SCHEDA PRODOTTO

Solo per uso web

Bitdefender

Endpoint Detection and Response per MSP.

Rilevamento delle minacce avanzate, indagini mirate e risposta efficace per MSP

www.bitdefender.it

Gli attacchi avanzati odierni stanno diventando sempre più difficili da rilevare. Utilizzando tecniche che individualmente sembrano comportamenti di routine, un aggressore potrebbe accedere alle tue infrastrutture aziendali e restare nascosto per mesi, aumentando sensibilmente il rischio di una costosa violazione dei dati.

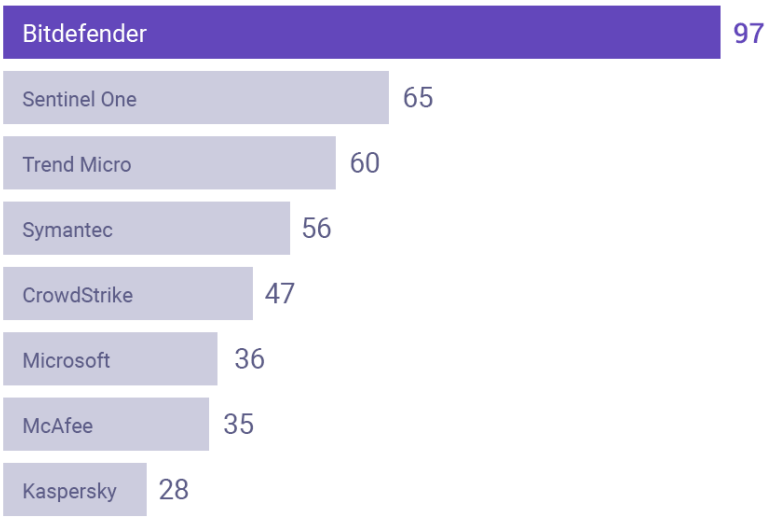
Bitdefender Endpoint Detection and Response monitora costantamente le reti alla ricerca di attività sospette, dandoti gli strumenti per combattere anche gli attacchi più evasivi. La visualizzazione delle minacce di EDR guida le tue indagini e rivela le lacune nella sicurezza, nonché l'impatto degli incidenti, supportando la conformità.

Integrando tecnologie di machine learning e comportamentali perfezionate costantemente dal 2009, Bitdefender EDR offre i rilevamenti più utilizzabili di qualsiasi altro fornitore, come dimostrato nei test MITRE 2020. Gli MSP possono minimizzare il proprio carico operativo con informazioni più contestuali, tecnologie aggiuntive che filtrano i disturbi, incidenti con priorità, indagini guidate e passaggi di risposta.

Benefici Chiave

- Massima efficacia nel rilevamento di attacchi avanzati, dimostrata nei test MITRE.
- Semplice da utilizzare con incidenti distinti per priorità, indagini guidate e ricche informazioni di contesto.
- Visibilità completa della sequenza d'attacco per identificare le lacune di sicurezza e l'impatto delle violazioni, oltre che per supportare la conformità.
- Meno allerte e sovraccarico con opzioni di rafforzamento, prevenzione ed EDR unificate di Bitdefender.
- Correlazione e analisi di eventi a livello aziendale, rilevamento di comportamenti anomali, ricerca di IOC.
- Risposta rapida con capacità di isolare gli endpoint o avviare connessioni shell remote.

Migliori rilevamenti di attacchi contestuali
Per MSP e organizzazioni di medie dimensioni



Somma del numero di avvisi per tecniche di attacco tattiche e rilevamenti generali rispetto ad altri fornitori di sicurezza. Ideale per organizzazioni di medie dimensioni e MSP, alla ricerca di dati pratici. Bitdefender ha anche dimostrato di fornire avvisi per ogni fase della sequenza di attacco nel round di valutazione di APT29 di MITRE ATT&CK 2020: https://attackevals.mitre.org/APT29/results/bitdefender/

