GravityZone XDR

Roberto Novasconi - Avangate Security
Senior Support and Training Specialist

AVANGATE
Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

Bitdefender

Definizioni

AVANGATE

EDR	**E**ndpoint **D**etection and **R**esponse
XEDR	e**X**tended **E**ndpoint **D**etection and **R**esponse
XDR	e**X**tended **D**etection and **R**esponse
MDR	**M**anaged **D**etection and **R**esponse

Endpoint Detection and Response

Bitdefender

La tecnologia di rilevamento e risposta che viene utilizzata per identificare comportamenti sospetti e minacce persistenti avanzate (APT) ed informare di conseguenza gli amministratori.

Lo fa raccogliendo e aggregando dati da **singoli endpoint**.

AVANGATE

eXtended Endpoint Detection and Response

Bitdefender

eXtended Endpoint Detection and Response è l'evoluzione delle soluzioni EDR

che aggiunge funzionalità di analisi e **correlazione degli eventi di sicurezza tra gli endpoint**.

AVANGATE

eXtended Detection and Response

Bitdefender

Il rilevamento e la risposta estesi funzionano **raccogliendo e correlando i dati da dispositivi di varia natura,** come server, e-mail, carichi di lavoro cloud ed endpoint.

Un sistema XDR aumenta la quantità di informazioni ed allarga lo sguardo su un numero più esteso di dispositivi, offrendo allo stesso tempo una visione sintetica ed efficace ai fini dell'analisi e della reazione in tempi rapidi.

AVANGATE

Managed Detection and Response

Bitdefender

Managed Detection and Response (MDR) indica **servizi** di sicurezza informatica **in outsourcing** progettati per tutelare i dati e le risorse anche se una minaccia elude i comuni controlli di sicurezza dell'organizzazione.

MDR prevede controllo di sicurezza avanzato **24 ore su 24, 7 giorni su 7**,

che spesso include una serie di attività di sicurezza fondamentali, quali la sicurezza gestita dal cloud, per le organizzazioni che non possono mantenere il proprio centro operativo di sicurezza. I servizi MDR combinano **analisi avanzate**, **intelligence** sulle minacce ed **esperienza umana** nell'indagine sugli incidenti e nella risposta distribuita a livello di host e di rete.

