Global Leader
In Cybersecurity

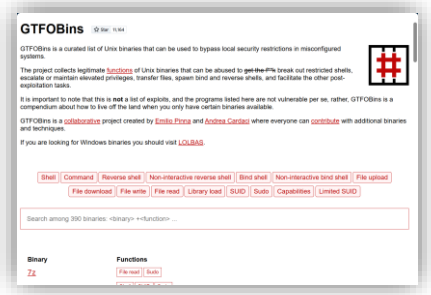
Bitdefender®

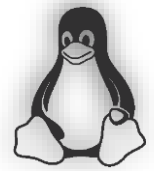
Bitdefender

Lessons from analyzing 700,000 incidents

150+
Windows binaries abused by threat actors

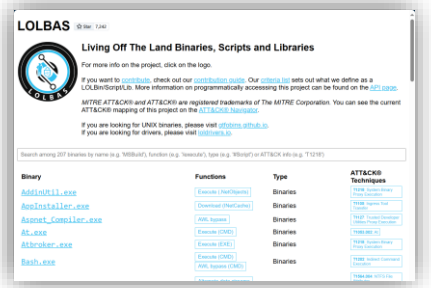
84% of major incidents and nearly all breaches involve Living off the Land (LotL) - a technique where attackers exploit legitimate tools already available on the system to blend in





Usual suspects and surprising findings

- **netsh.exe** most commonly involved in major attacks
- **powershell.exe**, **wscript**, **cscript**, all present
- **96% of orgs** use **Powershell, 73% of endpoints**
- **PowerShell.exe used by admin and 3rd party** applications



Unnecessary Attack Surface – Hundreds of risky legitimate tools that users don't leverage: mshta.exe, pwsh.exe, bitsadmin.exe used by attackers, rarely in administrative tasks.

Bitdefender

The Reality Today: Attackers Love LOTL

"If we use standard utilities, we won't be detected...we never drop tools on machines.“

Black Basta group leader (Ransomware)

Bitdefender

Organizations want to reduce risk, but...

It’s difficult to get all 3

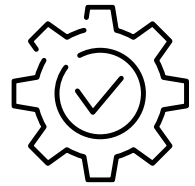
HARDENING

Small Attack Surface

USABILITY

No / low impact to business operations

MANAGEABILITY



Practical to implement

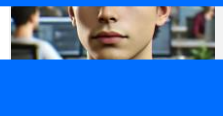
Bitdefender

Reducing The Attack Surface

Ransomware Attack
A common ransomware attack via email.

The conclusion is that:
THERE IS NO SUCH THING AS PERFECT SECURITY THAT WILL MATCH EVERYONES NEEDS

