



Bitdefender

GravityZone XDR Sensori

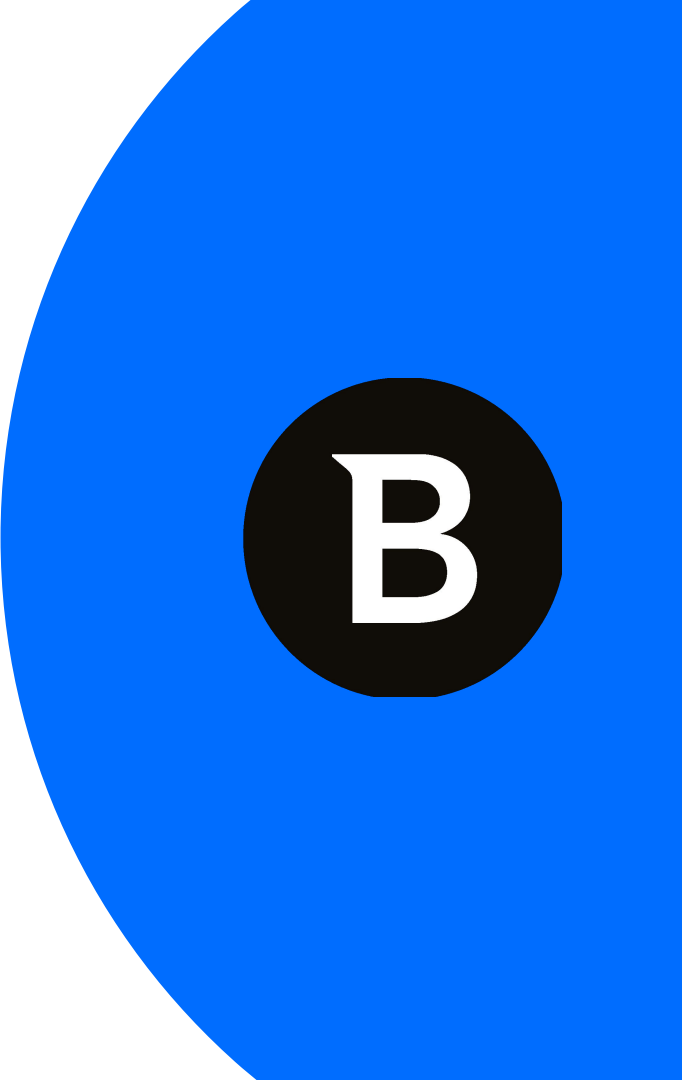
AVANGATE
SECURITY

Roberto Novasconi - Avangate Security
Senior Support and Training Specialist

Bitdefender
AUTHORIZED DISTRIBUTOR

Definizioni

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



B

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**.

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.**

eXtended Detection and Response

Bitdefender®

Il rilevamento e la risposta estesi funzionano **raccogliendo e correlando i dati da dispositivi di varia natura**, come endpoint, rete locale, domain controller, applicazioni cloud, cloud server.

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

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.

