



Bitdefender

GravityZone XDR

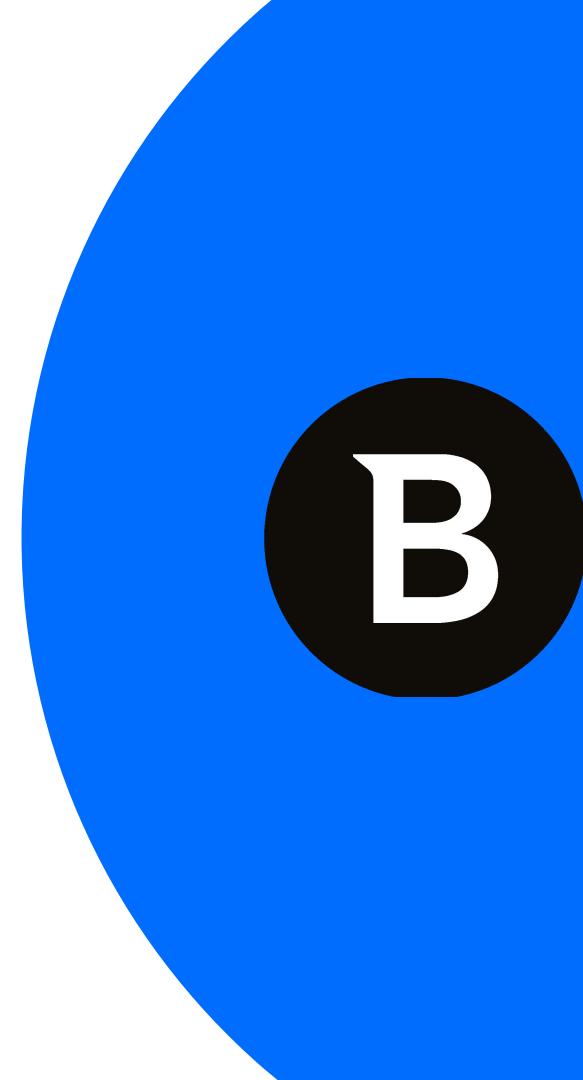
AVANGATE
Distributore a valore aggiunto

**Roberto Novasconi - Avangate Security
Senior Support and Training Specialist**

Bitdefender
AUTHORIZED DISTRIBUTOR

Definizioni

EDR	Endpoint Detection and Response
XEDR	e X tended Endpoint Detection and Response
XDR	e X tended Detection and Response
MDR	M anaged Detection and Response



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 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.

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.

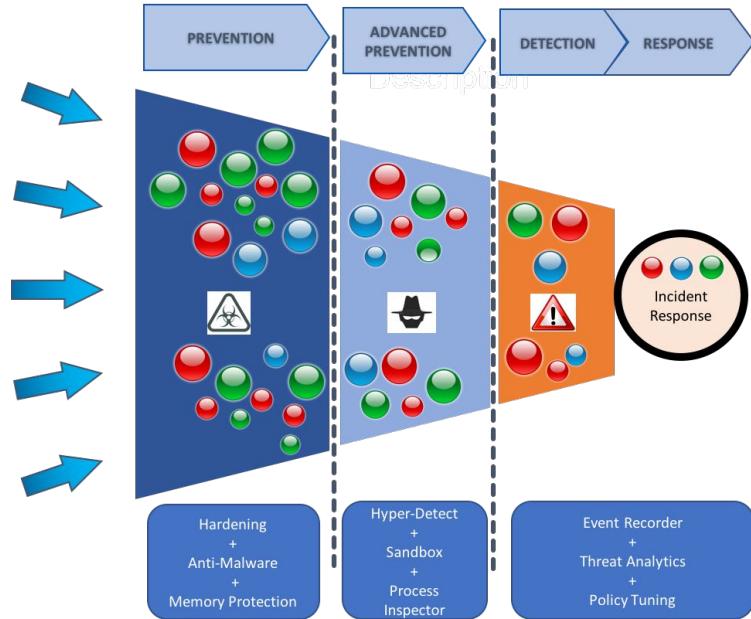
Bitdefender^(*)

