



# Servizi e Licensing per MSP

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

# BITDEFENDER

## A GLOBAL CYBER-SECURITY INNOVATOR

GLOBAL COMPANY	TRUSTED SECURITY LEADERSHIP	GROWING BUSINESS	INNOVATION RESEARCH & DEVELOPMENT
Founded in 2001	Bitdefender Labs Research Team	+20% business unit YOY growth	+50% workforce in engineering & R&D, across 6 innovation hubs
1800+ employees	Technology used by more than 150 leading technology companies	\$250+ Million in Billings in 2020	Strong support of open-source projects worldwide
Offices worldwide	Consistently ranked #1 in leading independent testing	+40,000 business customers worldwide	+111 issued patents, +200 patent pending
Customers in 170 countries			
+15,000 distributors and resellers			

# Bitdefender Labs

Global research and innovation since 2001

**30 billion**

Daily threat queries from hundreds of millions of sensors worldwide

**400+**

Threats discovered every minute

**18**

Ransomware decryptors provided to the market

**\$billions**

Helped law enforcement to take down major cybercrime groups with estimated worth in the billions



**260**

Elite security researchers across five research centers

**25**

Threat hunters, Security Analysts supporting MDR in San Antonio, TX SOC

**400+**

Employees in innovation for cloud infrastructure, emerging technology, IoT research and machine learning

# RECOGNIZED

By Global Security Analysts &  
Reviewers

*"the biggest EDR vendor you  
haven't consider but should  
have"*

The Forrester® Wave™: EDR, Q1 2020

# FORRESTER®



"Hardly any other software  
was able to achieve such  
**stellar results** in the  
category of protection in the  
annual test."

AV Test Best Protection 2019



**Five #1 rankings in 2019**  
for Real-World Protection  
and Malware Protection

Tests

AV Comparatives  
Jan – Dec 2019



# TRUSTED

By Enterprises And Law  
Enforcement Agencies

Protecting Key Organizations  
Worldwide

# Honeywell

# Mentor

A Siemens Business



SPEEDWAYMOTORSPORTS, INC.



Partnership Against Cyber Crime



FBI



Department of Justice



# MSP - Sfide per la Sicurezza



## MINACCIE NUMEROSE E COMPLESSE

Vulnerabilità Software e RDP  
Campagne di Email Phishing  
Attacchi Brute Force  
Port Scanning  
Credenziali Compromesse



## CARENZA COMPETENZE

Managing IT in WFH & WFO  
Increased workload  
More attacks targeting MSPs



## GESTIONE DIVERSIFICATA DI CLIENTI E SERVIZI

Ambienti Ibridi  
Diversi controlli di sicurezza  
Infrastrutture fluide  
Clienti in settori regolamentati



# GravityZone Cloud Security for MSPs

# Terminologia

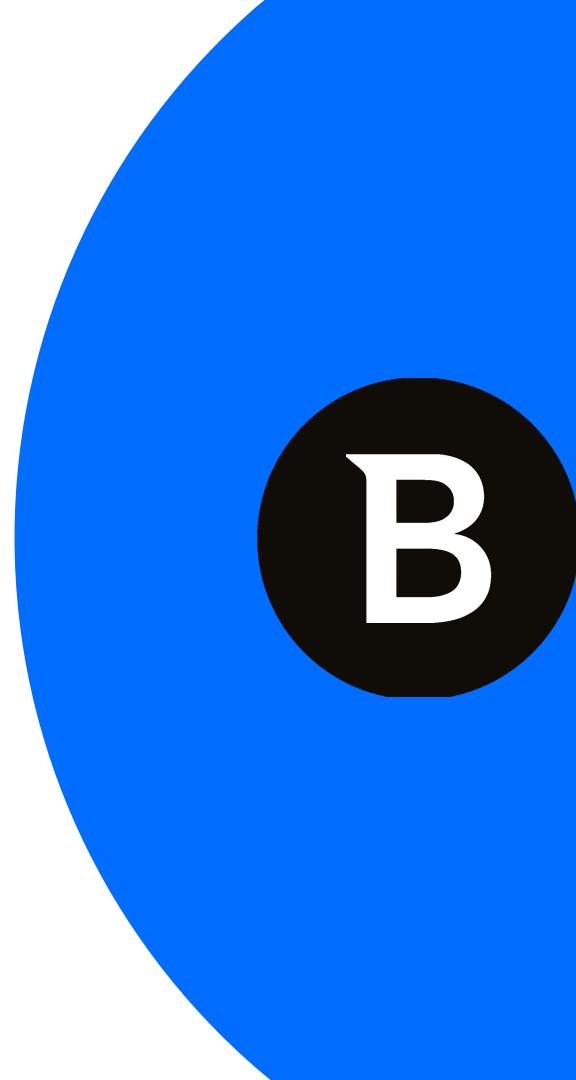
## MSP - Managed Service Provider

### GravityZone Cloud Security for MSPs

è un'offerta di licensing per la piattaforma GravityZone a cui ci riferiamo con tutte queste espressioni:

- *Licensing per MSP*
- *Licensing per Service Provider*
- *Licensing per Fornitori di servizi*
- *Monthly Subscription - Sottoscrizione Mensile*
- *Licenze Mensili (per MSP)*
- *Sottoscrizione per MSP*

Alcune funzionalità di reportistica della piattaforma sono specifiche per MSP.