XDR

Extended Detection and Response

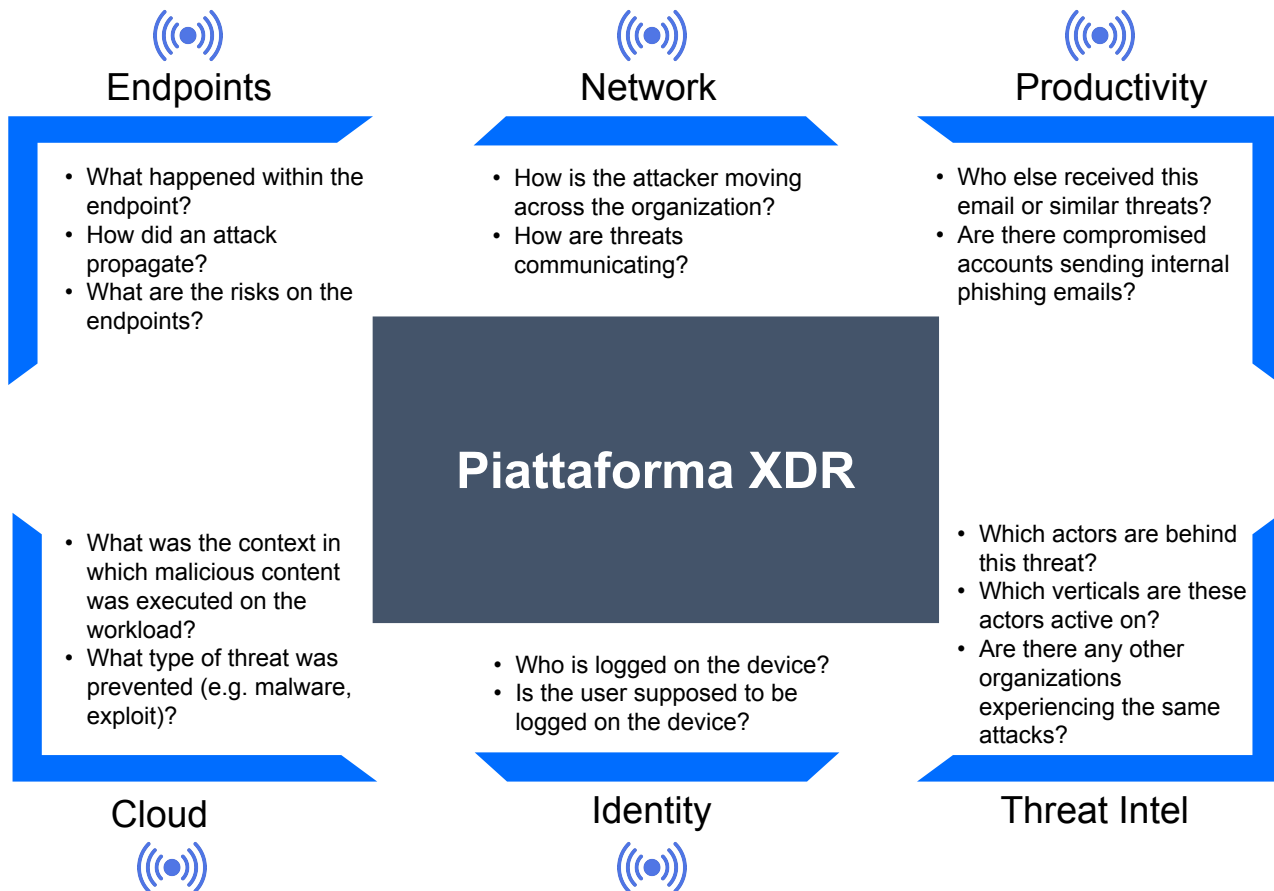
perchè XDR

Bitdefender®

- correlazione degli eventi fra dispositivi diversi
- intelligenza artificiale per la classificazione degli eventi (triage)
- ricerca degli indicatori di compromissione (Search, IOC Search)
- Blocklist, Custom Detection Rules e Custom Exclusion Roles
- Live Search sugli endpoint
- azioni di remediation (Block/Quarantine/Delete, Isolate, Patch, Remote shell, Disable Account)
- suggerimenti per la remediation

