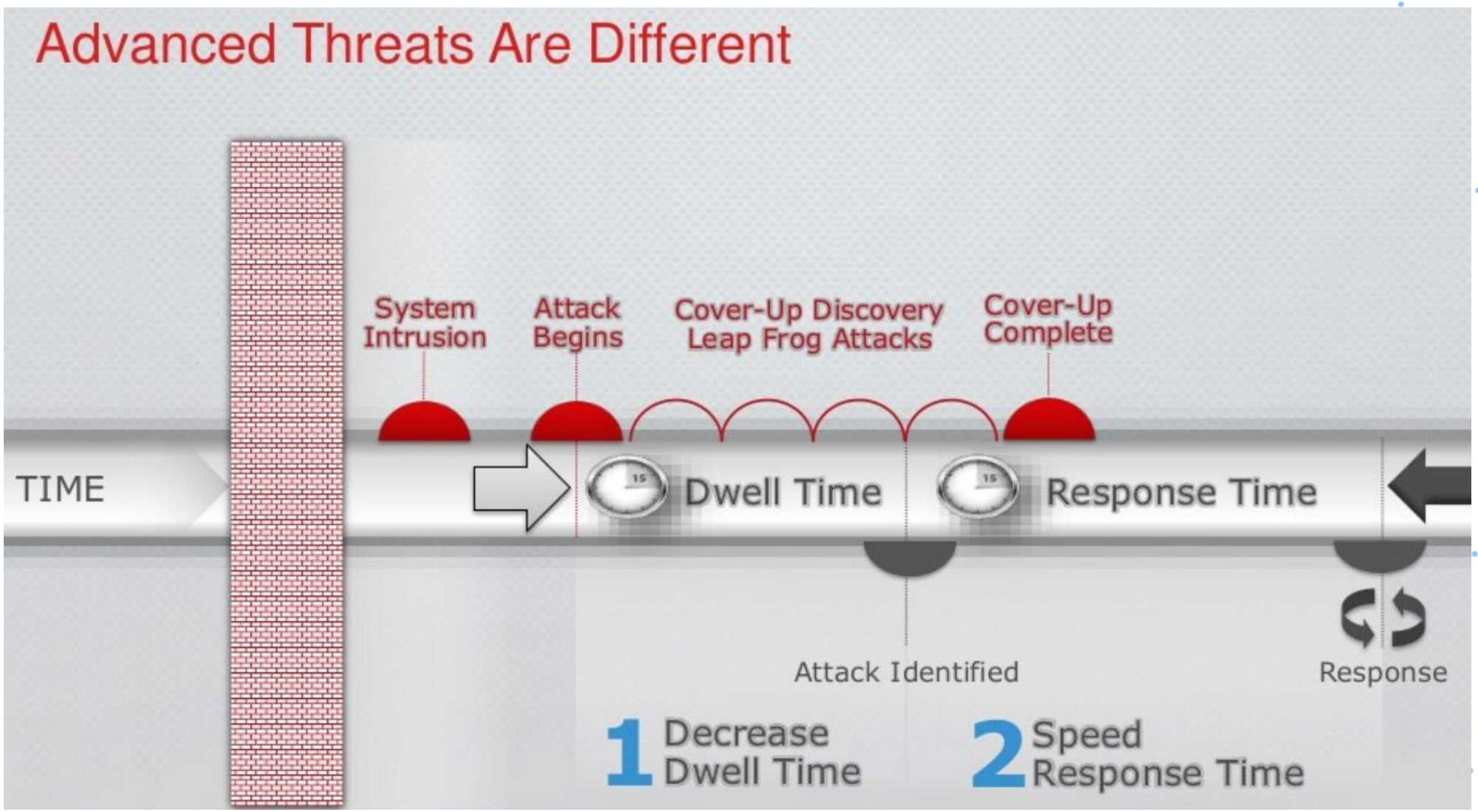
In a hyperconnected world where cyber attackers seek to do harm 24x7 and organizations face unpredictable risk, becoming resilient is the goal. This is where XDR comes in.