## GRAVITYZONE Cloud

*Console Cloud*  
multi-tenant, multi-user,  
multi-service

*Singola console*  
*Singolo agent*

### 1. RISK ASSESSMENT & HARDENING

Proactively reduce the attack surface  
at the endpoint, network & human

### 2. PREVENTION

Over 99% of attacks  
blocked  
from reaching any endpoint  
or server - physical, virtual  
and cloud



### 3. DETECTION

Fast and intuitive detection with  
360° visibility from endpoint to  
network to cloud and IoT



**Bitdefender®**  
GravityZone

### 4. RESPONSE

Automated response and actionable  
insights that enable remediation  
without system overloading



### 5. SERVICES

Expert 24x7 managed  
hunting and forensics  
services



## GRAVITYZONE Cloud Security for MSPs

*Console Cloud*  
*multi-tenant, multi-user, multi-service*

*Singola console*  
*Singolo agent*

Funzionalità CORE

Funzionalità ADD-ON

Servizi professionali



# GravityZone® Cloud Security for MSPs

## Offering

Bitdefender



# GravityZone® Cloud Security for MSPs

## Offering

Bitdefender

### CORE

Risk Management	Find and fix vulnerabilities, track & improve risk scores (i.e., device misconfigurations, application vulnerabilities). Includes human risk analytics.
Web Threat Protection	Behavioral traffic scan (incl. SSL, Anti-phishing).
Content Control	Restrict user access to applications, sites or web categories such as gambling.
Device Control	Control access and use of USB or other external devices (i.e., webcams, wireless NICs).
Advanced Anti-Exploit	Detect exploit techniques, stops 0-day exploits.
Cloud Intelligence & Machine Learning	Identifies known and unknown threats effectively and accurately.
Behavior Monitoring	0 - Trust process monitor, automatically blocks malicious processes.
Network Attack Defense	Blocks network-based attacks such as Brute Force or Password stealers.
Firewall	Two-way host firewall protecting endpoints anywhere.
Ransomware Mitigation (Automatic Disinfection, removal, rollback)	Restore files after ransomware attacks from secure copies.

# GravityZone® Cloud Security for MSPs

## Offering

Bitdefender

### ADD-ONS

Requires Core

ESG Email Security

Block advanced email ransomware, impersonation, phishing, spam etc.

PM Patch Management

Flexible, fast patching for Win OS and 3<sup>rd</sup> party apps.

FDE Full Disk Encryption

Simple key mgt. and compliance reporting, using native tech on Win and Mac.

SVE Security for Virtualized Environments

Minimal impact on resources with centralized scanning.

SFC Security for Containers

Protects container workloads against modern Linux and container attacks.

ATS Advanced Threat Security

Fileless Attack Defense.

HyperDetect Tunable Machine Learning (targeted attack protection, exploits, ransomware, grayware etc.).

Cloud Sandbox Analyzer (incl. automatic suspicious file submission, forensic analysis).

MDR Managed Detection and Response

Requires Core + ATS + EDR

24x7 Monitoring

Expert managed incident investigation.

Effective incident response or advice.

Recommendations to improve security posture.

Requires Core & ATS or 3<sup>rd</sup> Party EPP

EDR Endpoint Detection and Response

Cross-endpoint correlation at the organizational level to effectively detect complex cyber-attacks involving multiple endpoints.

Early Breach Detection.

Streamlined investigation and response options.



# Provisioning sul cliente

Bitdefender

The screenshot illustrates the Bitdefender provisioning process across three main sections:

- 1 CORE**: Shows the "LICENSING" section where "Monthly Subscription" is selected. A blue circle highlights the dropdown menu.
- 2 Impostazioni opzionali**: Shows the "SUBSCRIPTION DETAILS" section with options like "Reserve seats", "Add subscription end date", "Set auto-renewal", and "Select minimum usage". A blue circle highlights the "Add subscription end date" field.
- 3 Scroll down**: An arrow points downwards, indicating the user should scroll down the page.
- Add-on 4**: Shows the "OWN USE" section for "Endpoint Security" and a list of available add-ons:
  - Security for Exchange
  - Email Security
  - Full Disk Encryption
  - Security For Virtualized Environments
  - Container Protection
  - Patch Management
  - Advanced Threat Security
  - HyperDetect
  - Sandbox Analyzer
  - Endpoint Detection and ResponseA blue circle highlights the "Endpoint Detection and Response" option.

**LICENSING**

Options \*: Monthly Subscription

**SUBSCRIPTION DETAILS**

Subscription preferences:

- Reserve seats: 0
- Add subscription end date: day/month/year
- Set auto-renewal: 12
- Select minimum usage: 0

**PRODUCTS AND SERVICES**

**OWN USE**

With Endpoint Security, the company can access all features and add-ons available for Bitdefender Cloud MSP Security.  
[Learn more](#)

Bitdefender EDR monitors the company's network to early uncover suspicious activity, and provides the tools to fight-off cyber-attacks. It is suited to coexist with an endpoint security solution from a different vendor.  
[Learn more](#)

Select product type \*: Endpoint Security

Each add-on or service has a fee based on usage. Enabling the add-on or service will add the fee to your monthly subscription. You can view the usage details in the Monthly License Usage report.  
[Learn how to calculate the monthly usage](#)

Add-ons:

- Security for Exchange
- Email Security
- Full Disk Encryption
- Security For Virtualized Environments
- Container Protection
- Patch Management
- Advanced Threat Security
- HyperDetect
- Sandbox Analyzer
- Endpoint Detection and Response

**OWN USE**

With Endpoint Security, the company can access all features and add-ons available for Bitdefender Cloud MSP Security.  
[Learn more](#)

Bitdefender EDR monitors the company's network to early uncover suspicious activity, and provides the tools to fight-off cyber-attacks. It is suited to coexist with an endpoint security solution from a different vendor.  
[Learn more](#)

