

Bitdefender GravityZone Cloud Security for MSP

Roberto Novasconi - Avangate Italia
Senior Support and Training Specialist

AVANGATE
Distributore a valore aggiunto

Bitdefender®
AUTHORIZED DISTRIBUTOR

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

AVANGATE
Distributore a valore aggiunto

RECOGNIZED

By Global Security Analysts & Reviewers

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

The Forrester® Wave™: EDR, Q1 2020

FORRESTER®



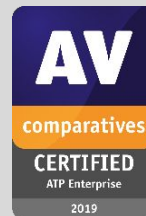
"Hardly any other software was able to achieve such stellar results in the category of protection in the annual test."

AV Test Best Protection 2019



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

AV Comparatives
Jan – Dec 2019



Bitdefender®

TRUSTED

By Enterprises And Law Enforcement Agencies

Protecting Key Organizations Worldwide

Honeywell

Mentor®
A Siemens Business



Partnering Against Cyber Crime



FBI



Department of Justice



RELIED

On In Key Technology Partnerships



MSP

Sfide per la sicurezza



MINACCE 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

HOW WE WIN WITH BITDEFENDER GRAVITYZONE SECURITY FOR MSPs

MOST EFFECTIVE AI-BASED CYBERSECURITY

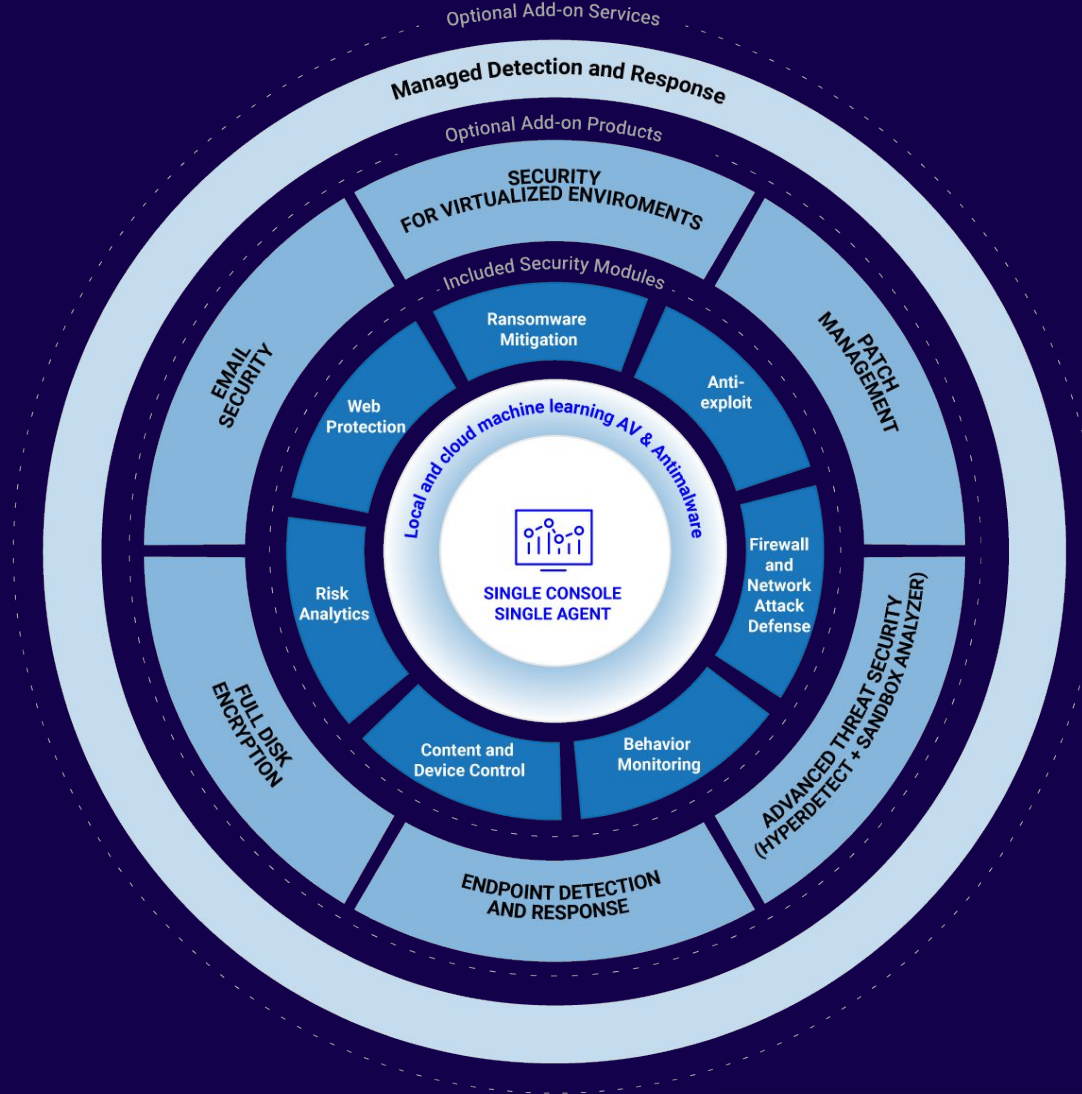
Thanks to 30+ technology layers and more mature AI, perfected since 2008, Bitdefender routinely ranks #1 for prevention and detection in independent AV & EDR tests.

END-TO-END UNIFIED SECURITY

The unified risk analytics, hardening next-gen AV, EDR, and MDR, in a single MSP platform with extensive API and RMM integrations automates tasks and reduces security efforts and costs.

MAXIMISE REMOTE WORK PROTECTION

Bitdefender includes extra risk analytics, host firewall with IDS, content and device control, and optional advanced security add-ons with flexible licensing to help MSPs maximize WFH protection.