eXtended Detection and Response

Bitdefender®



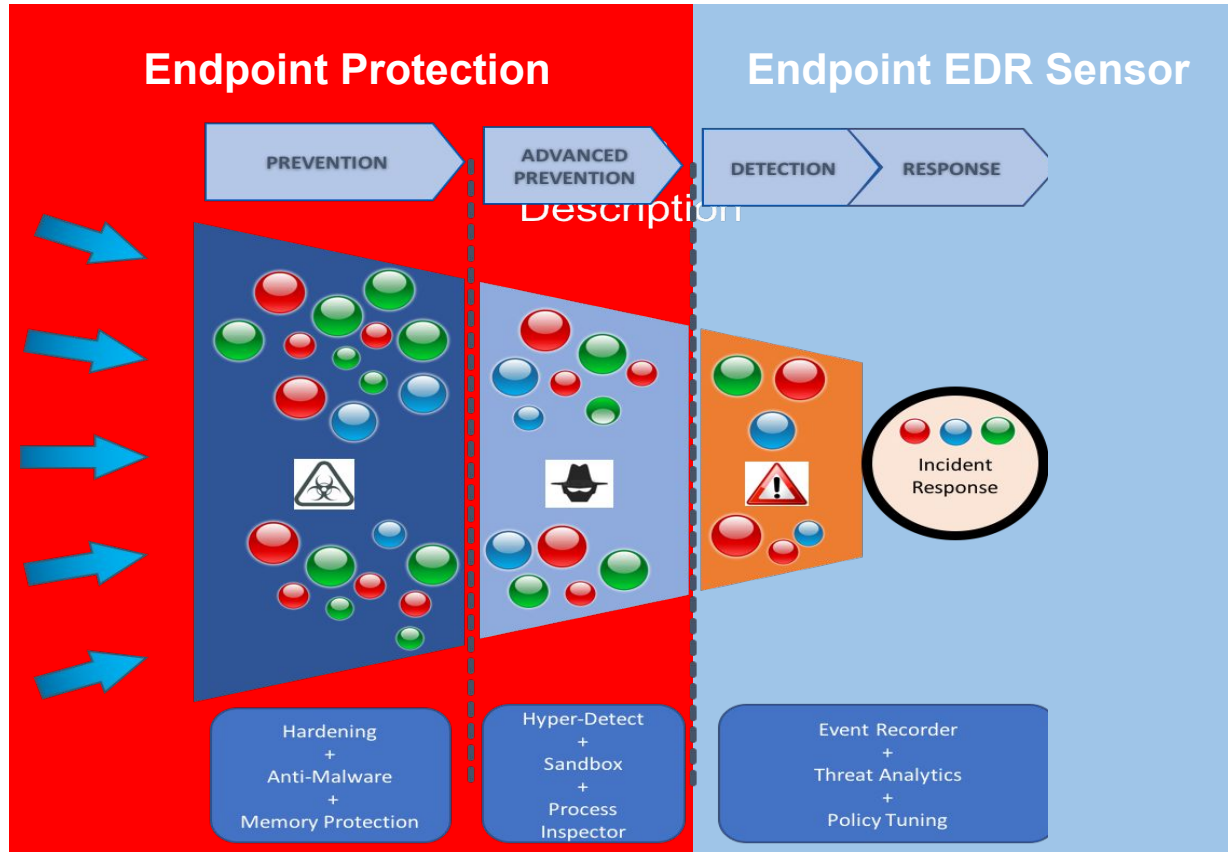
Bitdefender[®]