Bitdefender

Reducing Dwell Time to fight off Attacks

Reducing Dwell Time matters

Bitdefender



Tackling the Pyramid of Pain

Bitdefender

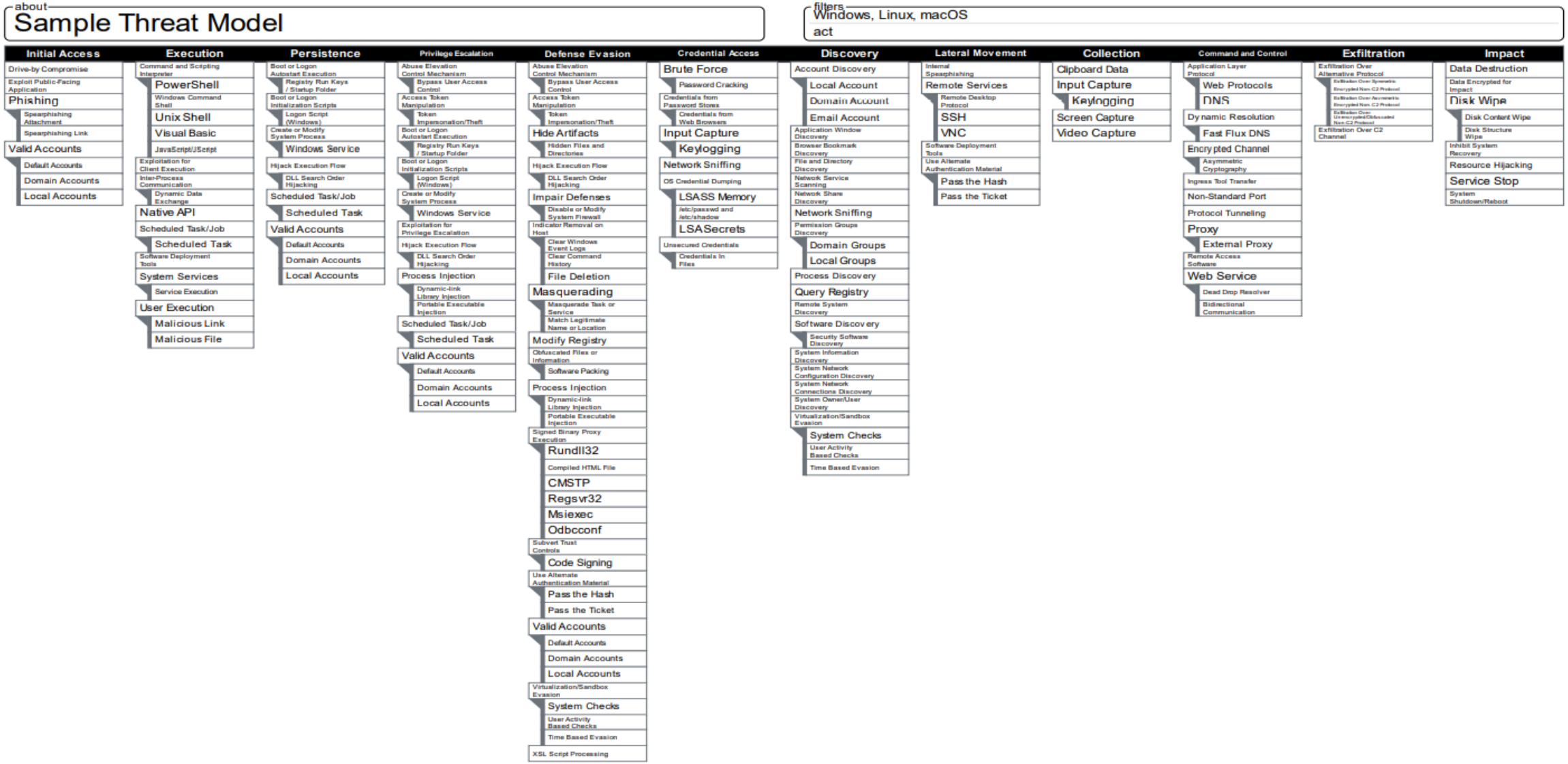
- ATT&CK Reflects tactics and techniques observed in the real world
- Why is this important?
  - Industry historically focused on methodology that is low on the pyramid
  - Forces adversary to change tools and behavior to avoid detection
    - Lowers their ROI
  - For the Defender:
    - Behavior focused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

Bitdefender



Bitdefender

How Bitdefender helps

Bitdefender

XDR Concepts

eXtended Detection and Response

Bitdefender

Endpoints

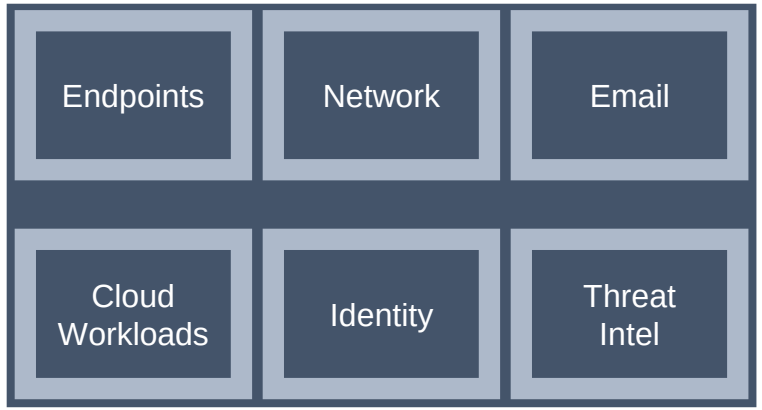
- What happened within the endpoint?
- How did an attack propagate?
- What are the risks on the endpoints?

