Bitdefender

Bitdefender GravityZone XDR

Agenda

- Defender’s Challenges
- What is XDR?
- Introducing GravityZone XDR
- Why Bitdefender?

Defender’s Challenges

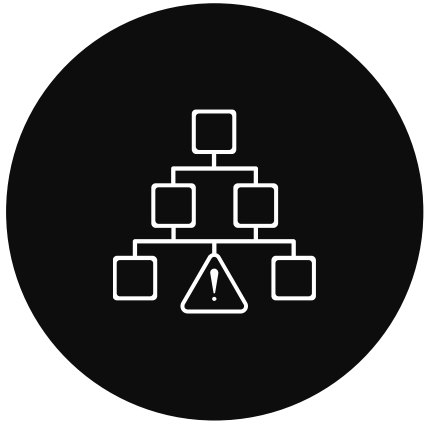
The attack surface is expanding

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

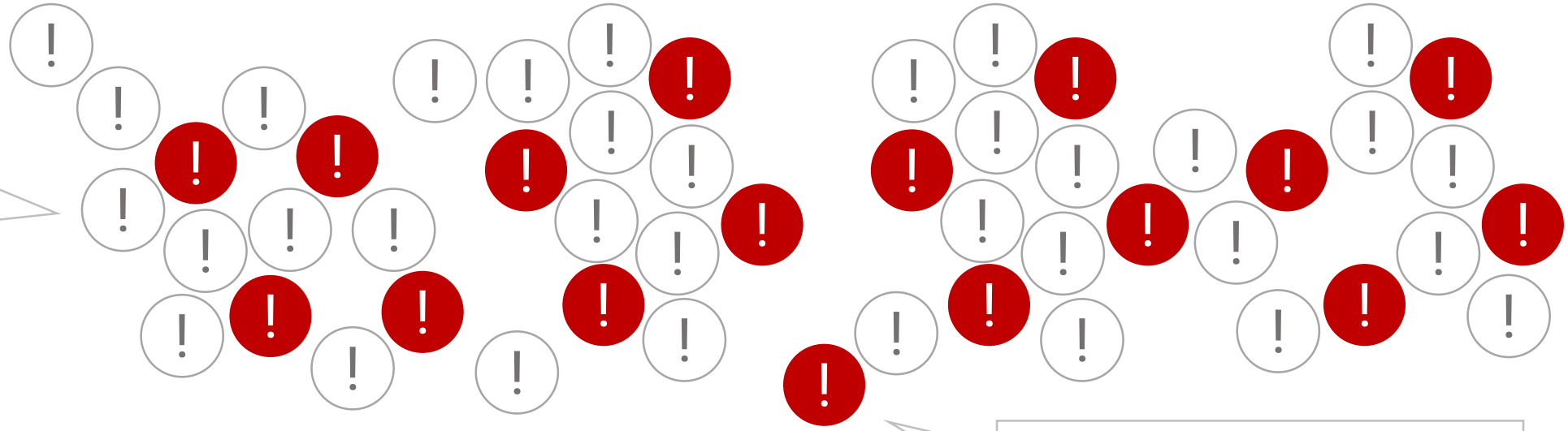
Email Security

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

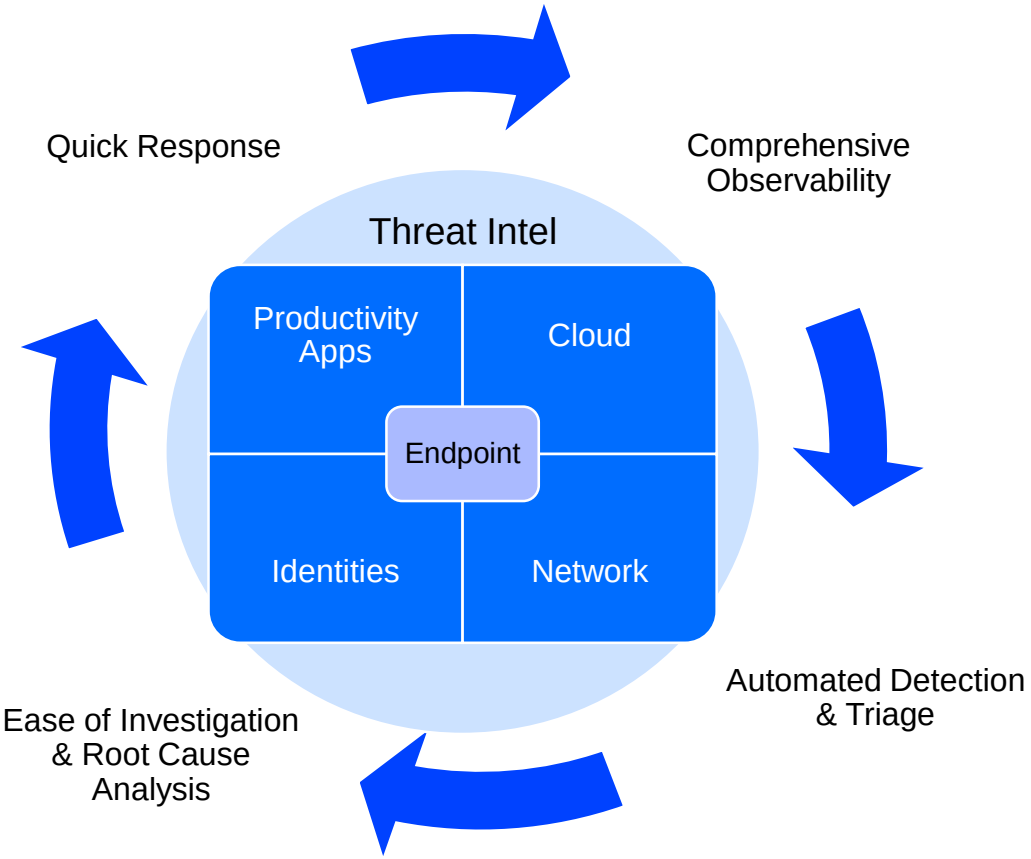
Reduce Risk with Prevention, Detection & Response

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.

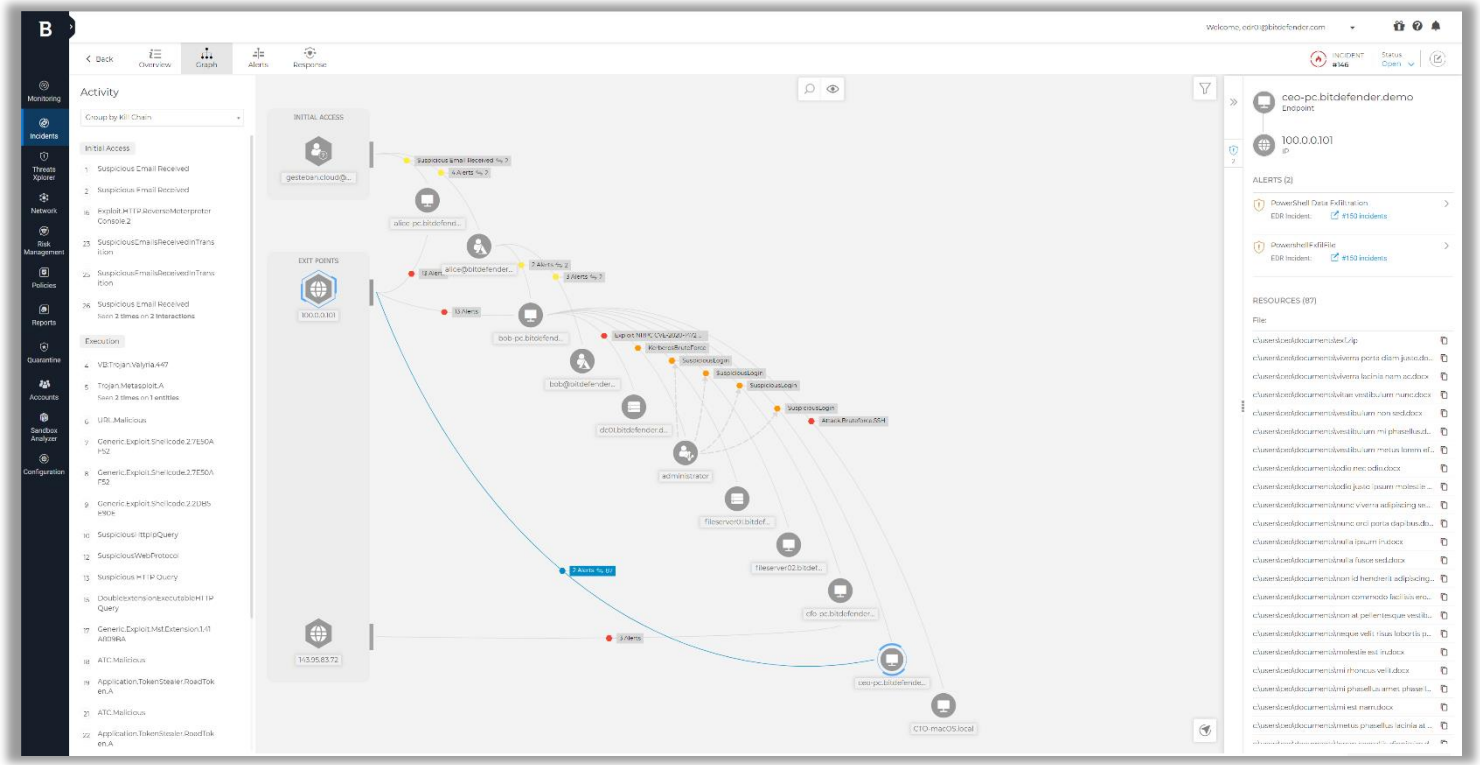
Bitdefender

GravityZone XDR

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.