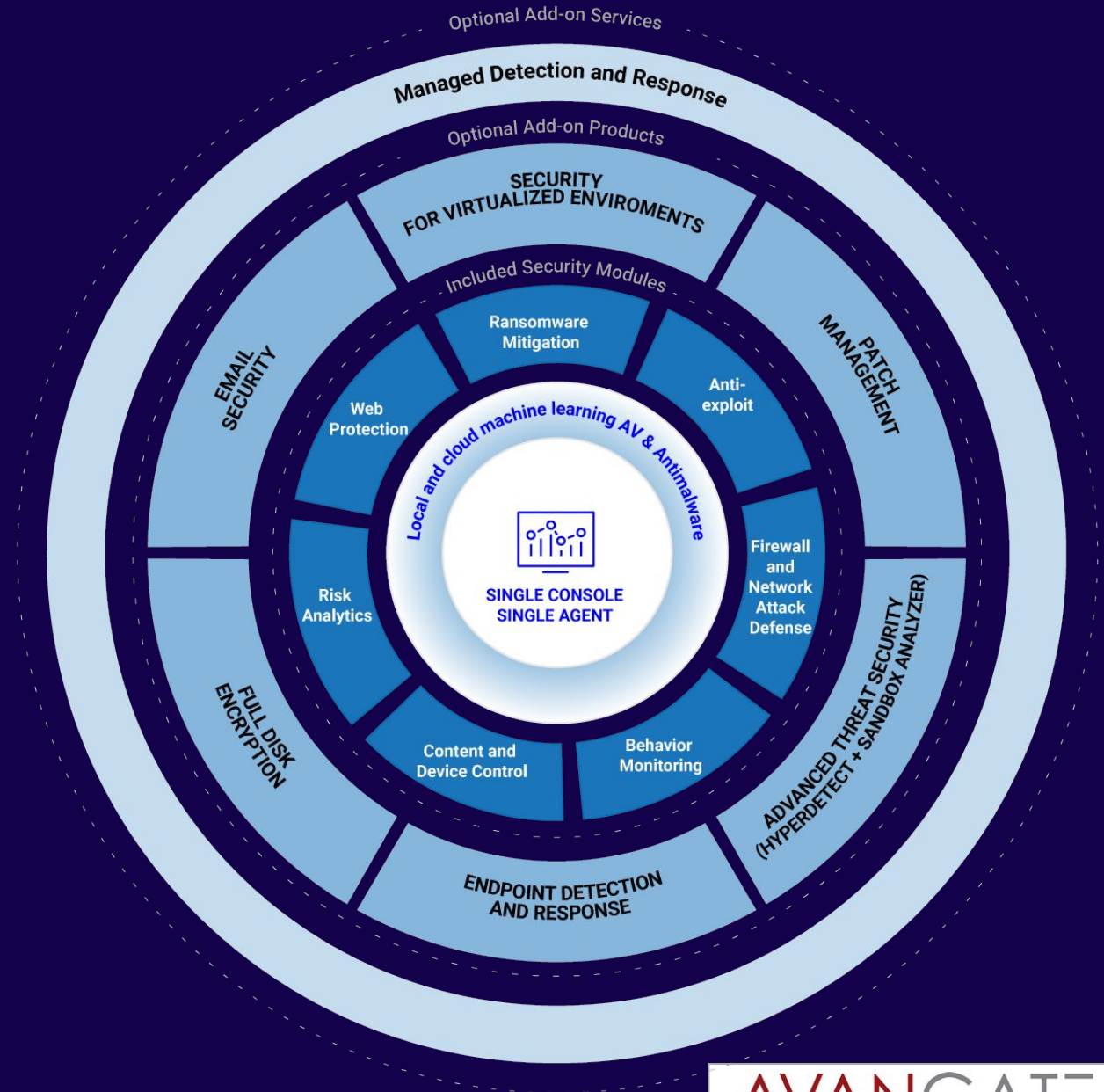


GRAVITYZONE SECURITY FOR MSPs services

Funzionalità di base

Funzionalità add-on:

Servizi professionali



GRAVITYZONE SECURITY FOR MSPs services

Monthly Subscription (EPP) Antimalware + Firewall + Device Control + Risk Management + AntiExploit + Content Control + Network Attack Defense + Ransomware Mitigation	per endpoint/mese
Advanced Threat Security (ATS) Fileless Attack Defense + Tunable Machine Learning (HD) + Sandbox Analyzer	per endpoint/mese
Endpoint Detection & Response (EDR) EDR Sensor + Intra Device Correlation + Incident Analysis	per endpoint/mese
Patch Management (PM) O.S. and applications update detection and install	per endpoint/mese
Encryption (FDE) Full Disk Encryption management + report + key recovery	per endpoint/mese
Email Security (ESG) Cloud mail gateway Antimalware/Antispam/Content Control	per mailbox/mese
Exchange Security (EXCHANGE) OnPremises Antimalware/Antispam/Content Control	per mailbox/mese
Security for Virtualized Environment (SVE) Central Scan for optimization in high density environments	per VDI/ora per VS/mese
Managed Detection and Response (MDR) monitoring and investigation by Bitdefender's SOC	per endpoint/mese

Nota 1 EPP è il servizio di base, obbligatorio con tutti gli altri servizi.
Nota 2 EDR comporta l'attivazione obbligatoria di BASE + ATS.
Nota 3 MDR comporta l'attivazione obbligatoria di ATS + EDR.

Abilitazione servizi sul cliente

Sottoscrizione per MSP di base

Abilitazione servizi add-on

License

Company type:

☒ Manage Networks

License type:

☐ Reserve seats

☐ Subscription end date

☐ Auto-renewal

☐ Minimum usage

Product type:

Information

Each service comes with an additional fee based on usage. Enabling the 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 from this [KB article](#).

☐ Security for Exchange

☐ Email Security

☐ Full Disk Encryption

☐ Security for Virtualized Environments

☐ Patch Management

☐ Advanced Threat Security

☐ HyperDetect

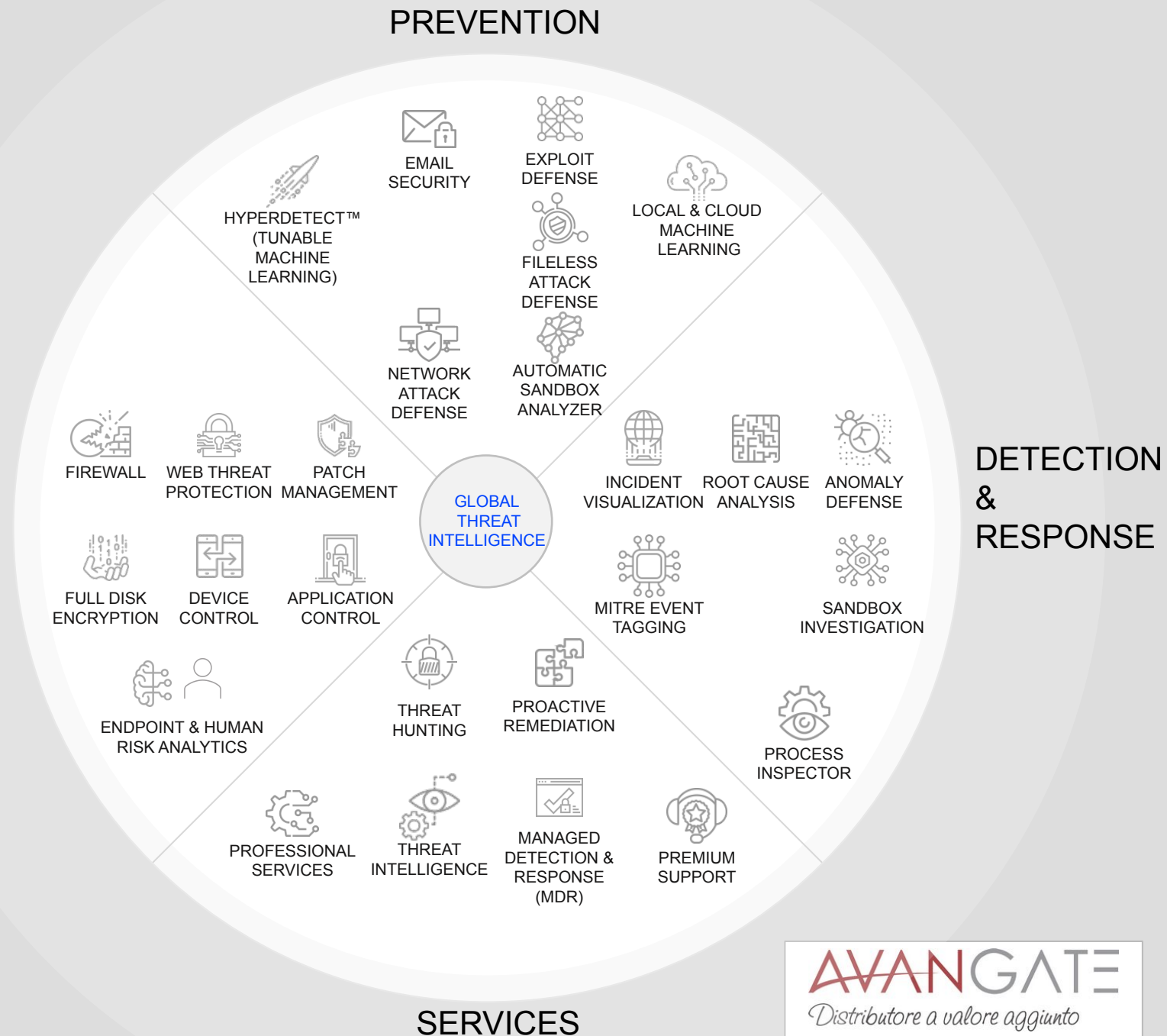
☐ Sandbox Analyzer

☐ Endpoint Detection and Response

Tecnologie e servizi

Tecnologie e Servizi

RISK
ANALYTICS
&
HARDENING



Caratteristiche incluse nella **sottoscrizione di base**

Risk Management

Correggi le misconfiguration.

Calcola il punteggio di rischio

Ordina e priorizza gli asset.