Network

- How is the attacker moving across the organization?
- How are threats communicating?

Email

- Who else received this email or similar threats?
- Are there compromised accounts sending internal phishing emails?



Cloud Workloads & Containers

- What was the context in which malicious content was executed on the workload?
- What type of threat was prevented (e.g. malware, exploit)?

Identity

- Who is logged on the device?
- Is the user supposed to be logged on the device?

Threat Intel

- Which actors are behind this threat?
- Which verticals are these actors active on?
- Are there any other organizations experiencing the same attacks?

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

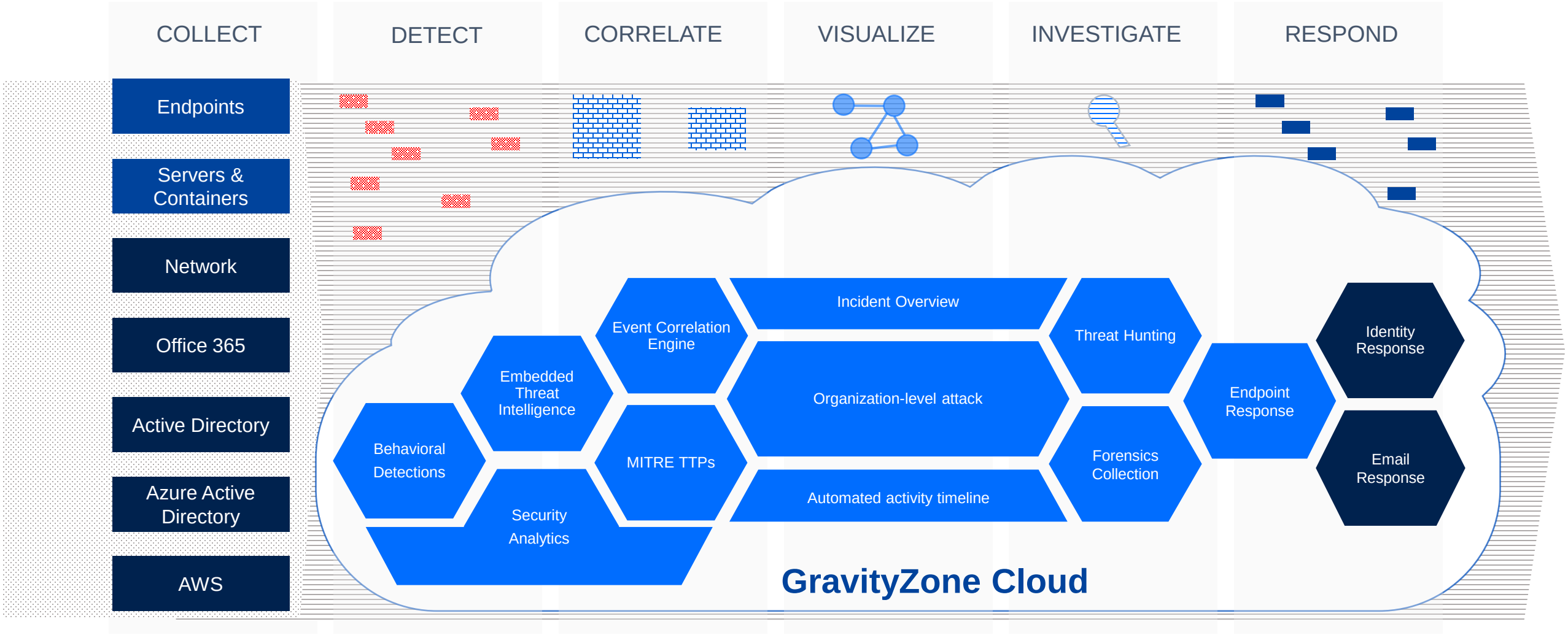
Collect	Detect	Correlate	Visualize	Investigate	Respond

GA Features

Collect	Detect	Correlate	Visualize	Investigate	Respond
▪ 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