Select product type \*: Endpoint Security

Each add-on or service has a fee based on usage. Enabling the add-on or service will add the fee to your monthly subscription. You can view the usage details in the Monthly License Usage report.  
[Learn how to calculate the monthly usage](#)

Add-ons:

- Security for Exchange

**SAVE** **CANCEL**

**OWN USE**

With Endpoint Security, the company can access all features and add-ons available for Bitdefender Cloud MSP Security.  
[Learn more](#)

Bitdefender EDR monitors the company's network to early uncover suspicious activity, and provides the tools to fight-off cyber-attacks. It is suited to coexist with an endpoint security solution from a different vendor.  
[Learn more](#)

Select product type \*: Endpoint Security

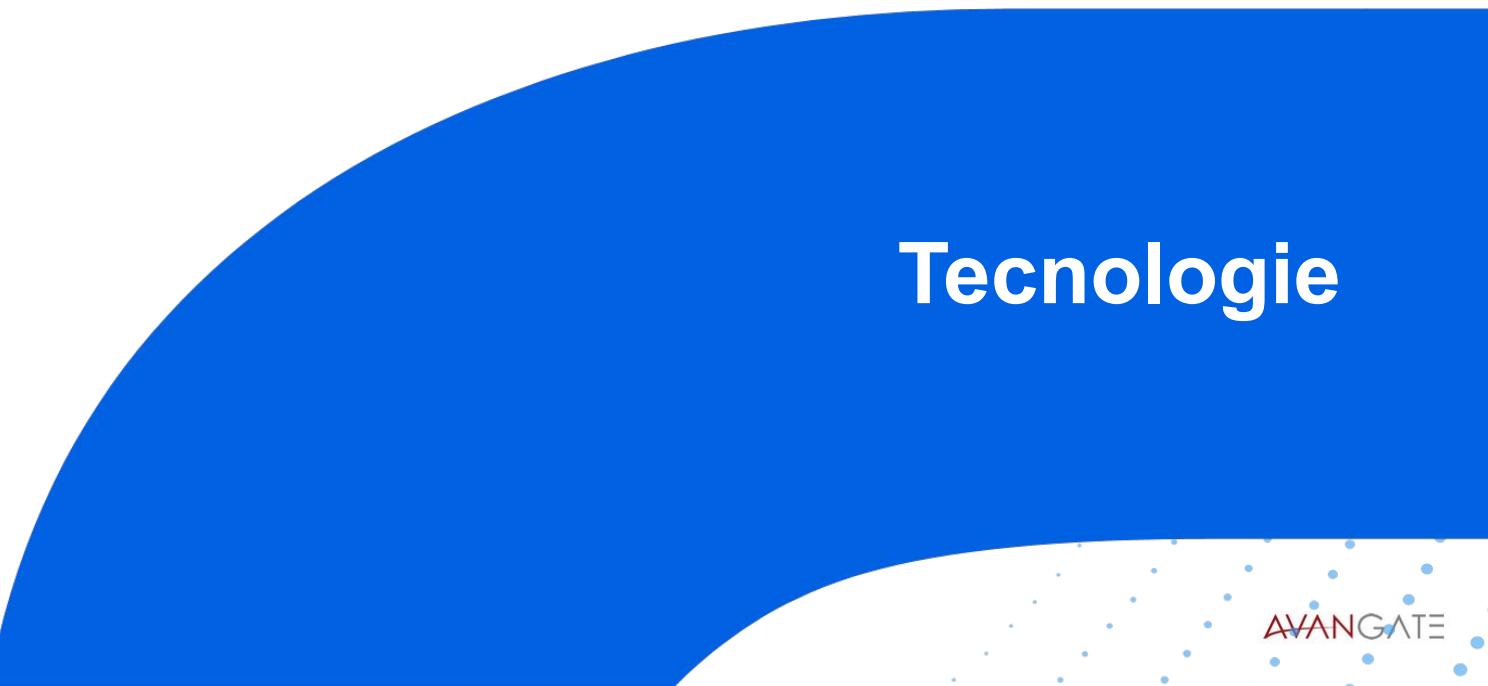
Each add-on or service has a fee based on usage. Enabling the add-on or service will add the fee to your monthly subscription. You can view the usage details in the Monthly License Usage report.  
[Learn how to calculate the monthly usage](#)

Add-ons:

- Security for Exchange
- Email Security
- Full Disk Encryption
- Security For Virtualized Environments
- Container Protection
- Patch Management
- Advanced Threat Security
- HyperDetect
- Sandbox Analyzer
- Endpoint Detection and Response

**SAVE** **CANCEL**

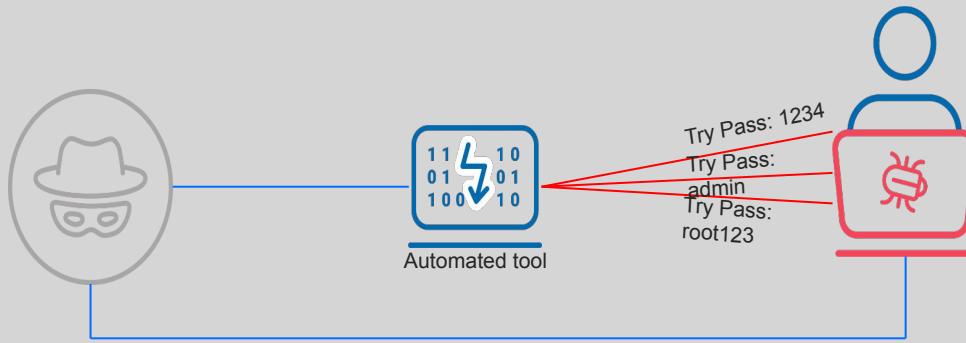
# GravityZone for MSP



Tecnologie

# Network Attack Defense

CORE



Bitdefender GravityZone

Dashboard      General       Network Attack Defense

Incidents      Antimalware      This feature is a security layer designed to detect network attack techniques that try to g...