XDR sensore Endpoint

Sensore Endpoint

Bitdefender®

Cyber
Attacks



XDR
Platform

AVANGATE

XDR Sensori

XDR Sensor - Productivity

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

XDR Sensor - Identity

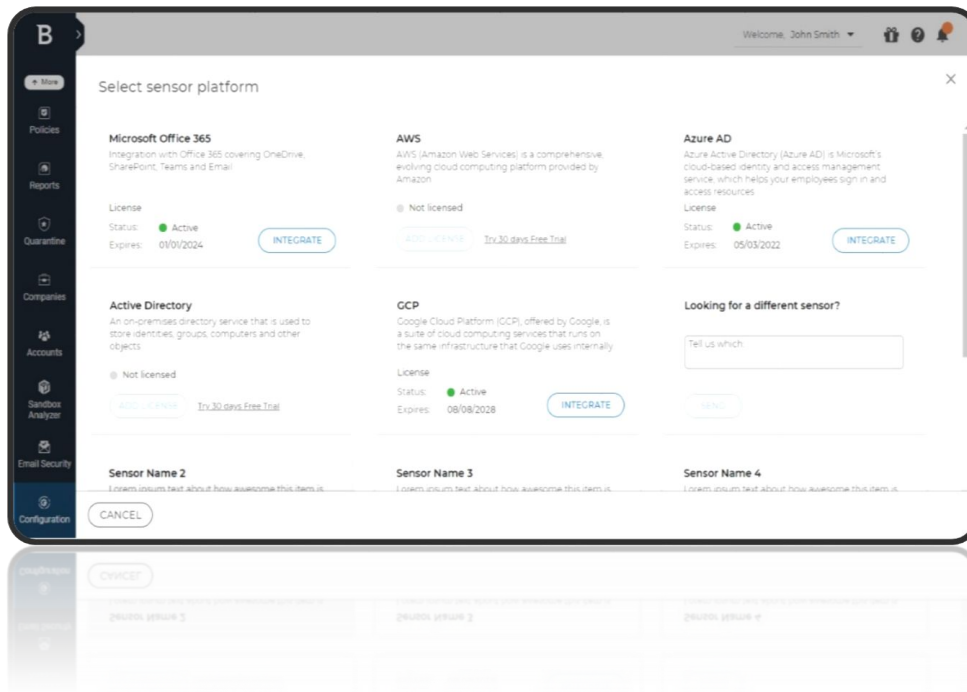
- ✓ On-premises AD
- ✓ Azure AD

XDR Sensor - Cloud

- ✓ AWS
- ✓ Google Cloud

XDR Sensor - Network

- ✓ Bitdefender Network Sensor



Bitdefender[®]

XDR sensore Productivity

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 - Productivity

Bitdefender®

Cosa fa

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 si attiva

- Acquisto licenza Add-On per XDR Sensor - Productivity
- Aggiungo il sensore alla console GravityZone e Configuro l'integrazione con MS365 (Configuration→Sensor Management→Add)



XDR sensore Identity

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 - Identity

Bitdefender®

Perchè

Active Directory è un obiettivo 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 fa

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 si attiva

- Acquisto licenza add-on per XDR Sensor - Identity
- Aggiungo il sensore alla console GravityZone e Configuro l'integrazione con AD (Configuration→Sensor Management→Add)
- L'integrazione con AD On-Premise richiede il modulo EDR Sensor di GravityZone installato su ciascun DC
- Azure AD richiede licenza Azure AD Premium P1 or P2



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 - Cloud

Bitdefender®

Perchè

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

Cosa fa

Colleziona eventi da AWS e poi

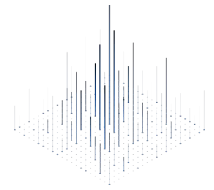
- Correla gli eventi per creare nuovi incidenti o completare gli esistenti
- Archivia gli eventi per consultazione storica.

Come si attiva

- acquisto licenza addon per XDR Sensor - Cloud
- In console GZ lo aggiungo alla gestione dei sensori e ne configuro l'integrazione con l'amministratore del tenant AWS.
Integrazione Cloud based (using AWS CloudTrail, AWS Config, Amazon SQS and Amazon SNS)
- Nota!: introduce dei costi aggiuntivi sui servizi AWS per il cliente



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 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.

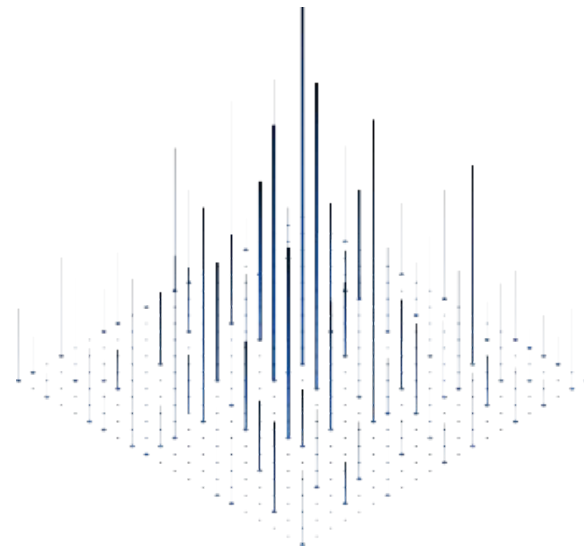
Cosa

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 nell'organizzazione.