EDR
Concetti

AVANGATE

Endpoint Detection and Response

Bitdefender®



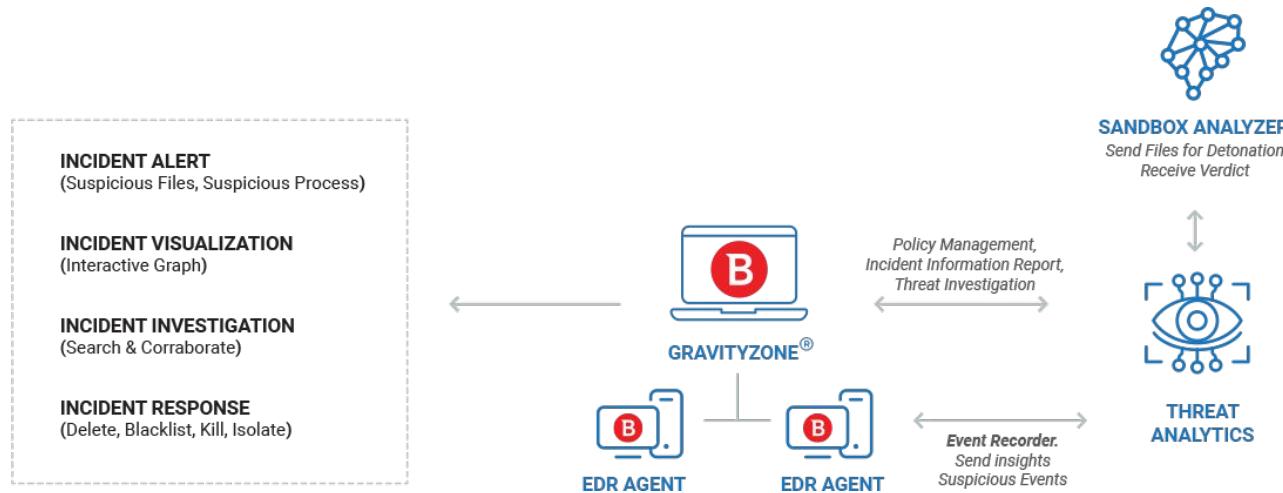
Bitdefender^(c)

XEDR
Concetti

AVANGATE

eXtended Endpoint Detection and Response

Bitdefender®



Bitdefender^(c)

XDR
Concetti

AVANGATE

eXtended Detection and Response

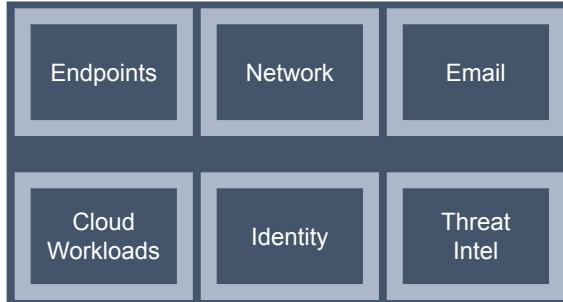
Bitdefender®

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?

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

Cloud Workloads & Containers

Identity

Threat Intel

Bitdefender^(*)

MDR
Concetti

AVANGATE

Managed Detection and Response

Bitdefender®



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

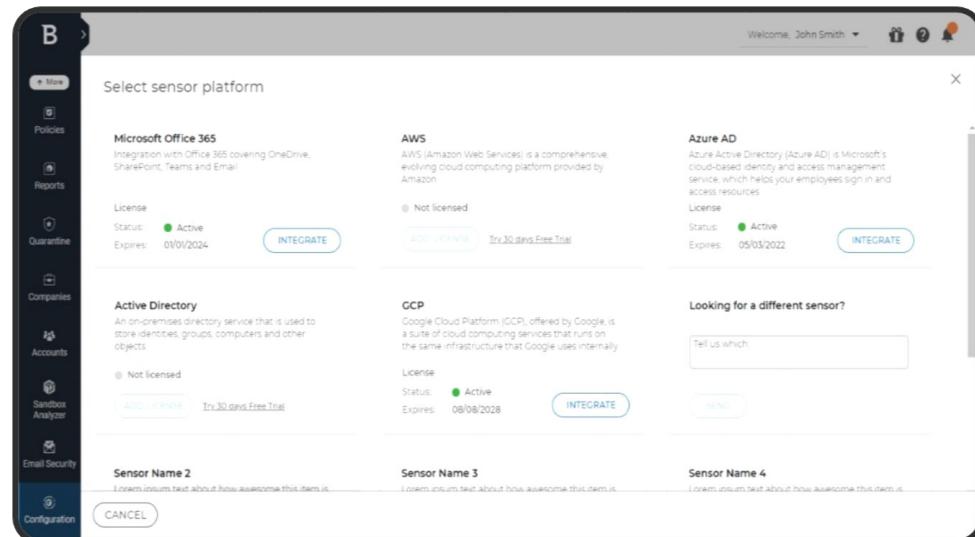
- ✓ On-premises AD
- ✓ Azure AD

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 là 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

Collezione 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



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 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.