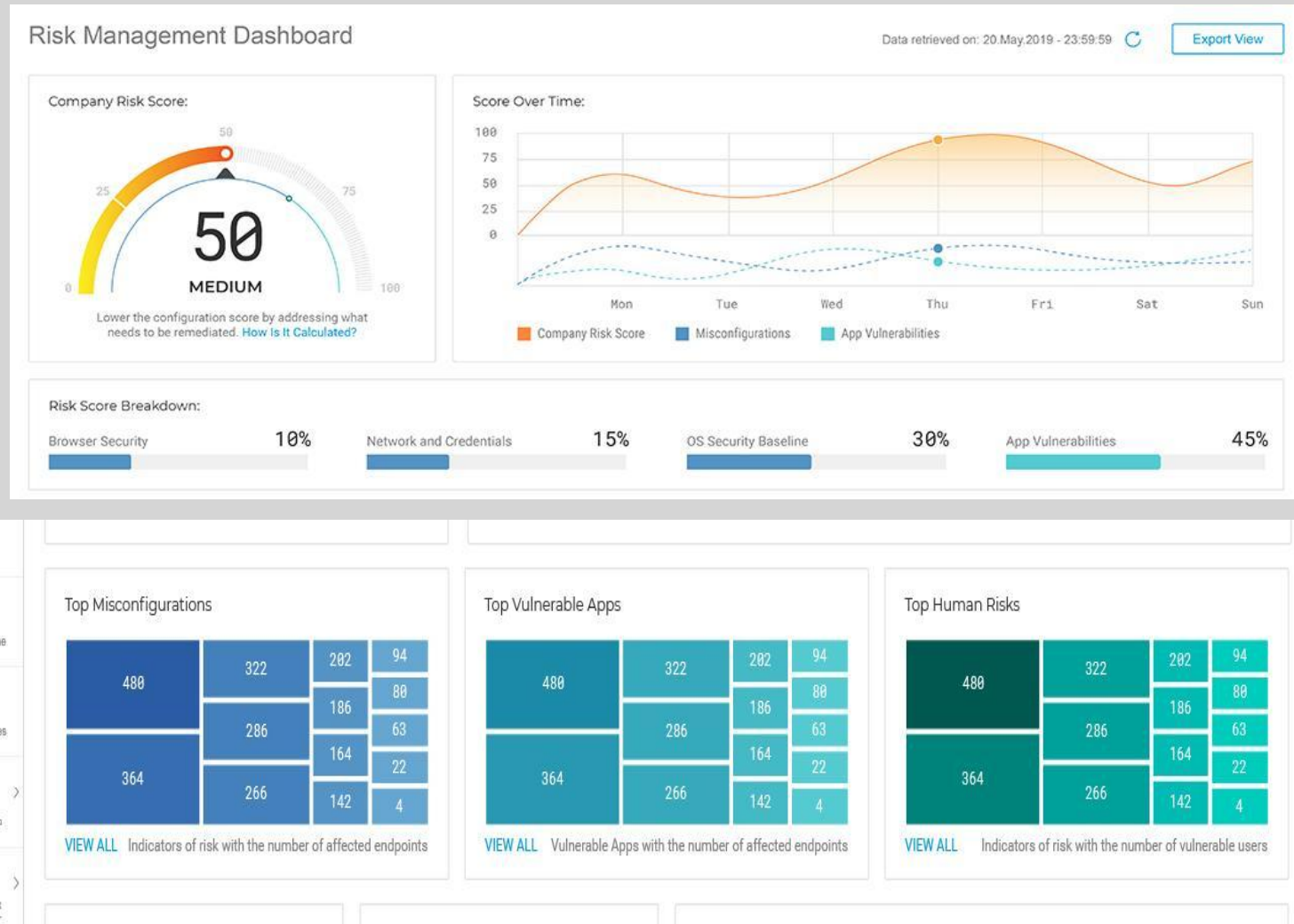
Prioritizza gli interventi sulla base della severità dei rischi.

Usa 206 indicatori di misconfiguration.

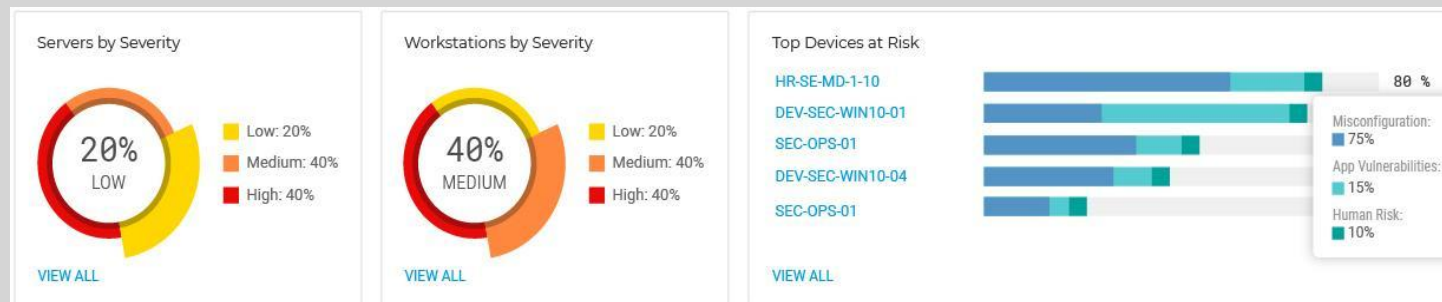
Correzione automatica disponibile per molti degli indicatori.

Abilita l'hardening degli endpoint grazie all'encryption, il Controllo Dispositivi, Controllo Applicazioni, Firewall, Patch Management.

Genera opportunità di upsell.



Bitdefender®



AVANGATE
Distributore a valore aggiunto

Risk Management - Human Risk

The screenshot shows the Bitdefender GravityZone 'User & Devices' section. The 'Human Risks' tab is selected. A message states: 'Here's a sneak peak into our brand new user behavior analytics technology. For now you can only view and ignore human based risks, but more will soon'. Below this are 'Ignore' and 'Export List' buttons. A table lists users with their risk levels and counts.

Users	Severity	No. Risk
<input type="checkbox"/> Lia Shepard	High (90%)	24
<input type="checkbox"/> Ziggy Ratcliffe	Medium (50%)	80
<input type="checkbox"/> TD default_user	Low (20%)	14
<input type="checkbox"/> TC Thelma Connor	High (90%)	40

95% dei security incidents
legato ad errore umano

Continuo aumento del fattore umano
quale causa di data breach,
dal 2015 ad oggi.

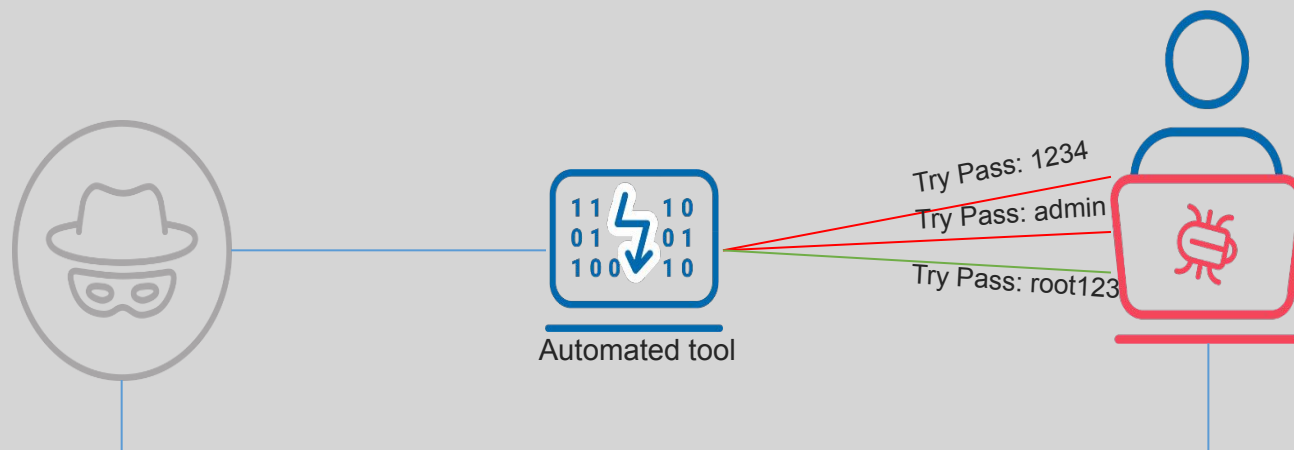
Phishing e whaling
cresciuti del 26% nel 2020.