AVANGATE

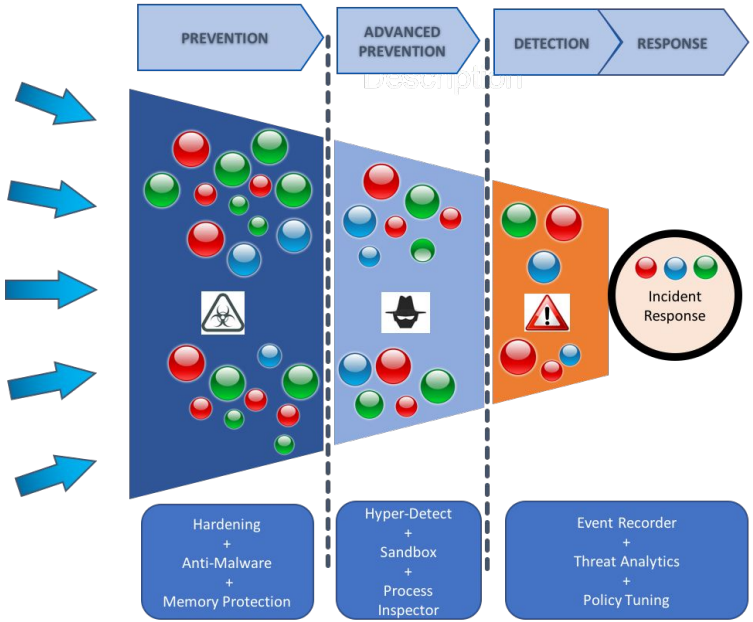
Bitdefender

EDR
Concetti

AVANGATE

Endpoint Detection and Response

Bitdefender



AVANGATE

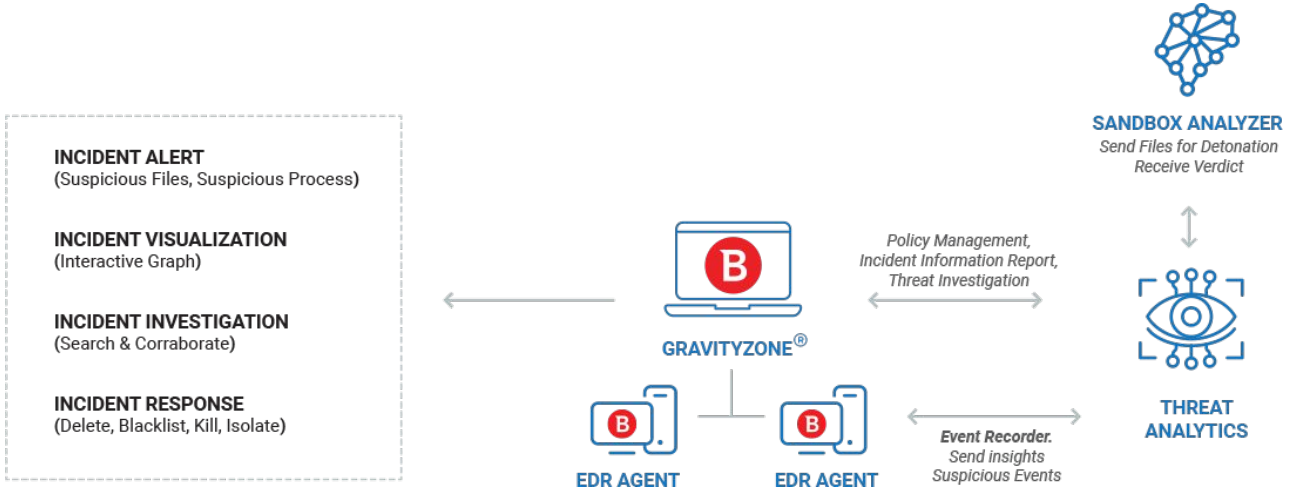
Bitdefender

XEDR
Concetti

AVANGATE

eXtended Endpoint Detection and Response

Bitdefender



AVANGATE

Bitdefender

XDR
Concetti

AVANGATE

eXtended Detection and Response

Bitdefender

Endpoints

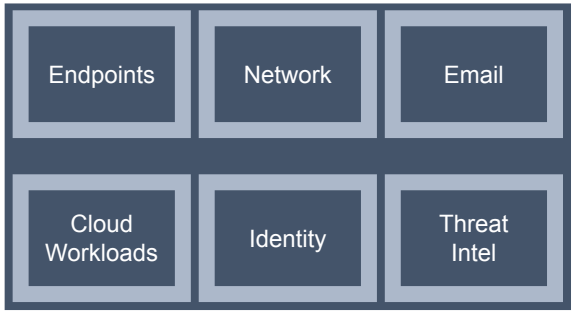
- What happened within the endpoint?
- How did an attack propagate?
- What are the risks on the endpoints?

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?