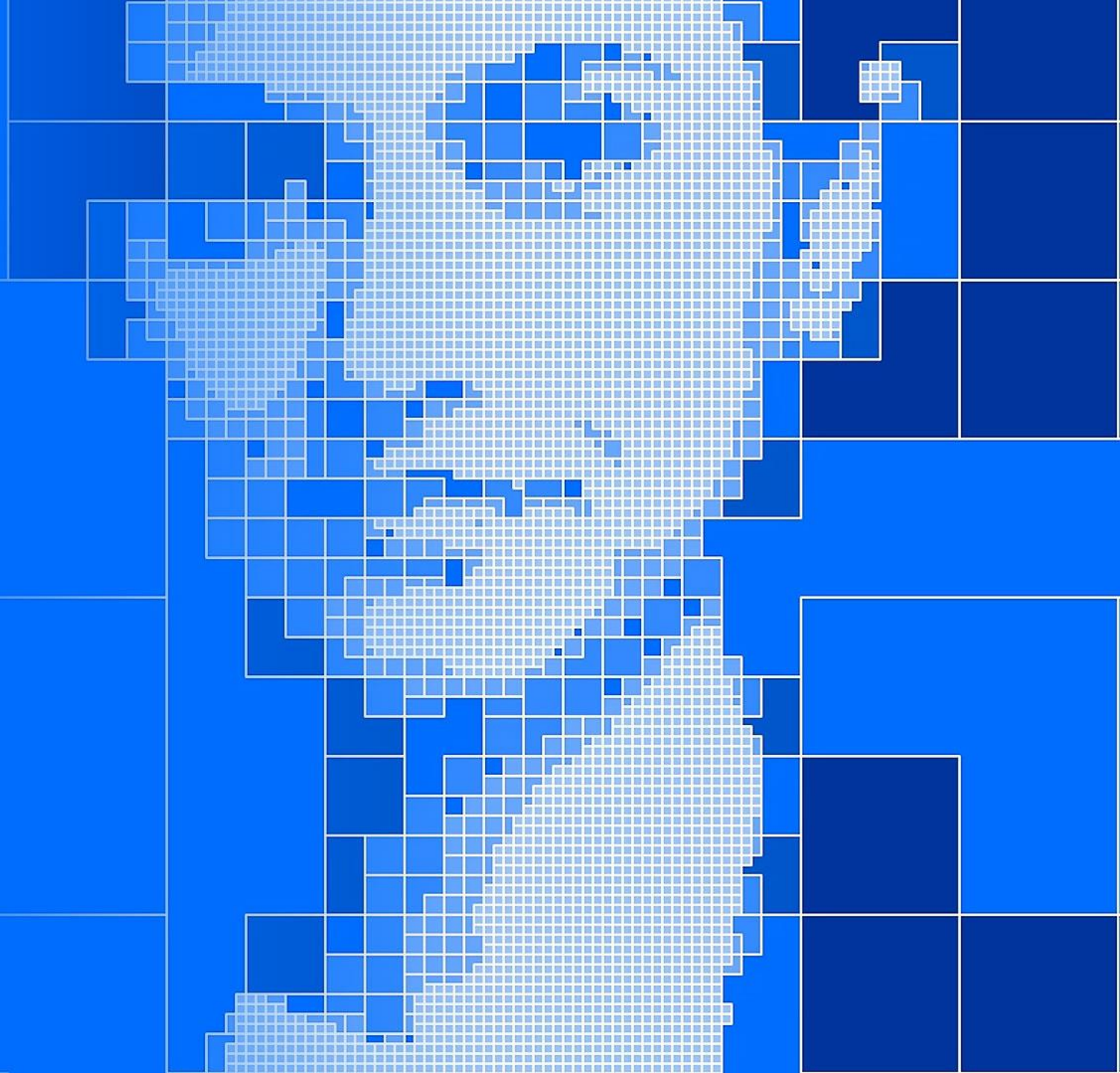
Users are unique.
Their security should be as well.

		 Work Laptop	 **Anne (IT)** Server Management
Disable email access	✗ Ne	✗ work	✓ No use on servers
Disable Office & Adobe	✗ Ne	✗ work	✓ No use on servers
Don't allow powershell, wscript, … to run	✓ No business impact	✗ Needed for work	✗ Needed for work
Don't allow macros in documents	✓ No business impact	✗ Needed for work	✓ No use on servers