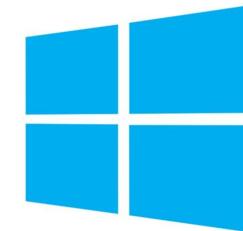
Cosa

Collezione 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



Active Directory

Identity - Active Directory



Active Directory

Analysis of user behavior/identity to detect

Detection category	Example
Kerberos attacks	<ul style="list-style-type: none">An attacker is executing a brute force attack on a service server that uses Kerberos loginAn 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 passwordA Kerberos ticket with weak encryption was requested indicating Kerberoasting activityAn 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

Collezione 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

Cloud - AWS



Analysis of cloud providers to detect

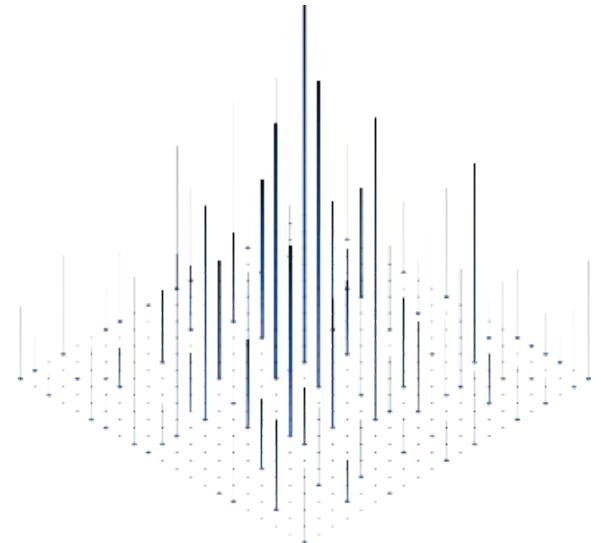
Detection category	Example
Suspicious recognition activity on Lambda functions	<ul style="list-style-type: none">An attacker has listed lambda functions, downloaded one of themA lambda function executing a suspicious action by updating an assume role policy to allow external access
Recognition activity 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	<ul style="list-style-type: none">A user has performed actions that are outside of the baselineA file with a suspicious extension has been uploaded outside of the baselineA 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

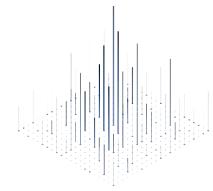
Collezionare eventi relativi al traffico di rete e poi

- 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 nell'organizzazione.

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



XDR Visualizzazione potenziata

Incident Overview Estesa

Bitdefender®

The screenshot displays the Bitdefender GravityZone interface for an incident titled 'Estesa'. The left sidebar shows navigation links for Monitoring, Incidents, Threats Xplorer, Network, Risk Management, Policies, Reports, Quarantine, Accounts, and User Activity. The main content area includes sections for Incident Severity Score (81/100), Organization Impact (4 assets affected), Response (Action Needed: 4, Executed: 0), Summary (details about network breach), Highlights (Exploit.PentestingTool.HTTP.3 Initial Access and Exploit.PentestingTool.HTTP.3 Command and Control), Root Cause (Exploit attempt from WIN-10), ATT&CK Tactics and Techniques (Command And Control T1095 and T1071), and a View in Graph button.

Bitdefender GravityZone

Monitoring

Incidents

Threats Xplorer

Network

Risk Management

Policies

Reports

Quarantine

Accounts

User Activity

Overview

Graph

Alerts

Response

Welcome, Stefano Maranzana

INCIDENT #162

Status Open

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

SUMMARY

A potential network breach originating from managed asset: [WIN-10](#), has been detected as part of alert: [Exploit.PentestingTool.HTTP.3](#), affecting the following: managed asset: [BD-DC01 BD Lab](#).

Multiple communication attempts to 3 unmanaged assets, and managed asset: [BD-DC01 BD Lab](#) have been detected as part of 8 alerts, originating from managed asset: [WIN-10](#).

ROOT CAUSE

The incident was triggered by an Exploit attempt originating in managed asset: [WIN-10](#) involving managed asset: [BD-DC01 BD Lab](#).