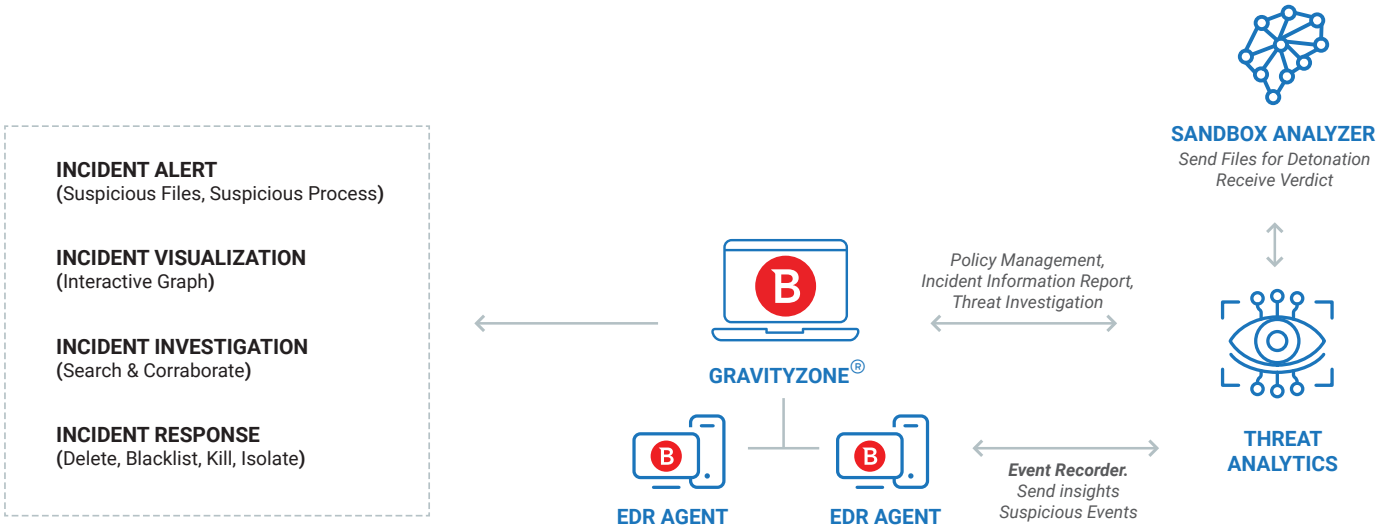
Usa EDR come parte di una suite di sicurezza MSP unificata o accanto a soluzioni AV/EPP di terze parti

Per organizzazioni la cui soluzione di sicurezza per endpoint esistente non fornisce la visibilità sugli attacchi avanzati e la risposta richieste, aggiungere Bitdefender EDR è un modo rapido ed efficace per rinforzare la sicurezza. Si consiglia di passare a EDR con l'AV di nuova generazione e le opzioni di rafforzamento di Bitdefender per bloccare automaticamente la maggior parte delle minacce prima dell'esecuzione, ridurre al minimo i rischi di violazione e semplificare la gestione della sicurezza.

Come funziona:

Bitdefender EDR è una soluzione fornita tramite cloud e basata sulla piattaforma cloud di Bitdefender GravityZone. Gli agenti EDR sono impiegati negli endpoint della tua organizzazione. Ciascun agente EDR ha un registratore di eventi che monitora costantemente l'endpoint e invia in modo sicuro dati di informazioni ed eventi sospetti al cloud di GravityZone.

In GravityZone, il modulo Threat Analytics raccoglie e distingue gli eventi dell'endpoint in un elenco di incidenti con priorità per ulteriori indagini e risposte. Invia i file sospetti per la detonazione nel Sandbox Analyzer e poi utilizza il verdetto del sandbox nei rapporti sull'incidente dell'EDR. È possibile accedere alla dashboard EDR in tempo reale da qualsiasi dispositivo per consentire agli amministratori di verificare le allerte e le visualizzazioni, per poi indagare e rispondere con efficacia alle minacce.



Funzionalità di Bitdefender Endpoint Detection and Response:

Analisi dei rischi

Analisi dei rischi di endpoint e fattore umano
Analizza costantemente i rischi dell'azienda utilizzando centinaia di fattori per identificare, assegnare priorità e fornire indicazioni sulla mitigazione dei rischi per endpoint, rete e utenti.

Rilevamento

Una tecnologia di rilevamento delle minacce leader del settore
Rileva le minacce avanzate, incluso gli attacchi privi di file, i ransomware e altre minacce zero-day in tempo reale. Completa la sicurezza degli endpoint per rafforzare il rilevamento.

