DATASHEET

Bitdefender

Bitdefender GravityZone Extended Email Security

Due livelli. Un'unica piattaforma. Una protezione per e-mail estesa.

Perché entrambi i livelli sono importanti

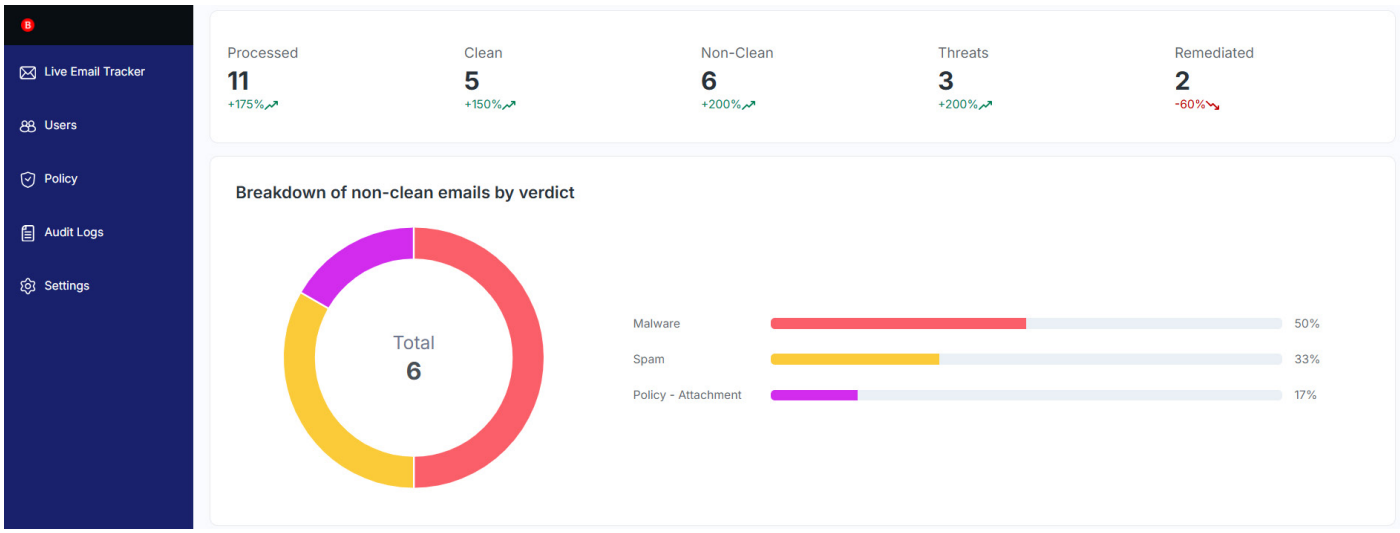
La maggior parte degli strumenti di sicurezza per e-mail consente alle organizzazioni di scegliere tra due strategie: un Secure Email Gateway (SEG) o una protezione delle caselle di posta elettronica basata su API. Ciascuna strategia copre solo una parte della superficie di attacco. Il SEG blocca le minacce sul perimetro, ma perde visibilità una volta che i messaggi raggiungono le caselle di posta. Gli strumenti basati su API possono agire dopo la consegna, ma non filtrano a livello di gateway.

Bitdefender GravityZone Extended Email Security ha entrambi i livelli. Il filtro SEG blocca phishing, spam e malware prima che raggiungono gli utenti, mentre l'integrazione basata su API esamina continuamente le caselle di posta per rilevare, mettere in quarantena o rimuovere le minacce che sfuggono a livello di perimetro. Questo approccio a doppio livello garantisce una protezione continua ed end-to-end contro ransomware, phishing, BEC, impersonificazione e rischi interni.

L'e-mail rimane il percorso più veloce per i criminali informatici per bloccare le attività delle aziende. Phishing, ransomware e compromissione delle e-mail aziendali (BEC) continuano ad aumentare, con il 66% dei responsabili della sicurezza che segnala un aumento degli attacchi BEC nell'ultimo anno (Bitdefender Cybersecurity Assessment Report 2025). I gateway di posta elettronica non sono più in grado di tenere il passo con queste minacce in evoluzione.

Le organizzazioni hanno bisogno di una protezione che vada oltre il filtraggio perimetrale per bloccare le minacce in ogni fase, prima o dopo che raggiungano la posta in arrivo. Devono inoltre semplificare le operazioni, ridurre la proliferazione degli strumenti e proteggere i dipendenti senza rallentarli.

