Bitdefender

Bitdefender MDR 2024 New Editions

Cesare Vellani - Avangate Security

Pre\Post Sales Engineer

AVANGATE
Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

Agenda

- **Da GDPR a NIS2**: nuove sfide
  - Direttive
  - Soggetti interessati
  - Date
  - Sanzioni
  - Perchè Bitdefender MDR

- **Bitdefender MDR**: nuova offerta 2024
  - Cosa offre
  - Caratteristiche principali
  - Ruolo della Human Expertise nei servizi MDR
  - MDR vs MDR PLUS
  - Cybersecurity Breach Warranty

Direttive

GDPR

Cercava di migliorare gli standard di privacy e sicurezza a livello *dei dati degli utenti*.

NIS2 (Network Information & Security)

Cerca di migliorare gli standard di privacy, gestione del rischio e sicurezza *per le aziende e le organizzazioni nel loro insieme*.

Direttiva NIS2

Secondo l'articolo 21, gli Stati Membri devono assicurare ***che le entità importanti e quelle essenziali prendano le adeguate e proporzionate misure tecniche, operative e organizzative per gestire i rischi relativi alla sicurezza della rete e ai sistemi informativi utilizzati per le loro operazioni o per erogare i loro servizi, per prevenire o minimizzare l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi***. Queste misure dovrebbero essere basate su un ***approccio che consideri tutti i rischi*** con lo scopo di proteggere i sistemi di rete e informativi, l'ambiente in cui operano tali sistemi e infine dovrebbe includere almeno i seguenti punti:

- Policy sull'analisi del rischio e sulla sicurezza dei sistemi informativi;
- Gestione degli incidenti;
- Continuità operativa, come gestione dei backup, disaster recovery e gestione delle crisi;
- Sicurezza della supply chain, tra cui aspetti legati alla sicurezza riguardanti il rapporto tra ogni entità e i suoi fornitori diretti o service provider;
- Sicurezza nell'acquisto, nello sviluppo e manutenzione dei sistemi di rete e informativi, inclusa la gestione e la comunicazione della vulnerabilità;
- Regole e procedure per valutare l'efficacia delle misure di sicurezza informatica relative alla gestione dei rischi;
- Pratiche di "igiene informatica" di base e formazione sul tema della sicurezza informatica;
- Policy e procedure riguardanti l'uso della crittografia e, laddove necessaria, encryption;
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione degli asset; laddove opportuno, autenticazione multi fattore o soluzioni di autenticazione continua; comunicazioni vocali, scritte e video protette; sistemi di comunicazione di emergenza protetti all'interno dell'ente.

NIS2 Directive

Date

NIS2 è stata ufficialmente **pubblicata il 27 dicembre 2022** ed è **entrata in vigore il 16 gennaio 2023**.

Gli Stati membri dell'UE erano tenuti ad incorporare NIS2 nella propria legislazione nazionale entro il 18 ottobre 2024.

Le organizzazioni interessate si sarebbero dovute **conformare a questa direttiva entro il 18 ottobre 2024**.

Soggetti interessati

Chi impatta NIS2?

Tutte le aziende che rientrano nelle definizioni di “**Entità importanti**” o “**Entità Essenziali**”. Vi rientrano aziende di **tutti i settori**, con dimensioni da **>50 addetti/10M** bilancio e **250 addetti/50M** bilancio rispettivamente.

Rientrano anche aziende con numeri inferiori, se si tratta di un “fornitore unico” fondamentale dal punto di vista sociale o economico per i paesi membri UE.

Sebbene siano ancora previste modifiche a NIS2, riteniamo che NIS2 possa applicarsi a qualsiasi azienda che operi all’interno dell’UE.

NIS2 Directive

Soggetti interessati

AVANGATE

NIS2 Directive

Sanzioni

Le organizzazioni che non rispettano la direttiva NIS2 possono incorrere in pesanti sanzioni:

- fino a 10 milioni di euro o il 2% del fatturato globale, per le “entità essenziali”.