XDR

Visualizzazione potenziata

Incident Overview Estesa

Bitdefender®

Bitdefender
CravityZone

Monitoring

Dashboard

Executive Summary

Incidents

Blocklist

Search

Custom Rules

Threats Xplorer

Network

Patch Inventory

Packages

Tasks

Risk Management

Security Risks

Policies

Configuration Profiles

Assignment Rules

Reports

Ransomware Activity

Quarantine

Accounts

User Activity

Welcome, Stefano Maranzana

INCIDENT #162

Status Open

Overview

Graph

Alerts

Response

81/100

Incident Severity Score

Created: 05 Apr 2022, 10:28:08

Last updated: 05 Apr 2022, 10:28:08

Type of attack: Exploit

ORGANIZATION IMPACT

4 1

HIGHLIGHTS

🔒

Exploit.PentestingTool.HTTP.3 Initial Access

Severity: High

Network Attack Defense has detected a potential breach in your network, caused by advanced_port_scanner.exe.

Detected by sensor: Endpoint on 05 Apr 2022 at 10:27:20

1 1

📄

Exploit.PentestingTool.HTTP.3 Command and Control

Severity: High

Network Attack Defense has detected a potential breach in your network, caused by advanced_port_scanner.exe.

Detected by sensor: Endpoint on 05 Apr 2022 at 10:27:21

2

+7 OTHER COMMAND AND CONTROL ALERTS

VIEW IN GRAPH

ATT&CK TACTICS AND TECHNIQUES

Command And Control

T1095 Non-Application Layer Protocol

T1071 Application Layer Protocol

RESPONSE

Last updated 14.17.29

ACTION NEEDED (4)

EXECUTED

CONTAINMENT

1 Endpoints to isolate

[VIEW DETAILS](#)

