

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)

Una Dynamic Attack Surface Reduction (DASR) rivoluzionaria

Gli attacchi moderni sono più veloci e sfruttano strumenti e azioni legittime per eludere il rilevamento, disattivando persino le piattaforme EDR.

Bitdefender GravityZone PHASR è una soluzione rivoluzionaria di Dynamic Attack Surface Reduction che blocca in modo proattivo i percorsi degli attacchi ransomware e potenzia qualsiasi soluzione EDR limitando fino al 95% gli strumenti e le azioni rischiose atipiche.

A differenza della sicurezza convenzionale, **GravityZone PHASR** usa modelli IA di autoapprendimento per apprendere continuamente il comportamento degli utenti e correlarlo con i vettori di minaccia, così da identificare e applicare automaticamente un hardening approfondito, senza richiedere eccezioni e regole statiche, o influire sulla produttività.

Le tecniche [Living off the Land](#), in cui gli aggressori sfruttano strumenti nativi del SO, sono ormai utilizzate nell'84% dei principali attacchi e praticamente in ogni violazione e attacco ransomware riuscito. Riduci drasticamente la superficie di attacco dei dipendenti e blocca gli attacchi stessi prima che si intensifichino:

↳ Blocca i ransomware in modo proattivo

La riduzione dinamica della superficie d'attacco di PHASR apprende continuamente il comportamento utente-macchina e limita in modo proattivo le azioni insolite prima che gli attacchi possano disattivare l'EDR.

↳ Riduci i rischi senza problemi

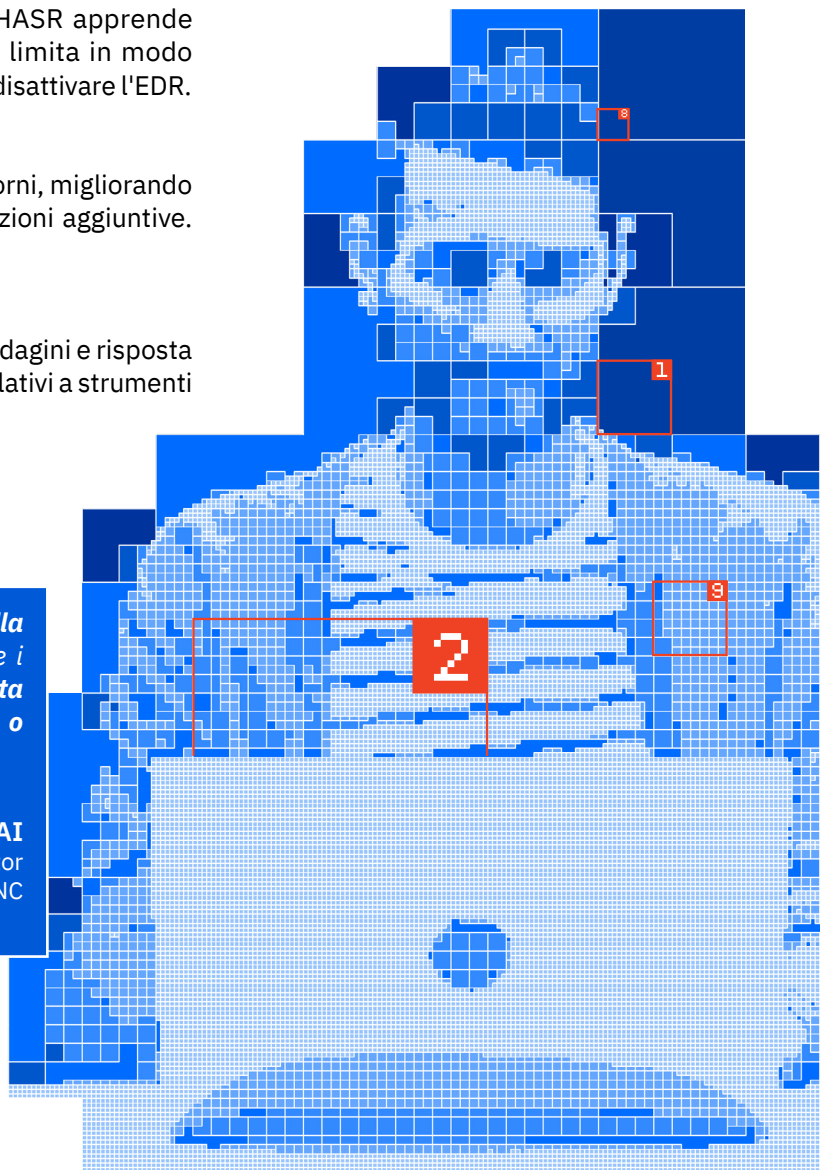
PHASR può ridurre i rischi inutili del 30% o di più in 30 giorni, migliorando il tuo attuale stack di sicurezza. Senza costi o complicazioni aggiuntive. Nessun impatto sulla produttività.