Human Risk Analytics

fornisce dati sugli atteggiamenti
in tema di sicurezza, i
comportamenti, ed il livello di
rischio portato all'azienda.

Sources: IBM Cyber Security Intelligence Index
Verizon Data Breach Investigation Report
The Indelible Impact of COVID-19
on Cybersecurity, Bitdefender

Network Attack Defense



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

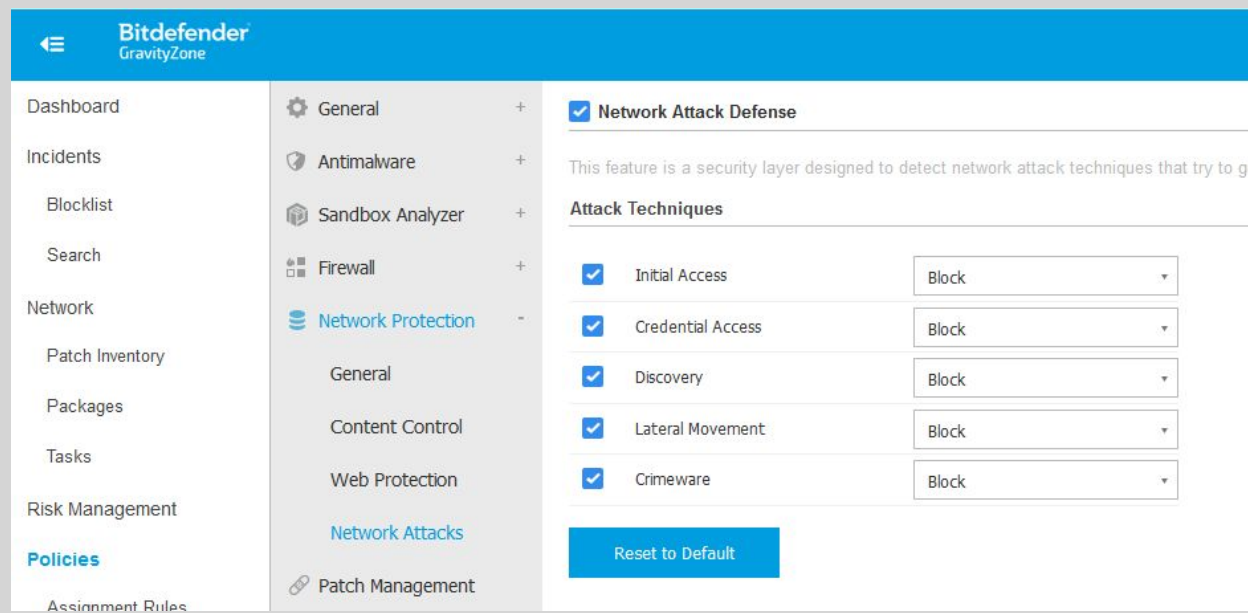
Network Attack Defense

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



Bitdefender®

JULY 21, 2021 | 17

AVANGATE
Distributore a valore aggiunto

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 Standalone interface. The left sidebar contains navigation options: Dashboard, Executive Summary, Incidents, 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 'Endpoint Incidents' with a table of open incidents. A detailed view of an incident (ID #11) is shown, including a timeline of events: wininit.exe (610) executed, services.exe (780) executed, sychost.exe (892) executed, and microsoftedgecp.exe... executed. The right sidebar shows 'Alerts' for 'microsoftedgecp.exe' with a severity of 'High' and a detection time of '06 Nov 2020, 14:30'. Below the alerts, there is an 'INVESTIGATION' section with 'NETWORK PRESENCE' showing 1 endpoint and 'FURTHER ANALYSIS' with links to 'Add to Sandbox', 'VirusTotal', and 'Google'. The 'REMEDIATION' section shows 'ACTIONS TAKEN' as 'No actions taken'.

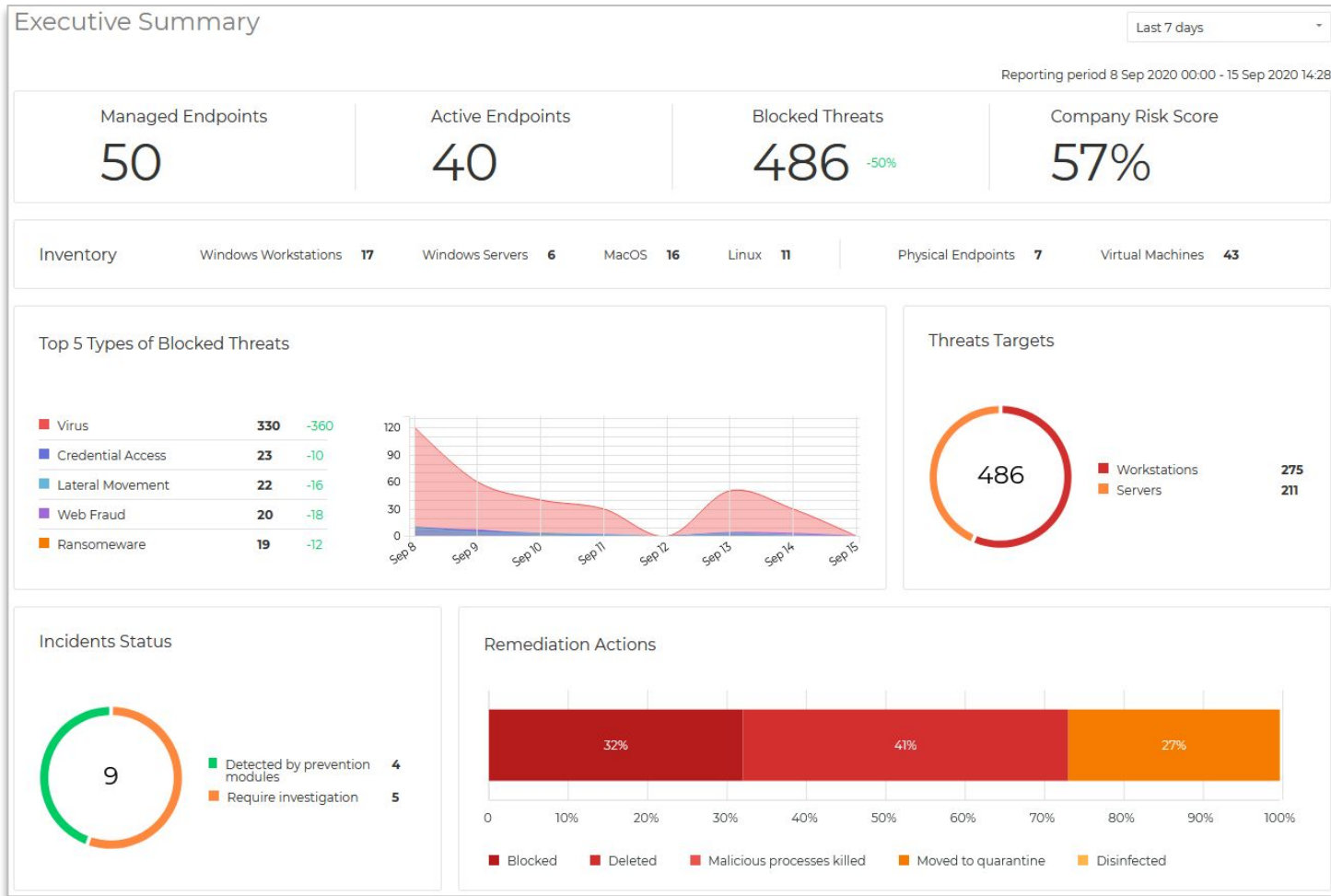
Ranked #1 for actionable detections and attack chain coverage, MITRE 2020 evaluations