AVANGATE

Bitdefender

MDR
Concetti

AVANGATE

Managed Detection and Response

Bitdefender

AVANGATE

Bitdefender

XDR
Nuovi Sensori

AVANGATE

XDR Additional Data Sources

Bitdefender

XDR Sensor - Productivity

- ✓ MS 365 OneDrive
- ✓ MS 365 SharePoint
- ✓ MS 365 Teams
- ✓ MS 365 Email

XDR Sensor - Identity

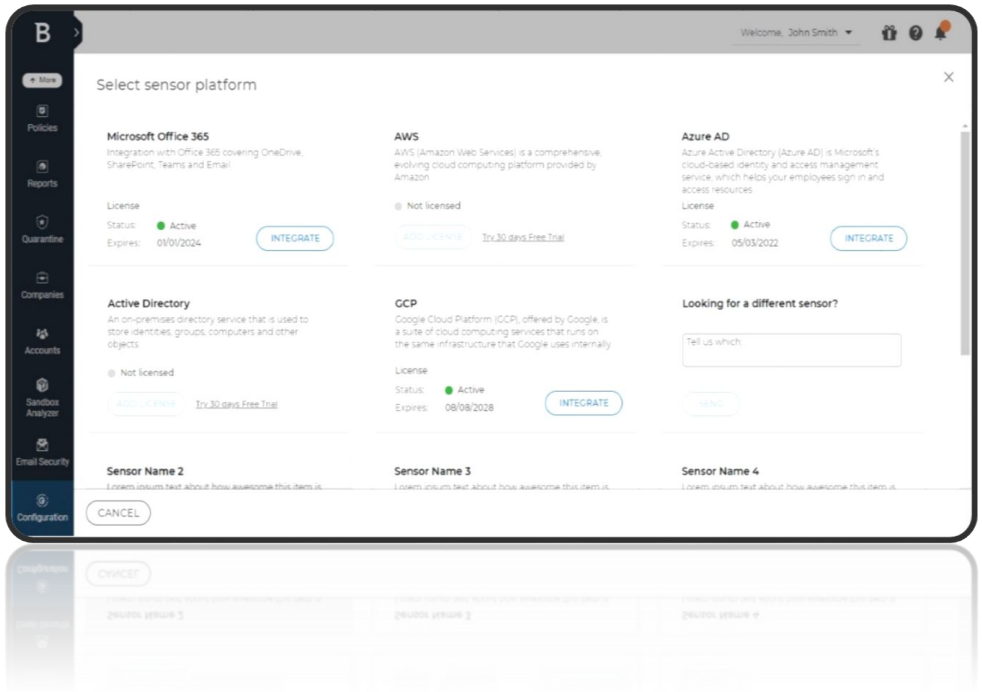
- ✓ On-premises AD
- ✓ Azure AD

XDR Sensor - Cloud

- ✓ AWS

XDR Sensor - Network

- ✓ Bitdefender Network Sensor



Bitdefender XDR Sensor - Productivity

Bitdefender

Perchè

Sempre più attacchi recano attacchi alle aziende tramite posta elettronica.
Diventa quindi essenziale estendere il campo dell'analisi al di la del singolo messaggio email, includendo l'analisi dell'intero flusso di posta elettronica all'interno di un'azienda, al fine di identificare e analisti della sicurezza all'interno di queste società di potenziali attacchi informatici (eventi di sicurezza).

Cosa

Colleziona Email ed eventi di audit di MS365 e

- Correla gli eventi per creare nuovi incidents e/o completare gli esistenti
- Archivia gli eventi di audit per la ricerca storica

Come

- Integrando MS365 nella Gestione dei Sensori
- Acquistando licenza Add-On
- Configurando l'integrazione Integrazione Cloud based

AVANGATE

Productivity - MS 365

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

Bitdefender XDR Sensor - Identity

Bitdefender

Perchè

Active Directory è un obbiettivo primario durante i cyber attacchi.

Statistiche su Active Directory

1. 90% delle imprese al mondo usa AD.
2. Gli attaccanti indirizzano 95 milioni di AD al giorno
3. 80% degli attacchi includono la compromissione di AD.

Cosa

Colleziona gli eventi utente da on-premise AD ed Azure AD e poi

- Correla gli eventi per creare nuovi incidents e/o completare gli esistenti
- Archivia gli eventi per la ricerca storica

Come

- Integrando AD e Azure AD nella Gestione dei Sensori
- Acquistando licenza add-on
- L'integrazione con AD On-Premise richiede il modulo EDR di GravityZone installato su ciascun DC
- Azure AD richiede licenza Azure AD Premium P1 or P2

AVANGATE

Identity - 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

Bitdefender XDR Sensor - Cloud

Bitdefender

Perchè

Mancanza di visibilità delle attività sospette nell'amministrazione delle piattaforme cloud.