Analisi della minaccia
Il raccoglitore di eventi basato su cloud distilla continuamente gli eventi degli endpoint in un elenco di incidenti con priorità per ulteriori indagini e risposte.

Registratore eventi
Monitoraggio continuo degli eventi degli endpoint che porta gli eventi all'analisi delle minacce per creare visualizzazioni delle minacce degli eventi coinvolti in un attacco.

Sandbox Analyzer
Esegue automaticamente payload sospetti in un ambiente virtuale confinato. Successivamente, il modulo di analisi delle minacce utilizza tale analisi per prendere le decisioni inerenti i file sospetti.

Indagine e risposta

Ricerca di IoC
Interroga il database degli eventi per svelare le minacce. Svela le tecniche MITRE ATT&CK e gli indicatori di compromissione. Fornisce le informazioni più recenti sulle minacce denominate e altri malware che potrebbero essere coinvolti.

Visualizzazione
Guide visive semplici da comprendere, arricchite da informazioni sul contesto e le minacce, evidenziano percorsi di attacchi critici, alleviando i carichi per il personale IT. Aiuta a identificare le lacune nella protezione e l'impatto degli incidenti per supportare la conformità.

Detonazione
L'indagine del sandbox avviata dall'operatore ti aiuta a prendere decisioni consapevoli sui file sospetti..

Lista bloccati
Ferma la diffusione di file o processi sospetti rilevati dall'EDR verso le altre macchine..

Blocco dei processi
Interrompe istantaneamente i processi sospetti per fermare potenziali violazioni in tempo reale..

Protezione rete
Blocca le connessioni per e dagli endpoint per fermare il movimento laterale e ulteriori violazioni durante le indagini sugli incidenti..

Shell remota
Esegui comandi remoti su qualsiasi workstation per reagire immediatamente agli incidenti in corso..

Notifica e avvisi

Dashboard e rapporti
Dashboard configurabili e complete capacità di segnalazione istantanee e programmate..

Notifiche
Notifiche e-mail programmate per restare informati.

Integrazione SIEM e supporto API
Supporta l'ulteriore integrazione con strumenti di terze parti.

Prestazioni e gestione

Agente EDR ottimizzato
Basso utilizzo di CPU, RAM e spazio sul disco.

Console web
Una gestione tramite cloud intuitiva.

PERCHÉ BITDEFENDER?

LEADER INDISCUSSO NELL'INNOVAZIONE.
Il 38% di tutti i fornitori di sicurezza informatica al mondo ha integrato almeno una tecnologia Bitdefender. Presente in 150 paesi.

LA MIGLIORE PREVENZIONE ALLE VIOLAZIONI END-TO-END AL MONDO
La prima soluzione di sicurezza che unisce rafforzamento, prevenzione, rilevamento e risposta tra endpoint, rete e cloud.

