Bitdefender

EDR, XEDR, XDR e MDR: le differenze dietro gli Acronimi

STEFANO MARANZANA, SALES ENGINEER ITALY

Bitdefender

Definitions

- EDR – Endpoint Detection and Response
- XEDR – eXtended Endpoint Detection and Response
- XDR – eXtended Detection ad Response
- MDR – Managed Detection and Response

Endpoint Detection and Response

Bitdefender

Endpoint detection and response technology is used to identify suspicious behavior and Advanced Persistent Threats on endpoints in an environment, and alert administrators accordingly. It does this by collecting and aggregating data from single endpoints.

eXtended Endpoint Detection and Response

Bitdefender

eXtended Endpoint Detection and Response is the evolution of Endpoint Detection and Response solutions that adds analysis and correlation functionality of security events between endpoints.

eXtended Detection and Response

Bitdefender

eXtended Detection and Response works by collecting and correlating data across various network points such as servers, email, cloud workloads, and endpoints. The XDR system helps organizations to have a higher level of cyber awareness, enabling cyber security teams to identify and eliminate security vulnerabilities.

Managed Detection and Response

Bitdefender

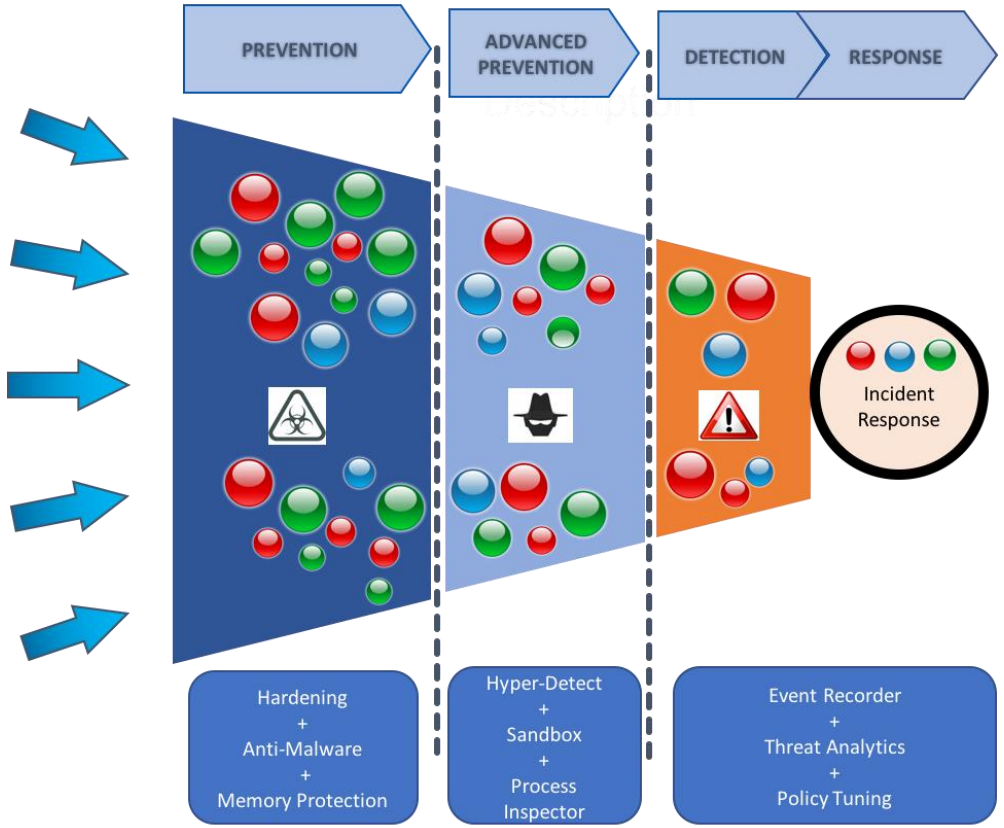
Managed Detection and Response (MDR) denotes outsourced cybersecurity services designed to protect your data and assets even if a threat eludes common organizational security controls.
An MDR security platform is considered an advanced 24/7 security control that often includes a range of fundamental security activities including cloud-managed security for organizations that cannot maintain their own security operations center. MDR services combine advanced analytics, threat intelligence, and human expertise in incident investigation and response deployed at the host and network levels.