Bitdefender Global Leader In Cybersecurity

Introducing GravityZone

PHASR



Bitdefender

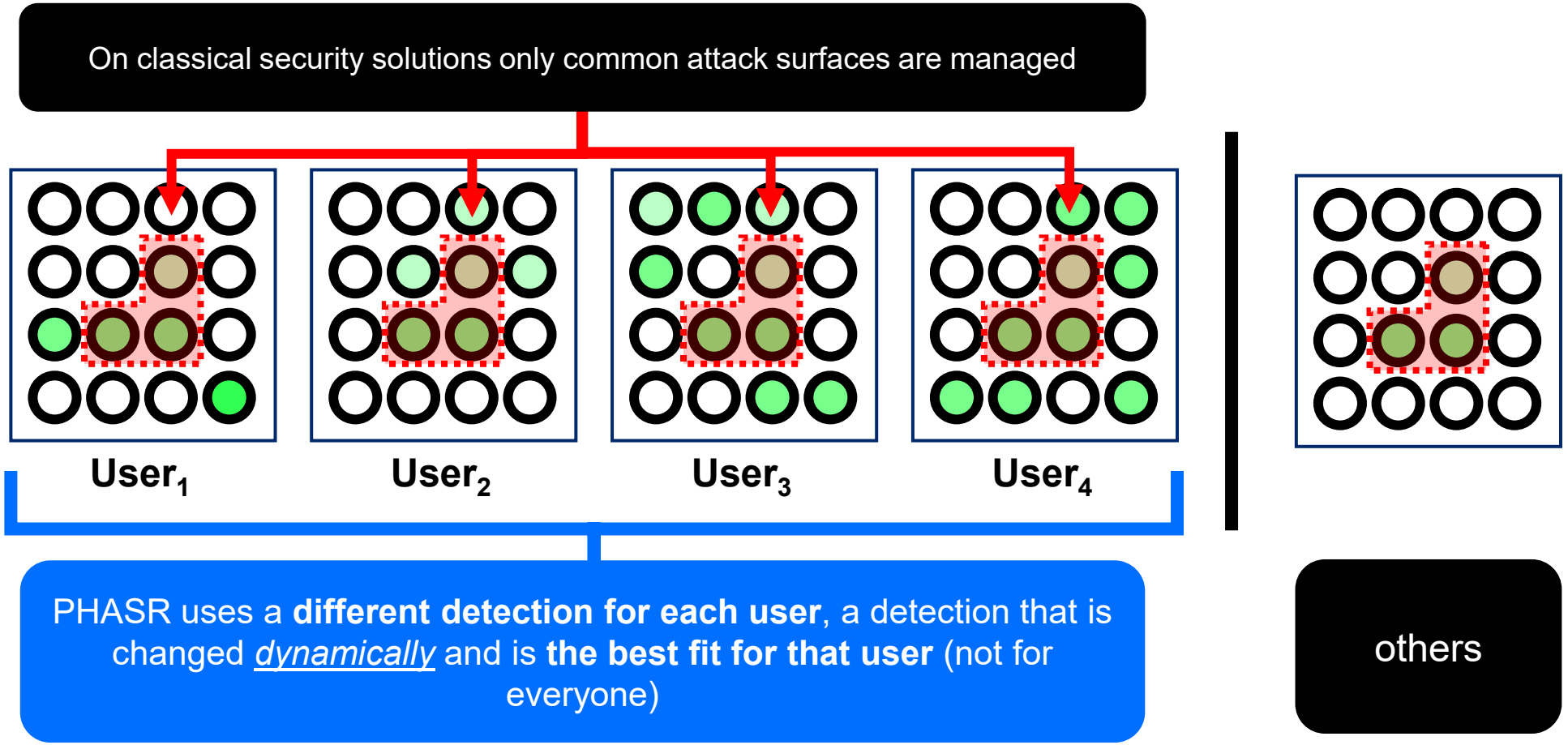
Bitdefender GravityZone PHASR

PROACTIVE HARDENING AND ATTACK SURFACE REDUCTION

- **Tailored hardening** based on unique user behavior and known threat vectors
- **Dynamic attack surface reduction solution** – continuously adapts to changing user behavior
- **Precise action-level restrictions:** allow tools, block atypical and risky behavior
- From one-size-fits-all to **optimal hardening** for each user
- **Avoids rigid policies,** adapts to actual user behavior
- **Closes unnecessary attack vectors** – tools such as PowerShell, WMIC, wscript, etc