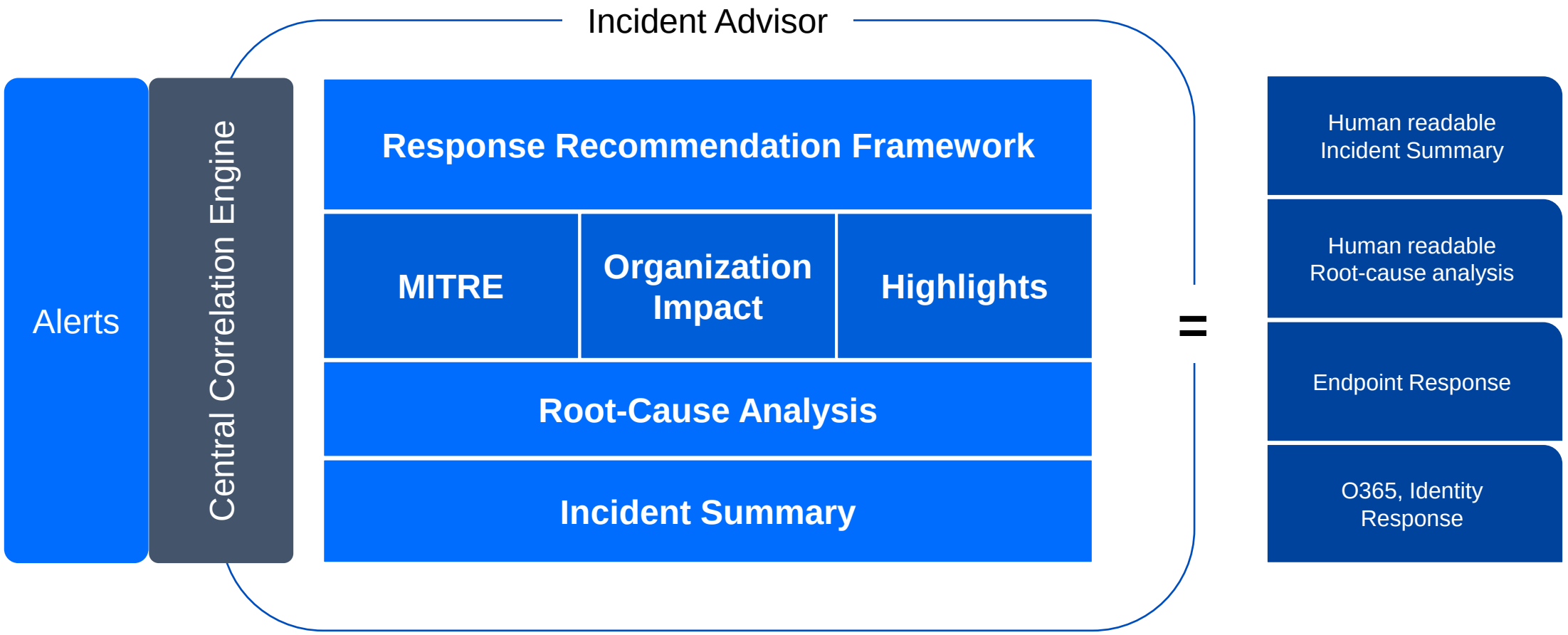


Bitdefender

Visualize, Investigate, Response

Incident Advisor

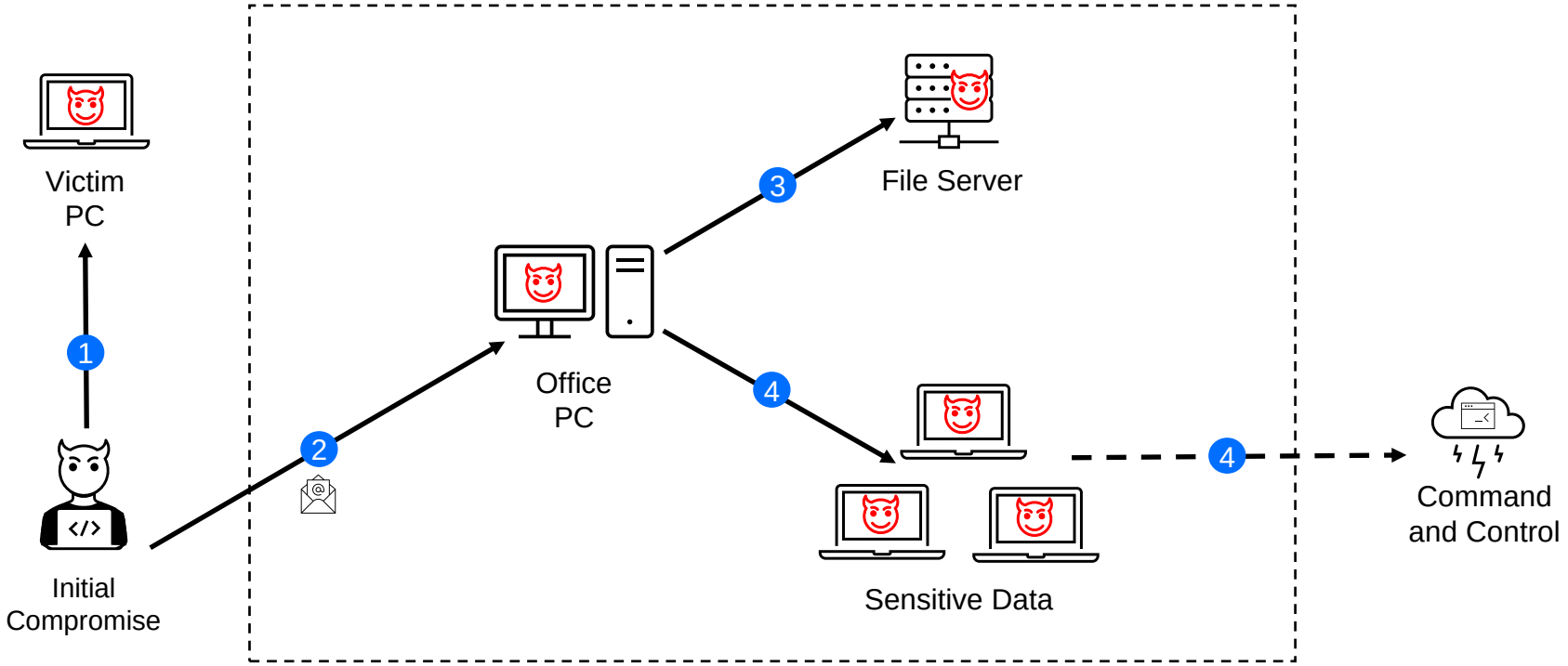
Bitdefender