Cosa

Colleziona eventi da AWS e poi

- Correla gli eventi per creare nuovi incidenti o completare gli esistenti
- Archivia gli eventi per consultazione storica.

Come

- Integrando AWS nella gestione dei sensori
- Venduto come licenza add-on
- Integrazione Cloud based (using AWS CloudTrail, AWS Config, Amazon SQS and Amazon SNS)
- Nota!: introduce dei costi addizionali sui servizi AWS per il cliente

AVANGATE

Cloud - AWS

Analysis of cloud providers to detect

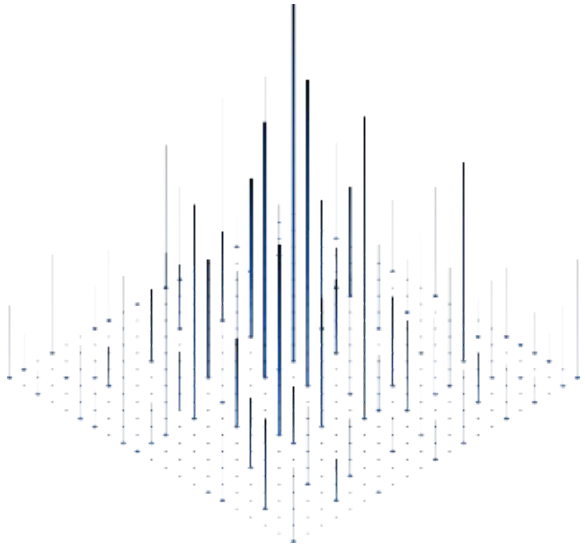
Detection category	Example
Suspicious recognition activity on Lambda functions	• An attacker has listed lambda functions, downloaded one of them • A lambda function executing a suspicious action by updating an assume role policy to allow external access
Recognition activity against S3 buckets	An attacker 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

Bitdefender XDR Sensor - Network

Bitdefender

Perchè

- Gli asset IT non sono fatti solo di Endpoint (anche IOTs, network devices, stampanti, etc).
- Le soluzioni EDR non sono in grado di rilevare attacchi che coinvolgono dispositivi diversi dagli endpoint, che NON possono essere protetti con un agent a bordo.



Cosa

Collezionare eventi relativi al traffico di rete e poi

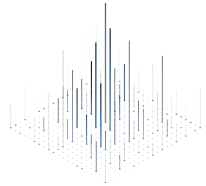
- Correlare gli eventi per creare nuovi incidenti e/o completare gli esistenti
- Archiviare gli eventi per consultazione storica

Come

- Analizzando il flusso dati con dei sensori OnPremise
- Acquistando licenza add-on
- Implementando manualmente i sensori di rete nellorganizzazione.