Bitdefender

EDR Concepts

Endpoint Detection and Response

Bitdefender



Bitdefender

XEDR Concepts

eXtended Endpoint Detection and Response

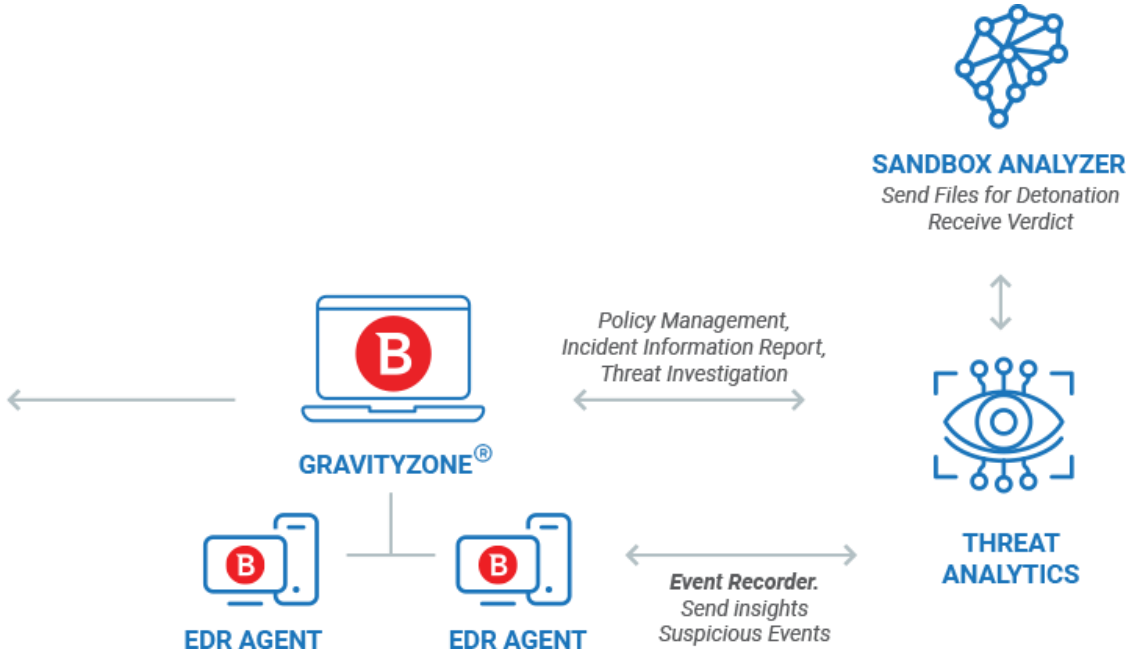
Bitdefender

INCIDENT ALERT
(Suspicious Files, Suspicious Process)

INCIDENT VISUALIZATION
(Interactive Graph)

INCIDENT INVESTIGATION
(Search & Corraborate)

INCIDENT RESPONSE
(Delete, Blacklist, Kill, Isolate)



Bitdefender

XDR Concepts

eXtended Detection and Response

Bitdefender

Endpoints

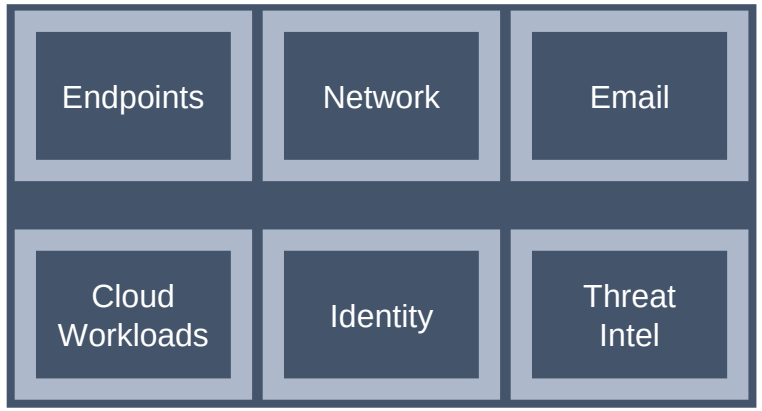
- What happened within the endpoint?
- How did an attack propagate?
- What are the risks on the endpoints?