Bitdefender

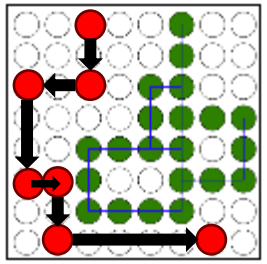
Security That Best Fits Each User



Bitdefender

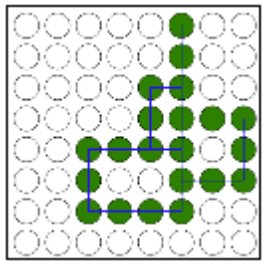
Defeating Attack Pattern Reuse

Attacker

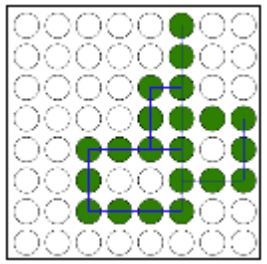


Attack Pattern Identified by the attacker

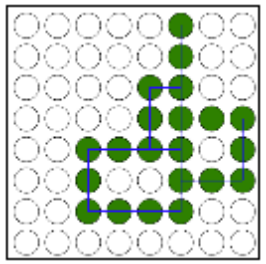
Company X protected by Product A



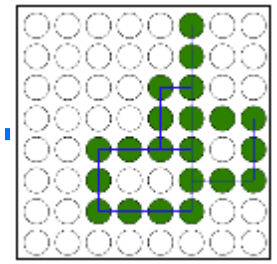
$User_1$ Attack Surface Protection



$User_2$ Attack Surface Protection



$User_3$ Attack Surface Protection

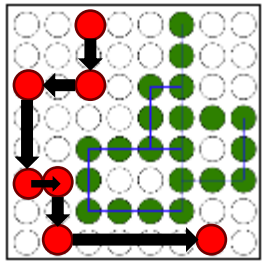


$User_n$ Attack Surface Protection

Bitdefender

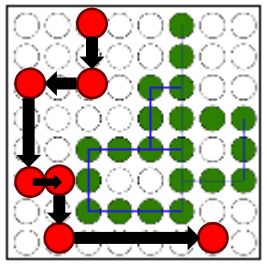
Defeating Attack Pattern Reuse

Attacker

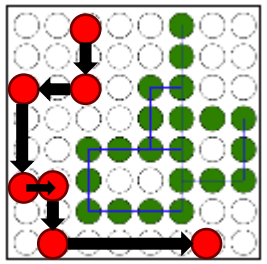


Attack Pattern Identified by the attacker

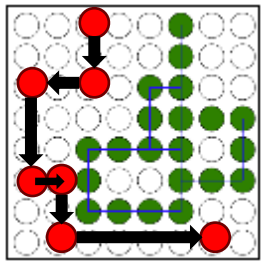
Company X protected by Product A



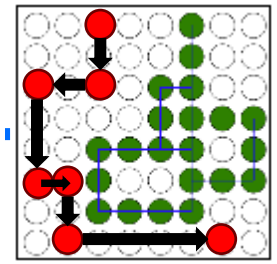
$User_1$ Attack Surface Protection



$User_2$ Attack Surface Protection



$User_3$ Attack Surface Protection

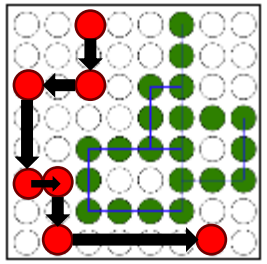


$User_n$ Attack Surface Protection

Bitdefender

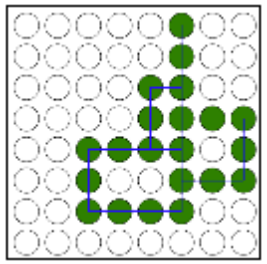
Defeating Attack Pattern Reuse

Attacker

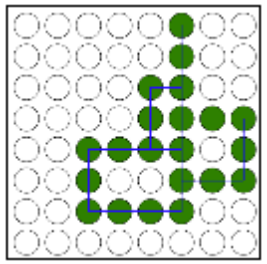


Attack Pattern Identified by the attacker

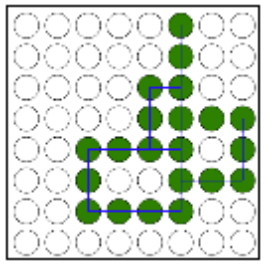
Company X protected by Product A



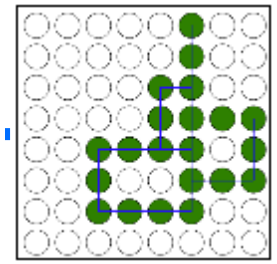
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection

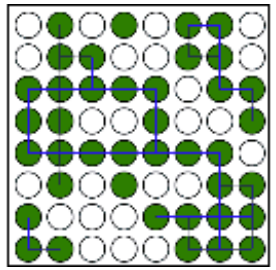


User$_3$ Attack Surface Protection

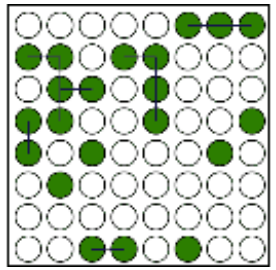


User$_n$ Attack Surface Protection

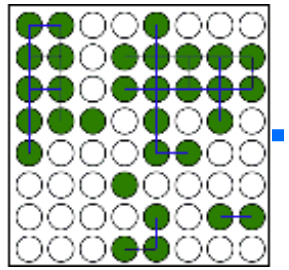
Company X protected by PHASR



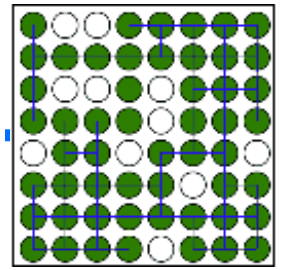
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection



