DATASHEET

Bitdefender

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)

Cierre la puerta a los ataques que se aprovechan de sus propias herramientas. Prevenga más y responda menos.

Actualmente, el 84 % de los ataques se aprovecha de herramientas legítimas como PowerShell, WMIC o Netsh para moverse lateralmente y alcanzar sus objetivos. La detección y la respuesta no pueden seguirles el ritmo a los responsables de las amenazas que se ocultan tras utilidades de confianza y usan la IA para acelerar y escalar sus actividades.

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR) ofrece un endurecimiento dinámico que detiene los ataques desde el principio cerrando las rutas de ataque. Aprende cómo trabaja cada usuario y restringe automáticamente el acceso a herramientas innecesarias y otras acciones peligrosas, lo que reduce la exposición sin ralentizar a los usuarios, sin complicar las políticas y sin sustituir su EPP/EDR.

La seguridad preventiva de PHASR refuerza sus defensas de la siguiente manera:

Previene el ransomware y las filtraciones de datos

PHASR cierra automáticamente las rutas que emplean los ataques modernos para el movimiento lateral, la elevación de privilegios y la filtración de datos.

Reduce hasta un 95 % su superficie de ataque

El hardening automatizado e impulsado por IA de PHASR disminuye drásticamente la superficie de ataque y ofrece una reducción rápida y cuantificable de los riesgos.

Aumenta hasta un 50 % la eficiencia de la seguridad

Al restringir proactivamente herramientas, acciones y privilegios innecesarios, PHASR reduce el ruido de las alertas y la carga que conlleva la investigación de incidentes.

EFICACIA PROBADA EN CLIENTES Y MSP:

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

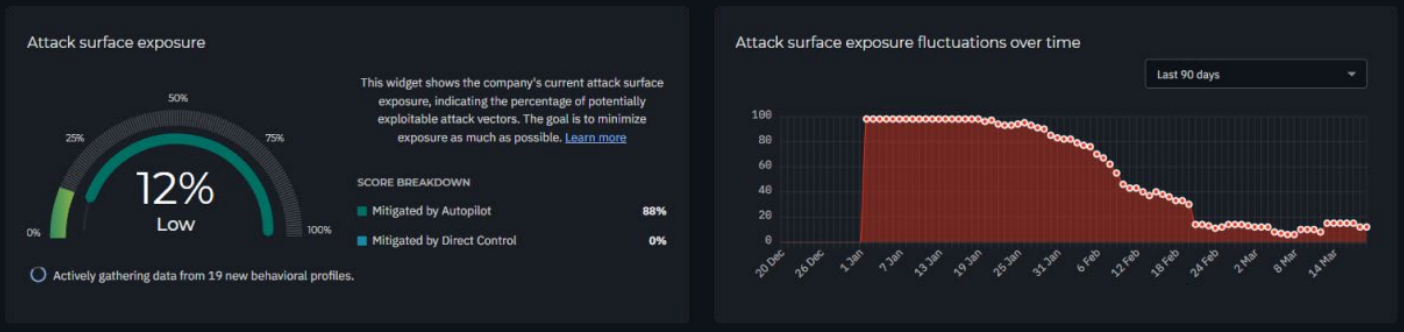
- **90% fewer alerts** for high-incident clients
- **20-40 hours saved** - monthly remediation

"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

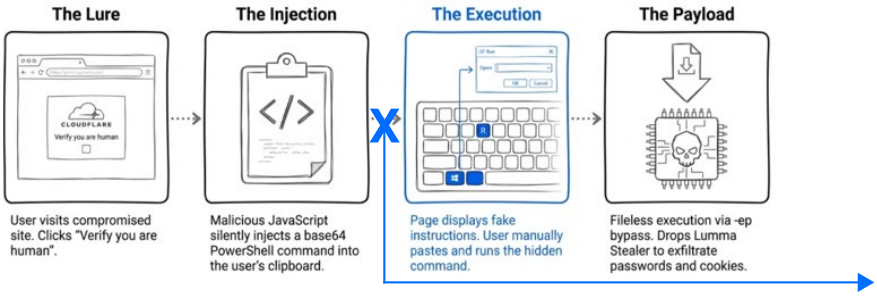
Bitdefender



Exposición a la superficie de ataque del cliente tras usar PHASR en modo Autopilot

Cómo funciona PHASR y qué lo hace diferente

- PHASR es una solución de Dynamic Attack Surface Reduction (DASR) que emplea modelos de IA individualizados para adaptar continuamente el hardening al comportamiento usuario-endpoint y a las amenazas.
- A diferencia de las herramientas convencionales basadas en listas de permitidos, que son estáticas y genéricas, PHASR personaliza el hardening,
  aplica restricciones de forma autónoma sin interrupciones y permite bloquear con precisión actividades de riesgo dentro de aplicaciones permitidas.
- Los principales analistas han elogiado a PHASR por constituir una innovación diferenciada que ha demostrado reducir autónomamente el riesgo sin afectar a la productividad.
- Categorías de herramientas monitorizadas: binarios living-off-the-land, herramientas de administración remota, herramientas de piratería, software de minería de criptomonedas y herramientas de manipulación.
- Cobertura: PHASR reduce la exposición al riesgo en Windows, macOS y Linux. Sus capacidades para la seguridad preventiva complementan GravityZone EDR y MDR o soluciones de endpoint de terceros.



Cómo derrota PHASR los ataques

Los ataques ClickFix son extremadamente habituales:
el 47 % de todos los ataques observados, según el Microsoft Digital Defense Report 2025.

PHASR impide la ejecución de PowerShell, interrumpe el ataque y evita la filtración de datos.

Descubra cómo PHASR puede protegerle proactivamente contra nuevos ataques sigilosos:
Descubra PHASR y solicite una demostración.

Descubra su exposición al riesgo antes de que los atacantes se aprovechen.
[Obtenga una evaluación gratuita de la superficie de ataque interna.]

Bitdefender es líder mundial en seguridad informática y ofrece las mejores soluciones de prevención, detección y respuesta ante amenazas en todo el mundo. Bitdefender, que vela por millones de entornos domésticos, empresariales y gubernamentales, es uno de los expertos más confiables en el sector para eliminar amenazas, proteger la privacidad, la identidad digital y los datos, y facilitar la resiliencia informática. Gracias a sus grandes inversiones en investigación y desarrollo, los laboratorios de Bitdefender descubren más de 400 nuevas amenazas por minuto y procesan diariamente 40 000 millones de consultas sobre amenazas. La empresa ha sido pionera en innovaciones revolucionarias en el campo de la seguridad de IoT, antimalware, análisis del comportamiento e inteligencia artificial (AI), y más de 150 de las marcas tecnológicas más reconocidas del mundo licencian su tecnología. Fundada en 2001, Bitdefender tiene clientes en más de 170 países con oficinas por todo el mundo.
Para obtener más información, visite https://www.bitdefender.com/es-es/.

Romania HQ
Orhideea Towers
Calle Orhideelor 15A,
Distrito 6,
Bucarest 060071

T: +40 21 4412452

Spain HQ
75-77 Calle Sants,
Principal 2ª, 08014
Barcelona