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

MDR Concepts

Managed Detection and Response

Bitdefender

Bitdefender

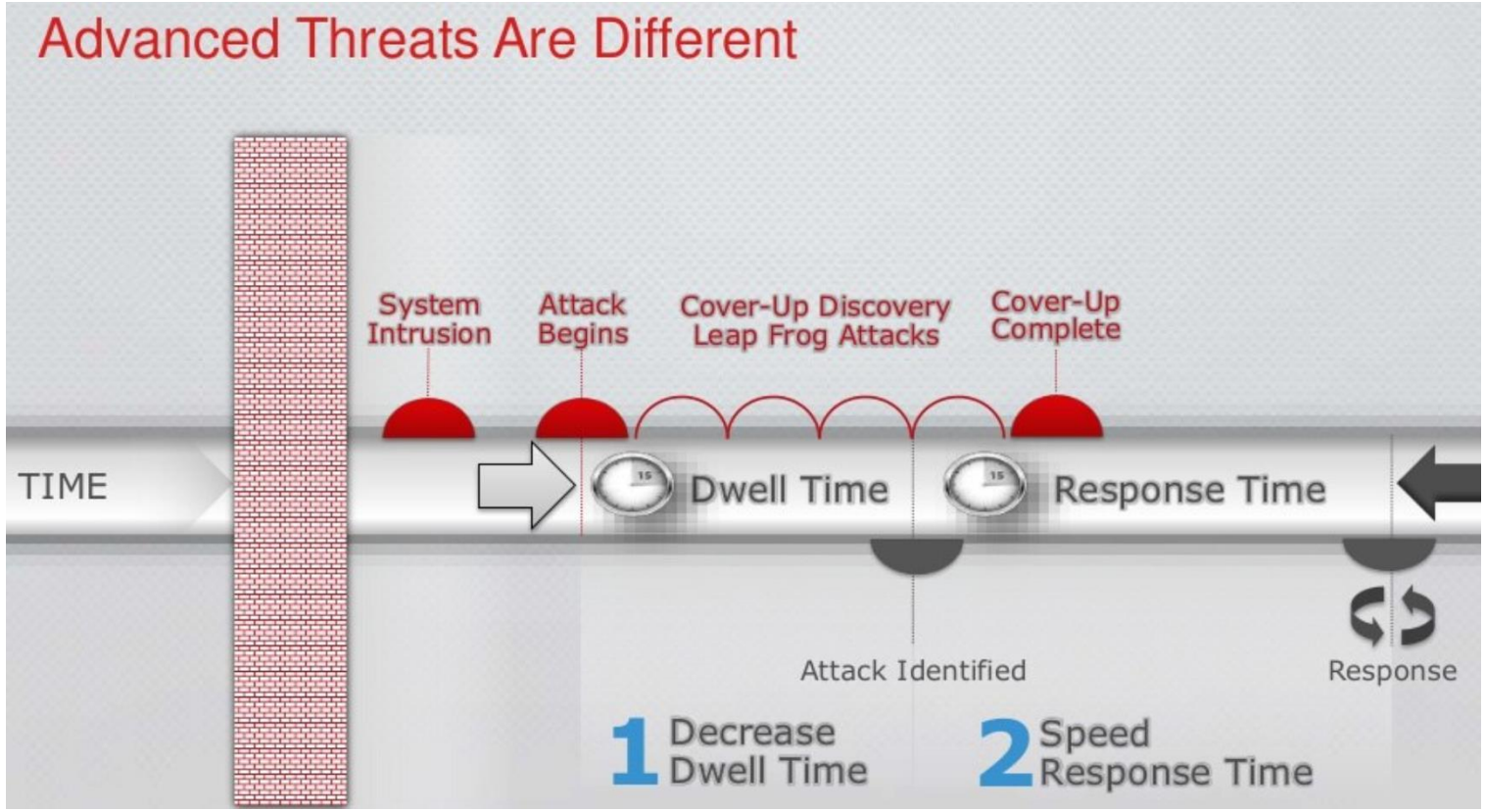
What are the steps of the anatomy of an attack?

Bitdefender

Dwell Time

DWELL TIME

Bitdefender



Pyramid of Pain

Bitdefender

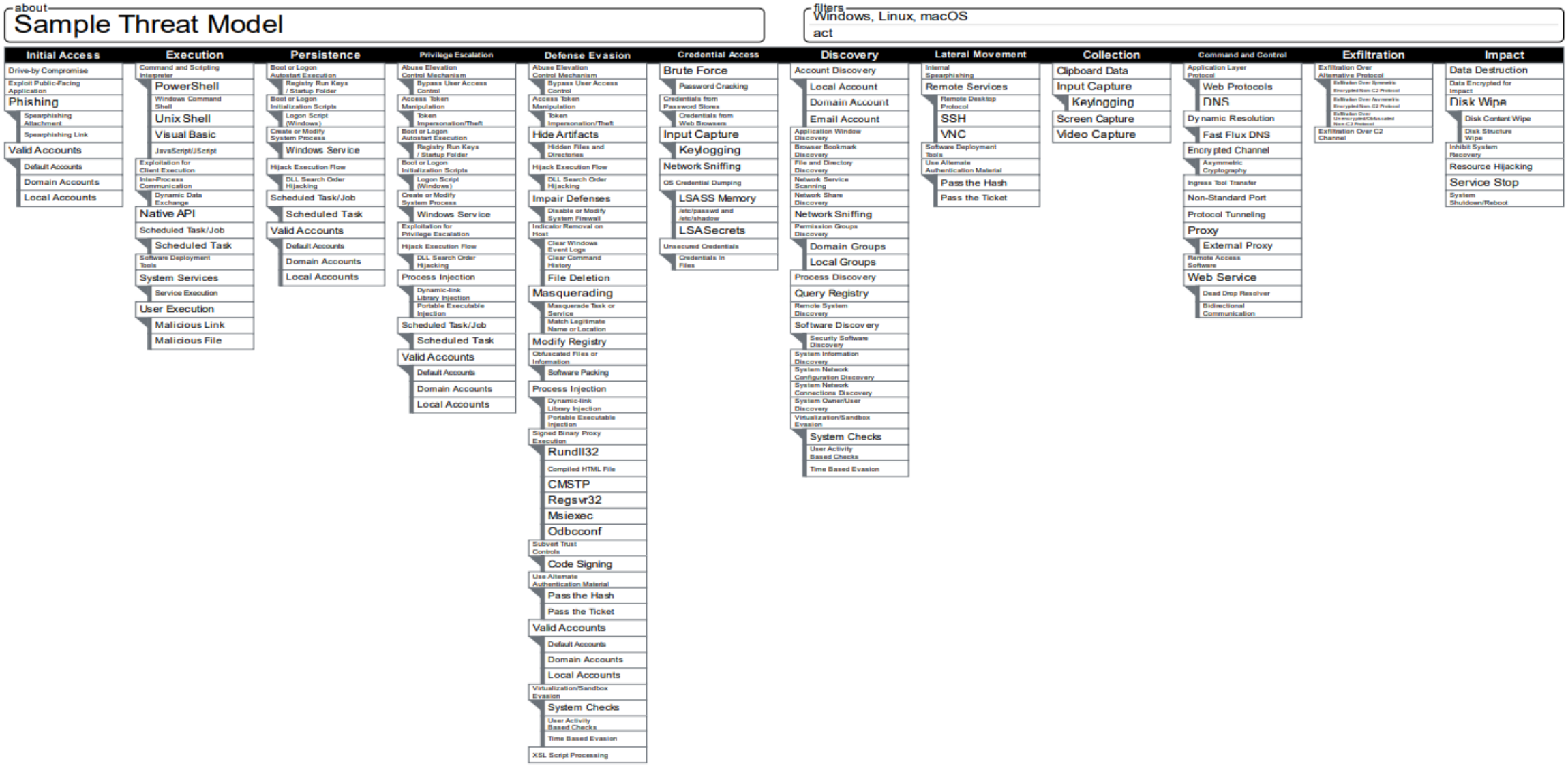
- ATT&CK Reflects tactics and techniques observed in the real world
- Why is this important?
  - Industry historically focused on methodology that is low on the pyramid
  - Forces adversary to change tools and behavior to avoid detection
    - Lowers their ROI
  - For the Defender:
    - Behavior focused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