Blocklist      Sandbox Analyzer

Search      Firewall      Attack Techniques

Network      Network Protection       Initial Access      Block

Patch Inventory      General       Credential Access      Block

Packages      Content Control       Discovery      Block

Tasks      Web Protection       Lateral Movement      Block

Risk Management      Network Attacks       Crimeware      Block

**Policies**     

Assignment Rules      Patch Management

113 milioni di attacchi Brute Force e Password Stealing solo in Ottobre perpetrati su 6700 organizzazioni.

## Network Attack Defense

Blocca attacchi Brute Force, Password Stealer, Port Scan, e tentativi di Exploitation delle applicazioni dalla rete.

Blocca vulnerabilità di RDP come BlueKeep

Controlla il traffico entrante, uscente e laterale.

Impiega analisi dei protocolli, scansione dei flussi di rete, machine learning, rilevamento delle anomalie, correlazione di eventi

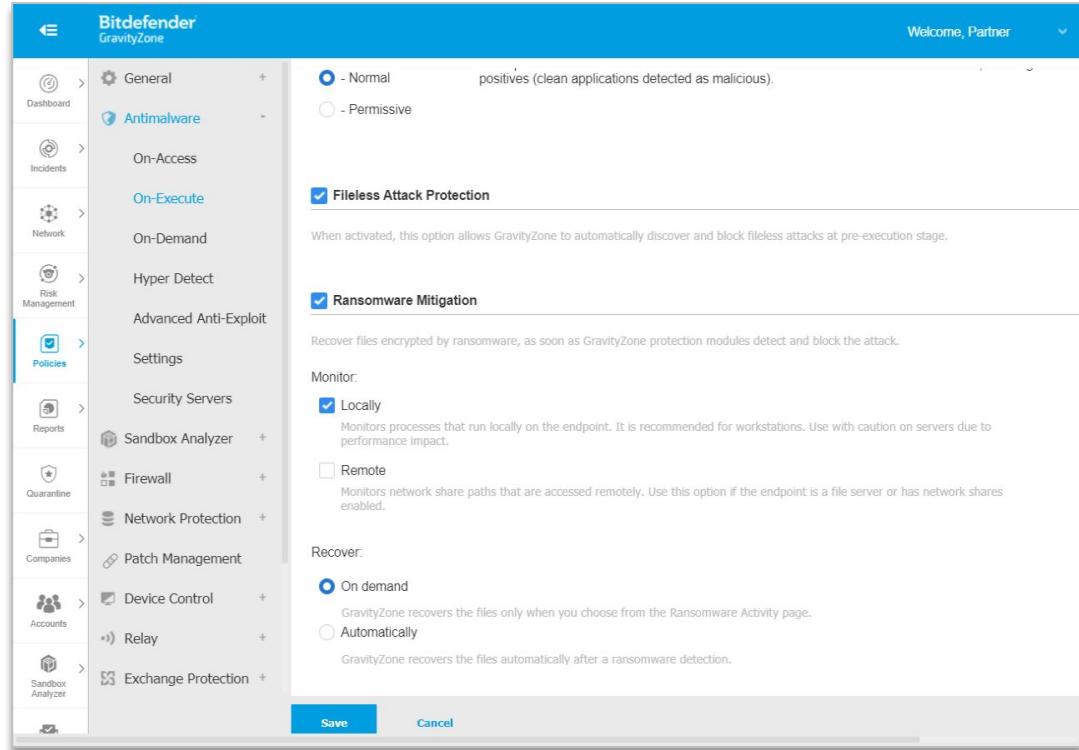
Ransomware mitigation helps organizations recover files after a blocked ransomware attack – without any downtime.

## Available in Core Product

### What's in it for MSPs

Gain peace of mind with fast recovery of encrypted files affected by ransomware

- **Tamper-proof, secure backup copies** to ensure data is protected
- **Stop attacks** coming from endpoints not protected by Bitdefender
- **Add more value** with affordable, advanced security features – **no upcharges** for Ransomware Mitigation



The screenshot shows the Bitdefender GravityZone interface. On the left, there's a navigation sidebar with various modules like Dashboard, Incidents, Network, Risk Management, Policies (which is currently selected), Reports, Quarantine, Companies, Accounts, and Sandbox Analyzer. The main content area is titled "Bitdefender GravityZone". It has two main sections: "Fileless Attack Protection" and "Ransomware Mitigation". Under "Fileless Attack Protection", there's a note about automatically discovering and blocking fileless attacks at the pre-execution stage. Under "Ransomware Mitigation", there's a note about recovering files encrypted by ransomware as soon as protection modules detect and block the attack. There are three monitoring options: "Locally" (selected), "Remote" (unchecked), and "On demand" (selected). "Locally" monitors processes running locally on the endpoint, while "Remote" monitors network share paths. The "On demand" option allows GravityZone to recover files only when chosen from the Ransomware Activity page. The "Automatically" option recovers files automatically after a ransomware detection. At the bottom, there are "Save" and "Cancel" buttons.