- fino a 7 milioni di euro ovvero l'1,4% del fatturato globale, le entità importanti.

AVANGATE

NIS2 Directive

NIS2 chiama, Bitdefender risponde: come prepararsi

Be prepared

10 things organizations should consider for NIS2 compliance:

1. Determine if NIS2 applies to your organization.
2. Identify your critical assets.
3. Develop a risk management strategy.
4. Implement appropriate security measures.
5. Implement incident response procedures.
6. Conduct regular security testing.
7. Train employees.
8. Consider third-party risks.
9. Maintain documentation.
10. Comply with reporting requirements.

AVANGATE

NIS2 proposes the following

"ALL-HAZARDS" APPROACH MEASURES:

Risk analysis and information system security	Incident handling & business continuity	Supply chain security with cyber hygiene & training	Security in network & vulnerability handling and disclosure	Policies for cryptography and encryption	Human resources security, access control policies and asset management
Is your system updated? Do you have risk?	Prevent and mitigate any type of attack	Bitdefender MDR can help with: 24x7 security monitoring, advanced attack prevention, detection and remediation, plus targeted and risk-based threat hunting	Protect your intelectual property	Protect your sensitive or critical information	Is your staff cyber trained and fully aware of the compliance risks and penalties?
Intelligence monitoring to identify external risks to your environment before they spread.	MDR surpasses traditional methods by providing continuous human-led monitoring, resulting in enhanced security and quicker response times.	24x7 security monitoring, advanced attack prevention, detection and remediation, plus targeted and risk-based threat hunting.	Advanced threat protection, attack containment through automatic and human-led guided response.	Fully encrypt each endpoint's hard drive and reduce the risk of accidental data loss or theft to achieve regulatory compliance.	Increase awareness in your company to decrease espionage and data loss.
Patch Management and Managed Detection & Response (MDR)	**Managed Detection & Response (MDR)**	**Managed Detection & Response (MDR)**	**Extended Detection & Response(XDR) & Managed Detection and Response(MDR)**	**Full Disk Encryption (FDE)**	**Cyber Compliance**

Le certezze vacillano

Hai consapevolezza della situazione sulla sicurezza?

Conosci il tuo profilo di attacco in tempo reale e la postura difensiva corretta in ogni situazione?

Puoi essere sicuro di essere protetto dagli attacchi più recenti e sicuro che le tue difese siano completamente ottimizzate?

Gli aggressori lavorano 24 ore su 24, 7 giorni su 7. Il tuo team di sicurezza fa lo stesso?

Le lacune chiave in azienda

Bitdefender

Tempo
Le indagini sugli incidenti di sicurezza richiedono molto tempo, sono complesse e possono richiedere più addetti.

Competenze
Sfida costante per reclutare, formare e trattenere personale InfoSec qualificato con incarichi sempre più brevi.

Visibilità
Il personale InfoSec interno ha visibilità limitata e/o tardiva sui fenomeni cybercriminali che fanno il giro del mondo in poche ore. Per lo più solo quando i fenomeni entrano in azienda.

Efficienza
Troppi strumenti e console in diverse tecnologie offuscano il quadro generale della sicurezza.

Risultati
Il rilevamento di attacchi avanzati e mirati è difficile, consentendo agli aggressori di prolungare il "tempo di permanenza".

AVANGATE

…e dai sondaggi…

Bitdefender

Carenza di staff nei SOC
Gli analisti della sicurezza sono una risorsa scarsa e costosa che è difficile assumere e conservare.
Un recente sondaggio di Ponemon ha mostrato che il 60% dei membri dei team SOC sta considerando di lasciare il proprio lavoro a causa dello stress.

