



PREVENT MORE. RESPOND LESS.

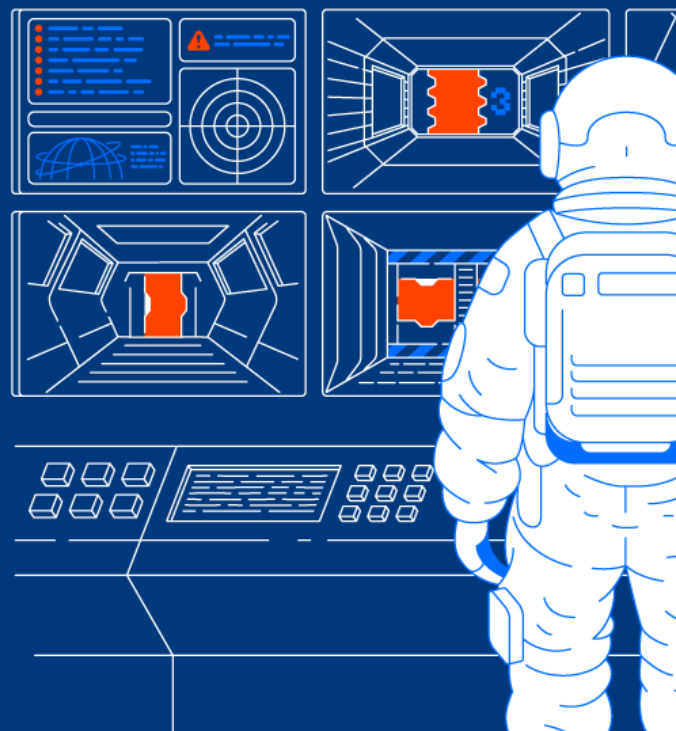
GravityZone PHASR for MSP

Shut the Front Door on Tool-Based Attacks

Detection alone does not stop attacks that abuse legitimate administrative tools. Uncontrolled access allows attackers to bypass defenses, move laterally, and trigger late-night incident response and escalations.

Bitdefender GravityZone PHASR delivers preemptive security by removing unnecessary access to administrative tools for each user and endpoint across Windows, Linux, and macOS. Built on behavioral analysis and adaptive machine learning models, PHASR prevents attackers from abusing legitimate tools frequently left unrestricted by traditional, rule-based controls, while allowing MSPs to retain their existing endpoint security stack.

Shift to prevention-first security with
Proactive **H**ardening and **A**ttack **S**urface **R**eduction.



What Sets PHASR Apart	What It Means for MSPs
Add Prevention Without Replacing What You Already Use	
Recognized under Gartner's DASR category*, PHASR adds preemptive, dynamic attack surface reduction alongside existing EPP, EDR, and XDR solutions without requiring stack replacement or architectural changes.	Deploy immediately without disrupting your existing security operations. Add a strategic prevention capability without migration complexity or integration challenges.
Automate Hardening Without Policy Overhead	
After a short behavioral learning period, PHASR automatically restricts unnecessary tool access using adaptive behavioral models and threat intelligence. Operate in Direct Control mode or enable fully automated Autopilot enforcement.	Scale prevention across multiple tenants without increasing headcount or administrative burden. Enable fast rollout with minimal operational complexity.
Eliminate Static Rules With Adaptive, Self-Tuning Security	
Unique machine learning models for each user and endpoint continuously adapt based on behavioral patterns and live threat intelligence to optimize security configurations. No static, one-size-fits-all policies that require constant manual tuning.	Streamline tuning and exceptions to reduce alert fatigue. Deliver adaptive prevention consistently across client environments at scale.
Prevent Attackers From Using Your Tools	
Restricts access to Living-off-the-Land Binaries (LOLBins), remote monitoring and management tools, and other legitimate software increasingly abused in ransomware, lateral movement, and defense evasion techniques often left unmanaged by static policies.	Prevent repeatable, playbook-style attacks before they become incidents. Reduce escalations and response workload.

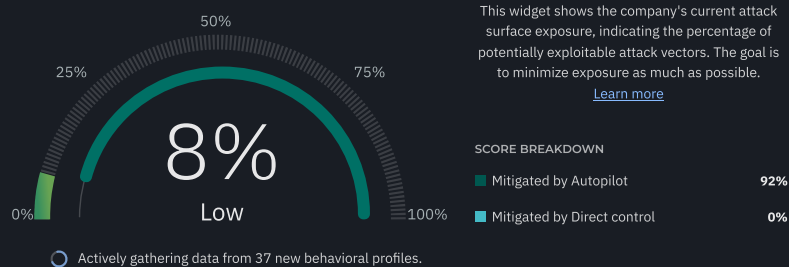
Turn Adaptive Prevention into Your Strategic Advantage

Add PHASR as a prevention layer within your existing security stack, enabling stronger protection with fewer incidents and less operational strain.

See PHASR in action



ATTACK SURFACE EXPOSURE



Detected incidents for monitored attack vectors categories

TOTAL INCIDENTS	283
Living off the land binaries	252 ▲
Remote admin tools	29 ▲
Tampering tools	1 ▲
Piracy tools	1 ▲
Crypto miners	0 ●

SEE ATTACK SURFACE REDUCE IN REAL TIME

- ↳ Up to 95% dynamic attack surface reduction
- ↳ Zero noise. Zero disruption. Zero tickets.
- ↳ Delivers measurable security outcomes
- ↳ Continuously adapts to each user and endpoint
- ↳ Eliminates unnecessary tool access
- ↳ Fully automated with optional control
- ↳ Replaces static rules with adaptive protection
- ↳ Strengthens your existing stack without disruption

"We haven't had a single ticket from any customer related to blocking anything legitimate."

And it's already stopped multiple attacks in their tracks."

OWEN WHITLOCK
Chief Technology Officer, BDR Group

Force Attackers Out of the Shadows

PHASR does more than block attack paths. It changes attacker behavior.

When tools like PowerShell, command-line utilities, or remote access are restricted, attackers do not stop. They're forced to switch tactics.

Real-world observations from Bitdefender's SOC indicate that attackers increase their activity and try different techniques when their preferred methods are blocked. These repeated attempts, tool switching, and alternative techniques create a surge in activity, exposing behavior that would otherwise stay hidden.

This shift enables security teams to act earlier in the attack lifecycle, before it escalates into a full incident.

PHASR enables MSPs to:

- ↳ Increase visibility into suspicious and abnormal activity
- ↳ Make attacker behavior easier to recognize and assess
- ↳ Detect and stop attacks at earlier stages
- ↳ Reduce reliance on post-compromise detection

*Gartner, Emerging Tech Impact Radar: Global Attack Surface Grid, Luis Castillo et al. (17 September 2025)

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 200 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

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

T: +40 21 4412452

US HQ
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309

T: +1 954-776-6262