GravityZone XDR

Bitdefender

Observes attacks and advanced threats

Consolidates monitoring across physical devices, virtual assets, connected devices and cloud platforms and workloads.

Out-of-the-box detection

Protects from day 1 while enabling customized detections for unique use-cases increasing security operations efficiency.

Reduces investigation and response time

Provides context to understand the root cause with incident details and overviews in an easy to consume view.

Automated & guided response recommendations

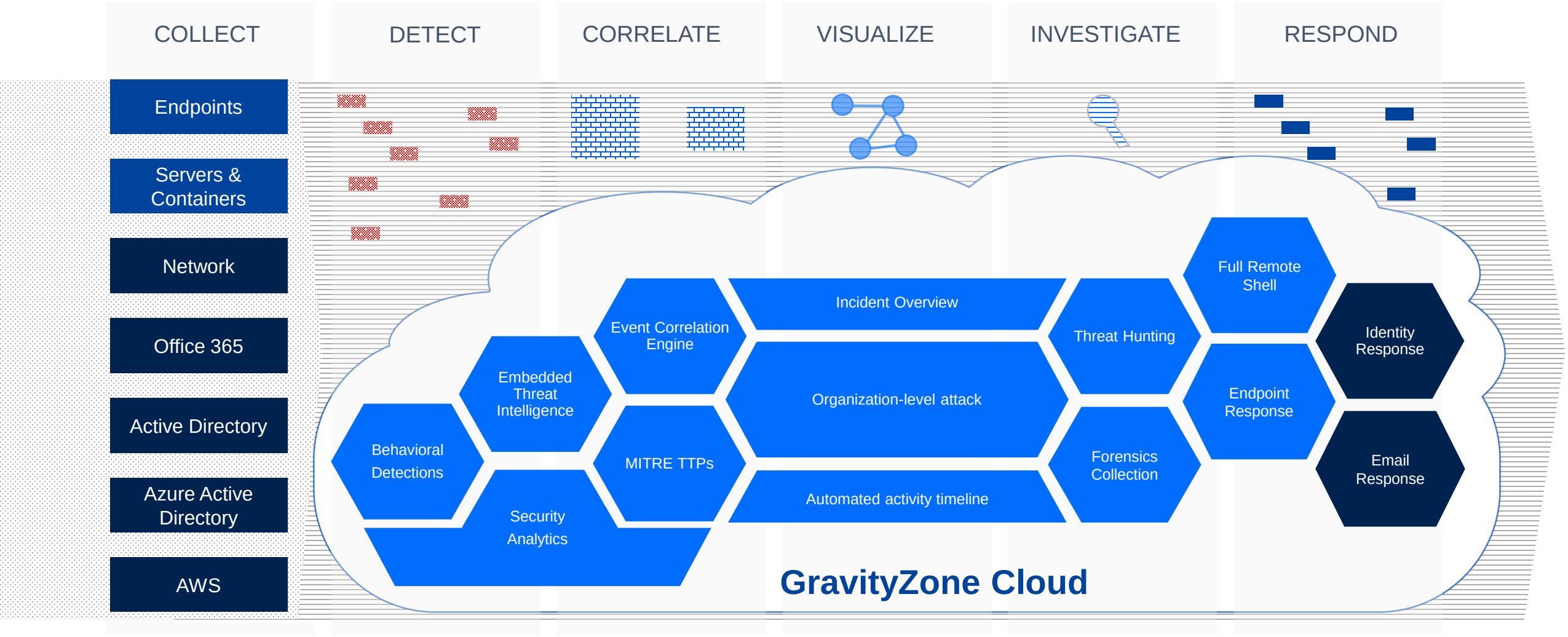
Enables rapid end-to-end response and incident containment by combining fully automated and guided response recommendations across the organization.

Easy to use and delivers value out of the box

No need for custom integrations, detection rule creation or third-party security tools.