AVANGATE

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

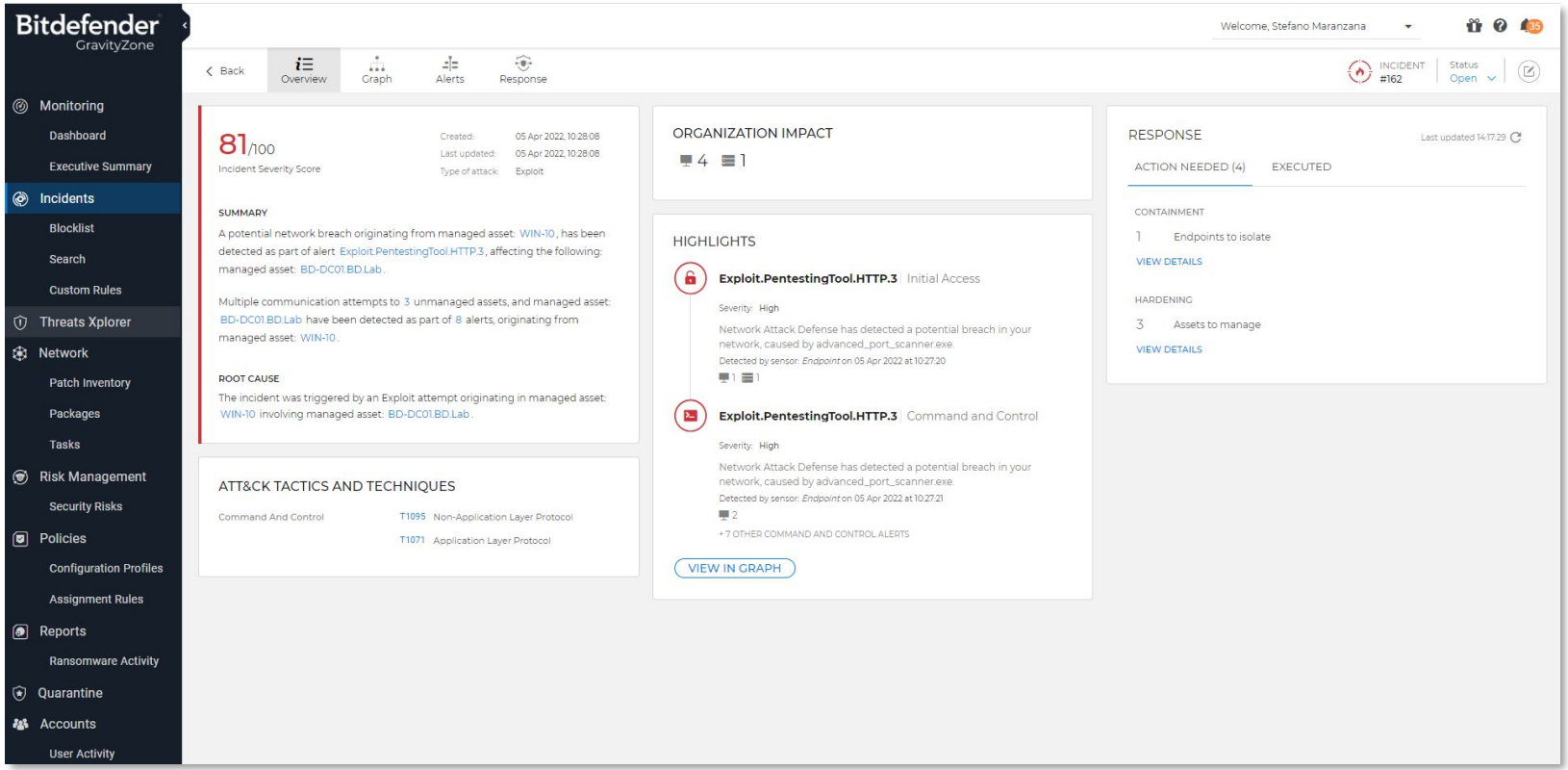
Bitdefender

XDR
Visualizzazione potenziata

AVANGATE

Incident Overview Estesa

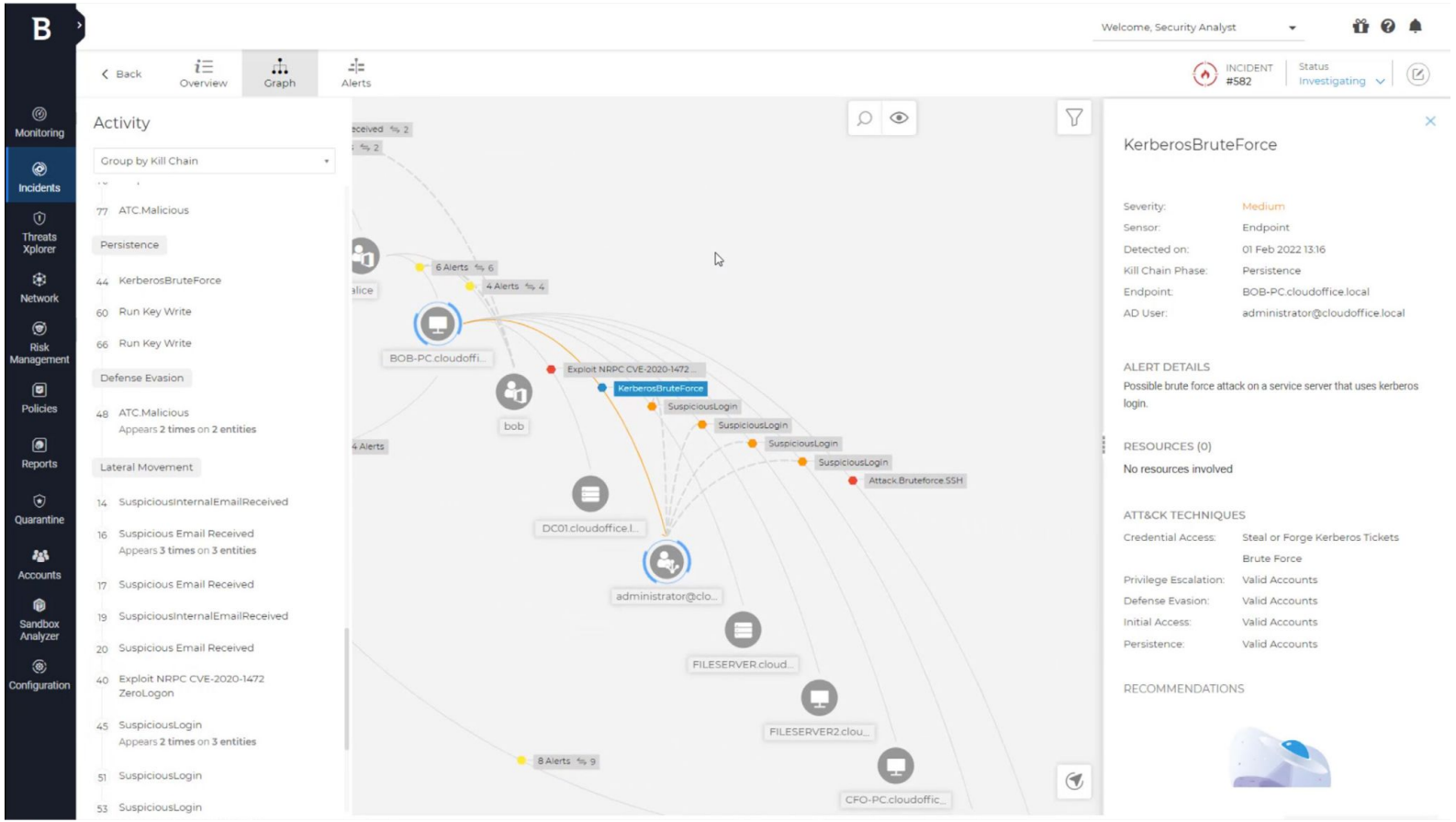
Bitdefender



AVANGATE

Incident Graph Estesa

Bitdefender



AVANGATE

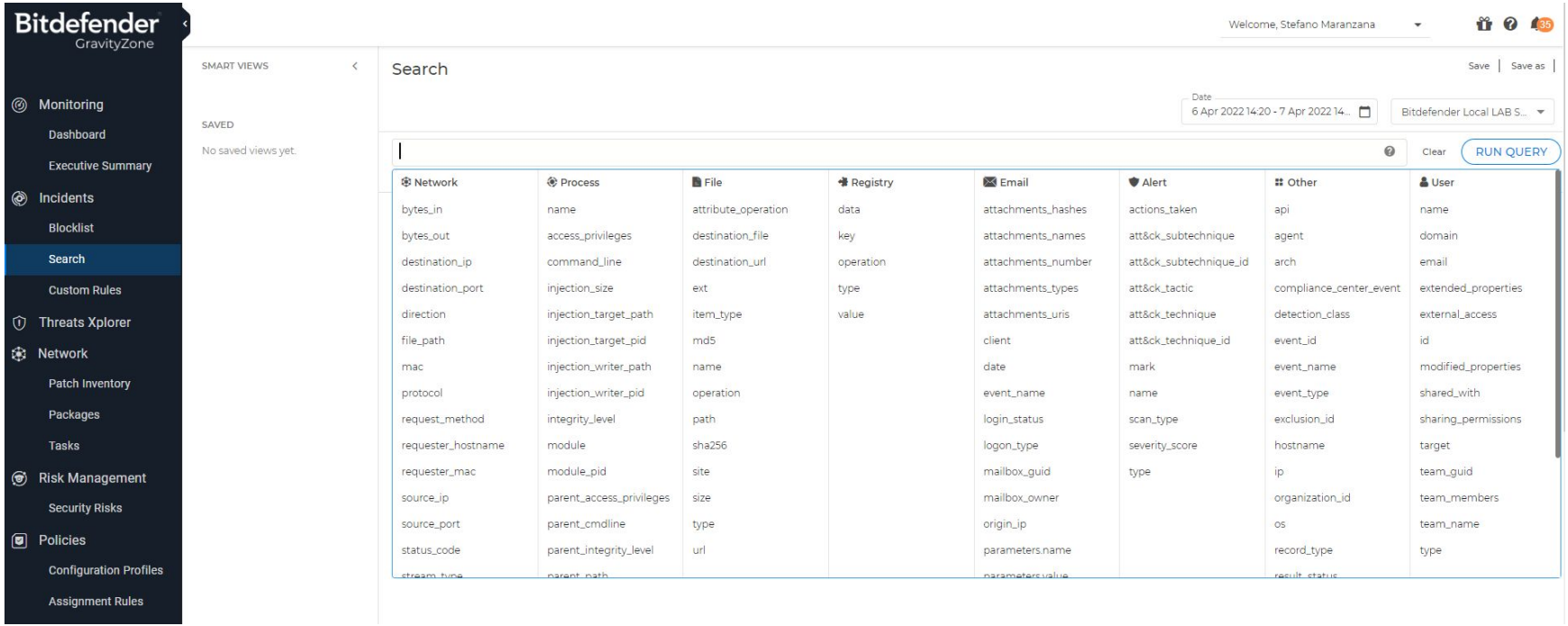
Bitdefender

XDR
Consultazione storica

AVANGATE

Ricerca Storica

Bitdefender



AVANGATE

Bitdefender