# Risk Management

CORE

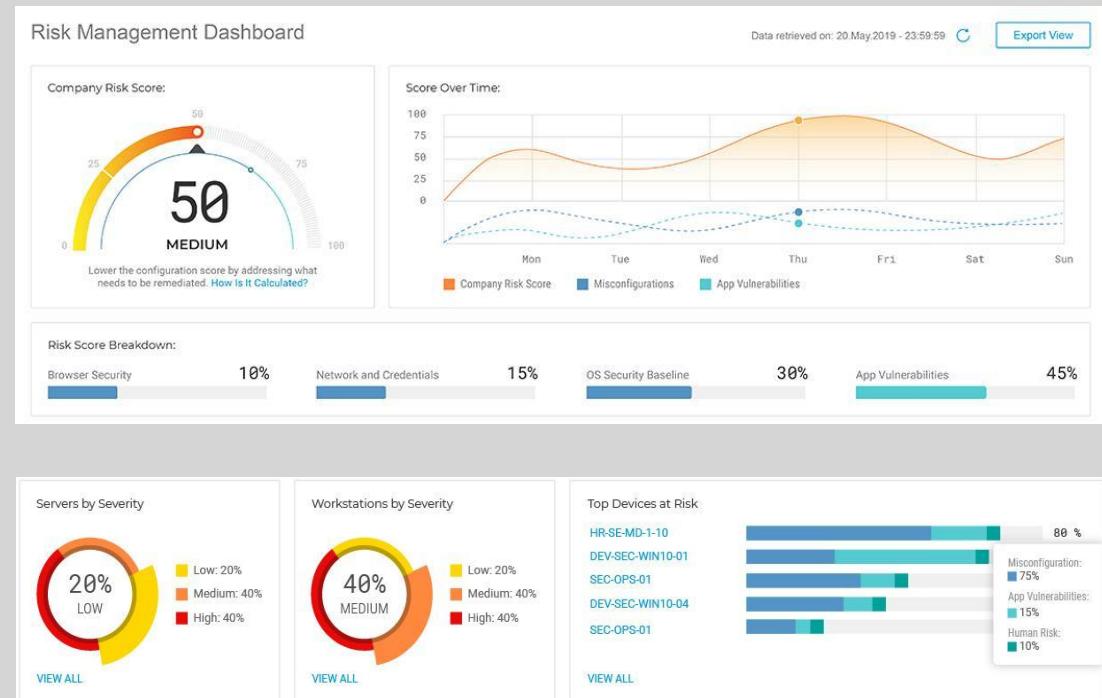
Calcola il punteggio di rischio

Rileva  
le misconfigurazioni, il software vulnerabile  
ed i comportamenti a rischio.

Prioritizza gli interventi  
sulla base della severità dei rischi.

Usa 206 indicatori di misconfigurazione.  
Correzione automatica disponibile per molti  
degli indicatori.

Genera opportunità di upsell.



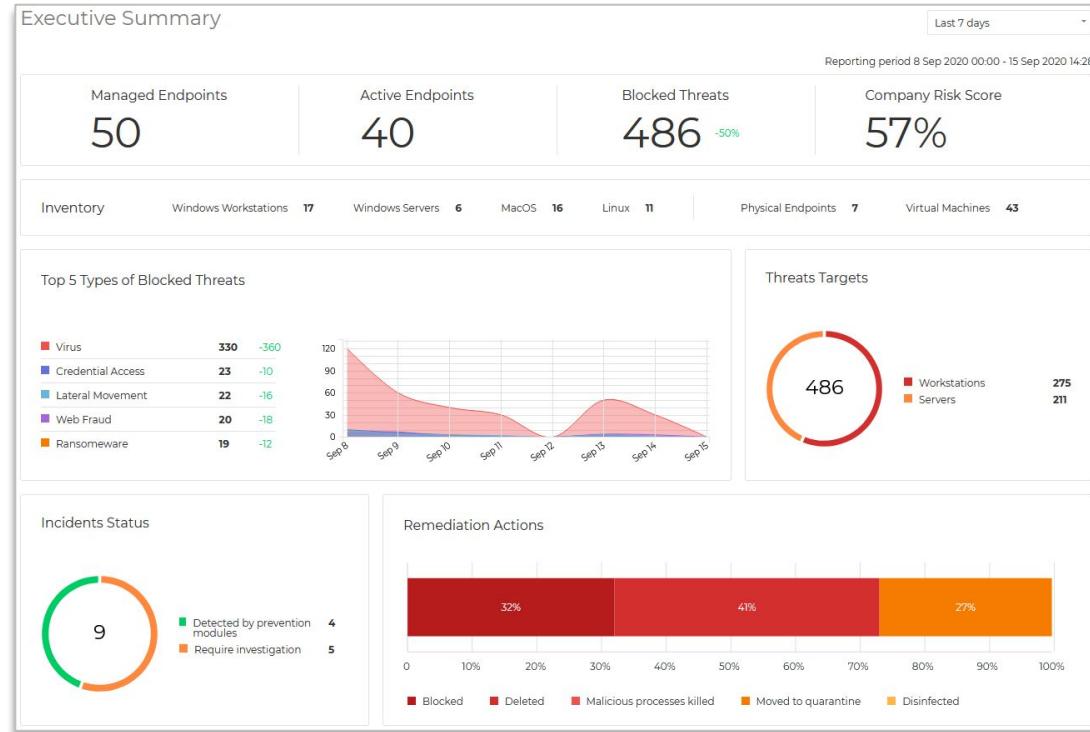
# Executive Summary

CORE

La nuova dashboard Executive Summary è progettata per aiutare gli MSP ad analizzare e monitorare la postura di sicurezza dei clienti.