HARDENING

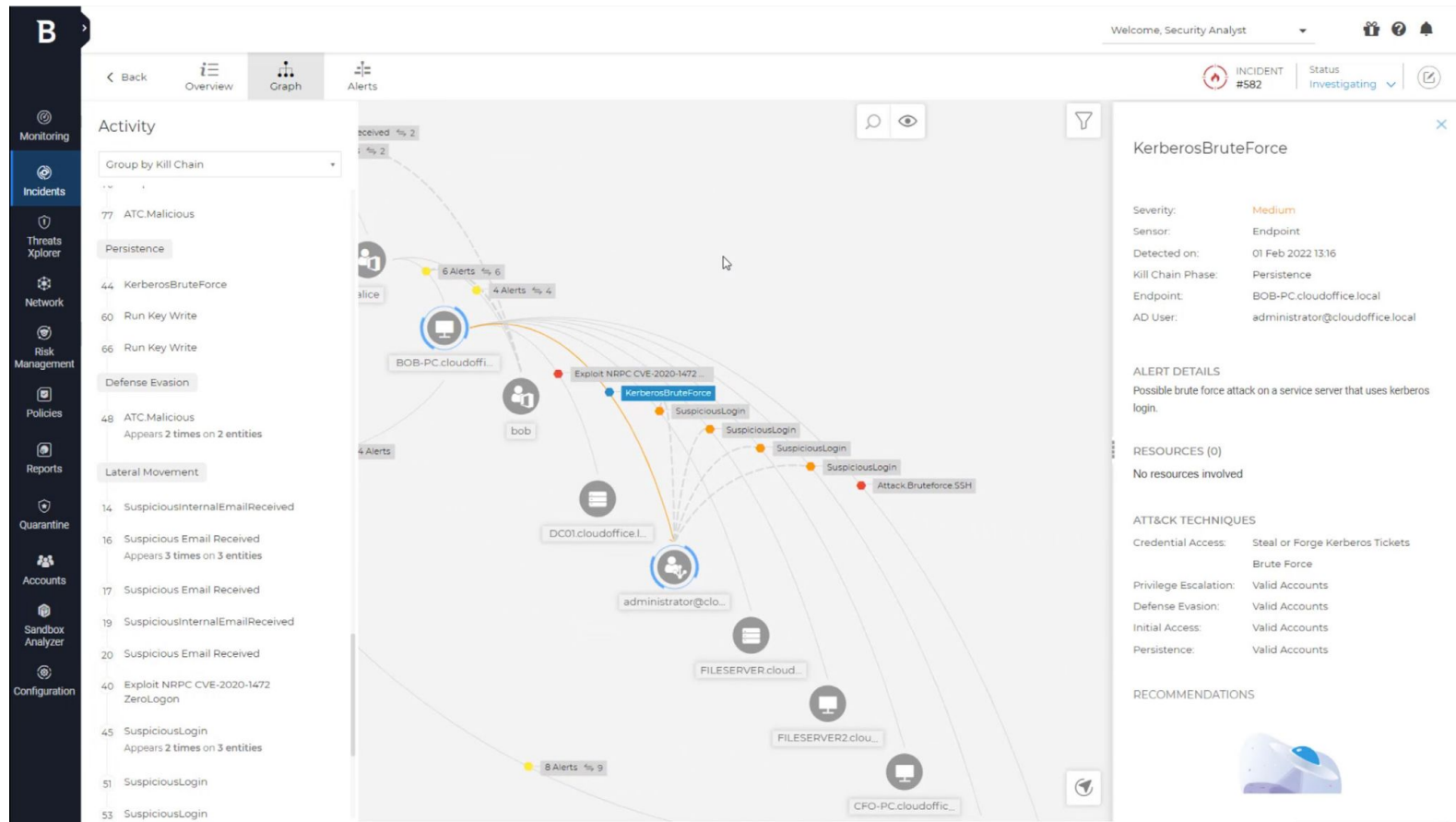
3 Assets to manage

[VIEW DETAILS](#)

AVANGATE

Incident Graph Estesa

Bitdefender®



AVANGATE

XDR

Consultazione storica

Ricerca Storica

Bitdefender

Bitdefender
Welcome, Stefano Maranzana
🔍 ? 📢

SMART VIEWS <

Monitoring

Dashboard

Executive Summary

Incidents

Blocklist

Search

Custom Rules

Threats Xplorer

Network

Patch Inventory

Packages

Tasks

Risk Management

Security Risks

Policies

Configuration Profiles

Assignment Rules

Search

SAVED
No saved views yet.

Date
 6 Apr 2022 14:20 - 7 Apr 2022 14...

Bitdefender Local LAB S...

[Save](#) | [Save as](#)

|
Clear
RUN QUERY

Network	Process	File	Registry	Email	Alert	Other	User
bytes_in	name	attribute_operation	data	attachments_hashes	actions_taken	api	name
bytes_out	access_privileges	destination_file	key	attachments_names	att&ck_subtechnique	agent	domain
destination_ip	command_line	destination_url	operation	attachments_number	att&ck_subtechnique_id	arch	email
destination_port	injection_size	ext	type	attachments_types	att&ck_tactic	compliance_center_event	extended_properties
direction	injection_target_path	item_type	value	attachments_uris	att&ck_technique	detection_class	external_access
file_path	injection_target_pid	md5		client	att&ck_technique_id	event_id	id
mac	injection_writer_path	name		date	mark	event_name	modified_properties
protocol	injection_writer_pid	operation		event_name	name	event_type	shared_with
request_method	integrity_level	path		login_status	scan_type	exclusion_id	sharing_permissions
requester_hostname	module	sha256		logon_type	severity_score	hostname	target
requester_mac	module_pid	site		mailbox_guid	type	ip	team_guid
source_ip	parent_access_privileges	size		mailbox_owner		organization_id	team_members
source_port	parent_cmdline	type		origin_ip		os	team_name
status_code	parent_integrity_level	url		parameters.name		record_type	type
stream_type	parent_path			parameters.value		result_status	

AVANGATE

Bitdefender[®]