Executive Summary

L'an 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



Ransomware Mitigation

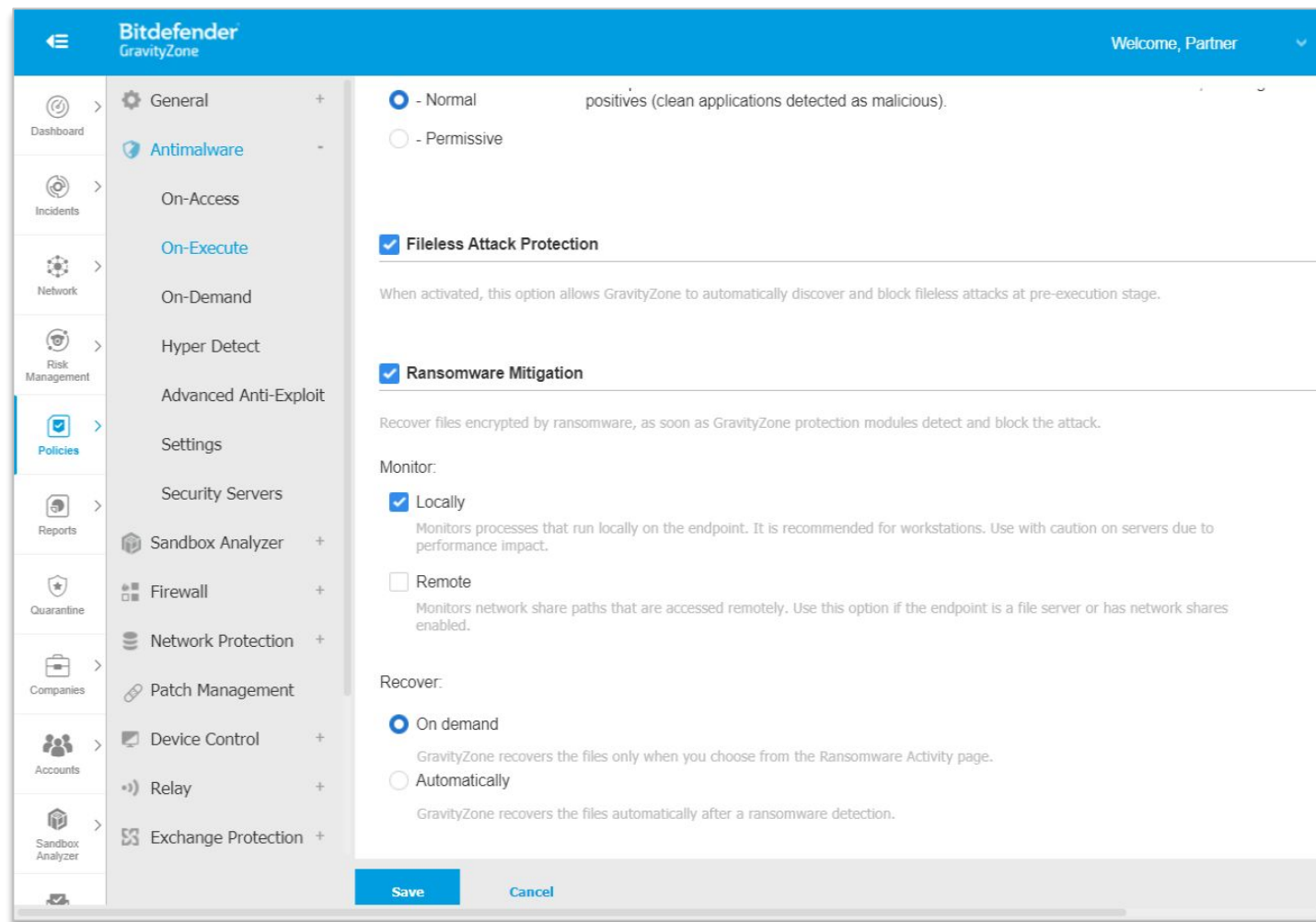
Ransomware mitigation helps organizations recover files after a blocked ransomware attack – without any downtime.

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



Caratteristiche Add-on

Advanced Threat Security ATS

Abilitazione di ATS →

License

Company type:

☒ Manage Networks

License type:

☐ Reserve seats

☐ Subscription end date

☐ Auto-renewal

☐ Minimum usage

Product type:

Information

Each service comes with an additional fee based on usage. Enabling the 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 from this [KB article](#).

☐ Security for Exchange

☐ Email Security

☐ Full Disk Encryption

☐ Security for Virtualized Environments

☐ Patch Management

☐ Advanced Threat Security

☐ HyperDetect

☐ Sandbox Analyzer

☐ Endpoint Detection and Response

Advanced Threat Security - Hyper Detect

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

The screenshot shows the Bitdefender Hyper Detect settings window. On the left is a sidebar with navigation options: General, Antimalware, 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 is titled 'Hyper Detect' and includes a description: '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.' Below this is a 'Reset to default' button. The 'Protection Level' section has three radio buttons: Permissive, Normal (selected), and Aggressive. A table below lists detection categories with checkboxes and radio buttons for each protection level. The 'Actions' section at the bottom has dropdown menus for 'Files' (set to 'Report Only') and 'Network traffic' (set to 'Block'), along with checkboxes for 'Extend reporting on higher levels'.

	Permissive	Normal	Aggressive
<input checked="" type="checkbox"/> Targeted Attack	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Suspicious files and network traffic	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Exploits	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Ransomware	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Grayware	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Actions

Files: Report Only ☐ Extend reporting on higher levels

Network traffic: Block ☒ Extend reporting on higher levels

Buttons: Save, Cancel

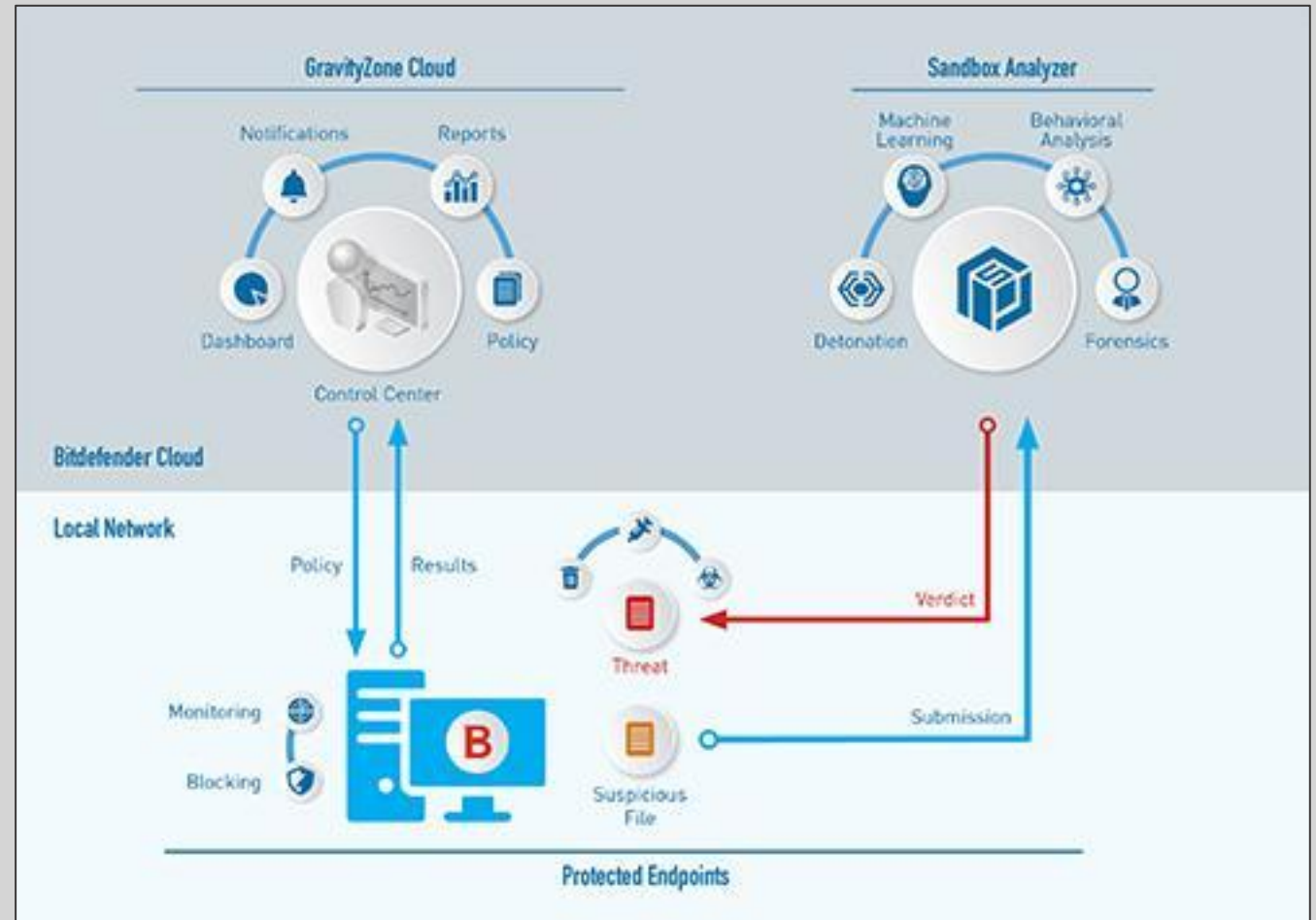
Advanced Threat Security - Sandbox Analyzer