Rilevamento degli attacchi avanzati
Gli attacchi avanzati sono difficili da rilevare, poiché usano Tattiche, Tecniche e Procedure (TTP) che, singolarmente, sembrano comportamenti normali. Il costo medio di un incidente informatico per le aziende è aumentato del 72% negli ultimi cinque anni, raggiungendo i 13 milioni di dollari - Rapporto del 2021 di Accenture, "Cost of Cybercrime"

Le indagini richiedono tempo
Gli analisti di sicurezza non hanno abbastanza tempo per valutare ogni singola allerta e impostare delle priorità per effettuare ulteriori indagini. Il tempo medio di risposta (MTTR) per la maggior parte delle organizzazioni è misurato in mesi, mentre gli aggressori compromettono ed esfiltrano i dati in giorni.

Troppi strumenti
Le organizzazioni dispongono di più console su diverse tecnologie per gestire l'architettura di sicurezza.
Circa il 40% degli intervistati del sondaggio di Ponemon ha dichiarato di avere troppi strumenti.
Il 71% ha bisogno di più automazione per gestire le allerte e raccogliere le prove.

AVANGATE

Bitdefender MDR: piattaforma + servizio

Strumenti

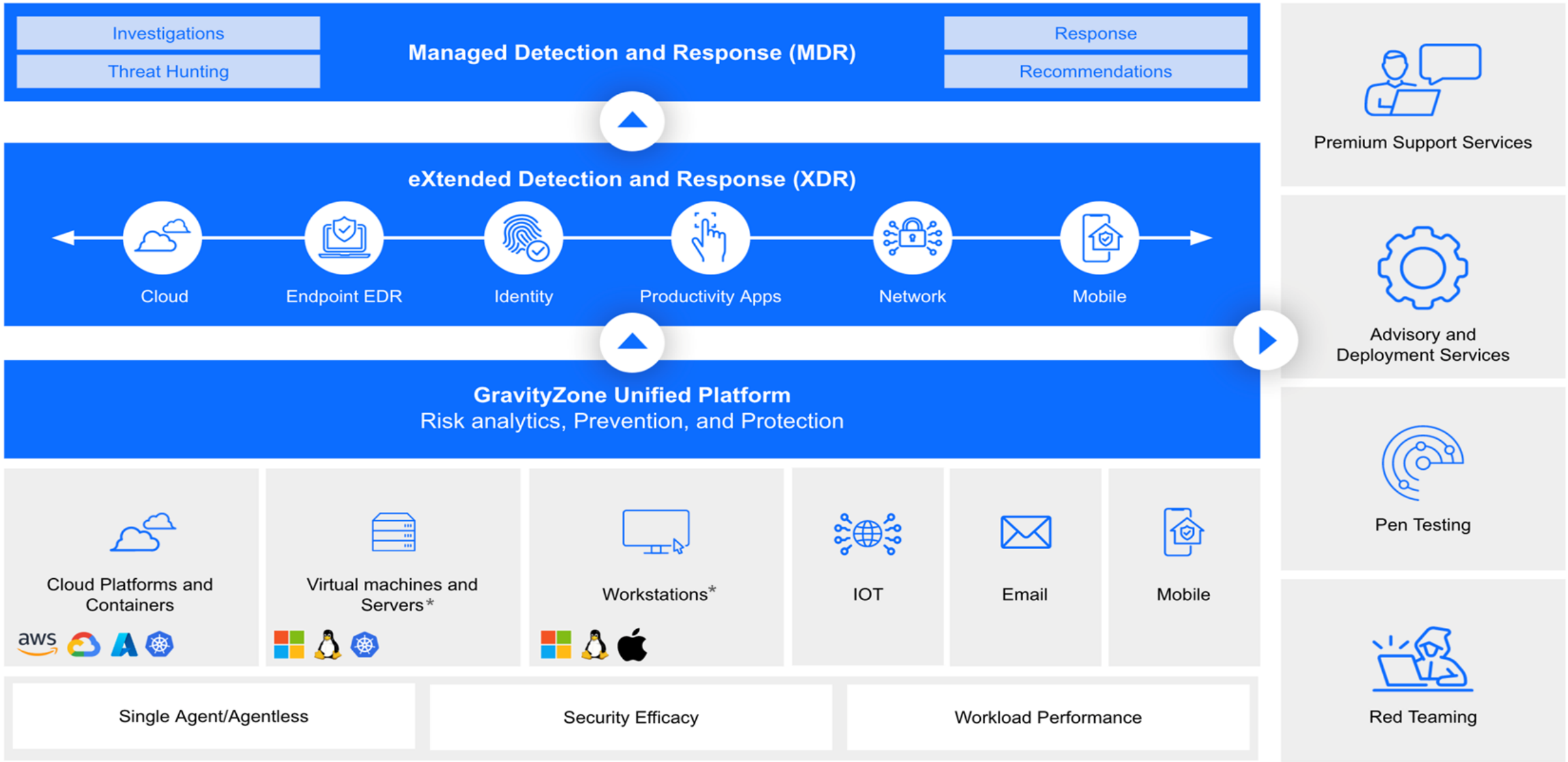
GravityZone Enterprise

+

Competenze e presidio

SOC Bitdefender

Bitdefender MDR: piattaforma + servizio



*continued Legacy OS support

“Human Expertise” disponibile 24/7

Bitdefender

Competenza ed esperienza sono ingredienti fondamentali per i team addetti al controllo della sicurezza. Con Bitdefender MDR ci avvaliamo di un team formato dai **migliori esperti ed analisti, reclutati presso aziende ed enti governativi di rilevanza mondiale** (US Air Force, Navy, NSA e servizi segreti britannici ad esempio).

La loro esperienza e competenza sono alimentate continuamente dalla visibilità su una mole incalcolabile di dati, e dal lavoro parallelo su realtà di tutti i settori. Ne deriva un **livello di servizio irraggiungibile per le singole organizzazioni**, per grandi e facoltose che possano essere.