Basato su un'architettura nativa per il cloud e che supporta le API, **GravityZone Extendend Email Security** offre un'implementazione rapida, scalabilità adattiva e visibilità in tempo reale. Progettato per ambienti cloud e ibridi, si implementa in pochi minuti, si sincronizza automaticamente con le caselle di posta degli utenti e fornisce un'interfaccia self-service intuitiva che riduce il carico di lavoro del reparto IT e dà maggiore autonomia ai dipendenti.



Funzionalità principali

Cloud-Native, API-Enabled Architecture (CAPES) - Un'architettura nativa per il cloud progettata per i moderni scenari di minacce. CAPES offre un'implementazione rapida, scalabilità adattiva e visibilità in tempo reale negli ecosistemi di posta elettronica. Combinando la forza di un Secure Email Gateway con la precisione dell'integrazione basata su API, fornisce una protezione continua e guidata dalle policy senza interrompere i flussi di lavoro.

Due livelli di protezione - Un modello di difesa continuo che opera sia a livello di perimetro che di casella di posta. Il filtro pre-consegna blocca i contenuti dannosi prima che raggiungano gli utenti, mentre il monitoraggio post-consegna rileva e neutralizza le minacce che bypassano le difese tradizionali. Dai ransomware ai phishing e BEC, fino a rischi interni, questo approccio a più livelli garantisce la resilienza end-to-end contro gli attacchi in evoluzione.

Flessibilità di implementazione - Le organizzazione possono scegliere SEG, filtri basati su API o entrambi per adattare la sicurezza delle e-mail ad architetture cloud, ibride o complesse. Questa flessibilità garantisce che ogni ambiente riceva il giusto livello di protezione, mentre l'implementazione a doppio livello resta l'opzione più potente per una resilienza completa nella sicurezza per le e-mail.

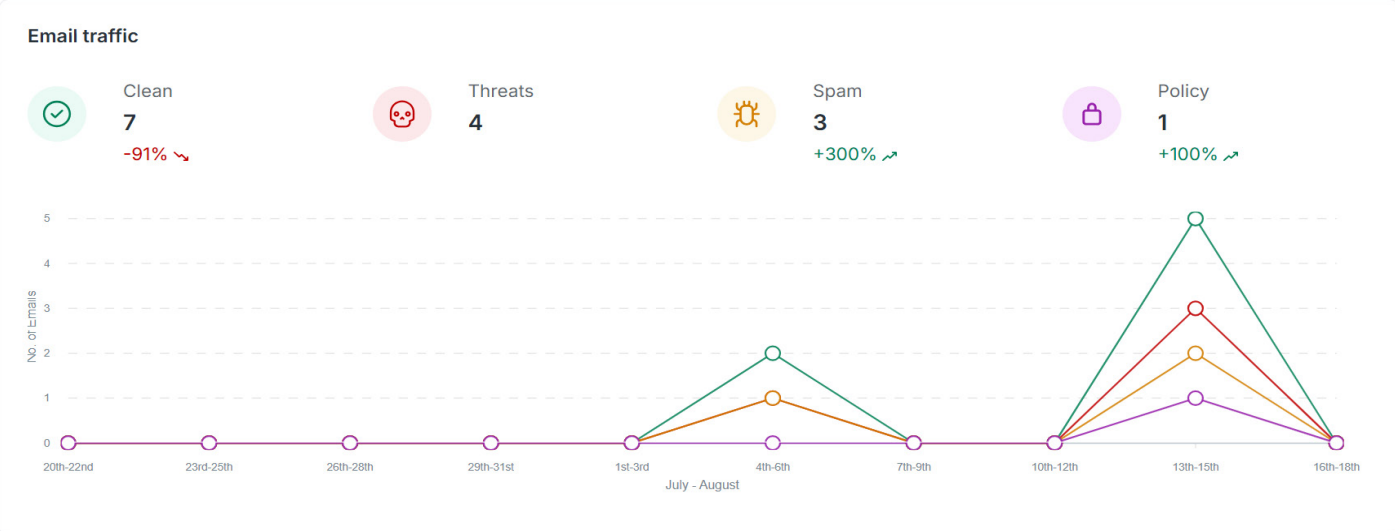
Vantaggio della piattaforma unica - Più che la sicurezza delle e-mail, la piattaforma ti aiuta a consolidare la protezione delle e-mail, la conformità, l'analisi dei rischi e le difese degli endpoint. L'organizzazione ottiene inoltre visibilità e controllo unificati, riducendo al contempo la proliferazione degli strumenti e il costo totale di proprietà.

Un'interfaccia utente moderna e intuitiva – Si tratta di una sicurezza che non rallenta le operazioni. Un'interfaccia self-service e intuitiva semplifica l'implementazione e la gestione giornaliera. Progettata per garantire velocità e scalabilità, offre agli amministratori e agli utenti finali una maggiore autonomia con una formazione minima.