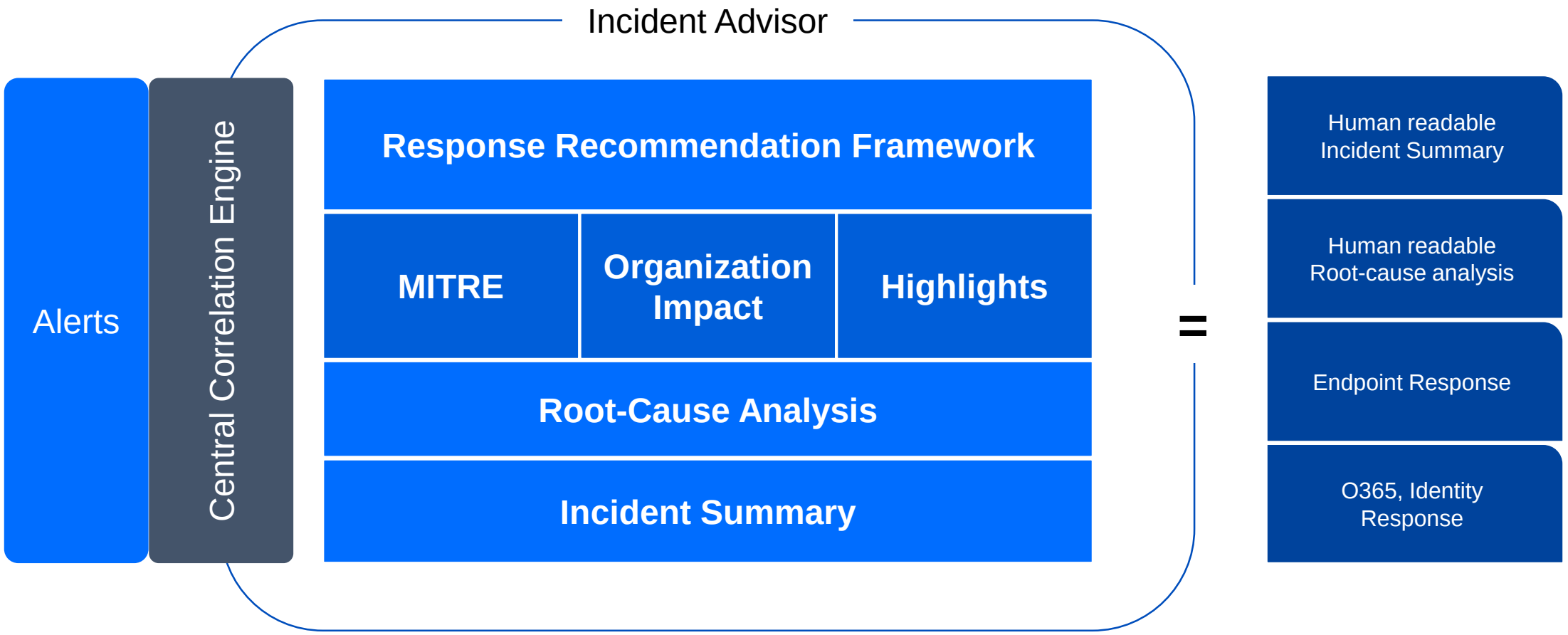
Enabled via licensing add-on

GravityZone XDR



Incident Advisor

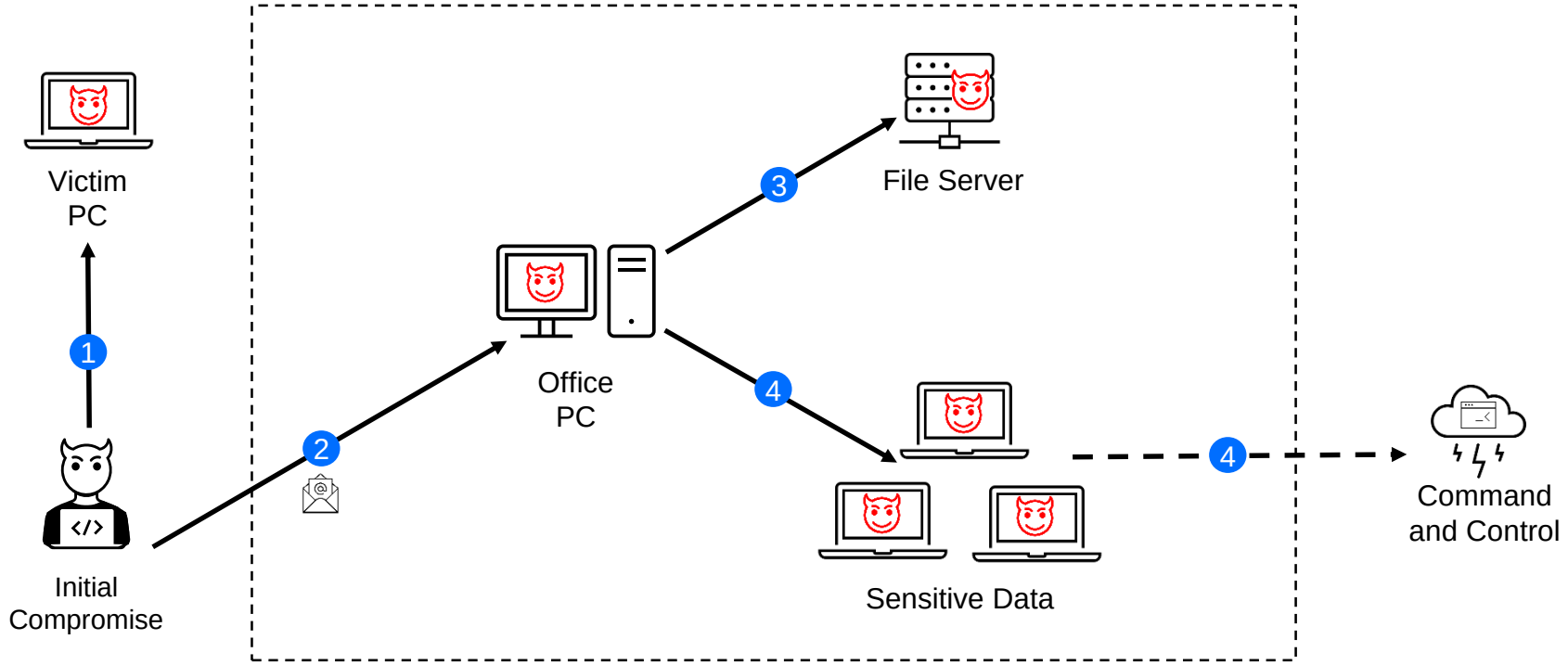
Bitdefender



XDR Scenario

Sensors

- EDR
- Office365
- Active Directory

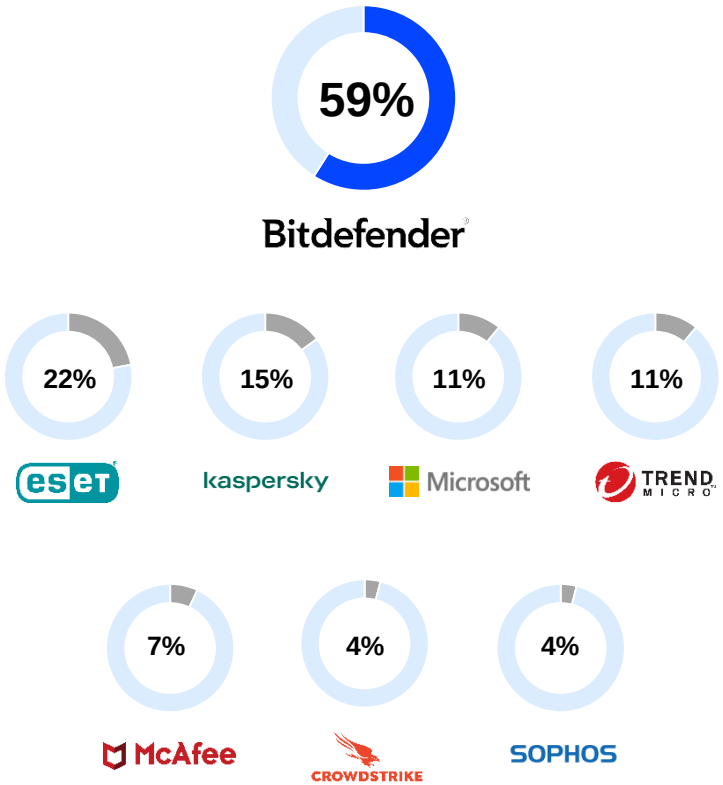


1 M365 Compromise
2 Lateral Movement
3 Ransomware Deployment
4 Data Exfiltration

Consistently High Security Efficacy

Bitdefender

#1 Attack prevention rankings from 2018–2021
% (Indexed to 100)[1]



Highest Prevention and Response Capability with Lowest 5 Year TCO[2]

Notes:
1. Represents number of times a given test participant took 1st place in any of the malware detection, real world & protection categories tests performed by AV Comparatives
2. Endpoint Prevention & Response Test 2021, AV Comparatives

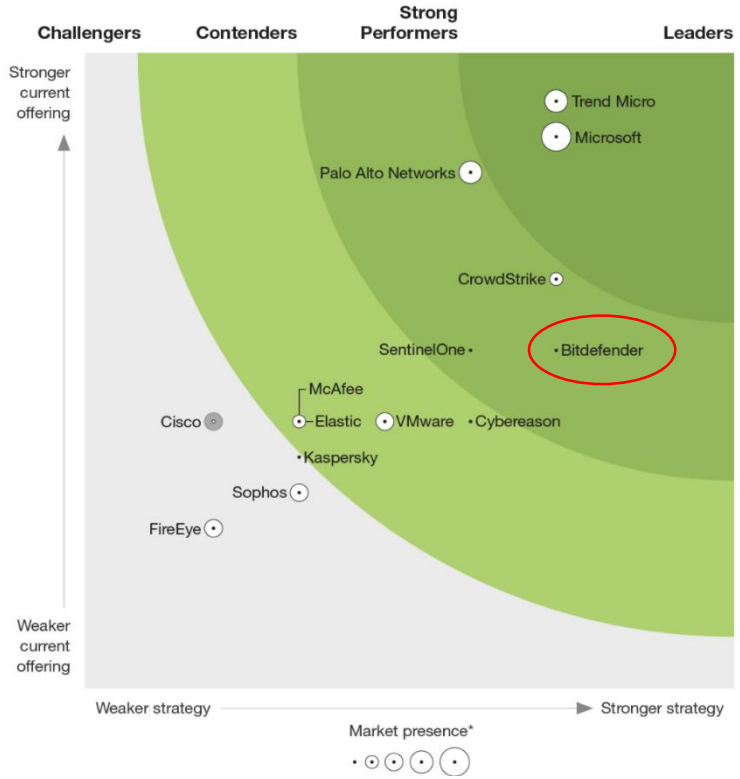
Named Strong Performer

Bitdefender

The Forrester Wave, EDR, Q2 2022 and The Forrester New Wave, XDR, Q4 2021

The only vendor to be specifically called out for its focus on resilience among all participating vendors

Achieved maximum 5/5 scores in the criteria of Product Vision, Investigation Capabilities, ATT&CK Alignment, Supported Systems, and Product Security



"The vendor gives customers incredible transparency and works closely with the community to improve its product security."

"(Bitdefender XDR) is the best fit for companies that need a reliable and easy-to-use offering."

XDR Early Access

Started in 2H ‘21

The Facts

78%
of active EAP customers have environments larger than 1500 endpoints

100%
of XDR EAP deployments were performed in PRODUCTION environments

100%
of XDR EAP customers praised the improvements around understanding Extended Incidents

Targeted customers

- ❑ 1000+ endpoints
- ❑ Bitdefender EDR/MDR customers
- ❑ Bitsociety customers
- ❑ BD InfoSec/MDR teams

Bitdefender

“As a CISO, I find the Incident Advisor useful in understanding what has happened and how my team should respond.”

Financial, 1000+

“I particularly like the Highlights provided in the Incident Advisor. Besides the fact that I know what happened on the organization level, I can quickly respond based on the provided Response Recommendations”

Healthcare, 1200+

“The improvements within the Graph and the Incident Advisor allow me to rapidly investigate an incident, compared to the old versions where I could have spent hours trying to figure out what happened”

Travel, 3500+

“Incident Advisor has the potential to be a clear differentiator for Bitdefender, as it helps the user understand what needs to be investigated and what not.”