ATT&CK TACTICS AND TECHNIQUES

Command And Control

T1095 Non-Application Layer Protocol

T1071 Application Layer Protocol

VIEW DETAILS

CONTAINMENT

1 Endpoints to isolate

HARDENING

3 Assets to manage

VIEW DETAILS

Last updated 14:17:29

Incident Graph Estesa

Bitdefender®

B

Overview Graph Alerts

Welcome, Security Analyst INCIDENT #582 Status Investigating

Activity

Group by Kill Chain

77 ATC.Malicious

Persistence

44 KerberosBruteForce

60 Run Key Write

66 Run Key Write

Defense Evasion

48 ATC.Malicious Appears 2 times on 2 entities

Lateral Movement

14 SuspiciousInternalEmailReceived

16 Suspicious Email Received Appears 3 times on 3 entities

17 Suspicious Email Received

19 SuspiciousInternalEmailReceived

20 Suspicious Email Received

40 Exploit NRPC CVE-2020-1472 ZeroLogon

45 SuspiciousLogin Appears 2 times on 3 entities

51 SuspiciousLogin

53 SuspiciousLogin

The graph illustrates a complex network attack. It starts with multiple endpoints (Alice, BOB-PC, cloudfi...; bob, DC01.cloudfi..., administrator@cloudfi..., FILESERVER.cloud, FILESERVER2.cloud, CFO-PC.cloudfi...) sending various alerts (SuspiciousInternalEmailReceived, SuspiciousEmailReceived, Exploit NRPC CVE-2020-1472 ZeroLogon, SuspiciousLogin) to a central service (FILESERVER2.cloud). The central service then initiates a 'KerberosBruteForce' attack on another endpoint (FILESERVER.cloud). The timeline shows the progression of these events over time.

KerberosBruteForce

Severity: Medium
Sensor: Endpoint
Detected on: 01 Feb 2022 13:16
Kill Chain Phase: Persistence
Endpoint: BOB-PC.cloudfi.local
AD User: administrator@cloudfi.local

ALERT DETAILS
Possible brute force attack on a service server that uses kerberos login.

RESOURCES (0)
No resources involved

ATT&CK TECHNIQUES
Credential Access: Steal or Forge Kerberos Tickets
Brute Force
Privilege Escalation: Valid Accounts
Defense Evasion: Valid Accounts
Initial Access: Valid Accounts
Persistence: Valid Accounts

RECOMMENDATIONS

AVANGATE



XDR Consultazione storica

Ricerca Storica

Bitdefender®

Welcome, Stefano Maranzana

SMART VIEWS < Search

SAVED No saved views yet.

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

Bitdefender^(*)