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



Endpoint Detection and Response EDR

Abilitazione di EDR →

License

Company type:

☒ Manage Networks

License type:

☐ Reserve seats

☐ Subscription end date

☐ Auto-renewal

☐ Minimum usage

Product type:

Information

Each service comes with an additional fee based on usage. Enabling the 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 from this [KB article](#).

☐ Security for Exchange

☐ Email Security

☐ Full Disk Encryption

☐ Security for Virtualized Environments

☐ Patch Management

☐ Advanced Threat Security

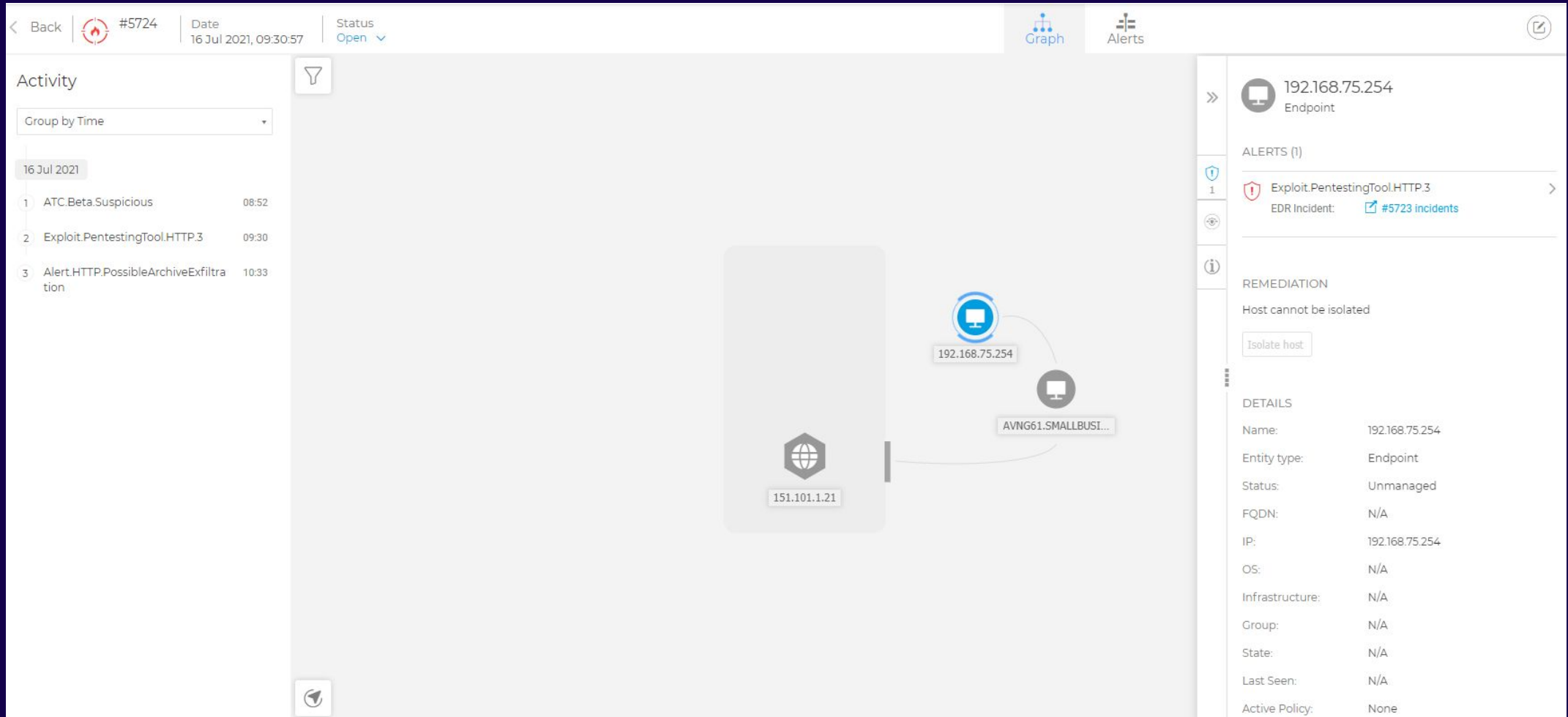
☐ HyperDetect

☐ Sandbox Analyzer

☐ Endpoint Detection and Response

eXtended Endpoint Detection and Response

xEDR - Visione estesa degli incidents



Back #5724 Date 16 Jul 2021, 09:30:57 Status Open

Graph Alerts

Activity

Group by Time

16 Jul 2021

- 1 ATC.Beta.Suspicious 08:52
- 2 Exploit.PentestingTool.HTTP.3 09:30
- 3 Alert.HTTP.PossibleArchiveExfiltration 10:33

151.101.1.21

192.168.75.254

AVNG61.SMALLBUSI...

192.168.75.254 Endpoint

ALERTS (1)

- 1 Exploit.PentestingTool.HTTP.3 EDR Incident: #5723 incidents

REMEDIATION

Host cannot be isolated

Isolate host

DETAILS

Name: 192.168.75.254

Entity type: Endpoint

Status: Unmanaged

FQDN: N/A

IP: 192.168.75.254

OS: N/A

Infrastructure: N/A

Group: N/A

State: N/A

Last Seen: N/A

Active Policy: None

Visione dei Security Incidents di tutti i clienti

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

385 items | [First Page](#) < of 20 > [Last Page](#) | Show

MDR

Managed Detection and Response

“What happens to your customers’ security when your teams log-off at the end of the day?”

BITDEFENDER MDR FOR MSPS OFFERINGS

Based on Cloud Security for MSP + ATS + EDR for endpoints
Available for 100 endpoints per customer and above

EXPERT ADVICE

Equip your security team with trusted expert advice

With Expert Advice you retain full control over your end customer environments, with the MDR team acting as your trusted advisor, providing curated recommendations to equip your team respond to customer incidents.

PREVENT

DETECT

COLLABORATE

EXPERT RESPONSE

Deliver managed threat hunting without doing the heaving lifting

Expert Response is designed to provide a fully managed threat hunting solution from prevention through to response. The Bitdefender MDR team will affect real-time changes in your customer's environments when security incidents are identified, based on a set of pre-approved actions agreed upon.