User$_3$ Attack Surface Protection

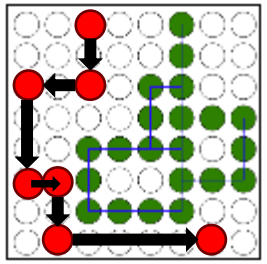


User$_n$ Attack Surface Protection

Bitdefender

Defeating Attack Pattern Reuse

Attacker



Attack Pattern Identified by the attacker

Company X protected by Product A

These patterns are dynamically updated

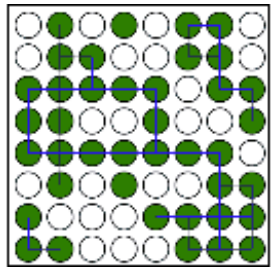
User$_1$ Attack Surface Protection

User$_2$ Attack Surface Protection

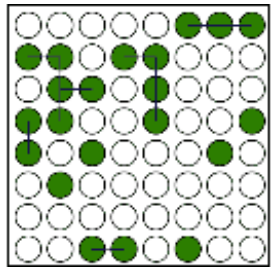
User$_3$ Attack Surface Protection

User$_n$ Attack Surface Protection

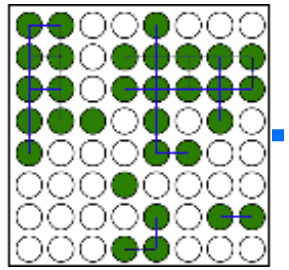
Company X protected by PHASR



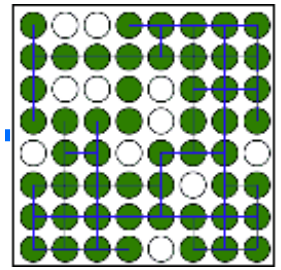
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection



User$_3$ Attack Surface Protection

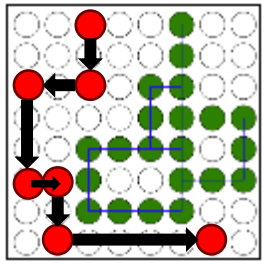


User$_n$ Attack Surface Protection

Bitdefender

Defeating Attack Pattern Reuse

Attacker



Attack Pattern Identified by the attacker

Company X protected by Product A

This is how **PHASR** looks in reality (constantly changing & evolving)

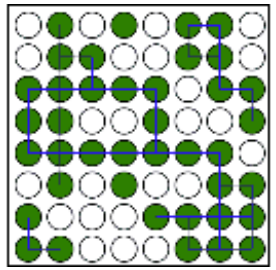
User$_1$ Attack Surface Protection

User$_2$ Attack Surface Protection

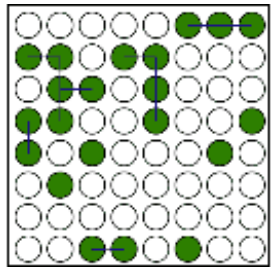
User$_3$ Attack Surface Protection

User$_n$ Attack Surface Protection

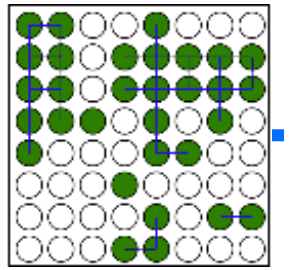
Company X protected by PHASR



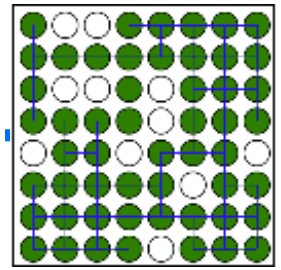
User$_1$ Attack Surface Protection



User$_2$ Attack Surface Protection



User$_3$ Attack Surface Protection



User$_n$ Attack Surface Protection

Bitdefender

GravityZone PHASR

Policy enabled

Instant Learning
for existing EDR customers

PHASR maps
attack surface exposure

AUTOPILOT
applies automatically

ACTIONABLE RECOMMENDATIONS

- LOLbins
- Tampering Tools
- CryptoMiners
- HackTools
- Remote Admin Tools

DIRECT CONTROL
provides granularity

PHASR continuously adapts to your environment, reduces exposure, and enforces control

Bitdefender

How PHASR Stands Out

Tailored

Builds behavioral risk profiles for each user, restricts what they don’t need.