Identifica rapidamente minacce e vulnerabilità nelle reti dei clienti

- Visibilità migliorata** over endpoint modules, threat types, company risk score and much more
- Easy-to-interpret** data for executive management insights



# Advanced Threat Security

## Hyper Detect

ADD-ON

- Block attacks at pre-execution
- Tunable Machine Learning
- Blocks Fileless attacks
- Blocks PowerShell  
and other script attacks

The screenshot shows the 'Hyper Detect' configuration page. On the left, a sidebar lists various security modules: General, Antimalware (selected), On-Access, On-Demand, Hyper Detect (selected), Settings, Security Servers, Sandbox Analyzer, Firewall, Content Control, Device Control, Relay, Exchange Protection, and Encryption. The main panel has a title 'Hyper Detect' with a checked checkbox. A descriptive text below it states: 'This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.' A 'Reset to default' button is present. The 'Protection Level' section contains five threat types: Targeted Attack, Suspicious files and network traffic, Exploits, Ransomware, and Grayware, each with radio buttons for Permissive, Normal (selected), and Aggressive. The 'Actions' section includes dropdown menus for 'Files' (Report Only) and 'Network traffic' (Block), both with 'Extend reporting on higher levels' checkboxes. At the bottom are 'Save' and 'Cancel' buttons.

# Advanced Threat Security Sandbox Analyzer

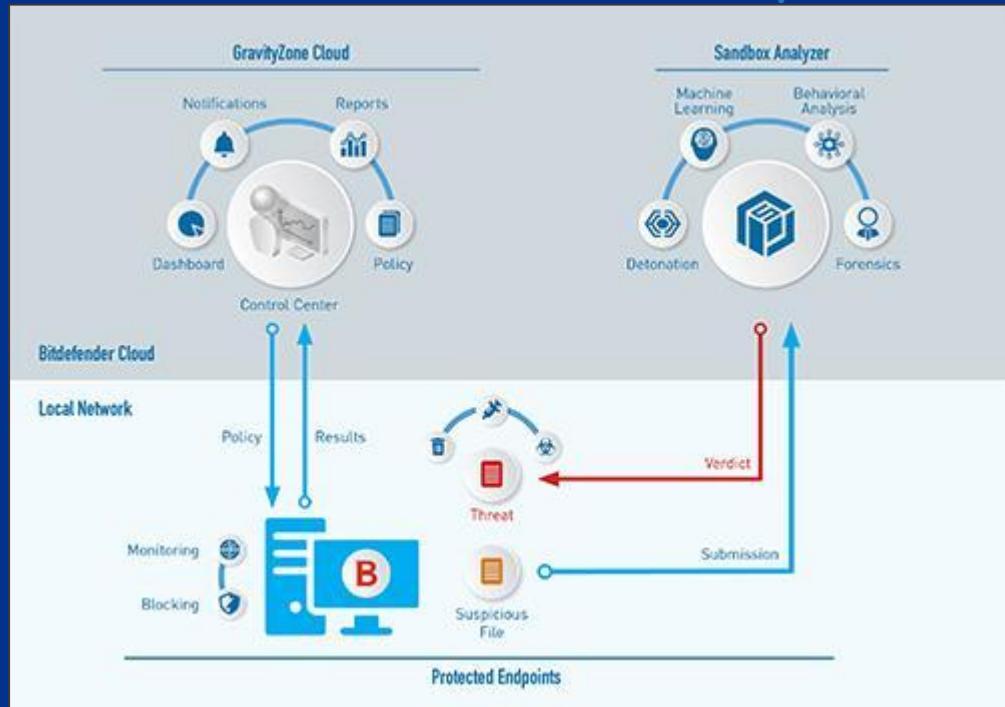
ADD-ON

## Enhanced Targeted Attack Detection

- Automatic and manual file submission
- Cloud hosted infrastructure
- Machine learning & behavior analysis

## Threat Context and visibility

- Suspicious activities, IOCs
- Detailed reports



## *Cloud Email Security Gateway*

Ful Mailflow Control

Mail Server agnostic

Multi-layered Approach

### **Executive Tracking List**

Detection of real names in external messages, linked to AD group

### **Threat Intelligence**

Domain and IP based risk scoring

### **Algorithmic Analysis**

10,000+ algorithms analyse over 134 message variables (< 200ms)

### **Message Categorization**

Accurate identification of marketing / commercial email

### **Content Analysis**

Lexical analysis of subject and message body (inc. attachments)

### **Pattern Matching / Message Attribute Analysis**

Unsubscribe, donotreply@ address etc.

### **AV**

Multiple signature and behaviour based AV engines (inc. static analysis)

### **Machine Checks**

Sender, Sending Server, Authentication Checks (inc. SPF)

# EDR - Overview

ADD-ON

**72/100**  
Incident Severity Score

Created: 04 May 2022, 14:03:34  
Last updated: 04 May 2022, 15:27:13  
Type of attack: N/A

**SUMMARY**  
A potential network breach originating from managed asset: **AVNG-PORT-01**, has been detected as part of alert **EncryptedFileUpload**, affecting the following: external ip: **13.107.42.14**.

Multiple communication attempts to **2** external ips have been detected as part of **10** alerts, originating from **2** managed assets. These **4** managed assets were the source of malicious actions detected in **11** alerts, affecting managed asset: **AVNGS1**, and **2** external ips. Sensitive data may have been exfiltrated to **2** external ips, based on **2** alerts, originating from managed asset: **AVNGS1**.

