DATASHEET

Bitdefender

Bitdefender GravityZone Security Data Lake e Data Lake for MDR

Il futuro del SIEM è arrivato

↳ Una piattaforma unificata

GravityZone Security Data Lake estende la piattaforma unificata di Bitdefender combinando funzionalità SIEM e Data Lake in un'unica soluzione fornita nel cloud, consolidando visibilità, analisi e gestione. I team di sicurezza non devono più unire vari strumenti o gestire infrastrutture separate, riducendo così i costi e migliorando velocità e coerenza.

↳ Una visibilità completa

I log provenienti da endpoint, cloud, rete e strumenti di terze parti sono analizzati in uno schema unificato e arricchiti con il contesto di risorse e cartelle, nonché correlati tra le diverse origini. Ciò garantisce che gli analisti (sia tuoi che nostri) possano lavorare con dati puliti e normalizzati, in grado di migliorare l'accuratezza, velocizzare le indagini e ridurre il rumore.

Infrastruttura pronta per l'audit e conformità

Automatizza la raccolta sicura di log, il mantenimento a lungo termine e la reportistica per soddisfare i severi requisiti normativi. Tutti i log vengono mantenuti in modo permanente in un archivio a prova di manomissione, preservando però l'integrità dei dati per anni per supportare le indagini e la prontezza degli audit nel tempo.

Rilevamento e risposta scalabili e guidati da esperti

Offre rilevamento e risposta di livello aziendale senza l'onere della gestione della propria infrastruttura. La piattaforma fornita nel cloud si implementa facilmente ed estende la visibilità MDR e SOC per indagini più approfondite e una risposta più rapida, mentre i SOC globali e i cercatori di minacce di Bitdefender garantiscono un monitoraggio 24/7 e una risposta rapida.

Costi prevedibili e inferiori

Un approccio di mantenimento dei dati a più livelli e una progettazione incentrata sull'archiviazione riducono drasticamente i costi di acquisizione e archiviazione rispetto ai SIEM tradizionali. Di conseguenza, le organizzazioni ottengono strutture di costo prevedibili e trasparenti che si adattano in modo efficiente man mano che i volumi di dati crescono.

Panoramica

Bitdefender GravityZone Security Data Lake ridefinisce il SIEM con un approccio moderno: combina operazioni SIEM, archiviazione scalabile del Data Lake e analisi avanzate in una soluzione fornita nel cloud. Offre alle organizzazioni e agli MSP la sicurezza di agire in modo più rapido e intelligente, con visibilità completa, conformità semplificata e costi inferiori. La soluzione espande anche la potenza di Bitdefender MDR, offrendo agli analisti SOC l'accesso ai dati di telemetria di terze parti per eseguire indagini più approfondite, ottenere un risanamento più rapido e rispondere con sicurezza.

Perché è importante

I SIEM tradizionali sono complessi e costosi. I log si trovano in compartimenti stagni, rendendo difficile per le organizzazioni integrarli e collegarli tra loro. L'acquisizione e l'archiviazione di livello hot nello storage diventano rapidamente costose, mentre i modelli di tipo "archivia e dimentica" rendono le indagini e le verifiche più difficili di quanto dovrebbero essere.

GravityZone Security Data Lake elimina tale complessità, combinando SIEM e Data Lake in un'unica piattaforma moderna e distribuita nel cloud che semplifica le operazioni.

DATASHEET **Bitdefender GravityZone Security Data Lake**

Bitdefender

Bitdefender GravityZone Security Data Lake trasforma i dati di telemetria di sicurezza grezzi in informazioni fruibili in tempo reale che favoriscono un rilevamento, una risposta e una conformità più rapidi.

Ottieni
Inoltra i log da strumenti, app e cloud

Assimila e normalizza
Analizza e organizza secondo uno schema comune per facilitarne la correlazione

Indirizza e archivia
Livelli hot, warm e archive per un mantenimento ottimizzato in termini di costi

Cerca e recupera
La ricerca in tempo reale e il recupero selettivo accelerano le indagini

Rileva e agisci
Dashboard, avvisi e risposte guidate da MDR

Funzionalità principali

↳ Rafforzare Bitdefender MDR
Espande Bitdefender MDR inserendo dati di telemetria di terze parti. Sfruttando sia GravityZone Security Data Lake che GravityZone XDR, i nostri esperti di sicurezza ti aiutano a beneficiare di una visibilità più approfondita e di indagini accurate.

↳ Data Lake scalabile con mantenimento a più livelli
I livelli hot, warm e archive con archiviazione automatica riducono i costi di inserimento e hot storage. Il Data Warehouse supporta l'archiviazione a lungo termine a costi contenuti con richiamo istantaneo per indagini e audit.

↳ Strumenti incentrati sugli analisti
Offre ai team di sicurezza possibilità di ricerca in tempo reale, valutazione delle vulnerabilità e correlazione tra le fonti. Ciò consente indagini rapide e widget basati sulle minacce in tempo reale che visualizzano le campagne e i rischi di attacco, insieme a flussi di lavoro MDR guidati con risultati ricchi di contesto e playbook di risposta per accelerare e semplificare la risposta.

↳ Normalizzazione e importazione dei log unificate
Ottieni e normalizza i dati degli eventi da oltre 100 strumenti di terze parti, tra cui firewall, endpoint, cloud e fonti personalizzate, in uno schema coerente per la correlazione e le analisi.

↳ Analisi avanzata e prioritizzazione basata sui rischi
Migliora l'accuratezza del rilevamento con un punteggio degli avvisi basato sui rischi arricchito dal contesto delle risorse e delle directory su endpoint, server e risorse cloud, e il rilevamento delle anomalie con la correlazione delle campagne per scoprire attacchi sofisticati in modo più precoce ed efficace.

↳ Infrastruttura pronta per l'audit e conformità
Semplifica i requisiti normativi con un Risk & Compliance Hub automatizzato per la gestione, conservazione e la reportistica dei log, il supporto integrato per PCI-DSS, HIPAA, ISO 27001, GDPR e altri, nonché un'archiviazione immutabile a lungo termine che garantisce uno storage a prova di manomissione e un'integrità dei dati pronta per l'audit.

Conclusione

Bitdefender GravityZone Security Data Lake offre chiarezza, velocità e controllo alle moderne operazioni di sicurezza, sostituendo la complessità e il costo dei SIEM tradizionali con una piattaforma unificata e distribuita nel cloud progettata per le esigenze di scalabilità odierne. Grazie alla visibilità approfondita, all'automazione della conformità e alle analisi guidate da esperti, le organizzazioni possono ottenere un rilevamento più veloce, rispondere in modo più intelligente ed essere sempre pronte per gli audit. **Contattaci** subito per programmare una dimostrazione o scoprire come Security Data Lake possa migliorare le tue operazioni di sicurezza.

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: ottobre 2025
Per maggiori informazioni, visitare https://www.bitdefender.com/it-it/