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

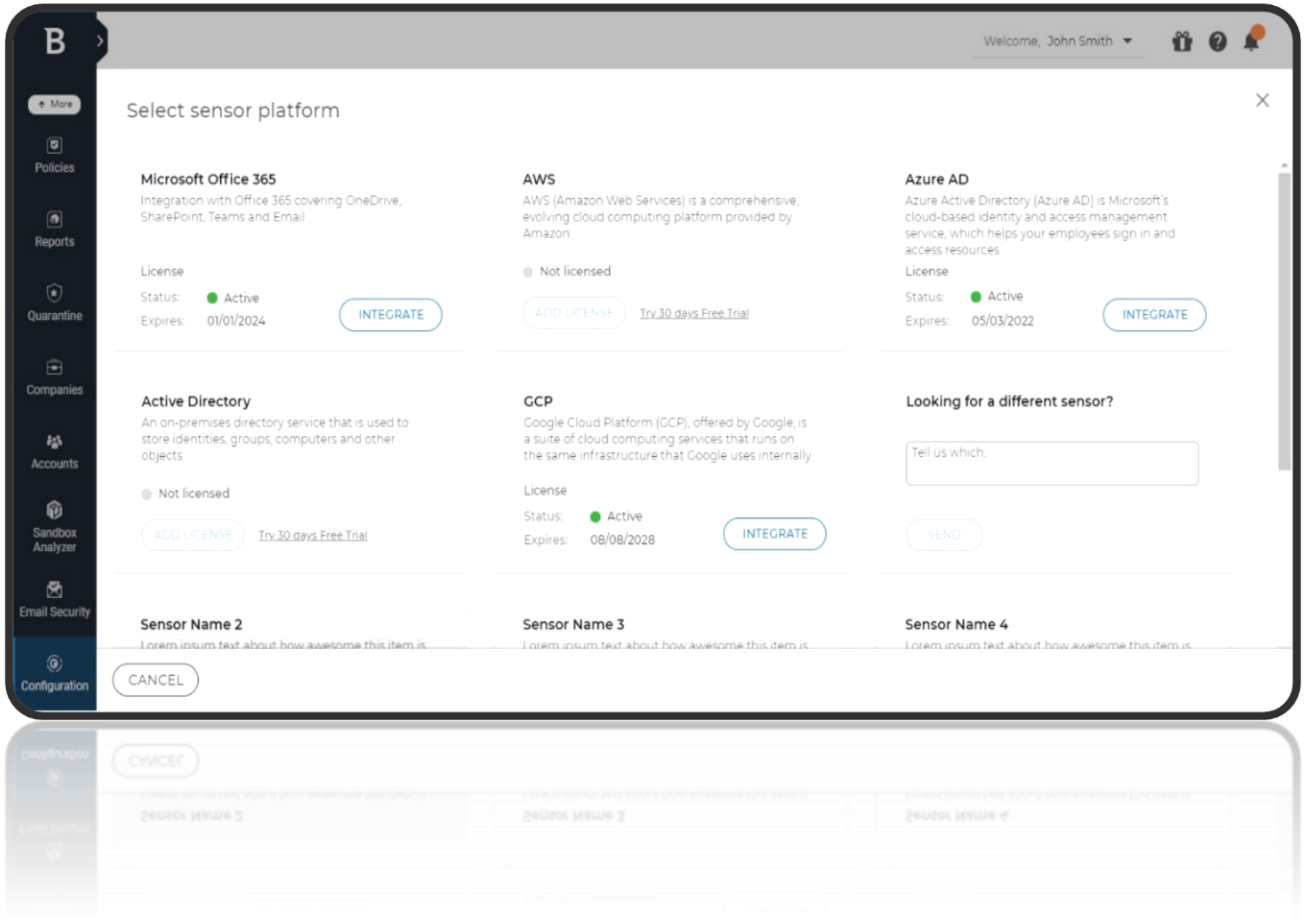
- ✓ On-premises AD
- ✓ Azure AD

Clouds

- ✓ AWS

Network

- ✓ Bitdefender Network Sensor