Il cybercrimine non conosce riposo: la notte e le festività sono le finestre temporali più ambite per mettere a segno attacchi di successo. Con 3 SOC (Texas, Romania e Singapore) distribuiti su base mondiale ed una turnazione ottimale, Bitdefender assicura una vera **copertura 24/7**.

AVANGATE

Bitdefender MDR - Come opera

Bitdefender

Previeni

La protezione degli endpoint leader di settore è integrata nella piattaforma di sicurezza EDR di Bitdefender per offrire la massima efficacia contro le minacce persistenti avanzate e bloccare la maggior parte degli attacchi prima dell'esecuzione. I sensori XDR opzionali offrono un rilevamento e una risposta unificati attraverso endpoint, rete, cloud, app di produttività e identità.

Rileva

Gli analisti della sicurezza di Bitdefender monitorano continuamente gli eventi e gli avvisi di sicurezza rilevati, a cui viene assegnata una priorità in base alla gravità, all'impatto e alla rilevanza per il livello di sicurezza della tua azienda (ad esempio, la linea di base). Utilizzando analisi avanzate, AI/ML, intelligence sulle minacce e conoscenze umane esperte, i nostri analisti valutano e analizzano gli avvisi per determinare la natura e la portata della minaccia.

Rispondi

Gli analisti della sicurezza di Bitdefender avviano rapidamente flussi di lavoro di risposta e azioni pre-approvate per contenere le minacce e mitigarne l'impatto. Per un incidente, un security account manager (SAM) ti contatterà entro 30 minuti dalla dichiarazione dell'incidente, inviandoti un rapporto che include i primi risultati. Una volta risolto l'incidente, riceverai un rapporto post-azione che fornisce ulteriori dettagli per l'audit.

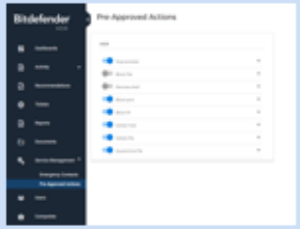
Rapporto

Le dashboard nel tuo portale MDR offrono informazioni in tempo reale relative a configurazione e servizio MDR. I rapporti mensili di MDR offrono informazioni di riepilogo e dettagliate su tutti gli aspetti del tuo servizio, incluso l'implementazione, gli eventi sospetti, le indagini e i suggerimenti. Se si verifica un incidente, tutti i relativi rapporti e le azioni di risposta intraprese.