**ROOT CAUSE**  
Not enough data to establish how these actions were possible.

**ATT&CK TACTICS AND TECHNIQUES**

Command And Control	<b>T1095</b> Non-Application Layer Protocol <b>T1071</b> Application Layer Protocol <b>T1105</b> Ingress Tool Transfer
Exfiltration	<b>T1041</b> Exfiltration Over C2 Channel
Execution	<b>T1059</b> Command and Scripting Interpreter <b>T1204</b> User Execution

**ORGANIZATION IMPACT**

 **6**

**HIGHLIGHTS**

 **EncryptedFileUpload** | Initial Access  
Severity: Low  
An encrypted file was uploaded.  
Detected by sensor: *Endpoint* on 04 May 2022 at 10:38:31  
 1  
+1 OTHER INITIAL ACCESS ALERTS

 **URL.Malicious** | Command and Control  
Severity: High  
Unwanted activity has been detected while accessing supporto.s8group.it/admin/admin\_ticket.php?track=GRJ-7LA-Q9G4&Refresh=96353.  
Detected by sensor: *Endpoint* on 04 May 2022 at 12:47:37  
 1  
+9 OTHER COMMAND AND CONTROL ALERTS

 **Trojan.GenericKD.39603946** | Execution  
Severity: High  
Antimalware static engines have detected a potential security breach, generated by this malicious artifact: richiesta - 0503.docx.  
Detected by sensor: *Endpoint* on 04 May 2022 at 14:03:34  
 1  
+10 OTHER EXECUTION ALERTS

**RESPONSE**

Last updated 12:52 

**ACTION NEEDED (6)** **EXECUTED**

**CONTAINMENT**

**6** Endpoints to isolate

[VIEW DETAILS](#)

AVANGATE

# EDR - Graph

ADD-ON

Activity

Group by Time ▾

04 May 2022

1. EncryptedFileUpload 10:38

2. URL.Malicious  
Seen 11 times on 8 Interactions

3. EncryptedFileUpload 12:05

4. URL.Malicious  
Seen 8 times on 3 interactions

5. Trojan.GenericKD.39603946  
Seen 2 times on 1 entities

6. EncryptedFileUpload 15:27

INITIAL ACCESS

The graph visualization shows a network flow starting from an 'INITIAL ACCESS' point (avng-port-01) on the left. This leads to several 'EXIT POINTS' (13.107.42.14, 176.56.131.59, 195.110.124.133) which then connect to various endpoints (avng51.smallbusin..., desktop-at2sm86). Each endpoint node contains a red dot indicating the number of alerts: 4 Alerts for the first two exit points, 2 Alerts for the third, and 2 Alerts for the desktop endpoint. A yellow dot on the desktop endpoint indicates a correlation point. The desktop endpoint also has a label '3 Endpoints'.

Visione estesa degli incidenti.

Correlazione eventi.

# EDR - Incidents di tutti i clienti

ADD-ON

ID	Date	Status	Severity Score	Company	Organization Impact	Last Kill Chain Phase	Attack type	
	<input type="text" value="Search..."/>	<input type="button" value="Select..."/>	<input type="button" value="Open, Investigat..."/>	<input type="button" value="100-30"/>	<input type="button" value="All Compan..."/>	<input type="button" value="Choose..."/>	<input type="button" value="Choose..."/>	
#764	Updated 29 minutes ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 7 <span style="color: grey;">■</span> 0	Lateral Movement	N/A	
#199	Created 47 minutes ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 5 <span style="color: grey;">■</span> 0	Lateral Movement	N/A	
#198	Created 47 minutes ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 3 <span style="color: grey;">■</span> 0	Execution	N/A	
#1086	Created 58 minutes ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 2 <span style="color: grey;">■</span> 0	Execution	N/A	
#1087	Created 58 minutes ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 3 <span style="color: grey;">■</span> 0	Execution	N/A	
#9	Created 1 hour ago	Open	<span style="color: orange;">●</span> 50		<span style="color: grey;">■</span> 2 <span style="color: grey;">■</span> 0	Lateral Movement	N/A	
#13021	Updated 3 hours ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 2 <span style="color: grey;">■</span> 0	Execution	N/A	
#617	Updated 4 hours ago	Open	<span style="color: red;">●</span> 80		<span style="color: grey;">■</span> 3 <span style="color: grey;">■</span> 0	Lateral Movement	N/A	
#1081	Updated 4 hours ago	Open	<span style="color: red;">●</span> 90		<span style="color: grey;">■</span> 4 <span style="color: grey;">■</span> 0	Lateral Movement	N/A	
#765	Created 5 hours ago	Open	<span style="color: red;">●</span> 80		<span style="color: grey;">■</span> 2 <span style="color: grey;">■</span> 0	Execution	N/A	

385 items

First Page



1 of 20



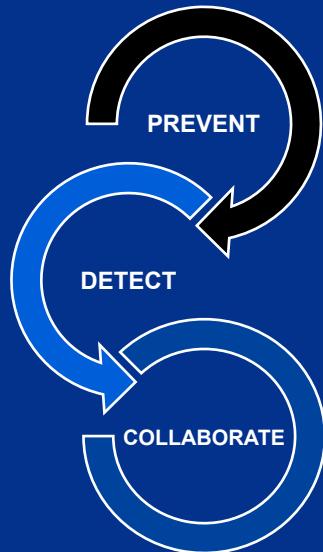
Last Page

Show

20

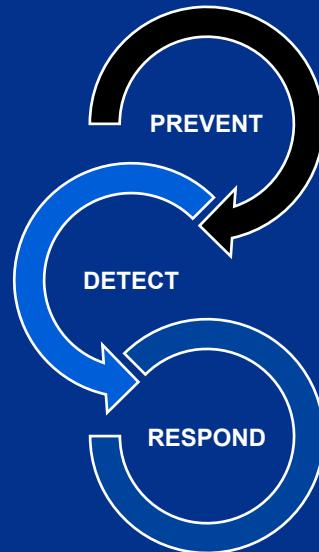
### EXPERT ADVICE

Equip your security team with trusted expert advice



### EXPERT RESPONSE

Deliver managed threat hunting without doing the heavy lifting



*Requires MSP + ATS + EDR  
Available for 100 endpoints per customer and above*

# Security for Containers

ADD-ON

NEW!