Know the attacker

Bitdefender

Adversaries are extremely skilled at obtaining access and experts at going unnoticed; and it is not uncommon for an organization to be unaware of an intrusion for days, weeks, or even months.

- Before you can begin threat hunting, you must first understand the adversaries you will be facing.
- Their techniques may be similar, however the motivation behind each can be very different.

Bitdefender

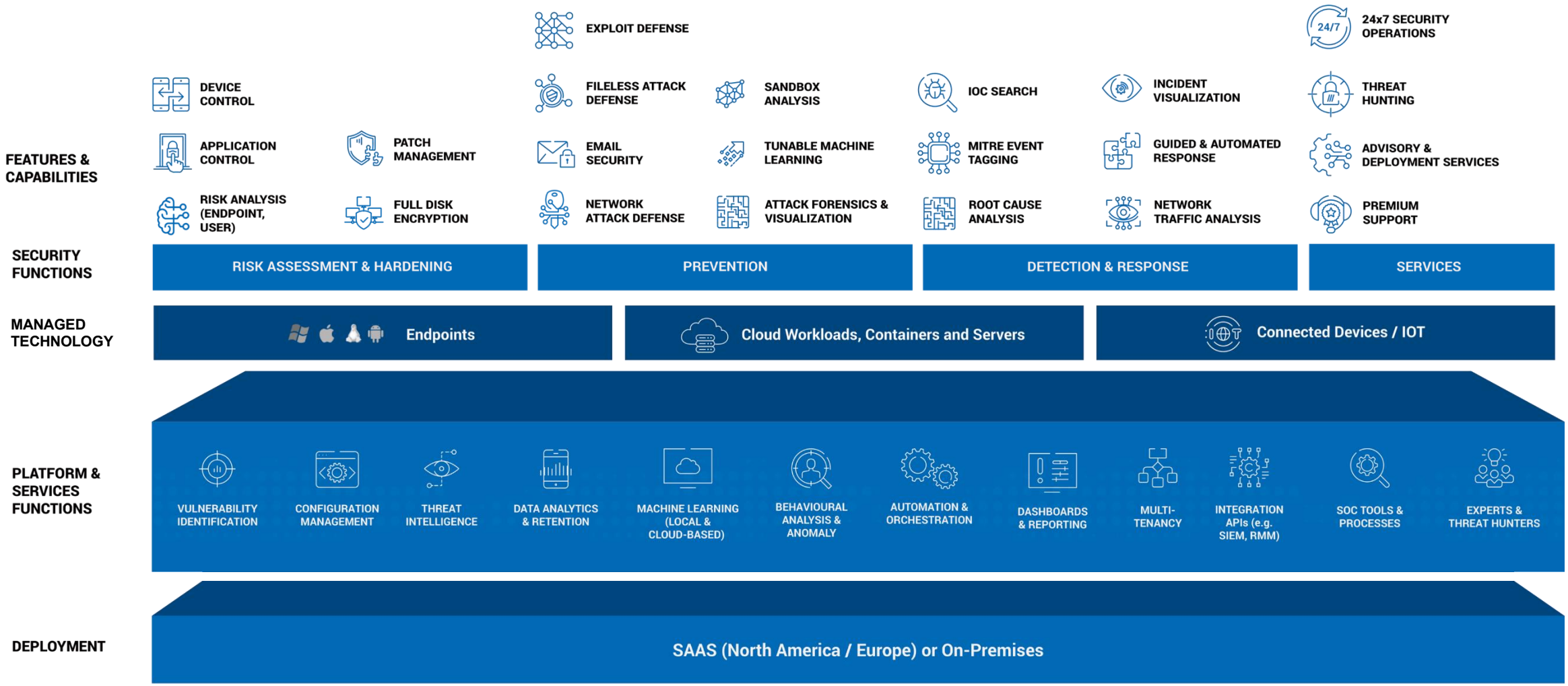
How Bitdefender can help you?