Reazione

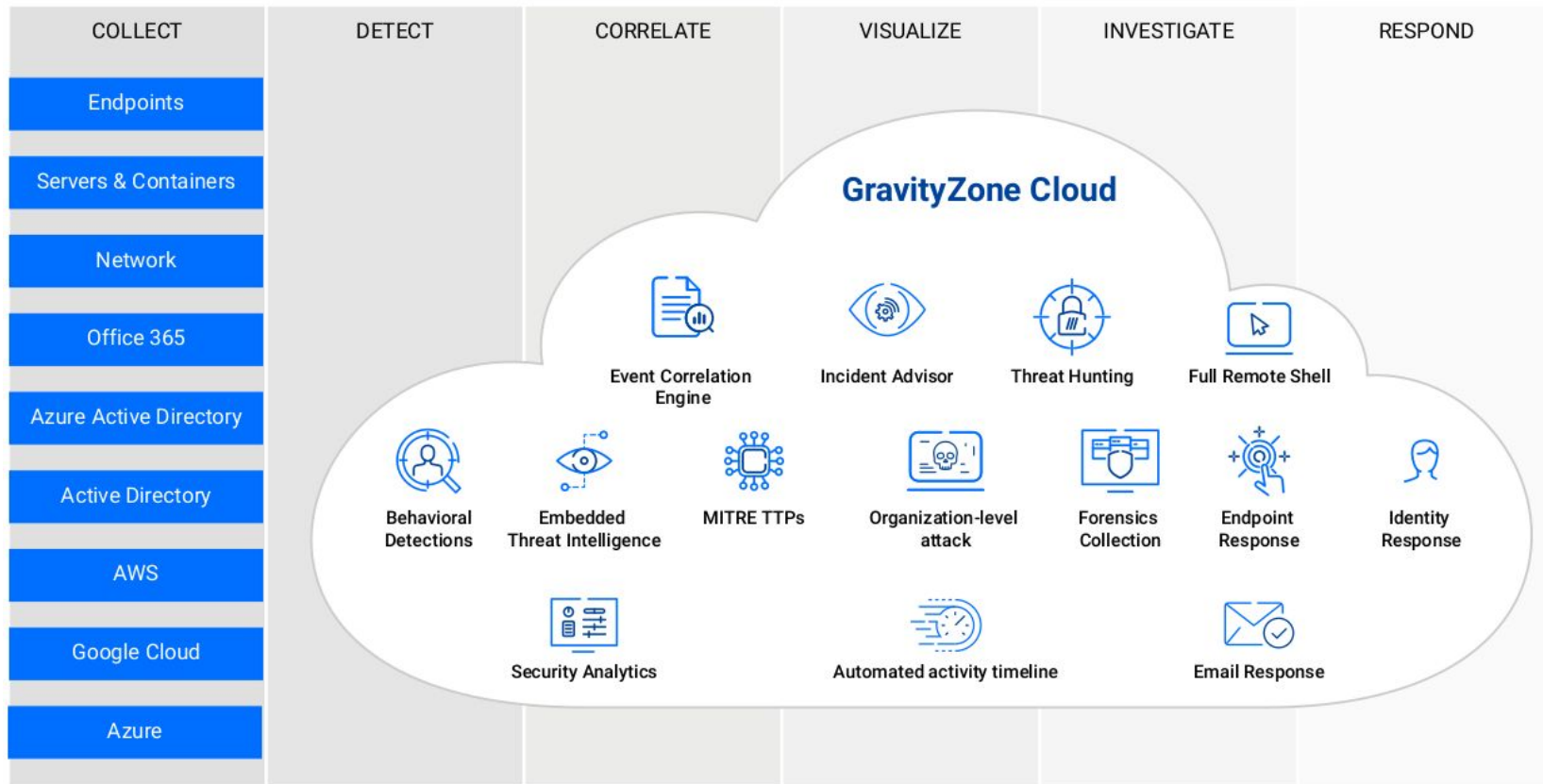
Reazioni Extra Endpoint

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.

XDR - Overview

Bitdefender®



Bitdefender[®]

Licensing

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/Google Workspace User license

XDR Sensor - Identity

Per active AD User license

XDR Sensor - Cloud

Per EC2 Instance license

XDR Sensor - Network

Per endpoint license



Risorse

allegati sezione Documenti di GoToWebinar



Slide di questa presentazione



GravityZone XDR - Datasheet ITA



YouTube

EDR/XDR Live Search DEMO

<https://youtu.be/VmJiVMGhrRY>



EDR/XDR Documentazione OnLine

<https://www.bitdefender.com/business/support/en/77209-151139-edr---xdr.html>

Domande

Sezione Domande del pannello GoToMeeting



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



Roberto Novasconi

GRAZIE