SCHEDA PRODOTTO

Solo per uso web

Bitdefender

Endpoint Detection and Response

Rilevamento delle minacce avanzate, indagini mirate e risposta efficace

www.bitdefender.it

Le attuali sfide delle minacce avanzate che devi affrontare

I criminali informatici stanno diventando sempre più sofisticati e gli attuali attacchi avanzati sono sempre più difficili da rilevare. Utilizzando tecniche che individualmente sembrano comportamenti di routine, un aggressore potrebbe accedere alla tua infrastruttura e restare nascosto per mesi, aumentando sensibilmente il rischio di una costosa violazione dei dati.

In che modo Bitdefender Endpoint Detection and Response (EDR) può aiutarti?

Quando la tua soluzione di sicurezza per endpoint non garantisce la visibilità sugli attacchi avanzati e la risposta richiesta, aggiungere l'intuitivo Bitdefender Endpoint Detection and Response (EDR) può rafforzare rapidamente ed efficacemente le tue operazioni di sicurezza.

Rilevamento e risposta agli attacchi avanzati

Bitdefender EDR monitora la tua rete per svelare attività sospette in anticipo e fornirti gli strumenti per consentirti di affrontare gli attacchi informatici.

- EDR integra le pluripremiate funzionalità di machine learning, scansione cloud e sandbox analyzer di Bitdefender per rilevare tutte le attività che eludono i tradizionali meccanismi di prevenzione degli endpoint.
- Visibilità totale su tecniche, tattiche e procedure (TTP) utilizzate per attaccare i tuoi sistemi.
- Funzionalità di ricerca complete per determinati indicatori di compromissione (IoC), tecniche MITRE ATT&CK e altri artefatti per scoprire gli attacchi nella fase iniziale. Nella valutazione MITRE ATT&CK dell'aprile 2020, Bitdefender eccelleva nelle rilevazioni e nelle allerte utilizzabili in ogni fase dell'intera procedura di attacco.
- Intraprendi azioni di risposta per chiudere eventuali vulnerabilità ed eliminare il rischio di attacchi ricorrenti.

Colmare i divari di competenze in materia di sicurezza informatica

- I flussi di lavoro di risposta integrati e facili da seguire consentono al tuo team di rispondere in modo efficace, limitare la diffusione laterale e fermare gli attacchi in corso.
- La visualizzazione delle minacce focalizza le tue indagini, aiutandoti a comprendere rilevamenti complessi, identificare la causa principale degli attacchi e massimizzare la tua capacità di rispondere direttamente.
- Assegnazione automatica delle priorità alle allerte con funzionalità di risoluzione con un clic.

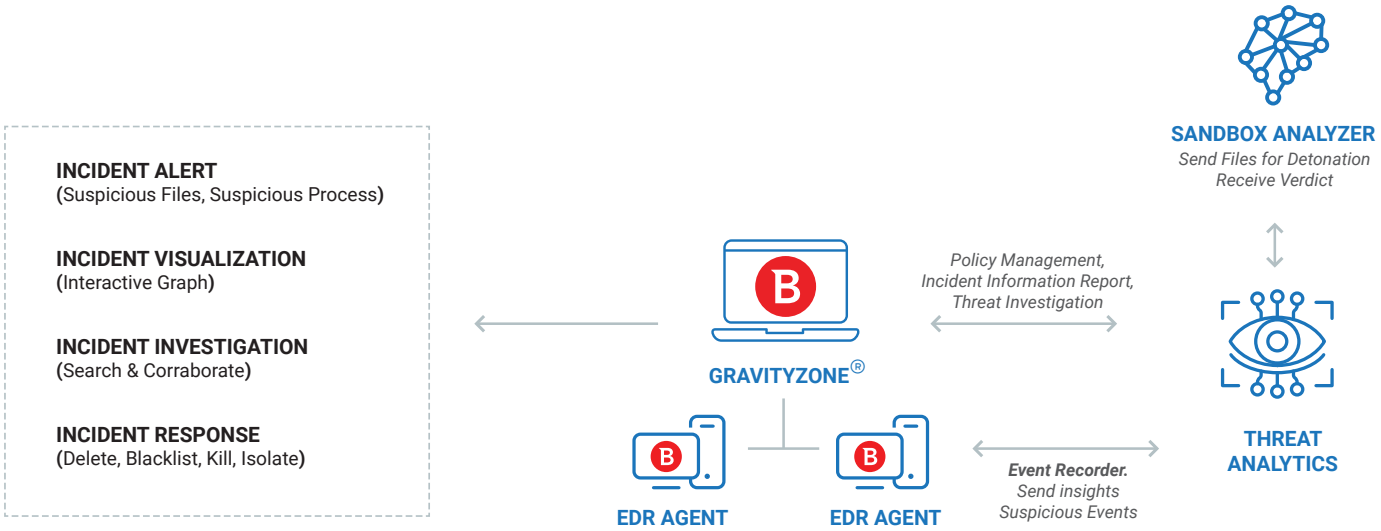
Ridurre i rischi dell'organizzazione

- EDR analizza costantemente la tua organizzazione utilizzando le sue capacità uniche per identificare i rischi attraverso centinaia di fattori. Fornisce una chiara guida per aiutarti ad attenuare i rischi derivanti da sistema operativo, rete e utenti.