Bitdefender GravityZone

Addressing the Challenge:
TOO MANY TOOLS & TOO LITTLE VISIBILITY

Bitdefender

Bitdefender GravityZone Blueprint for Cyber Resilience



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

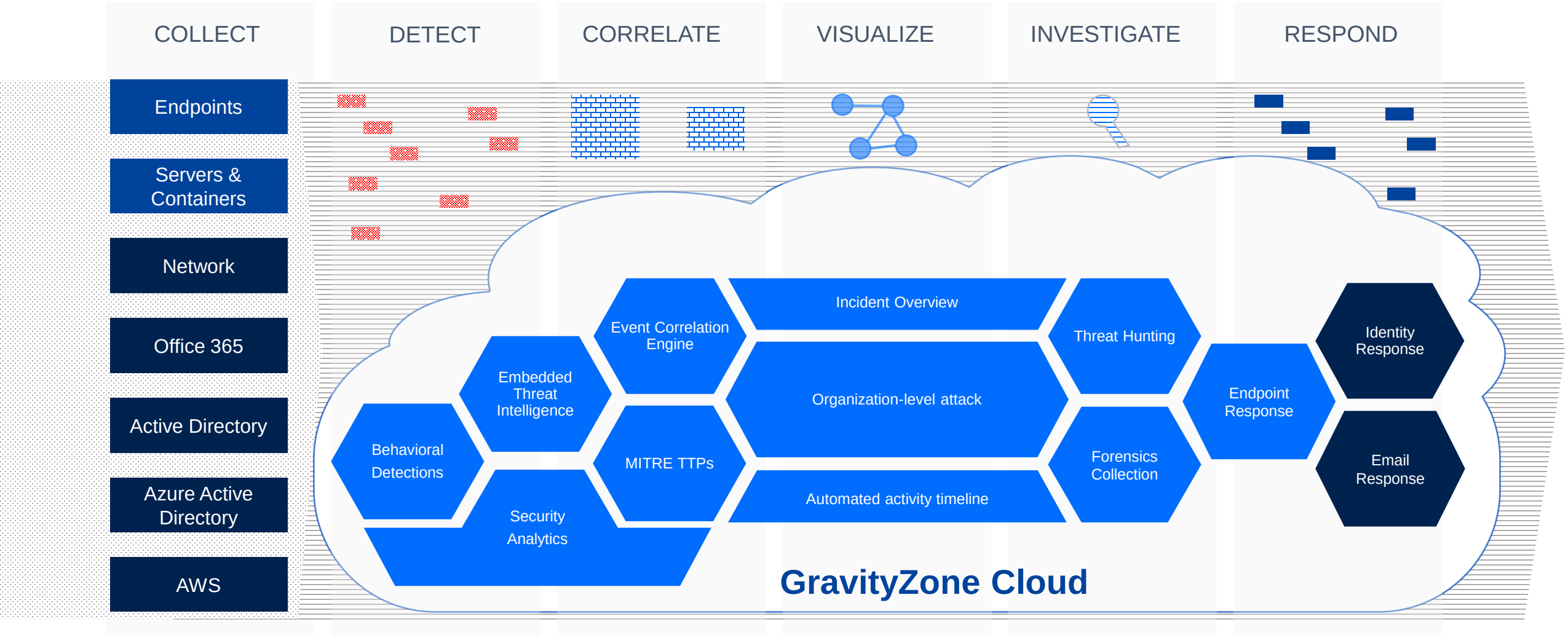
Collect	Detect	Correlate	Visualize	Investigate	Respond

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

Enabled via licensing add-on

GravityZone XDR



Bitdefender

Collect, Detect, Correlate

Bitdefender XDR Sensor - Productivity

Bitdefender

Why … are we doing this?

Given the increasingly diverse methods of cyberattacks by email to companies, it becomes essential to analyze possible attacks not only by individually scanning each email box in a domain, but including the analysis of the entire flow of emails within a company, in order to identify and security analysts within these companies of potential cyberattacks (security events).

What … are we doing?

Collect O365 mail and audit events and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (only audit at GA)

How … are we delivering this?

- O365 integration in Sensors Management
- Sold as a separate license
- Cloud based integration

Bitdefender XDR Sensor - Identity

Bitdefender

Why … are we doing this?