Bitdefender MDR - Come opera

Bitdefender

ACTIVE MONITORING & RESPONSE



Threat Hunt

MDR Detection

Investigation

Identification

AMR Notification to CST

Containment

Eradication

Dashboards & Records
MDR Portal

Notification & Flash Reports
MDR Portal

SECURITY ACCOUNT MANAGER

1 Initial phone call to customer
2. Communicates with SOC via slack channel apart of ticket/case
3. Periodic updates flash report Email/Portal
4. Final AAR sent

Notification & After Action Reports
MDR Portal

Timely and comprehensive

- SLA: 30 min to contact for critical / high incidents
- Containment using wide-ranging set of actions (PAA)
- Flash reports/updates
- After action reports
- 72 hours targeted monitoring

AVANGATE

Bitdefender MDR – Piani di licenza

Bitdefender

Service Component	Bitdefender MDR	Bitdefender MDR PLUS
Industry leading security platform	✓	✓
24x7 SOC	✓	✓
Pre-approved Actions (PAAs)	✓	✓
Threat Hunting	✓	✓
Expert Recommendations	✓	✓
Incident Root Cause & Impact Analysis	✓	✓
MDR Portal & Reporting	✓	✓
24x7 Security Account Manager (Customer Success)		✓
Professional Services On-boarding		✓
Global Threat Intelligence Feeds and Analysis		✓
Dark Web Monitoring		✓
Security Baselining and Tailored Threat Modeling		✓
Brand & IP Protection		✓
High Priority Target Monitoring		✓
XDR Sensors	Add-ons	Add-ons

AVANGATE

Bitdefender MDR – Licenze

- MDR\MDR Plus comprendono GZ Enterprise
- Numero minimo di nodi: 50
- Sensori XDR (Cloud, Identity, Productivity, Network, Business Application) disponibili come “add-on”
- Trial disponibile: da richiedere ad Avangate

Bitdefender MDR – Perchè sceglierlo?

- **Processo di Onboarding**
- **XDR nativo**
- **Human-Driven Analysis su MDR e MDR PLUS**
- **Threat Response su MDR e MDR PLUS**
- **Bitdefender MDR PLUS ->** priority target monitoring, dark web monitoring, domain registration monitoring, asset monitoring, brand\IP protection, tailored threat monitoring e targeted threat hunting.
- **NEW!!!** -> Bitdefender MDR Cybersecurity Breach Warranty

Bitdefender MDR – Cybersecurity Breach Warranty

Bitdefender

Certification Warranty Indemnification			
Bitdefender MDR		**Bitdefender MDR PLUS**	
Ransomware[2]	$100,000	Compliance Event	$200,000
		Ransomware Event & BEC Event	$200,000
		Cyber Legal Liability Event[3]	$500,000
		Business Income Event[4]	$100,000
		TOTAL	$1,000,000

I clienti saranno idonei per un'assistenza finanziaria fino a:

- **$100.000 per MDR da 50 a 999 endpoint;**
- **$1.000.000 per MDR da 1000 a 5000+ endpoint;**
- **$1.000.000 per MDR PLUS da 50 a 5000+ endpoint**

- FAQ: https://shorturl.at/SNLJ9

AVANGATE

Bitdefender MDR – Risorse utili

Bitdefender

- Pagina ufficiale - https://www.bitdefender.it/business/products/managed-detection-response-service.html
- Demo interattiva - https://shorturl.at/JCCpl
- Guida online - https://www.bitdefender.com/business/support/en/124809-124812-about-mdr.html
- Masterclass BD - https://register.gotowebinar.com/register/3573539670078281567

AVANGATE

AVANGATE

Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

GRAZIE