Detection & Response (GA)

Bitdefender

Incident Advisor

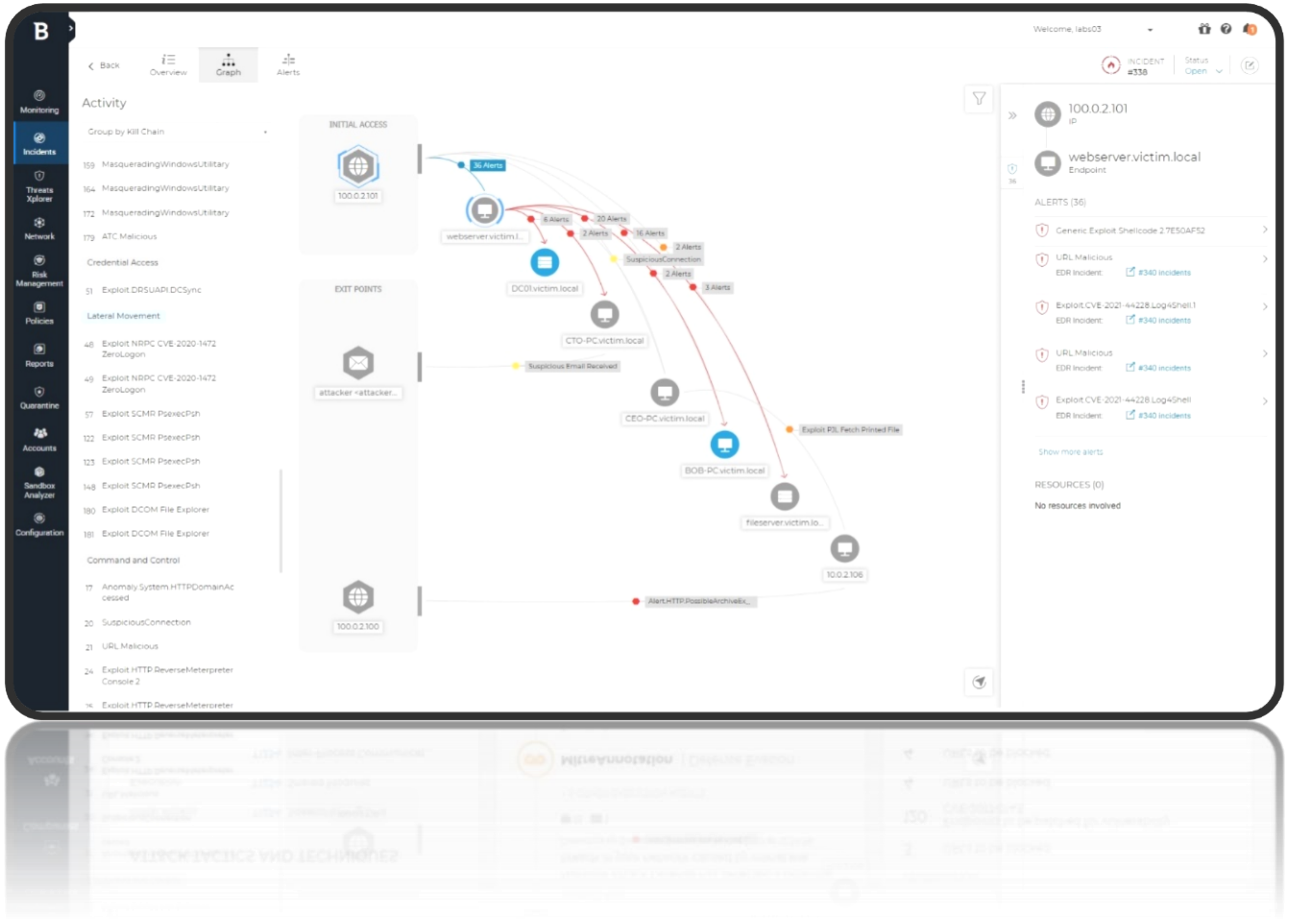
- ✓Summary
- ✓Root Cause
- ✓Organization Impact
- ✓Highlights

