Bitdefender

Scheda tecnica

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)

Hardening rivoluzionario, personalizzato e dinamico

I criminali informatici operano in un nuovo modo: sfruttano le credenziali rubate, si infiltrano nelle normali attività utilizzando tool legittimi in attacchi Living off the Land (LOTL) e successivamente riutilizzano i propri playbook tra vittime ed endpoint.

Dato che il comportamento di ogni utente è unico e le regole di controllo delle applicazioni e di riduzione della superficie d'attacco sono statiche e progettate per adattarsi a tutti, in genere offrono un hardening limitato, sono troppo restrittive e soprattutto sono ingestibili per i normali team IT.

GravityZone PHASR è una soluzione rivoluzionaria che blocca gli attacchiLiving off the Land senza ostacolare la produttività o i team IT.

Attualmente, le tecniche Living off the Land sono usate nel 70% degli attacchi. Riduci drasticamente la superficie d'attacco dei dipendenti e blocca gli attacchi furtivi prima che causino danni:

- **Aumenta l'hardening** – PHASR offre un hardening approfondito e personalizzato apprendendo il comportamento degli utenti e limitando in modo sicuro gli strumenti non necessari ma rischiosi per determinati utenti.
- **Blocca gli attacchi LotL in anticipo** – Limitando l'accesso a strumenti come PowerShell o WMI, gli aggressori non sono in grado di avanzare e integrarsi nelle normali attività.
- **Neutralizza il riutilizzo dei playbook** – Dato che PHASR consente alla sicurezza di ogni endpoint di comportarsi in modo diverso, gli aggressori non possono riutilizzare un modello su più sistemi.

Bitdefender

Capacità principali di Bitdefender GravityZone PHASR:

- **Hardening su misura** – PHASR offre un hardening approfondito e personalizzato apprendendo il comportamento degli utenti e limitando in modo sicuro gli strumenti non necessari ma rischiosi per determinati utenti.

- **Riduzione dinamica della superficie d'attacco** – PHASR si adatta continuamente e autonomamente ai cambiamenti del comportamento degli utenti e ai nuovi vettori di minaccia, minimizzando lo sforzo amministrativo.

- **Controllo preciso** – 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.

- **Una protezione basata sull'intelligence** – PHASR integra la threat intelligence di Bitdefender, garantendo che l'efficienza costante dell'hardening contro i vettori di minaccia più recenti.

- **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.

- **Gestione di sicurezza e rischi unificata** – PHASR si integra perfettamente nelle architetture esistenti come parte della piattaforma GravityZone XDR che fornisce visibilità, definizione delle priorità e mitigazione dei rischi a 360°, nonché prevenzione, protezione, rilevamento e risposta alle minacce.

IDC

"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:
Contattaci e richiedi una demo