Government, 2300+

“For me, the Incident Advisor provides the right level of detail into what I need to do. Furthermore, it helps me understand things before looking into the Incident Graph. The O365 response allowed me to quickly take action against a compromised user”

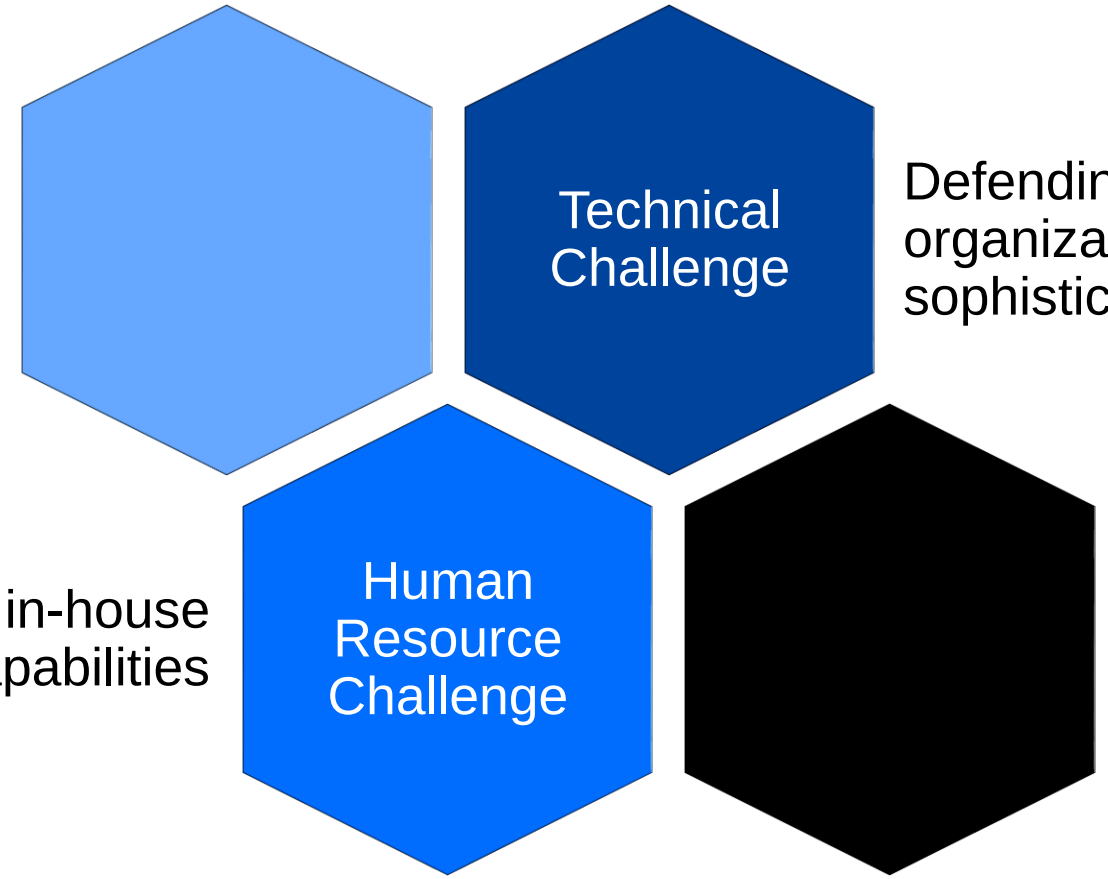
Education, 3200+

“Our team has different skilled analysts and all of us find usefulness in the human readable description from the Incident Advisor. ”