Response

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

New Graph

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



Investigation (GA)

Bitdefender

Historic Search

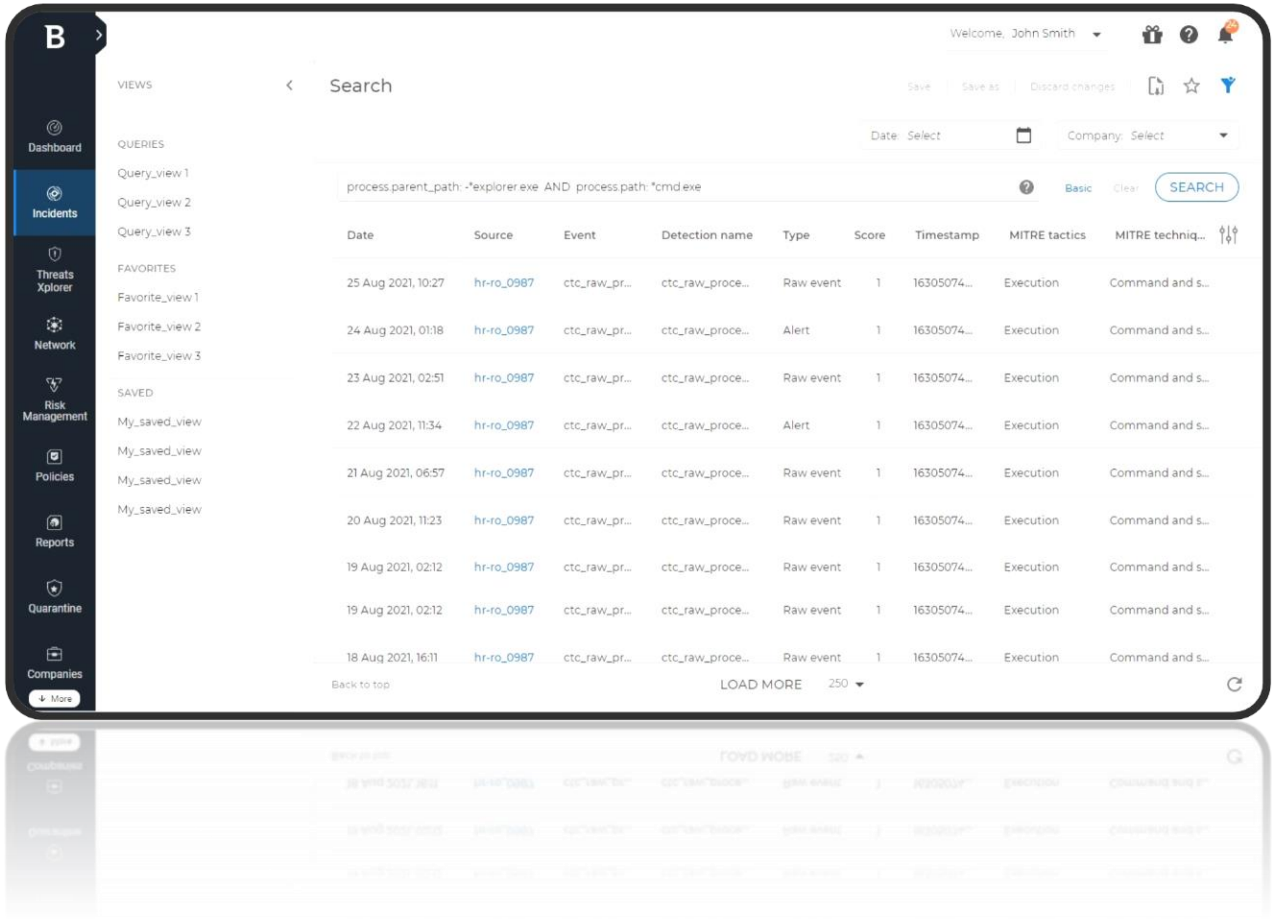
- ✓ Advanced filtering
- ✓ Enhanced data display
- ✓ Multiple data sources
- ✓ Smart views