Dynamic

Using innovative, AI-driven hardening that adapts to changing behavior and threats

Precise

Enabling action-level restrictions within actively used tools, blocking risky, atypical behavior only

Bitdefender

Bitdefender GravityZone for MSPs

INTEGRATED COVERAGE ACROSS ATTACK SURFACES

Proactive
Identify and address risks before they materialize.

Effortless
Enterprise-grade security, risk and compliance management, made accessible and easy.

Proven
Consistently top-ranked, widely trusted technology

Extended Detection and Response & Managed Detection and Response
- GravityZone Cloud MSP Security – Secure Extra
- GravityZone Cloud MSP Security – Secure Plus

Advanced Protection, Endpoint Detection and Response
- GravityZone Cloud MSP Security - Secure

Unified Risk & Compliance (Visibility, Prioritization, Resolution)
- CSPM+
- Offensive Services
- External Attack Surface Management
- Compliance Manager

Groundbreaking Hardening
- Proactive Hardening and Attack Surface Reduction **(PHASR)**

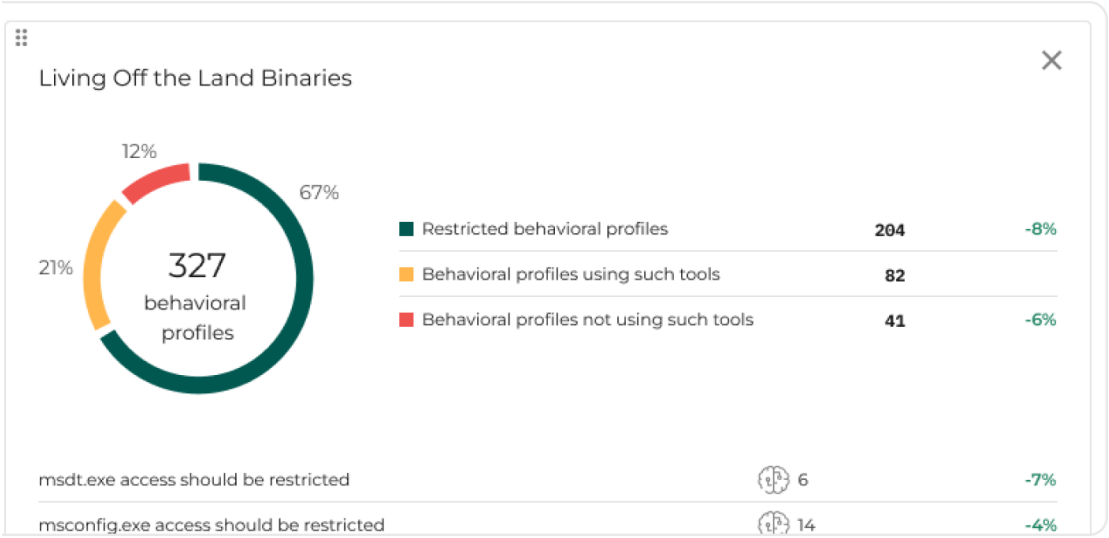
Foundational Endpoint Controls
- Endpoint Risk Analytics
- Patching
- Encryption
- Content and Device Control

Bitdefender

Early Results and Validation for PHASR

EARLY ACCESS RESULTS AND ANALYST RECOGNITION

- “More than 30% attack surface reduction in one month.”
  Enterprise Customer, Manufacturing
- Uncovered risky tools they were not aware of.
- Demonstrated proactive security posture improvement to the board.



IDC

"Bitdefender has consistently performed well in independent tests including MITRE Engenuity and has introduced innovative features such as Deep Process Inspector and Advanced Reasoning. Most recently, in 2024 **Bitdefender** Proactive Hardening and Attack Surface Reduction **(PHASR), a groundbreaking technology** that transforms how defense-in-depth-security is applied and managed across businesses."

IDC, IDC ProductScape: Worldwide Small and Medium-Sized Business Endpoint Protection Market, 2024–2025: Technology Supplier Solution Functionality, doc #US52830124, January 2025


Thank you!