PREVENT

DETECT

RESPOND

Email Security (Gateway)

Abilitazione ESG



License

Company type:

☒ Manage Networks

License type:

☐ Reserve seats

☐ Subscription end date

☐ Auto-renewal

☐ Minimum usage

Product type:

! Information

Each service comes with an additional fee based on usage. Enabling the 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 from this [KB article](#).

☐ Security for Exchange

☐ **Email Security**

☐ Full Disk Encryption

☐ Security for Virtualized Environments

☐ Patch Management

☐ Advanced Threat Security

☐ HyperDetect

☐ Sandbox Analyzer

☐ Endpoint Detection and Response

Email is the #1 attack vector – it only takes one wrong click to comprise an entire network.

93%

of malware is delivered via email

67%

of SMBs have faced a cyberattack and **58%** experienced a data breach

96%

of data breaches are a direct result of phishing attacks and pretexting

85%

of organizations have been victims of phishing or social engineering attacks

84%

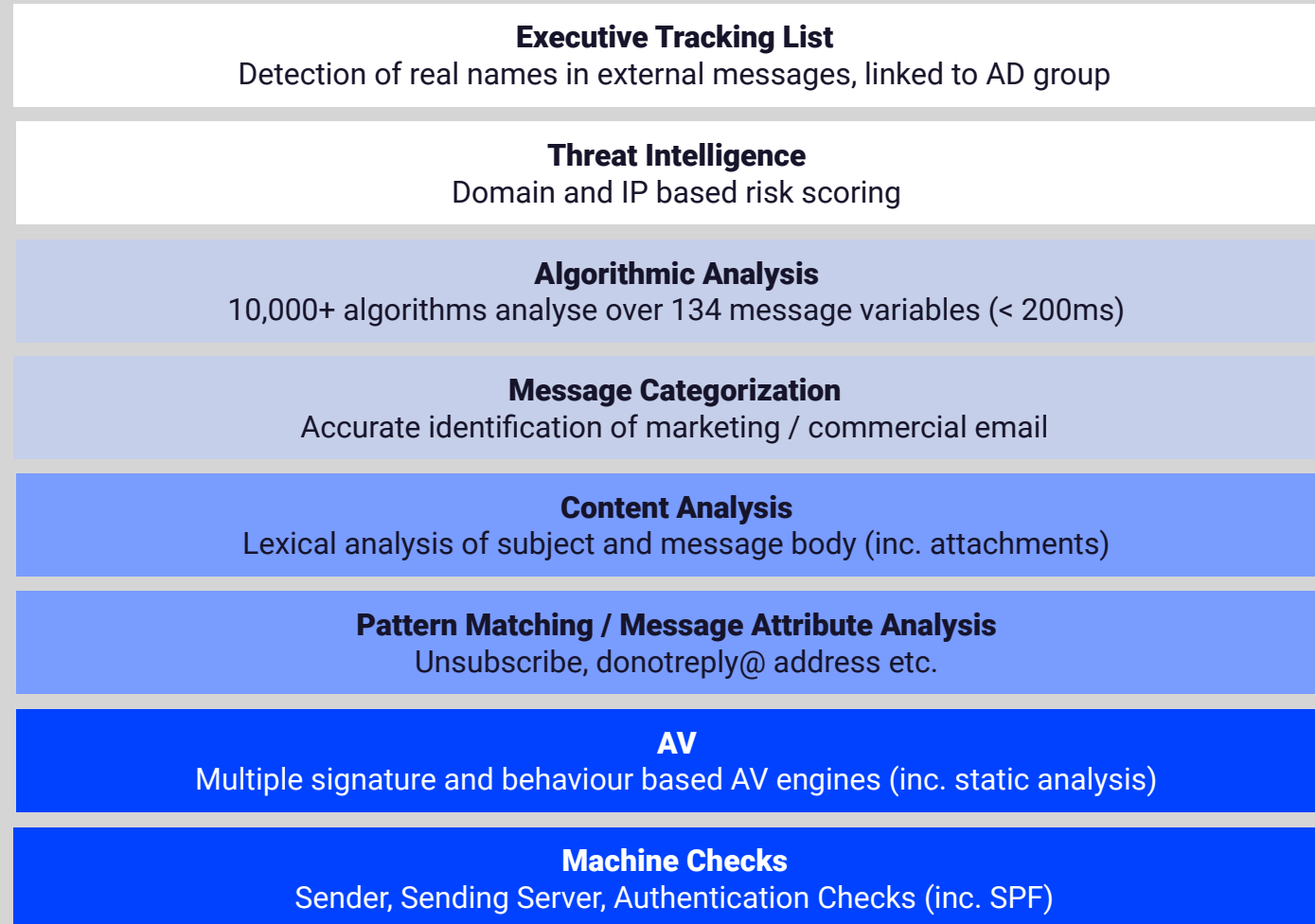
of social attacks involve phishing emails

BEC accounts for 1%+ of all traffic at an avg. cost of

\$37K to an organization

EMAIL SECURITY

Multi-layered Approach



Security for Virtualized Environments

Abilitazione SVE →

License

Company type:

☒ Manage Networks

License type:

☐ Reserve seats

☐ Subscription end date

☐ Auto-renewal

☐ Minimum usage

Product type:

! Information

Each service comes with an additional fee based on usage. Enabling the 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 from this [KB article](#).

☐ Security for Exchange

☐ Email Security

☐ Full Disk Encryption

☐ **Security for Virtualized Environments**

☐ Patch Management

☐ Advanced Threat Security

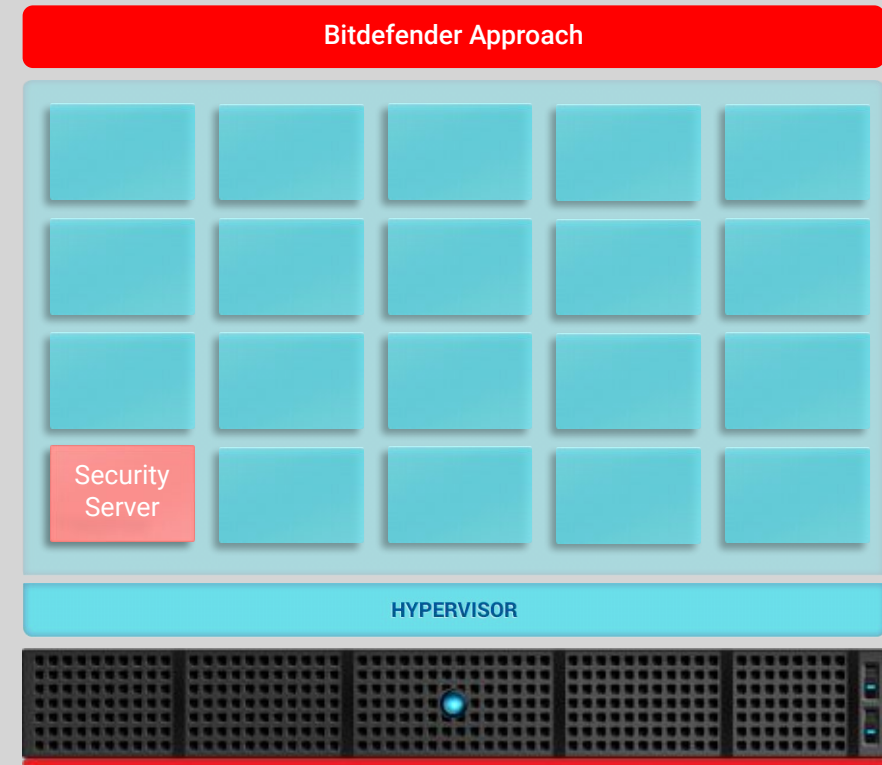
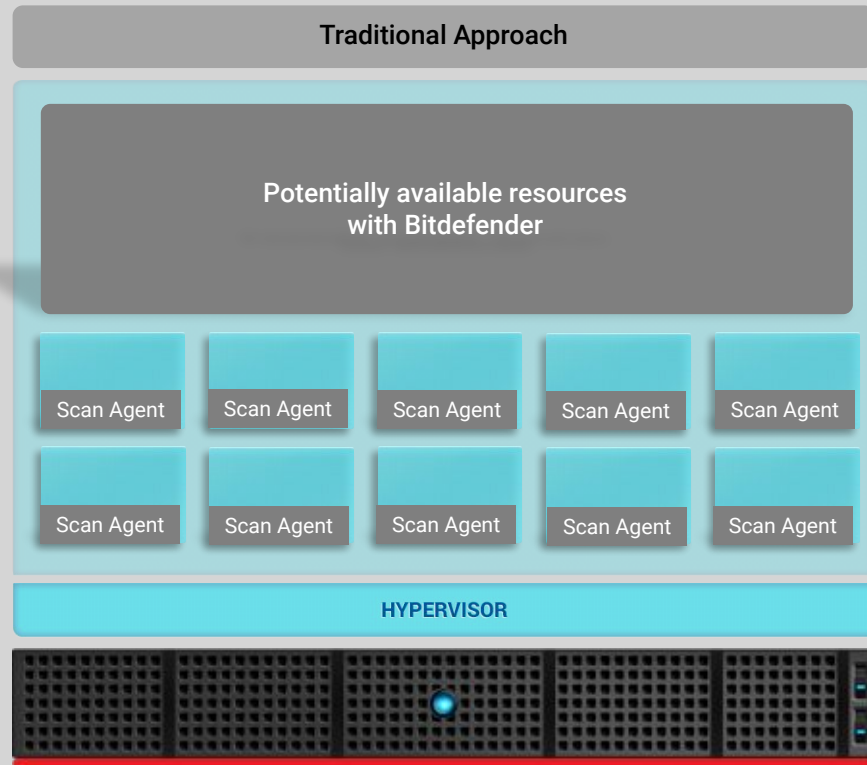
☐ HyperDetect