Insurance, 1400+

Customer challenges

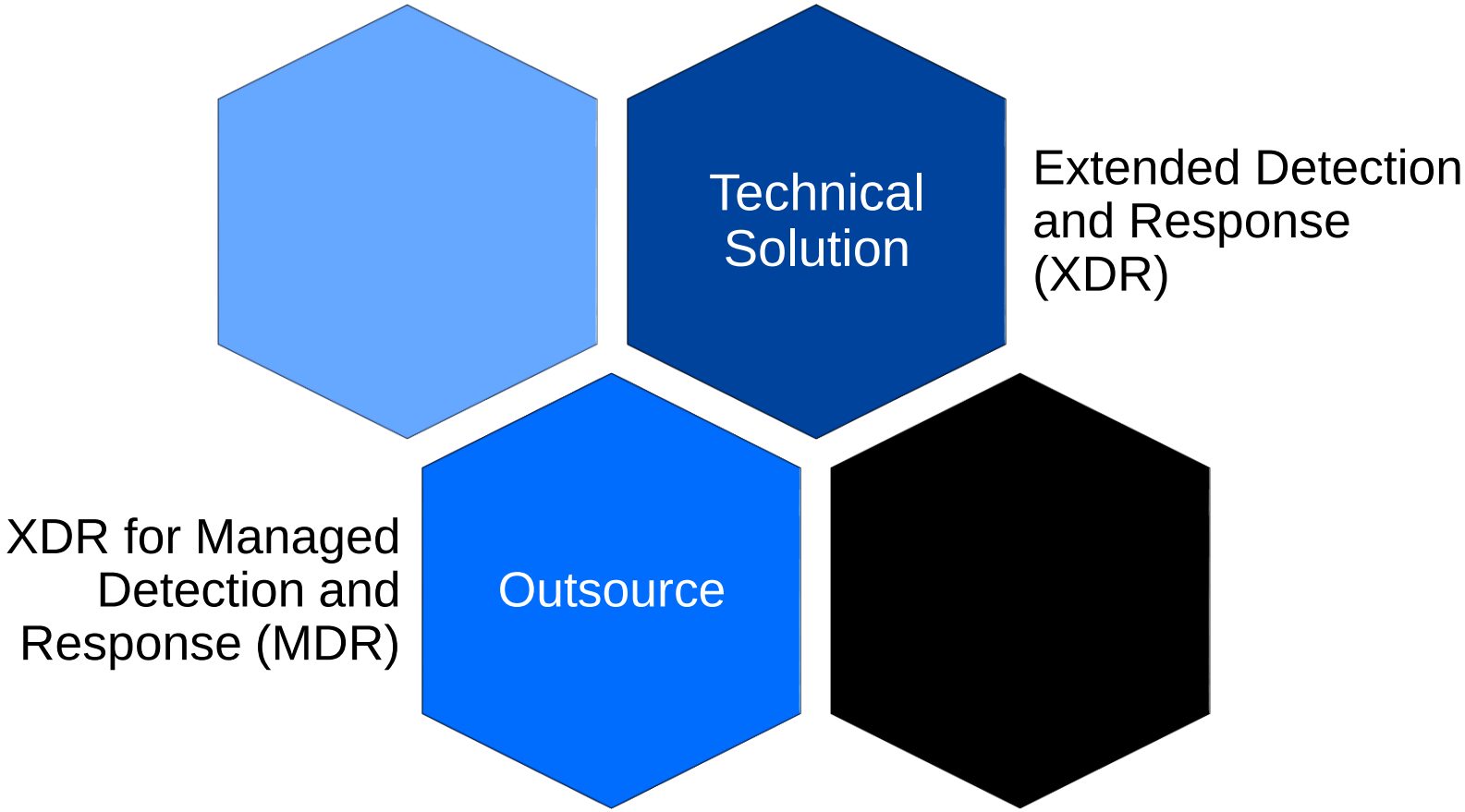
Bitdefender



Defending the organization against sophisticated threats

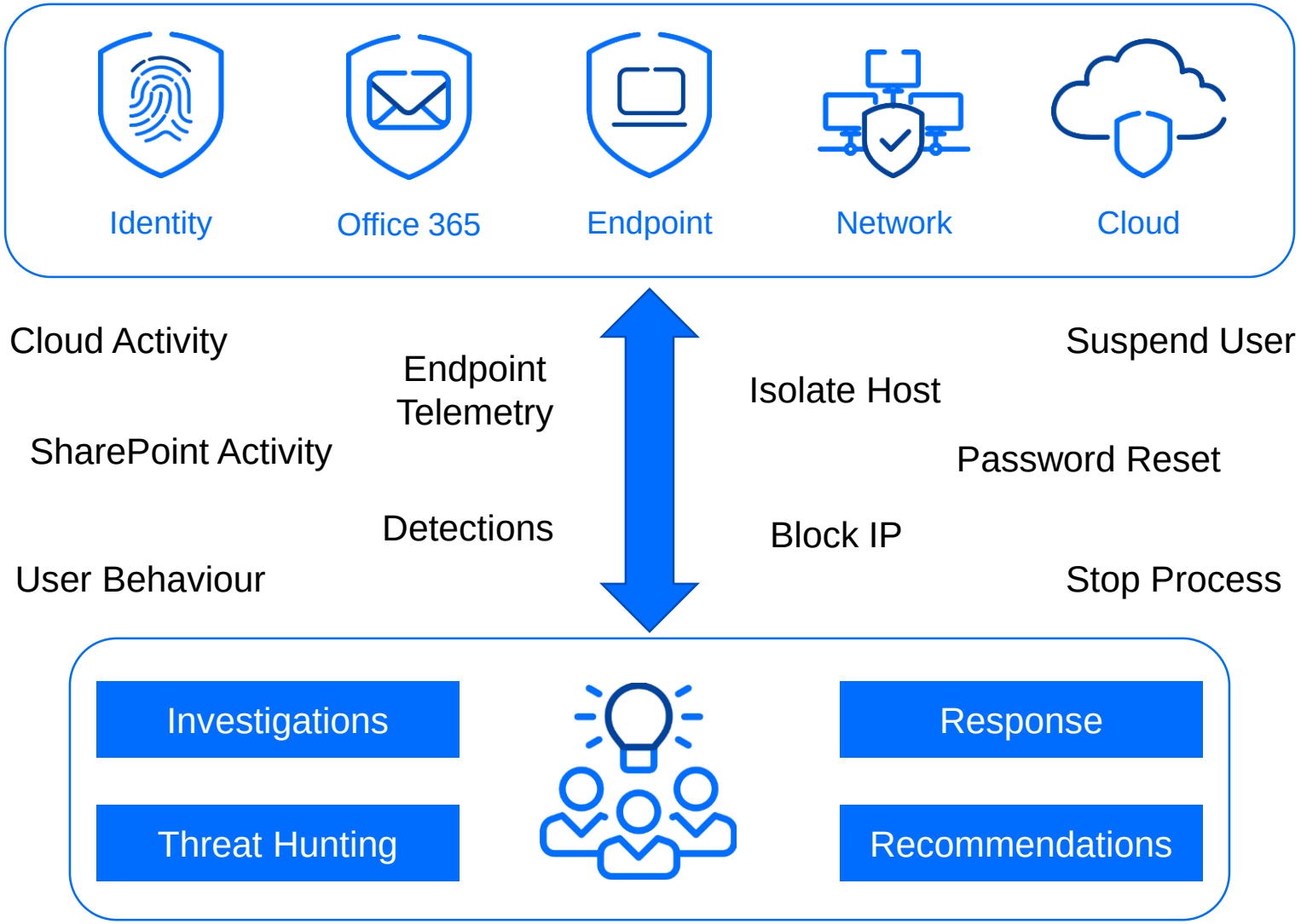
Limited in-house security capabilities

Options to address the problems



GravityZone XDR for MDR

Bitdefender



Bitdefender

Built from the ground up with our customers

"GravityZone XDR ***excels at connecting and correlating incidents*** *over time throughout our entire operations and* ***we experienced immediate value.*** *The benefit of having a single-vendor solution with* ***out-of-the-box detection capabilities for identifying and investigating known and unknown threats*** *and providing our analysts with the* ***knowledge of what and how an incident happened with the best ways to respond cannot be overstated****."*

Mahmood Haq
CISO, MyVest

Bitdefender®

BUILT FOR RESILIENCE

XDR Data Sources (GA)

Bitdefender

Microsoft Office365

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

Active Directory

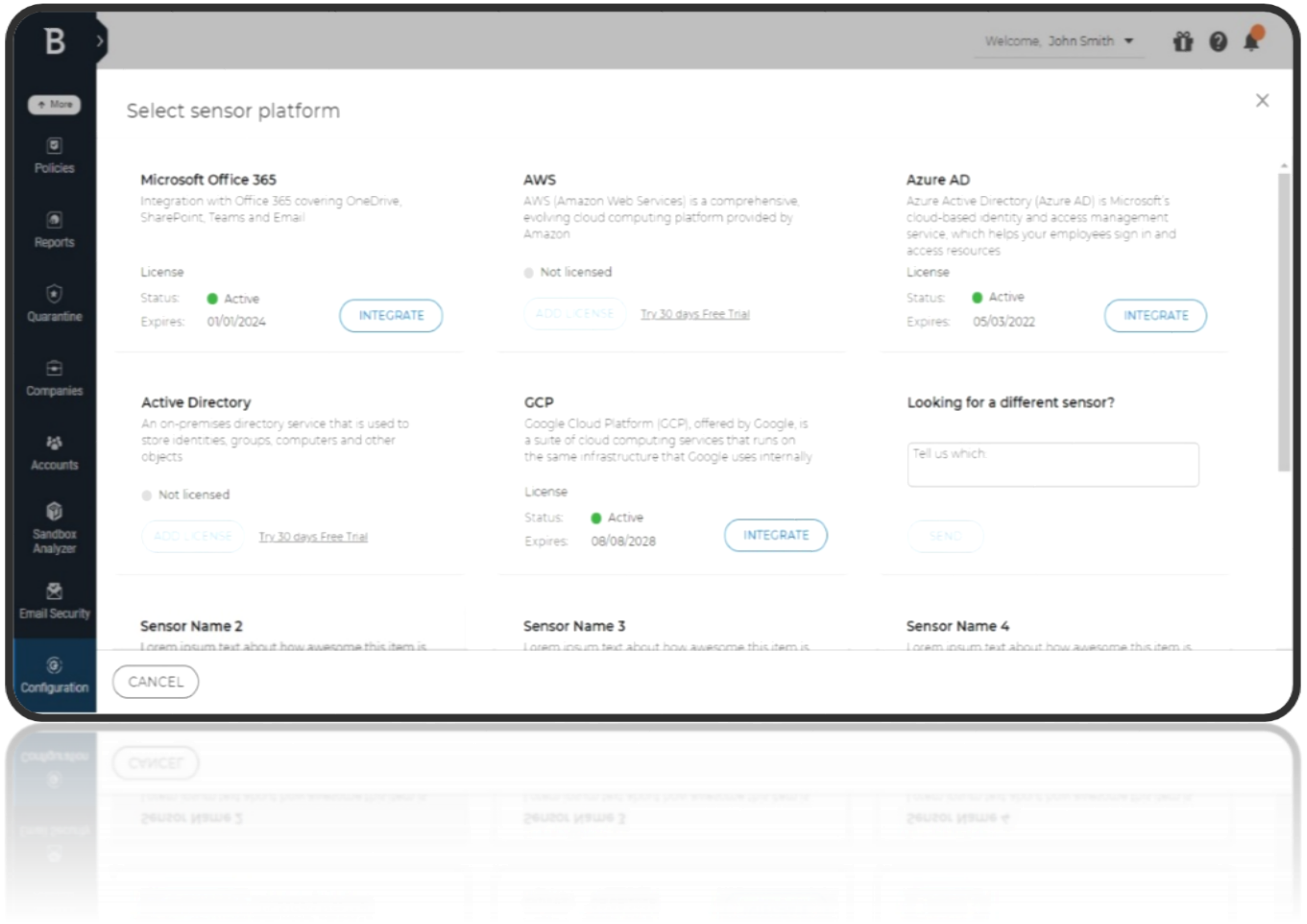
- ✓ On-premises AD
- ✓ Azure AD

Clouds

- ✓ AWS

Network

- ✓ Bitdefender Network Sensor



Detection & Response (GA)