Active Directory is a prime target during cyberattacks

Active Directory Stats

1. 90% of enterprises globally use AD.
2. Attackers target 95 Million AD accounts daily.
3. 80% of attacks include compromising AD.

What … are we doing?

Collect user events from on-premise AD and Azure AD and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (Q2)

How … are we delivering this?

- on-premise AD and Azure AD integration in Sensors Management
- Sold as a separate license
- On-premise AD integration requires EDR module on every DC
- Azure AD requires Azure AD Premium P1 or P2 license

Bitdefender XDR Sensor - Cloud

Bitdefender

Why … are we doing this?

- Lack of visibility in suspicious activities from cloud platforms administration

What … are we doing?

Collect events from AWS and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (Q2)

How … are we delivering this?

- AWS integration in Sensors Management
- Sold as a separate license
- Cloud based integration (using AWS CloudTrail, AWS Config, Amazon SQS and Amazon SNS)
- Important!: implies additional costs for the customer

Bitdefender XDR Sensor - Network

Bitdefender

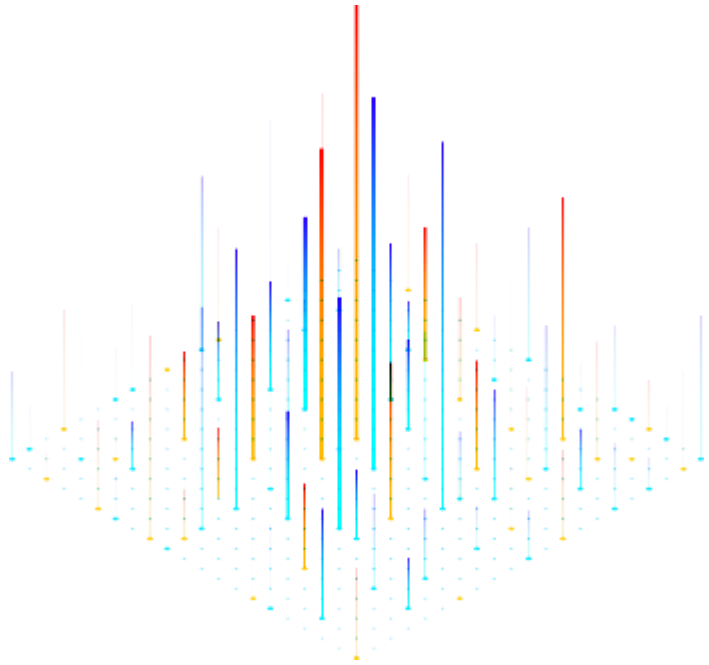
Why … are we doing this?

- Organizations are NOT BUILT JUST FROM Endpoints (it's also IOTs, network devices, printers, etc).
- EDR solutions are not able to detect attacks involving non-endpoint or non-protectable devices.

What … are we doing?

Collect network events and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search



How … are we delivering this?

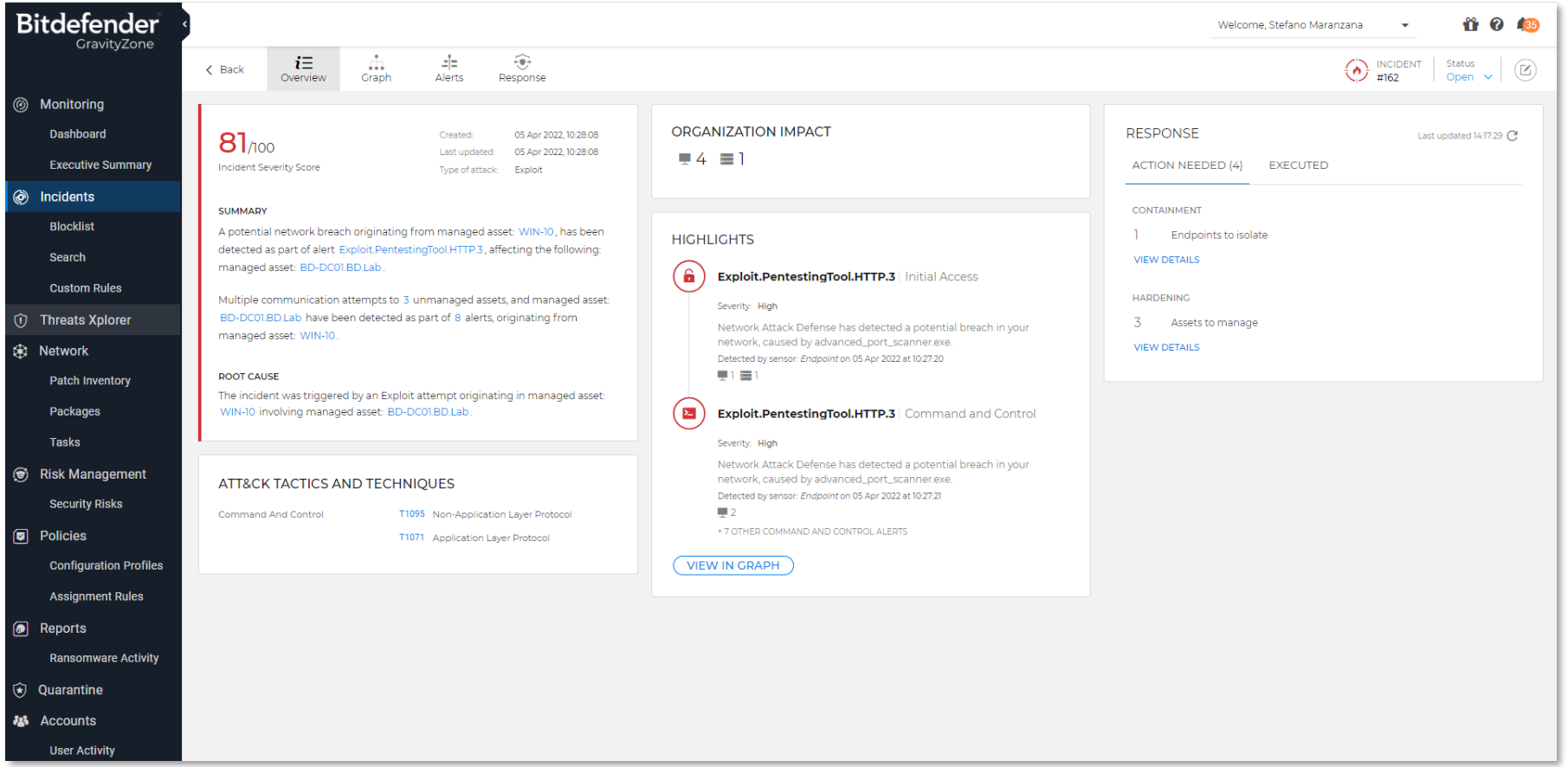
- Network events flow (no integration in Sensors Management at GA)
- Sold as a separate license
- Manual deployment of network probes