☐ Sandbox Analyzer

☐ Endpoint Detection and Response

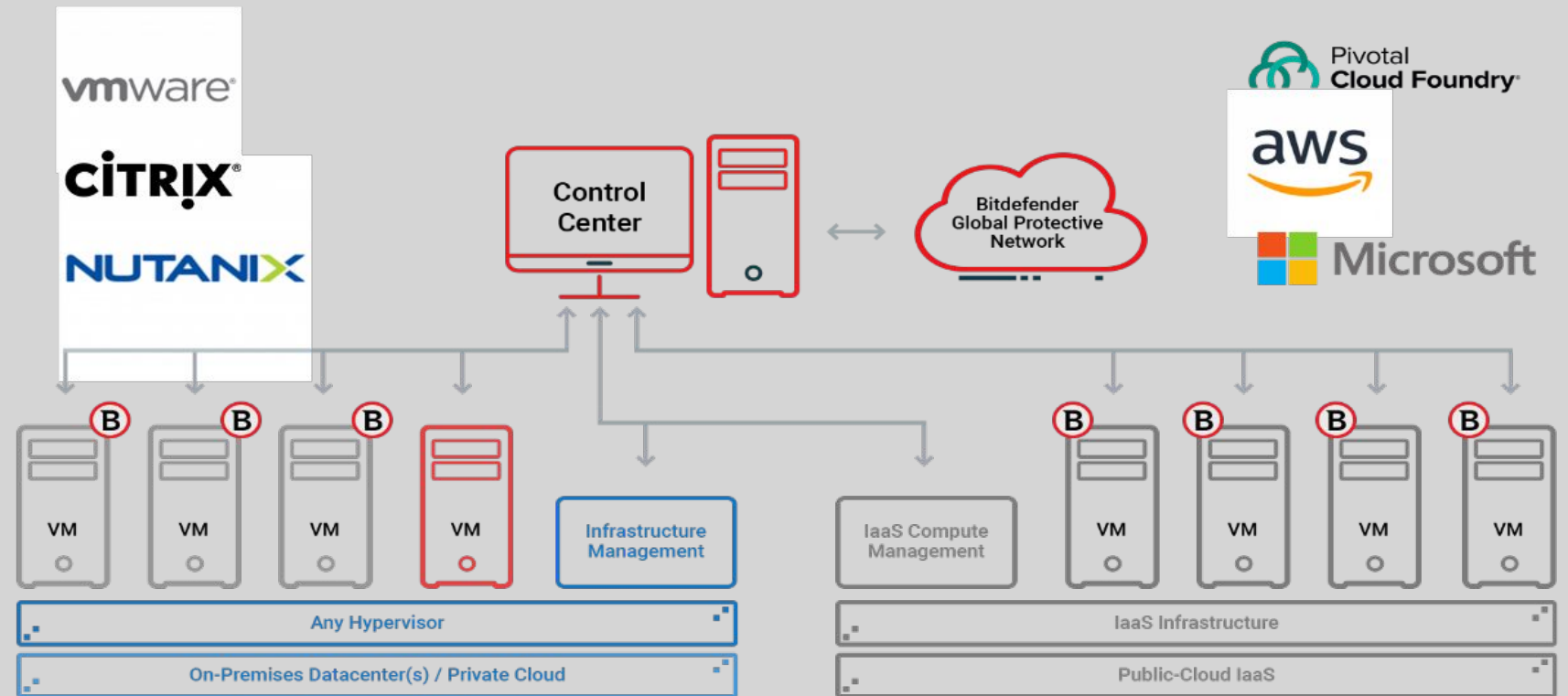
SVE

Traditional vs. Bitdefender Approach



GravityZone for Hybrid Cloud Environments

Protect servers and virtual desktops in any cloud effectively and consistently



Bitdefender®

AVANGATE
Distributore a valore aggiunto

Cloud Workload Defense

**Up to 36% Faster
Application Response**



**Up to 55% Higher
Virtualization Density**



**Consistent
Workload
Protection**

**SINGLE-PANE-OF-GLASS
VISIBILITY & REPORTING**

Consistent policy enforcement across clouds. Native integration with all major public and private clouds.

**Efficient
Infrastructure
Operations**

**SINGLE-CONSOLE
MANAGEMENT OF ALL VMS.**

Security-workflow automation.
Non-persistent VDI licensing.

**Unmatched
performance**

**MINIMAL IMPACT ON
PERFORMANCE & LATENCY**

Optimal end-user experience & higher ROI. 55% higher virtualization density. 36% faster application response.



NEW!

GravityZone Security for Containers

Proteggi gli host Linux ed i container,
tra cui Docker e Kubernetes

Bitdefender®

AVANGATE
Distributore a valore aggiunto

Security for Containers



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

GravityZone per MSP Integrazioni

GravityZone MSP Integrations

We work with the tools that you use every day to help automate your security workflows.



Integrazioni

RMMS, ERP, TICKETING, BILLING, SIEM

- **integrazione nativa** con **Kaseya** e **Connectwise**
- integrazione via **API/SOAP con qualsiasi sistema** anche homemade
- esposizione di **eventi push** (per SIEM e monitoring systems)

Licensing per MSP

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**

Termini e condizioni per i ServiceProvider

<https://www.bitdefender.it/site/view/legal-terms-xsp.html>

Bitdefender[®]

AVANGATE
Distributore a valore aggiunto

1-2-3 MSP

attivo con GravityZone per MSP in 3 semplici mosse



Ti registri come Partner Avangate Italia

<https://nova.avangate.it/register.php>



Chiedi l'attivazione come partner Bitdefender

<https://nova.avangate.it> → Support → Inserisci una richiesta:
Tipo: GravityZone Cloud - abilitazione partner



Chiedi l'abilitazione al licensing per MSP

<https://nova.avangate.it> → Support → Inserisci una richiesta:
Tipo: GravityZone Cloud - abilitazione MSP

Bitdefender®

AVANGATE
Distributore a valore aggiunto

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

Domande

Utilizza la 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