Bitdefender

Incident Advisor

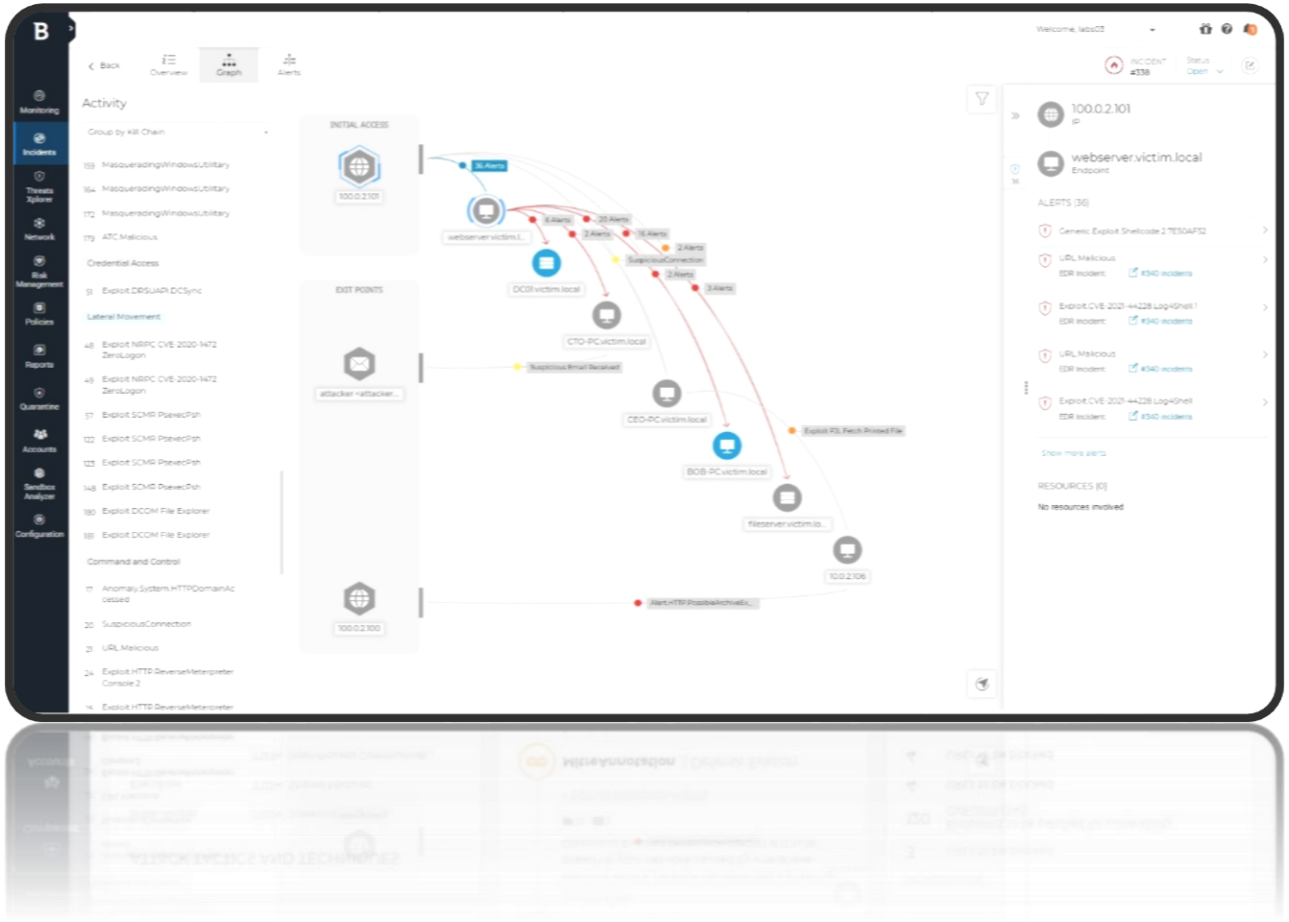
- ✓Summary
- ✓Root Cause
- ✓Organization Impact
- ✓Highlights

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

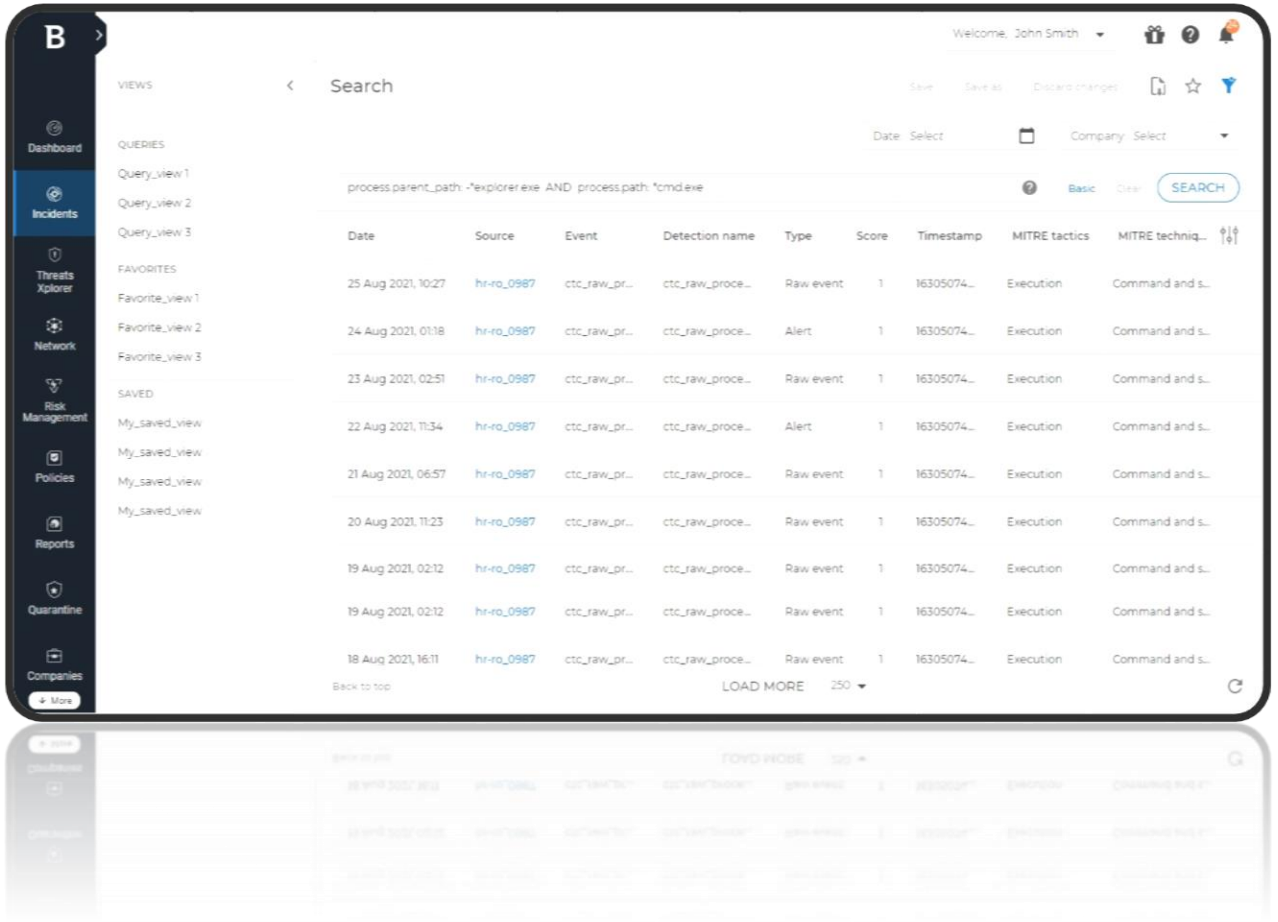
- ✓ Advanced filtering
- ✓ Enhanced data display
- ✓ Multiple data sources
- ✓ Smart views

Investigation Package

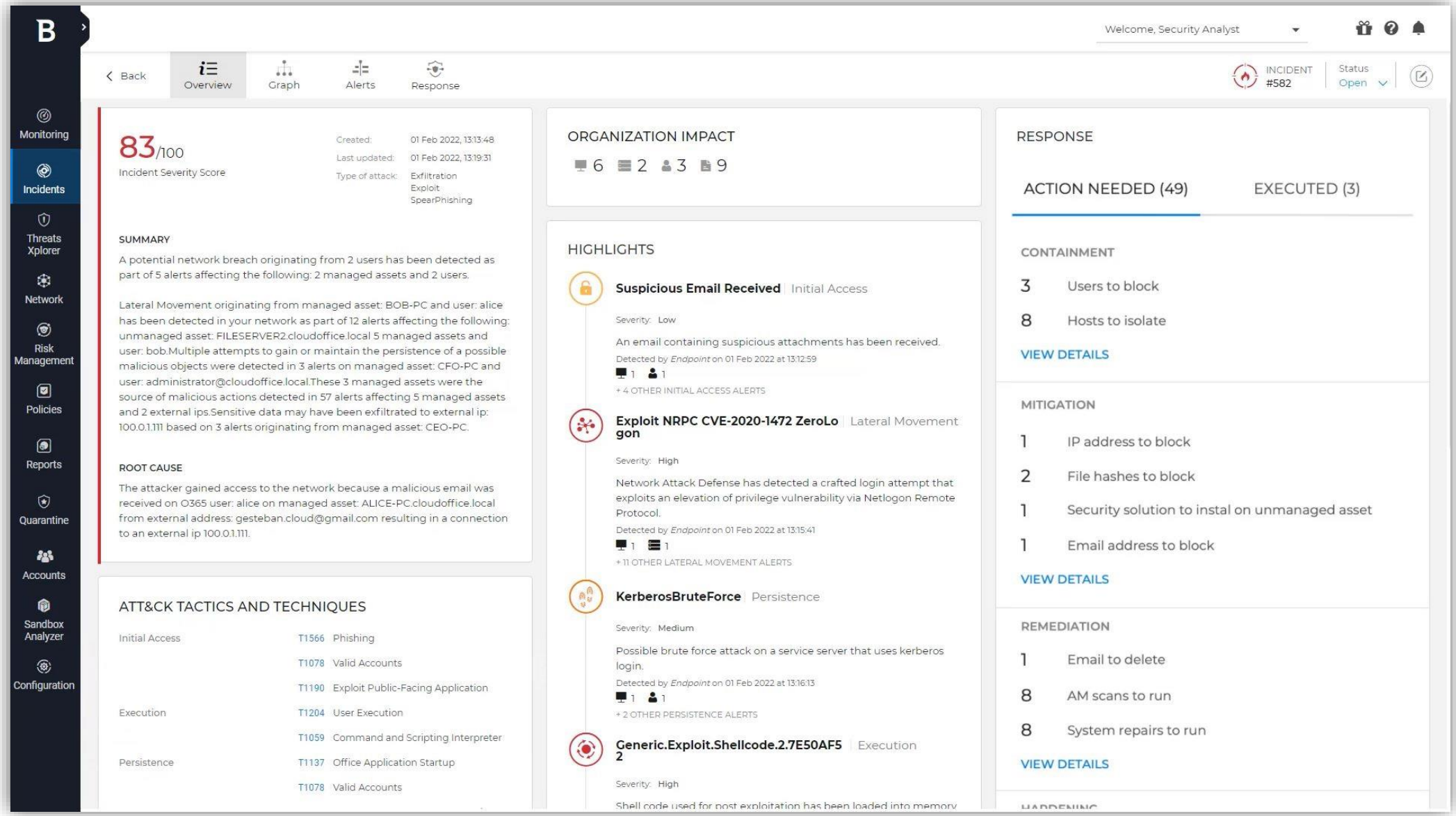
- ✓ Collect forensic endpoint data
- ✓ OS: Windows, Linux, Mac