Minimizzare il carico operativo

- Fornito dal cloud e con scarsa manutenzione, EDR è facile da impiegare nella tua architettura di sicurezza esistente e pienamente compatibile con la tua soluzione antivirus per endpoint.
- L'agente leggero ha un carico minimo sulle risorse relative a spazio su disco, banda e CPU.
- Flessibile, scalabile e aggiornabile alla completa piattaforma di protezione degli endpoint di Bitdefender e al rilevamento e risposta gestiti (MDR).

Come funziona



A monte: Bitdefender Endpoint Detection and Response

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 informazioni ed eventi sospetti al cloud di GravityZone.

In GravityZone, il modulo Threat Analytics raccoglie e distilla 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 in tempo reale le minacce avanzate, incluso gli attacchi privi di file, i ransomware e altre minacce zero-day. Integra la tua soluzione di sicurezza per endpoint esistente rinforzando 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 informazioni aggiornate al minuto 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
Dashboard configurabile e notifiche e-mail.

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 davvero 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.

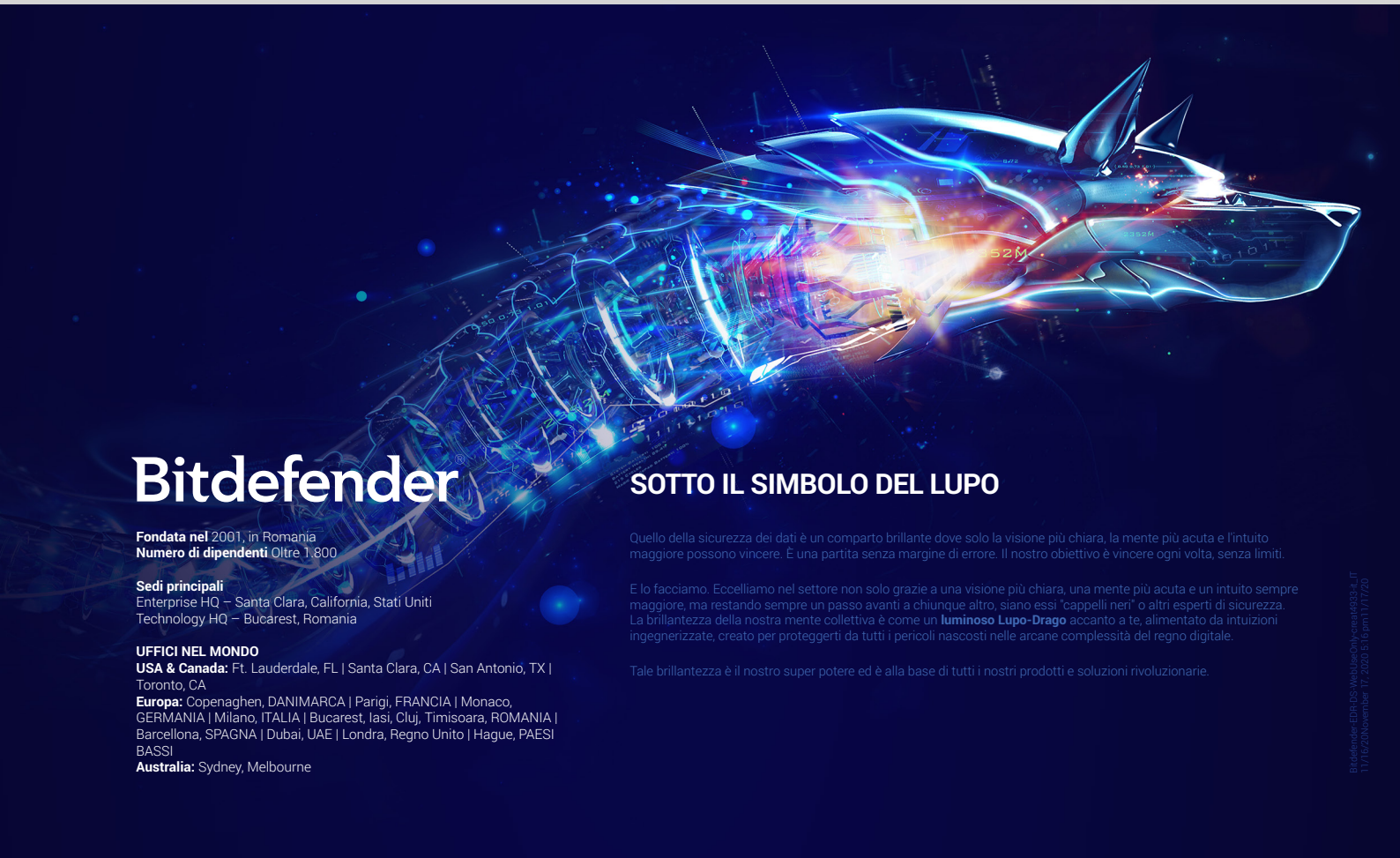
LA MIGLIORE SICUREZZA. PREMIATA SU TUTTA LA LINEA.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER ADVANCED ENDPOINT PROTECTION NSS Labs 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-DS-WebUseOnly-creat4933-4_IT
1/16/20November 17, 2020 5:16:pm11/17/20