Autenticazione e-mail – Proteggi il tuo dominio e la tua reputazione con l'applicazione di Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) e Domain-based Message Authentication, Reporting & Conformance (DMARC). Questi standard sono essenziali per bloccare lo spoofing e l'impersonificazione, garantire la conformità alle policy e mantenere la fiducia in ogni messaggio inviato dall'organizzazione. Senza di essi, gli aggressori possono facilmente sfruttare il tuo dominio, danneggiare la credibilità e bypassare i filtri tradizionali.

Scansione in uscita e filtro per le graymail - Proteggi il tuo brand all'interno e all'esterno. La scansione in uscita previene le fughe di dati e protegge la reputazione del mittente, mentre il filtro per le graymail mantiene le caselle di posta in arrivo libere da ingombri non necessari.

End-User Quarantine Digest - Responsabilizza gli utenti e facilita il lavoro del reparto IT. Con la gestione della quarantena self-service, i dipendenti possono rilasciare messaggi mentre gli amministratori mantengono una supervisione basata su policy. Questo equilibrio riduce il carico di lavoro per i team di sicurezza e migliora l'esperienza dell'utente finale.



DATASHEET

Bitdefender GravityZone Extended Email Security

Bitdefender

Rafforziamo la sicurezza delle e-mail

Le e-mail restano l'obiettivo principale degli attacchi informatici, ma proteggerle non deve essere complesso. Bitdefender GravityZone Extended Email Security offre gli strumenti, le intelligence e la piattaforma di cui le organizzazioni hanno bisogno per rafforzare le proprie difese contro phishing, ransomware e BEC. Grazie alle difese a due livelli e a un'integrazione perfetta in GravityZone, puoi ottenere una protezione più forte, un'efficienza maggiore e la massima tranquillità.

Che ne dici di semplificare la sicurezza delle e-mail e ottenere una protezione a doppio livello?

Contattaci

Vantaggi principali

- **Riduzione dei rischi e allineamento alla conformità**
  Difenditi da phishing, BEC e altri attacchi trasmessi via e-mail per prevenire perdite finanziare, violazioni dei dati e sanzioni normative. Soddisfa i requisiti di conformità e riduci l'esposizione legale, migliorando la resilienza organizzativa e alleggerendo i team di sicurezza, nonché fornendo interazioni e-mail più sicure per i dipendenti.

- **Continuità aziendale**
  Mantieni le operazioni aziendali operative bloccando i ransomware e le minacce avanzate che interrompono i sistemi o danneggiano i dati sensibili. Aumenta la produttività con il filtro per le graymail e consenti ai dipendenti di rilasciare i messaggi in modo sicuro attraverso la gestione della quarantena self-service.

- **Efficienza operativa per i team di sicurezza**
  Un'interfaccia utente moderna e intuitiva e l'automazione semplificano l'amministrazione, riducono i carichi di lavoro ripetitivi e consentono una risposta più rapida. I team di sicurezza possono concentrarsi sulle attività strategiche, riducendo significativamente il sovraccarico IT.

- **Visibilità unificata**
  L'integrazione completa con la piattaforma di GravityZone riunisce e-mail, endpoint e analisi dei rischi in un unico posto. In questo modo, si eliminano gli strumenti frammentati, si riduce il costo totale di possesso e si offre alla leadership una visione chiara e unificata del livello di sicurezza dell'organizzazione.

Bitdefender è il leader nella cybersecurity che fornisce le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Proteggendo milioni di utenti, aziende ed enti governativi, Bitdefender è uno degli esperti* di riferimento del settore per eliminare le minacce, proteggere la privacy e i dati, e consentire la resilienza informatica. Grazie a importanti investimenti nella ricerca e sviluppo, Bitdefender Labs scopre più di 400 nuove minacce ogni minuto, identificate con oltre 40 miliardi di dati analizzati giornalmente. La società ha introdotto innovazioni rivoluzionarie in vari campi, come anti-malware, sicurezza IoT, analisi comportamentale e intelligenza artificiale. Inoltre, la sua tecnologia viene usata su licenza da oltre 150 brand tecnologici più conosciuti al mondo. Fondata nel 2001, Bitdefender ha clienti in più di 170 paesi con uffici in tutto il mondo.

Sede in Romania
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

Sede negli Stati Uniti
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309

T: +1 954-776-6262

Data di uscita: agosto 2025
Per maggiori informazioni, visitare https://www.bitdefender.com/it-it/.

Tutti i diritti riservati. © 2025 Bitdefender.
Tutti i marchi, i nomi commerciali e i prodotti a cui si fa riferimento nel presente documento appartengono ai rispettivi proprietari.