Investigation Package

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

Full Remote Shell

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

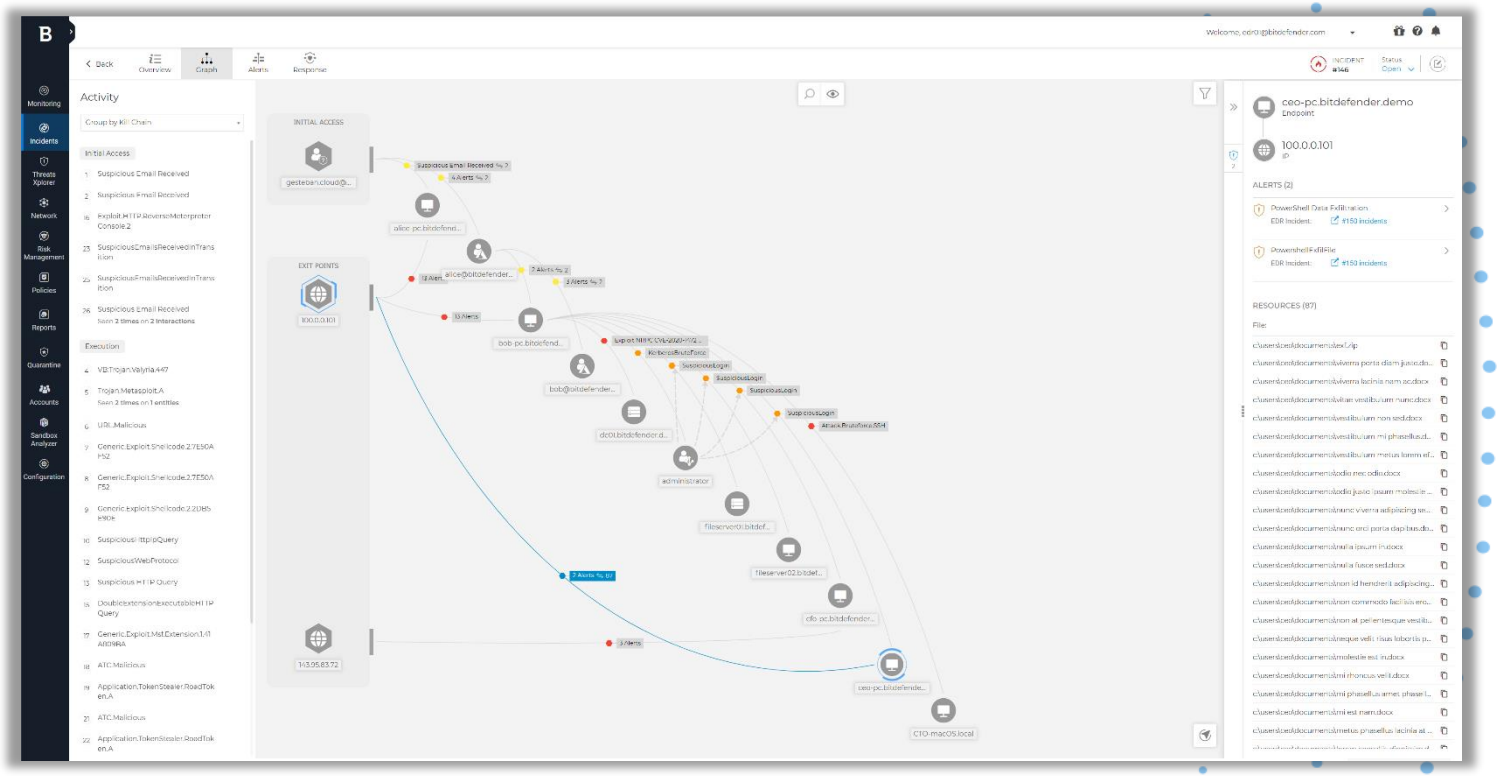


Bitdefender

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.

Bitdefender®

BUILT FOR RESILIENCE