Bitdefender

Visualize

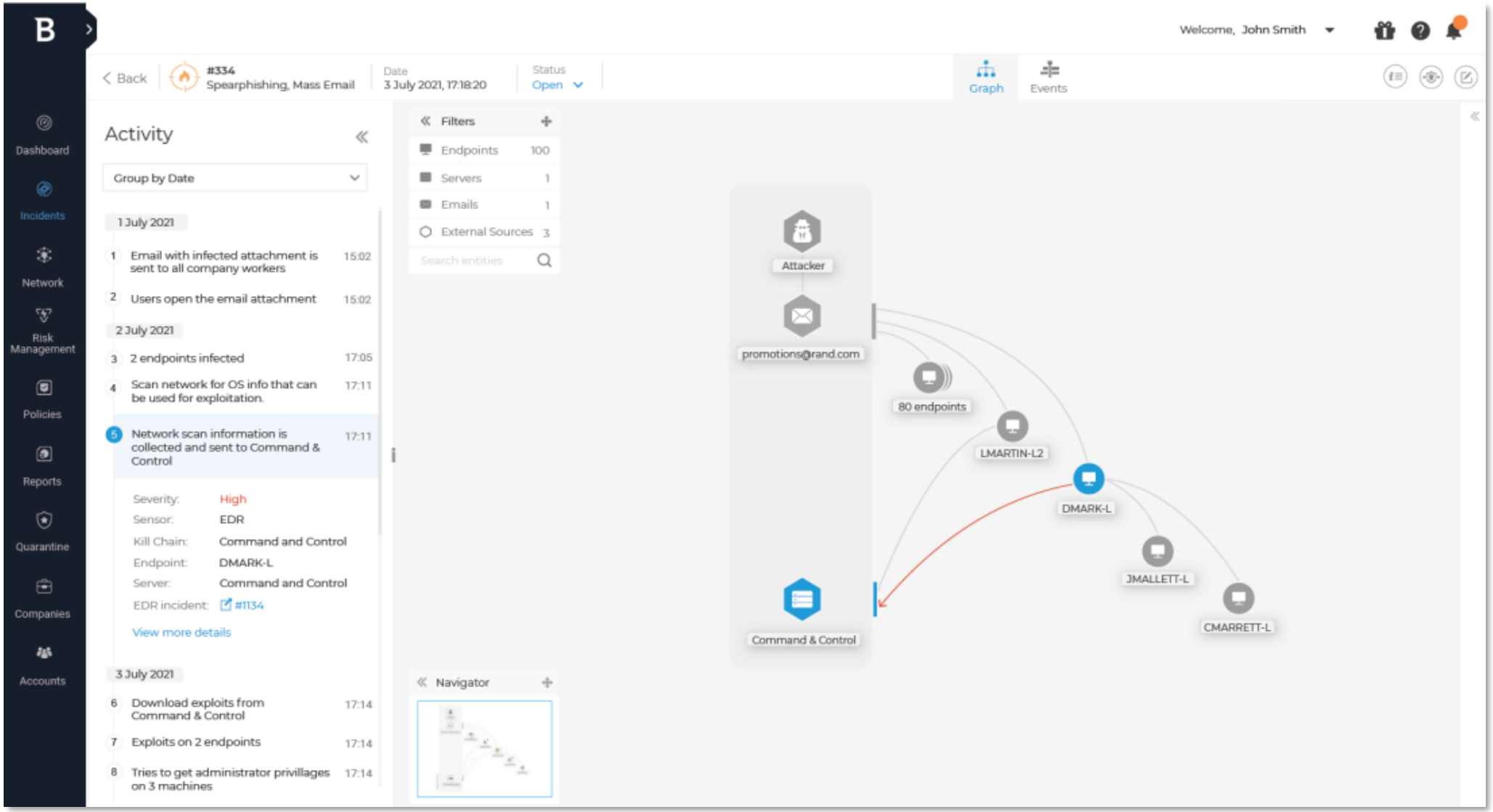
Extended Incident Overview

Bitdefender



Extended Incident Graph

Bitdefender

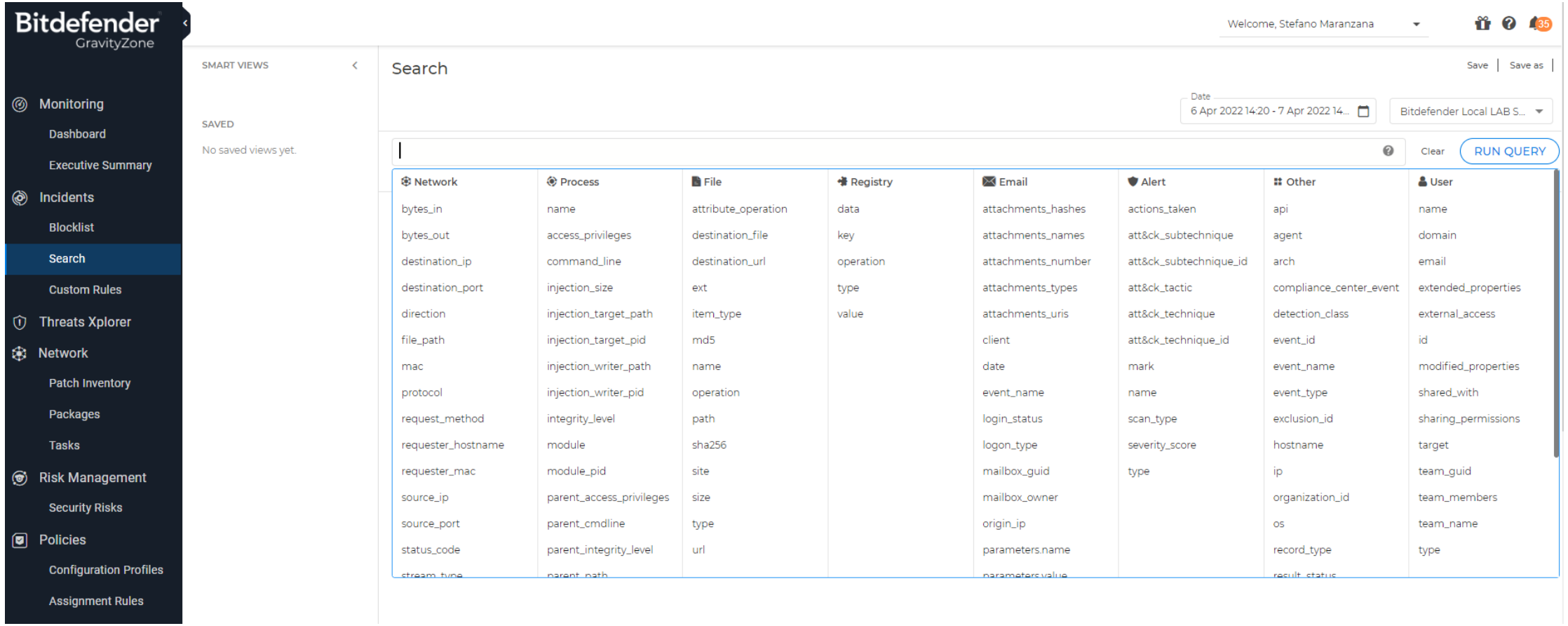


Bitdefender

Investigate

Historic Search

Bitdefender



Bitdefender

Respond

Non-endpoint Response Actions

Bitdefender

Platform	Action name	Available through	What it does
O365	Disable user	• Incident Graph • Incident Response	• Disables the user account at the O365 Azure AD level. • Also forces an expiry on all active sessions.
	Force credentials reset		• Marks the account password as expired, forcing it to be changed at the next login. • Also forces an expiry on all active sessions.
	Delete email	• Incident Response	• Deletes a specific suspicious email from the Exchange Online mailbox.
Active Directory (onpremise)	Disable user	• Incident Graph • Incident Response	• Disables the user account at the Active Directory level
	Force credentials reset		• Marks the account password as expired, forcing it to be changed at the next login. • If set, it removes the “Password never expires” and “User cannot change password” attributes from the account.

Bitdefender

Q&A

Bitdefender®

BUILT FOR RESILIENCE