Full Remote Shell

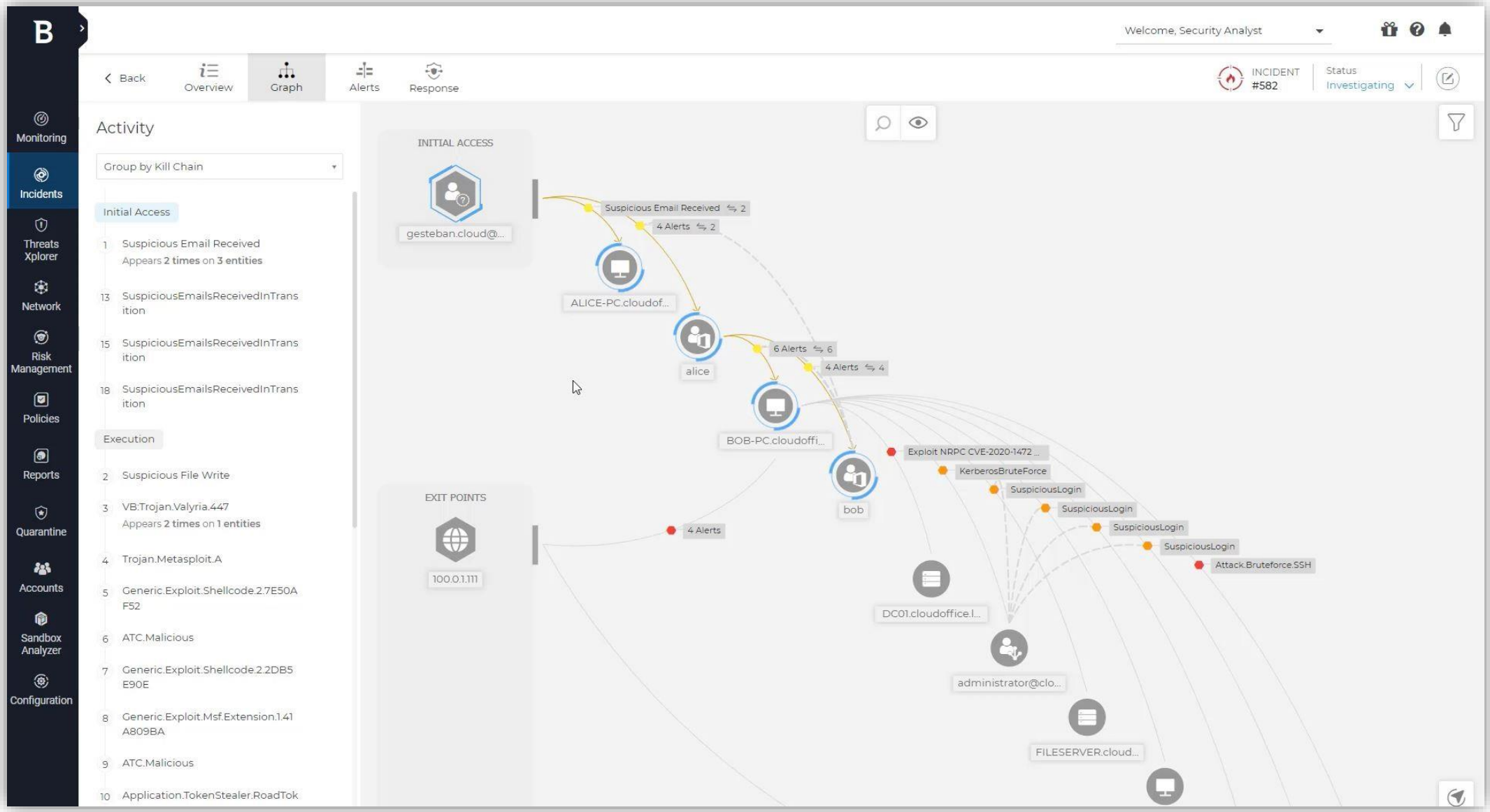
- ✓ Direct investigation & response across endpoints
- ✓ OS: Windows, Linux, Mac



GravityZone XDR – Incident Advisor



GravityZone XDR – Incident Graph



Detection use cases

Bitdefender

Identity Compromise

- User credentials
- Workload/Service Tokens
- Platform Auth
- Service Account

Analysis of user behavior/identity to detect

- Suspicious login patterns
- Identification of improper user account usage
- Credential probing
- Account creations & lockouts
- Service account misuse
- Admin privilege misuse
- Account Manipulation

Lateral Movement

- Identity <=> Workload
- Workload <=> Service
- Platform <=> Service

Analysis of identities and lateral movement to detect

- Compromised authentication credentials
- Suspicious interactions (baseline violations)
- Risky entities

…across identity providers, workloads, platforms and services

Office365

Analysis of cloud productivity suites/email to detect

Detection category	Example
Email exfiltration	A suspicious application (an application that requests read access to all users documents) was used to download files from a user's account
Spearphishing attempts	Users receive emails with spearphishing URLs in the body(correlation between EDR and O365)
Suspicious Mailbox Permissions created/updated	A certain user has received permissions to many mailboxes in a short amount of time
Suspicious User created/updated	A newly created user has been immediately excluded from MFA
Antiphishing Protection Disabled	A user has disabled/removed the phishing filter policy/rule
Documents with Macros re-uploaded on SharePoint/OneDrive	A user has downloaded a document and then re-uploaded it. The re-uploaded document contains macros that can be used to infect others
Executable File Uploaded to a different account	A user uploaded an executable file to a different Office365 account
Multiple Access Requests created in SharePoint	A user requested access to multiple files or directories on different sites in a very short amount of time
Multiple Emails Deleted in non-owned mailboxes	A user started to delete a large number of emails in mailboxes it doesn't own across multiple sites
Anomaly detection	A user had an unusual frequency of administrative activities or document manipulation activities in the last day.

and to respond

- ❑ Delete email across O365 organization
- ❑ Suspend O365 account

Active Directory

Analysis of user behavior/identity to detect

Detection category	Example
Kerberos attacks	• An attacker is executing a brute force attack on a service server that uses Kerberos login • An attacker is able to extract the TGS tickets from memory, or captures them by sniffing network traffic, and extracts the service account's password hash and attempts an offline brute force attack to obtain the plaintext password • A Kerberos ticket with weak encryption was requested indicating Kerberoasting activity • An intruder steals a packet from the network and forwards that packet to a service or application as if the intruder was the user who originally sent the packet (replay attack)
Pass-the-hash attacks*	An attacker authenticates to a remote server or service by using the underlying NTLM hash of a user's password, instead of requiring the associated plaintext password as is normally the case
Pass-the-ticket attacks*	An attacker "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls
Suspicious operations performed on AD object*	An attacker is performing various activities(create/update/delete/move) on an Active Directory object
DCShadow attacks*	An attacker registers a rogue Active Directory Domain Controller and uses that to inject malicious Active Directory objects (e.g. credentials) to other Domain Controllers that are part of the same Active Directory infrastructure.
Suspicious logins	A TGS request was granted after a brute-force attack

and to respond

- ❑ Disable AD account
- ❑ Force password reset for AD

AWS

Analysis of cloud providers to detect

Detection category	Example
Suspicious recognition activity on Lambda functions	• An attacker has listed lambda functions, downloaded one of them • A lambda function executing a suspicious action by updating an assume role policy to allow external access
Recognition activity against S3 buckets	An attacker performs multiple Recon events against S3 buckets by listing various buckets, functions etc
User login from multiple regions	An attacker has logged in from multiple regions simultaneously
Deleted bucket encryption	An unfamiliar user or host removes default encryption from the S3 bucket exposing all objects that were encrypted (using server-side encryption) in that S3 bucket
Suspicious Ingress Port allowed via Lambda function	An attacker has executed a lambda function triggering a suspicious action by updating a security group to allow ingress on a port
Evading defenses by disabling/removing monitoring services	An attacker is attempting to delete audit data by stopping CloudTrail or by deleting a log group or stream from CloudWatch
Suspicious IAM user via Lambda function	An attacker has triggered a suspicious action by executing a lambda function that created an access key to backdoor an IAM user
AWS anomaly detection	• A user has performed actions that are outside of the baseline • A file with a suspicious extension has been uploaded outside of the baseline • A cloud function has been used to perform an action outside of the usual scope