Reazione

AVANGATE

Reazioni Extra Endpoint

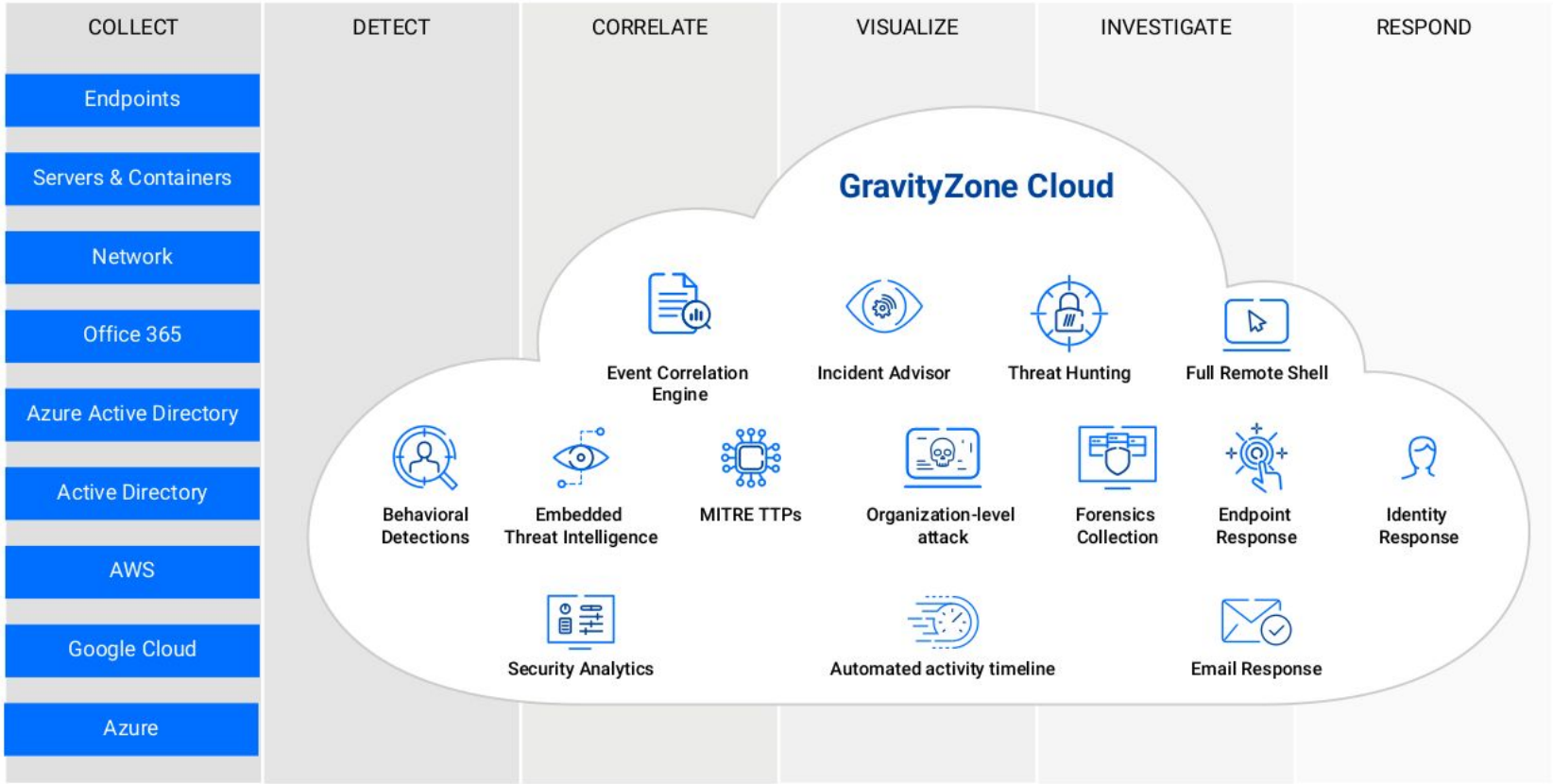
Bitdefender

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.

AVANGATE

XDR - Overview

Bitdefender



AVANGATE

Bitdefender

Licensing

AVANGATE

XDR - Prepaid License

XDR - Base license

- GravityZone Business Enterprise
- Bitdefender Cloud EDR

XDR - Sensors (add-on)

- XDR Sensor - Productivity
- XDR Sensor - Identity
- XDR Sensor - Cloud
- XDR Sensor - Network

XDR Sensors - Licensing

Bitdefender

XDR Sensor - Productivity

Per MS 365 Seat license

XDR Sensor - Identity

Per active AD User license

XDR Sensor - Cloud

Per EC2 Instance license

XDR Sensor - Network

Per endpoint license.

Risorse

sezione Documenti di GoToWebinar

- Slide di questa presentazione
- GravityZone XDR - Datasheet
- GravityZone XDR - Scheda Tecnica
- GravityZone XDR - Presentazione Ufficiale

AVANGATE

Domande

Sezione Domande del pannello GoToMeeting

AVANGATE

Distributore a valore aggiunto

contatti pubblici

www.avangate.it → Assistenza Live

contatti per i partner

Login AREA PARTER Avangate Italia https://nova.avangate.it

Chat	In alto a destra:	**LiveSupport**
Telefono	In alto a sinistra:	**Linea Diretta Partner**
Ticket	Menu Supporto:	**Inserisci una richiesta**

AVANGATE

Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

Roberto Novasconi

GRAZIE