Bitdefender | GPI

CASE STUDY

Greenman-Pedersen Deploys PHASR to Block LOLBins and Strengthen Security Posture

Greenman-Pedersen, Inc (GPI) delivers engineering and design solutions while reducing cyber risk with Bitdefender PHASR to block unauthorized tools and secure operations.

- **Industry:** Construction, Engineering
- **Employees:** 1,800 employees across 55 offices
- **Headquarters:** Babylon, New York, USA

"Knowing PHASR blocks unauthorized tools and shadow IT means I don't have to worry about those risks anymore. It's one less thing for our team to investigate, and it gives us confidence that those gaps are being covered."

JASON KRAAI
Systems Administrator
Greenman-Pedersen, INC

Attack Surface Reduction

"Close to a 70% reduction in attack surface by locking down living-off-the-land binaries and remote tools."

Rapid Shift

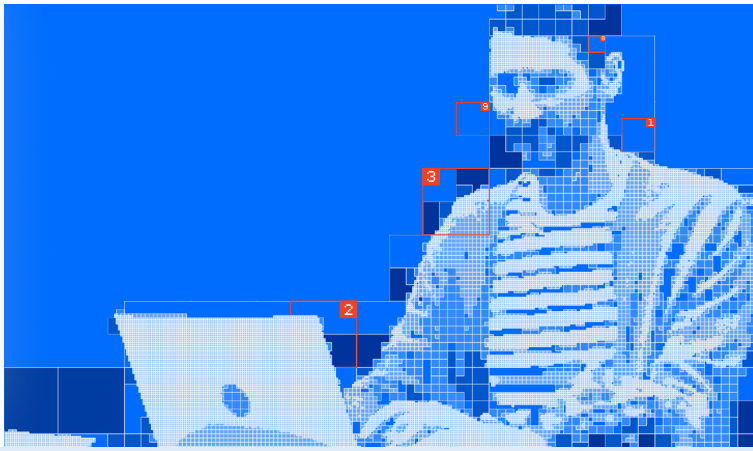
"We moved from discovery to blocking LOLBins in weeks, without investigation or disruption."

Zero Incidents

"We haven't had any incidents since implementing PHASR, and it even blocked pen test attempts."

Business Objectives:

- ✓ After a remote access incident, GPI wanted to control the use of tools like PowerShell and regedit without disrupting staff productivity.
- ✓ Identify a dynamic approach to hardening that accounts for user behavior and needs while reducing exposure.
- ✓ Implement a cost-effective solution that integrated with Bitdefender GravityZone, avoiding new platforms and additional manual oversight.



Our Solution:

GPI rolled out PHASR in discovery mode, then switched to autopilot within weeks, describing deployment as "just a matter of modifying the policy and turning it on."

PHASR uses behavior-driven intelligence to block tools attackers might exploit, closing unnecessary risks without relying on rigid application control.

Running in autopilot, PHASR enforces hardening and reveals patterns of tool usage, giving the IT team insight into everyday activity and potential exposure.

Results:

A third-party pen test confirmed PHASR blocked attempted actions, showing its ability to prevent real-world threats before they escalate.

PHASR surfaced extensive LOLBin activity across the environment, exposing patterns that would have likely gone unnoticed using traditional controls.

PHASR removed the need to investigate remote access tools and shadow IT manually, giving GPI confidence those risks are being actively managed.

Bitdefender Footprint

- PHASR
- GravityZone Business Security
- Enterprise
- Managed Detection and Response
- GravityZone Full-Disk Encryption