Network

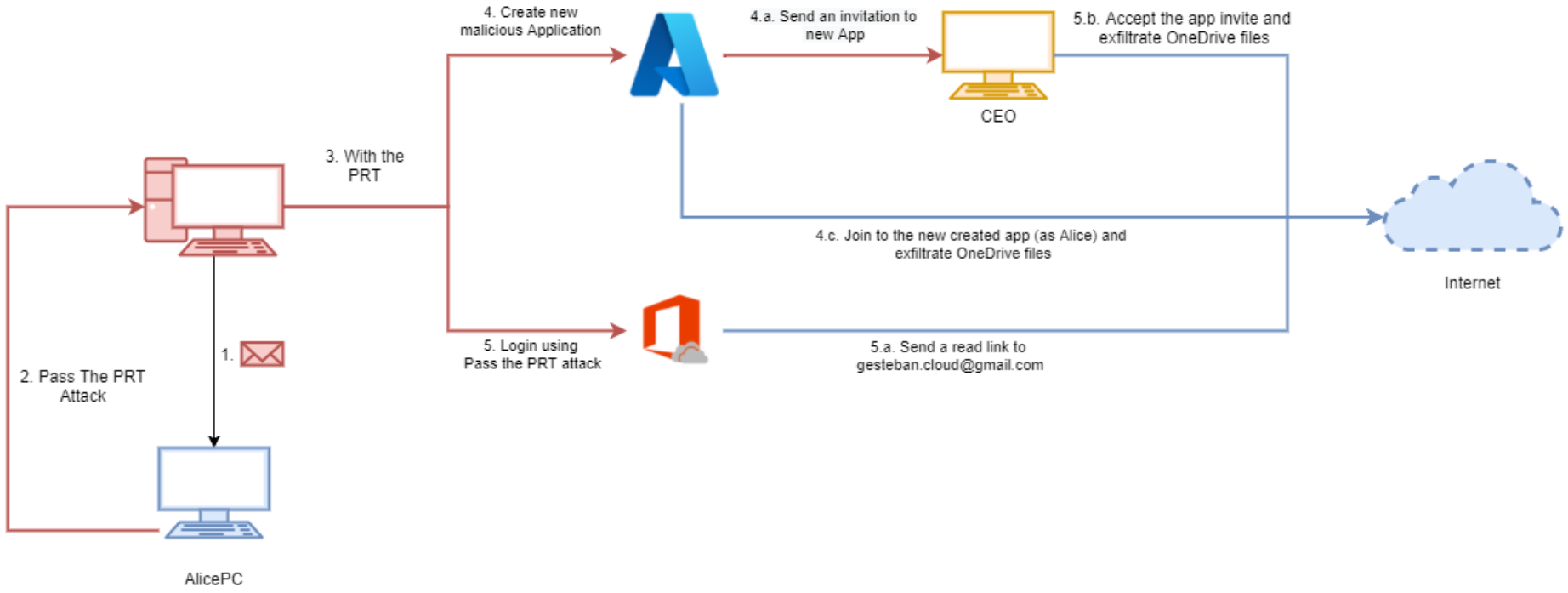
Analysis of internal and external traffic to detect

Detection category	Example
Lateral movement within the organization	An attacker is moving within the network
Data Exfiltration	An attacker exfiltrates data outside of the organization
Brute-force attempts	An attacker is trying to login into a system using brute-force
Port scanning	An attacker is leveraging external custom tools and open-source tools for port scanning in an attempt to map the network and devices

Office365 - Scenario

Sensors

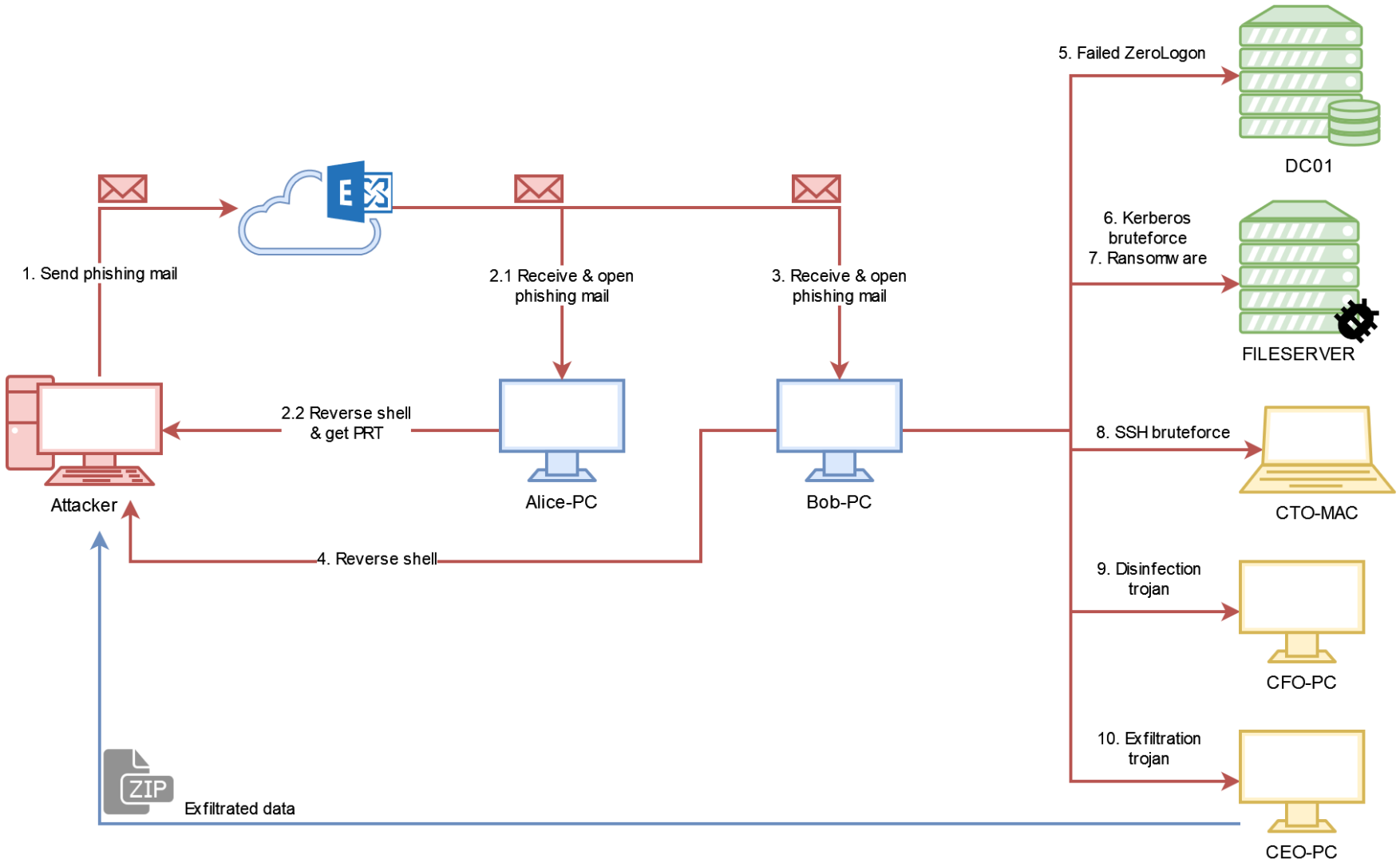
- EDR
- Office365



Active Directory - Scenario

Sensors

- EDR
- Office365
- Active Directory



Network - Scenario

Sensors

- EDR
- Network Sensor