↳ Aumenta l'efficienza della sicurezza

PHASR rafforza l'efficienza e riduce i carichi di lavoro di indagini e risposta alle minacce fino al 50%, eliminando gli avvisi rumorosi relativi a strumenti legittimi.

*“Abbiamo ottenuto una riduzione di quasi il **70% della superficie di attacco** bloccando gli strumenti remoti e i binari living-off-the-land. Siamo passati **dalla scoperta al blocco dei LOLBins in settimane, senza indagini o interruzioni.**”*

JASON KRAAI
Systems Administrator
Greenman-Pedersen, INC



Capacità principali di Bitdefender GravityZone PHASR:

↳ Hardening su misura

PHASR utilizza modelli IA per identificare gli schemi di comportamento degli utenti e le configurazioni di hardening ottimali, limitando gli strumenti atipici per l'utente.

↳ Dynamic Attack Surface Reduction (DASR)

PHASR si adatta continuamente e autonomamente ai cambiamenti nel comportamento degli utenti e ai nuovi vettori di minaccia utilizzando l'intelligence sulle minacce in tempo reale e minimizzando lo sforzo amministrativo.

↳ Implementazione autonoma

La Dynamic Attack Surface Reduction (DASR) di PHASR chiude in modo proattivo i percorsi di attacco, potenziando sia Bitdefender GravityZone che le soluzioni EDR/XDR per fermare le minacce prima che si intensifichino.

↳ Controllo e precisione

PHASR consente alcune restrizioni sulle app inutilizzate ma rischiose, ma anche precise limitazioni a livello di azioni all'interno delle app utilizzate, bloccando solo i comportamenti atipici.

↳ Smart Clustering

PHASR raggruppa gli utenti con comportamenti simili per consentire un'applicazione efficiente della riduzione della superficie d'attacco in tutta l'organizzazione.

↳ Mitigazione dei rischi autonoma

La modalità Autopilot di PHASR consente modifiche adattabili e autonome alla superficie d'attacco senza alcun intervento, mentre la modalità Direct Control offre suggerimenti e richiede decisioni amministrative.

↳ Rafforza GravityZone o gli strumenti EPP/EDR di terze parti

PHASR offre un percorso verso una solida esposizione e gestione della conformità, sia per il potenziamento degli strumenti EPP-EDR di terze parti, sia per la riduzione della complessità e del rischio come parte della piattaforma GravityZone XDR.

*"Bitdefender ha costantemente ottenuto buoni risultati nei test indipendenti, tra cui MITRE Engenuity, oltre ad aver introdotto funzionalità innovative come Deep Process Inspector and Advanced Reasoning. **Più di recente, nel 2024, Bitdefender Proactive Hardening and Attack Surface Reduction (PHASR), una tecnologia rivoluzionaria che trasforma il modo in cui la difesa in profondità della sicurezza viene applicata e gestita in tutte le aziende.**"*

IDC, IDC ProductScape: Worldwide Small and Medium-Sized Business Endpoint Protection Market, 2024-2025: Technology Supplier Solution Functionality, doc #US52830124, gennaio 2025



Scopri come PHASR può proteggerti in modo proattivo dai nuovi attacchi furtivi:

[Scopri PHASR e richiedi una demo.](#)

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, l'identità digitale e i dati, e consentire la resilienza informatica. Grazie ai suoi investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida circa miliardi di query sulle minacce ogni giorno. La società ha introdotto innovazioni pionieristiche in molti ambiti, come antimalware, sicurezza IoT, analisi comportamentale e intelligenza artificiale, e la sua tecnologia è usata su licenza da oltre 200 dei marchi tecnologici più noti al mondo. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo.

Data di uscita: novembre 2025

Per maggiori informazioni, visitare <https://www.bitdefender.com>.

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.

Sede centrale -
Romania

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

T: +40 21 4412452

Sede centrale - Stati
Uniti

111 W. Houston
Street, Suite 2105,
Frost Tower Building
San Antonio, Texas
78205, USA