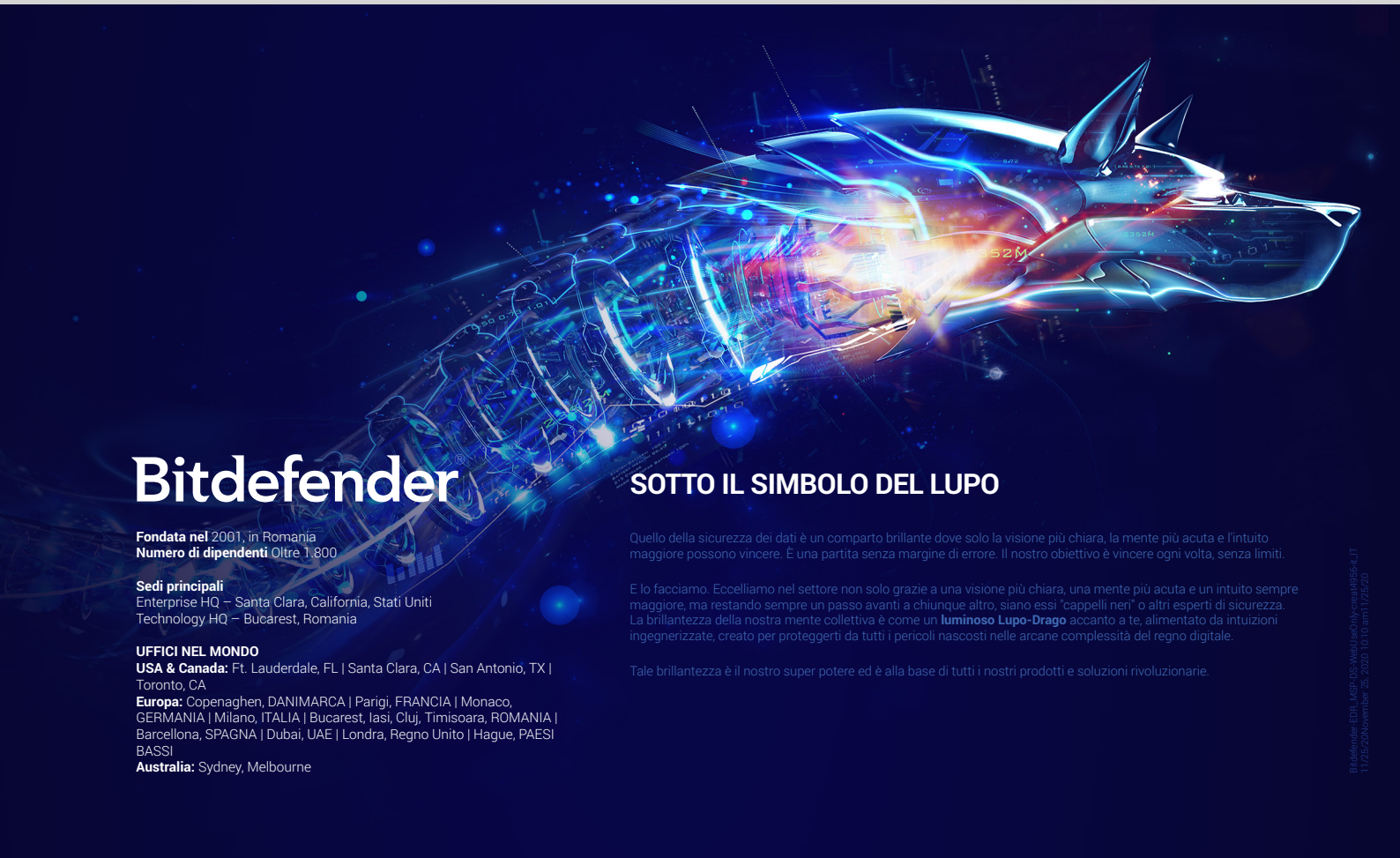
LA MIGLIORE SICUREZZA. PREMIATA SU TUTTA LA LINEA.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER GravityZone Ultra v6.6.7.166 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED



Bitdefender

Fondata nel 2001, in Romania
Numero di dipendenti Oltre 1.800

Sedi principali
Enterprise HQ – Santa Clara, California, Stati Uniti
Technology HQ – Bucarest, Romania

UFFICI NEL MONDO
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europa: Copenaghen, DANIMARCA | Parigi, FRANCIA | Monaco, GERMANIA | Milano, ITALIA | Bucarest, Iasi, Cluj, Timisoara, ROMANIA | Barcellona, SPAGNA | Dubai, UAE | Londra, Regno Unito | Hague, PAESI BASSI
Australia: Sydney, Melbourne

SOTTO IL SIMBOLO DEL LUPO

Quello della sicurezza dei dati è un comparto brillante dove solo la visione più chiara, la mente più acuta e l'intuito maggiore possono vincere. È una partita senza margine di errore. Il nostro obiettivo è vincere ogni volta, senza limiti.

E lo facciamo. Eccelliamo nel settore non solo grazie a una visione più chiara, una mente più acuta e un intuito sempre maggiore, ma restando sempre un passo avanti a chiunque altro, siano essi "cappelli neri" o altri esperti di sicurezza. La brillantezza della nostra mente collettiva è come un **luminoso Lupo-Drago** accanto a te, alimentato da intuizioni ingegnerizzate, creato per proteggerti da tutti i pericoli nascosti nelle arcane complessità del regno digitale.

Tale brillantezza è il nostro super potere ed è alla base di tutti i nostri prodotti e soluzioni rivoluzionarie.

Bitdefender-EDR_MSP-DS-WebUseOnly-creat4956-it_IT
11/25/20November 25, 2020 10:10 am11/25/20