## Sviluppato per container e Linux

Utilizza tecnologie avanzate di prevenzione, rilevamento e risposta per proteggere da tecniche di attacco, Tattiche e Procedure (TTP) e attacchi ai container specifici per Linux, come "Container Escape". Ha dimostrato la massima efficacia nella sicurezza, ottenendo il 100% di rilevamento delle tecniche di attacco per Linux nelle valutazioni MITRE 2021



## Sicurezza multi-distribuzione

Elimina le sfide di compatibilità della sicurezza per Linux con un agente di sicurezza che va oltre il kernel Linux, consentendoti di impiegare le distribuzioni Linux più recenti ancora più velocemente, senza il classico ritardo di altri prodotti che richiedono le componenti del kernel



## Visibilità e controllo consistenti

La piattaforma di sicurezza dei carichi di lavoro cloud di GravityZone usa un agente ad alte prestazioni e indipendente dalla piattaforma, fornendo visibilità e controllo completi per tutti i container e i carichi di lavoro negli ambienti ibridi e multi-cloud

# EDR Standalone

New Standalone EDR SKU available for MSPs starting December 2020  
(Controlled Availability)

## What's in it for MSPs

- Win new business with EDR
- Strengthen customer's security posture by adding Bitdefender EDR alongside 3rd party AV/EPP
- Increased visibility across customer networks with EDR enhancements
- Leverage from added prevention layers when upgrading to the full MSP suite

The screenshot displays the Bitdefender GravityZone EDR interface. On the left, a sidebar navigation includes: Dashboard, Executive Summary, Incidents (selected), Blocklist, Search, Custom Rules, Network, Packages, Tasks, Risk Management, Security Risks, Policies, Assignment Rules, Reports, Accounts, User Activity, Sandbox Analyzer, Manual Submission, and Configuration. The main area shows the 'Endpoint Incidents' section with 'OPEN INCIDENTS' (High: 0, Medium: 0, Low: 9) and 'TOP ALERTS' (HTTP Resource Download, Process Create, Network Connection Start). Below this is a table of tasks. To the right, the 'Endpoint DESKTOP-92T167' details are shown, featuring a process execution graph. The graph illustrates a sequence of events: 'wininit.exe (640)' → '1. Executed' → 'services.exe (780)' → '2. Executed' → 'svchost.exe (892)' → '3. Executed' → 'microsoftedgecp.exe...'. A red circular icon with a question mark is positioned over the final node. The right panel contains sections for 'ALERTS' (listing 'microsoftedgecp.exe Process Execution' as a 'PROCESS DETECTED AS MALWARE BY ANALYSIS'), 'INVESTIGATION' (listing 'URL.Malicious' and 'Process Create'), 'FURTHER ANALYSIS' (with 'Add to Sandbox', 'VirusTotal', and 'Google' links), 'REMEDIALION' (with 'ACTIONS TAKEN' and 'No actions taken'), and 'FIX & REMEDIATE'.

Ranked #1 for actionable detections and attack chain coverage, MITRE 2020 evaluations

AVANGATE

# Integrazioni

## RMM to GravityZone

*Collabora con  
gli strumenti che usi ogni giorno  
per automatizzare  
il tuo security workflow,  
riducendo i costi e gli sforzi.*



# Integrazioni

GravityZone to any

Oltre agli strumenti nativi  
per Kaseya e ConnectWise  
infinite possibilità di integrazione  
grazie a RESTful API



{REST<sup>ful</sup> API}

# Licensing per MSP semplice e flessibile

Formula **pay-per-use**

Servizi **a-la-cart**

Nessun **costo fisso**

Nessun **impegno di spesa/minimo attivazioni**

Contabilizzazione **mensile**

Prezzi **decrescenti** per volume di attivazioni

Completamente **self-service**

# MSP con GravityZone in 3 semplici mosse



## Rivenditore Avangate Security

Sul sito <https://www.avangate.it>

RIVENDITORI -> Diventa Rivenditore



## GravityZone Partner

Nell'AREA PARTNER Avangate Security.

<https://nova.avangate.it>

Supporto

Inserisci una richiesta:

Tipo:

GravityZone Cloud - abilitazione Partner



## GravityZone MSP

Nell'AREA PARTNER Avangate Security.

<https://nova.avangate.it>

Supporto

Inserisci una richiesta:

Tipo:

GravityZone Cloud - abilitazione MSP

# Risorse

**Slide di questa presentazione**

*sezione Documenti di GoToWebinar*

**GravityZone MSP - Servizi**

*sezione Documenti di GoToWebinar*

**GravityZone EDR - datasheet ITA**

*sezione Documenti di GoToWebinar*

**GravityZone Tips & Tricks per MSP (webinar)**

<https://attendee.gotowebinar.com/recording/8256681820767322127?source=WEBINAR>

**GravityZone Licensing e Reportistica per MSP (webinar)**

<https://attendee.gotowebinar.com/recording/5087404431569791500?source=WEBINAR>

**GravityZone Security for Containers (video)**

[https://youtu.be/CG3BntY-D\\_U](https://youtu.be/CG3BntY-D_U)

## **Domande**

*Sezione Domande del pannello GoToMeeting*



## *contatti pubblici*

[www.avangate.it](http://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**