DATASHEET

Bitdefender

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)

Fermez la porte aux attaques qui abusent de vos outils. Plus de prévention. Moins de réactions.

Aujourd'hui, 84 % des attaques utilisent des outils légitimes, tels que PowerShell, WMIC ou Netsh pour se déplacer latéralement et atteindre leurs objectifs. La détection et la réponse ne peuvent pas suivre le rythme des cybercriminels qui se dissimulent derrière des services publics de confiance et qui ont recours à l'IA pour accélérer et étendre leurs opérations.

GravityZone PHASR offre un durcissement dynamique qui bloque les attaques en amont en fermant les chemins d'attaque. Il apprend comment chaque utilisateur travaille et restreint automatiquement les accès inutiles aux outils et aux actions à risque, réduisant ainsi les risques sans ralentir les utilisateurs, sans alourdir la gestion des règles, ni remplacer votre solution EPP/EDR.

Comment la sécurité de PHASR axée sur la prévention renforce-t-elle vos défenses :

Prévenez les attaques par ransomware et les fuites de données

PHASR ferme automatiquement les voies empruntées par les attaques modernes pour le mouvement latéral, l'escalade des privilèges et l'exfiltration des données.

Réduisez votre surface d'attaque de 95 %

Le durcissement automatisé et piloté par l'IA réduit considérablement les surfaces d'attaque et permet une réduction rapide et quantifiable des risques.

Améliorez l'efficacité de votre sécurité de 50 %

En limitant de manière proactive les outils, les actions et les privilèges inutiles, PHASR réduit le nombre d'alertes et la charge de travail liée aux enquêtes.

RÉSULTATS PROUVÉS CHEZ NOS CLIENTS :

BDR Group

- 7 Ransomware attacks stopped
- 80% attack surface reduction

"As soon as we put it on a client site, it was like shining a torch into a previously dark corner. Suddenly everything was visible."

OWEN WHITLOCK
CTO

Greenman Pedersen

- 70% attack surface reduction
- No disruption
- 0 incidents

"Knowing PHASR blocks unauthorized tools and shadow IT means I don't have to worry about those risks anymore."

JASON KRAAI
Systems Administrator

SecureMe

- 60% attack surface reduction
- 30-40% faster detection and response
- 20-30% operational cost savings

"With PHASR, prevention happens early, quietly, and accurately. It reduces attack surface by ~60%, cuts down alert noise, and gives me confidence that my customers are protected without impacting their productivity."

WALTER RUSSO
Founder

Technology By Design

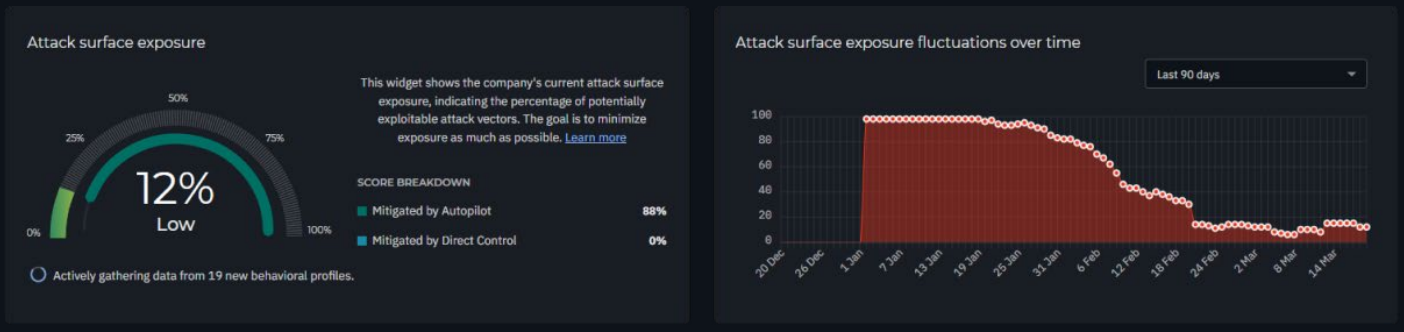
- 90% fewer alerts for high-incident clients
- 20-40 hours saved - monthly remediation

"We needed a solution that would help us prevent more threats and spend less time responding to incidents. Our previous tools simply weren't stopping enough activity before it became a problem."

BRANKO GRUJIC
Lead Security Engineer

DATASHEET

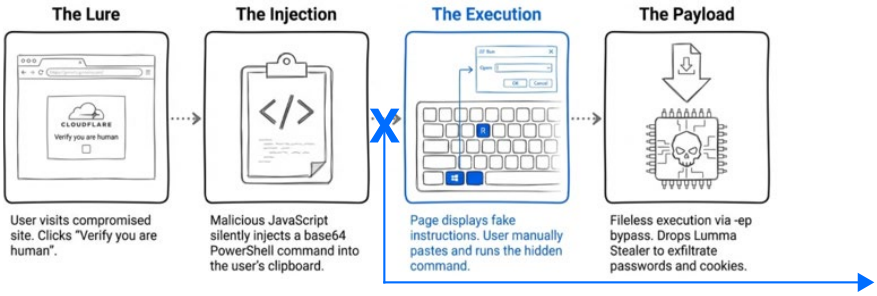
Bitdefender



Exposition de la surface d'attaque du client après l'utilisation de PHASR en mode Autopilot

Comment fonctionne PHASR et en quoi se distingue-t-il

- PHASR est une solution de réduction dynamique de la surface d'attaque (DASR) qui utilise des modèles d'IA personnalisés pour adapter en permanence le durcissement au comportement des endpoints des utilisateurs et aux menaces.
- Contrairement aux outils conventionnels, qui sont statiques et génériques, PHASR adapte le durcissement au comportement spécifique de chaque utilisateur, applique des restrictions de manière autonome sans causer de perturbations et permet de bloquer avec précision les actions à risque au sein des applications autorisées.
- PHASR a été reconnu comme une innovation distinctive par les principaux analystes et a démontré sa capacité à réduire les risques de manière autonome sans impacter la productivité.
- Catégories d'outils surveillés : les attaques Living off the Land, les outils d'administration à distance, les outils de piratage, les cryptomineurs et les outils de falsification.
- Couverture : PHASR réduit l'exposition aux risques sous Windows, macOs, Linux. Ses fonctionnalités de sécurité préventive complètent les solutions EDR et MDR de GravityZone ou la sécurité des endpoints d'un tiers.



Comment PHASR déjoue les attaques

Les attaques de type ClickFix sont répandues : 47 % des attaques observées (2025 Microsoft Digital Defense Report).

PHASR empêche l'exécution de PowerShell, perturbant ainsi l'attaque et empêchant l'exfiltration.

Découvrez comment PHASR peut vous protéger de manière proactive contre de nouvelles attaques furtives : **Découvrez PHASR et demandez une démonstration.**

Identifiez votre exposition au risque avant que les attaquants ne s'en servent.
[Obtenez une évaluation gratuite de votre surface d'attaque interne.]

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T : +40 21 4412452

France HQ
49 rue de la Vanne,
92120 Montrouge
T : +33 1 47 35 72 73