Reazione

AVANGATE

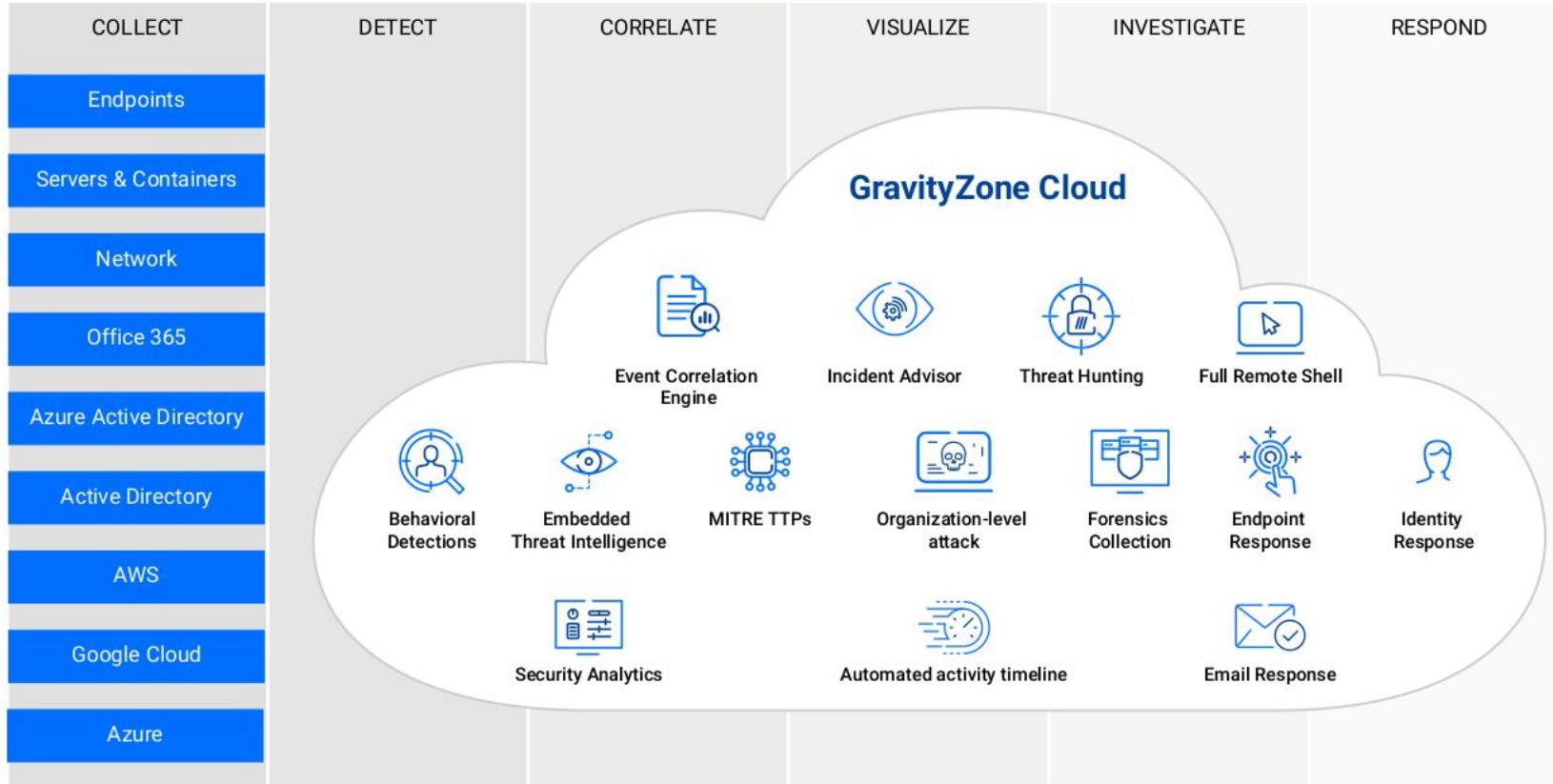
Reazioni Extra Endpoint

Bitdefender®

Platform	Action name	Available through	What it does
O365	Disable user	<ul style="list-style-type: none">• Incident Graph• Incident Response	<ul style="list-style-type: none">• Disables the user account at the O365 Azure AD level.• Also forces an expiry on all active sessions.
	Force credentials reset		<ul style="list-style-type: none">• 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		<ul style="list-style-type: none">• Deletes a specific suspicious email from the Exchange Online mailbox.
Active Directory (onpremise)	Disable user	<ul style="list-style-type: none">• Incident Graph• Incident Response	<ul style="list-style-type: none">• Disables the user account at the Active Directory level
	Force credentials reset		<ul style="list-style-type: none">• 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®





Licensing

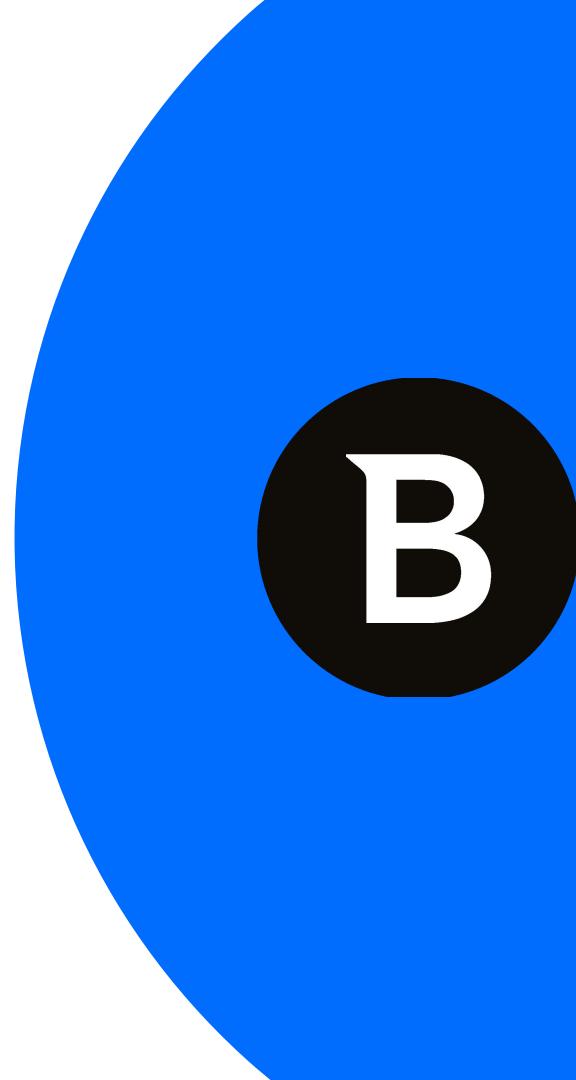
XDR - Prepaid License

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

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**

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**

AVANGATE
Distributore a valore aggiunto



Roberto Novasconi

GRAZIE