

Bitdefender presenta la nuova evoluzione delle soluzioni di rilevamento e risposta per endpoint: eXtended EDR (XEDR)

L'analisi e la correlazione delle minacce rilevate attraverso gli endpoint e le reti in ambienti ibridi migliora l'efficacia della sicurezza contro i cyberattacchi

BUCHAREST, Romania e SANTA CLARA, California — 13 luglio 2021 — Bitdefender, leader mondiale nella sicurezza informatica, ha presentato oggi **eXtended EDR (XEDR)** l'evoluzione delle soluzioni di Rilevamento e Risposta degli Endpoint che aggiunge funzionalità di analisi e correlazione degli eventi di sicurezza tra gli endpoint alla piattaforma [Bitdefender Endpoint Detection and Response \(EDR\)](#) e [GravityZone Ultra](#), la piattaforma di prevenzione, rilevamento e risposta degli endpoint e analisi dei rischi. Queste nuove funzionalità aumentano l'efficacia della sicurezza per identificare e bloccare la diffusione di attacchi ransomware, minacce avanzate persistenti (APT) e altri attacchi sofisticati prima che abbiano un impatto sull'operatività aziendale.

Con il rilevamento e la risposta integrati su sistemi operativi (Windows, Linux, Mac) e ambienti ibridi (cloud pubblico e privato, on premise), Bitdefender offre una visione completa e in tempo reale delle operazioni di sicurezza, migliorando notevolmente la capacità delle aziende di tutte le dimensioni, comprese quelle che non dispongono di analisti di sicurezza a tempo pieno, di rilevare attacchi nascosti che altrimenti passerebbero inosservati con l'analisi e il rilevamento su singoli endpoint.

Gli attacchi sofisticati progettati per eludere il rilevamento da parte delle tecnologie di sicurezza spesso imitano processi "normali" o vengono eseguiti in più fasi attraverso diversi vettori, tra cui endpoint, reti, supply chain, servizi IT in hosting e servizi cloud. Bitdefender XEDR contrasta gli attacchi complessi acquisendo, esaminando e correlando la telemetria degli endpoint per individuare indicatori di compromissione (IOC), tecniche APT, presenza di malware, vulnerabilità e comportamenti anomali. Questo monitoraggio avanzato automatizza il rilevamento precoce degli scenari di attacco, fornendo ai team IT e della sicurezza un'unica dashboard ovunque sia iniziato l'attacco.

Le nuove funzionalità XEDR migliorano anche il [rilevamento e la risposta gestita \(MDR\)](#) di Bitdefender, fornendo maggiore visibilità e informazioni di contesto relative agli incidenti durante le indagini. Tutto ciò consente di accelerare la convalida delle minacce, le azioni di risposta e neutralizzazione necessarie.

“Le aziende di tutte le dimensioni e di tutti i settori sono nel mirino delle APT e di gruppi di criminali informatici esperti”, ha dichiarato Steve Kelley, presidente e direttore generale di Bitdefender Business Solutions Group. “Ogni applicazione, email, vulnerabilità senza patch, relazione con i partner o con servizi di terze parti rappresenta un potenziale punto di ingresso per un attacco di sicurezza informatica con conseguenze catastrofiche. Poiché i criminali informatici evolvono le loro tecniche per aggirare le difese e muoversi negli ambienti senza essere individuati, la correlazione degli eventi oltre i confini di un singolo endpoint è fondamentale per la resilienza informatica. Bitdefender XEDR fornisce una correlazione tra i diversi endpoint per individuare ed eliminare più velocemente le minacce in ogni fase di un attacco, dalla ricognizione iniziale al payload finale”.

In un recente rapporto¹, l'analista di Forrester Allie Mellen scrive che "i fornitori di soluzioni XDR saranno limitati o abilitati dall'EDR su cui si basano. Scegliete il vostro XDR basato su un EDR con rilevamenti ad alta efficacia, solide partnership con terze parti o capacità native estese, e raccomandazioni per la risposta automatica".

XEDR si basa sulle soluzioni EDR leader del settore dell'azienda e sull'intelligence avanzata contro le minacce fornita da [Bitdefender Global Protective Network](#) (GPN), che include centinaia di milioni di sensori che raccolgono continuamente dati sulle minacce per gli endpoint in tutto il mondo. Nelle valutazioni indipendenti, Bitdefender ha sempre ottenuto il punteggio più alto nel rilevamento di tattiche e tecniche APT. Nel più recente [test MITRE ATT&CK](#), Bitdefender ha ottenuto il più alto numero di rilevamenti tra i 29 vendor di sicurezza informatica presi in esame.

XEDR con funzionalità di correlazione di eventi su più endpoint è attualmente disponibile ed incluso nei servizi Bitdefender EDR, GravityZone Ultra e MDR. I clienti interessati possono partecipare all'Early Access Program attualmente in corso.

¹ Forrester Research, Allie Mellen, "Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR" April 28, 2021

A proposito di Bitdefender

Bitdefender, leader riconosciuto nel settore della cybersecurity, offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Responsabile della protezione di milioni di sistemi in ambienti consumer, business e governativi, Bitdefender è l'esperto più affidabile del settore* per eliminare le minacce, proteggere la privacy e i dati per favorire la resilienza informatica. Grazie agli investimenti in ricerca e sviluppo, Bitdefender Labs rileva 400 nuove minacce ogni minuto con 30 miliardi di query giornaliere. L'azienda ha rilasciato innovazioni rivoluzionarie in materia di antimalware, IoT, analisi comportamentale e intelligenza artificiale e la sua tecnologia viene concessa in licenza a oltre 150 brand di cybersecurity, i più conosciuti al mondo. Fondata nel 2001, Bitdefender vanta clienti in 170 paesi e ha uffici in tutto il mondo. Per maggiori informazioni <https://www.bitdefender.it>.

*Bitdefender si è classificata al primo posto nel 54% di tutti i test di AV-Comparatives 2018-2021 per protezione del mondo reale, prestazioni, protezione dai malware & protezione dalle minacce avanzate.

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it