

GravityZone Proactive Hardening and Attack Surface Reduction (PHASR)

Rewolucyjne, spersonalizowane i dynamiczne zabezpieczenia

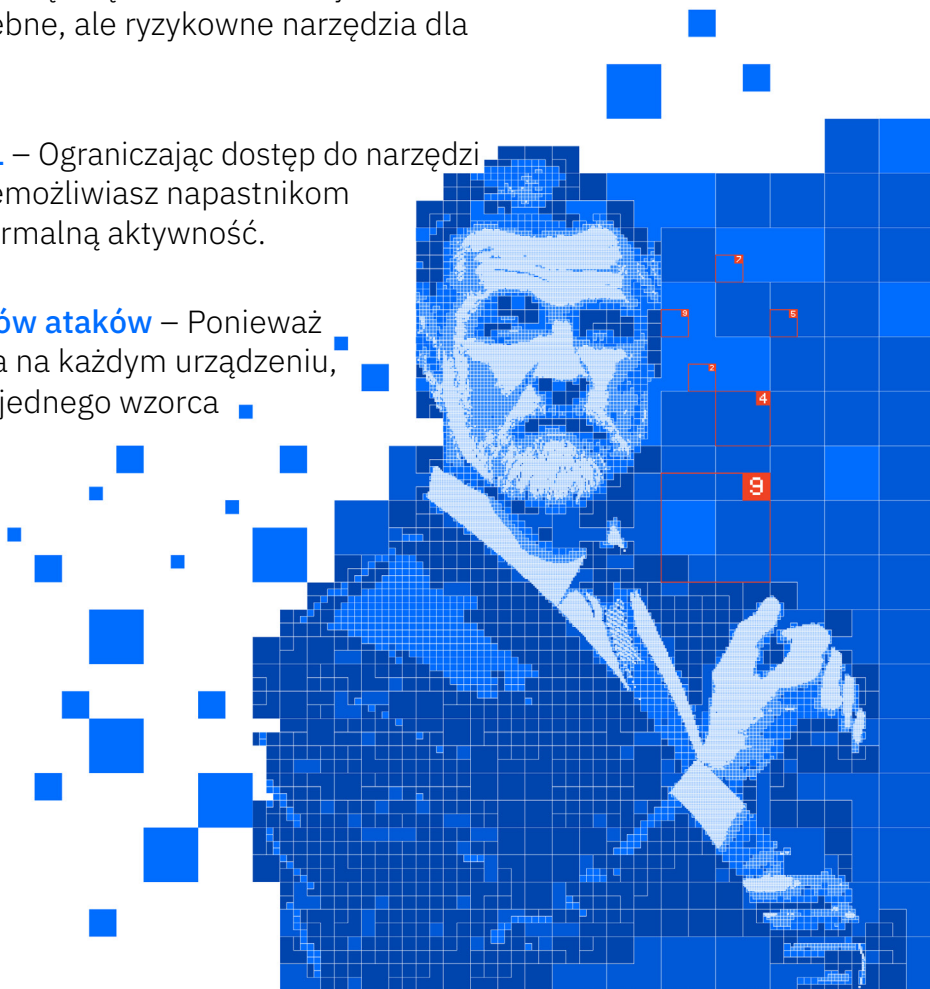
Cyberprzestępcy stosują nowe metody działania: wykorzystują skradzione dane uwierzytelniające, wtapiają się w normalną aktywność, używając legalnych narzędzi w atakach typu Living off the Land (LOTL), i skutecznie wykorzystują te same schematy na różnych ofiarach i punktach końcowych.

Ponieważ zachowanie każdego użytkownika jest unikalne, a reguły kontroli aplikacji i redukcji powierzchni ataku są statyczne i zaprojektowane dla wszystkich, zwykle oferują ograniczone zabezpieczenia, są zbyt restrykcyjne i trudne w zarządzaniu dla standardowych zespołów IT.

GravityZone PHASR to przełomowe rozwiązanie, które powstrzymuje ataki [Living Off The Land](#) bez ograniczania produktywności lub obciążania zespołów IT.

Techniki Living off the Land są obecnie wykorzystywane w 84% ataków. Radykalnie zmniejsz powierzchnię ataku swoich pracowników i zatrzymaj podstępne ataki, zanim wyrządzą szkody:

- ↳ **Zaawansowane zabezpieczenia** – PHASR zapewnia głębokie, spersonalizowane zabezpieczenia, ucząc się zachowania użytkownika i bezpiecznie ograniczając niepotrzebne, ale ryzykowne narzędzia dla konkretnych osób.
- ↳ **Wczesne blokowanie ataków LOTL** – Ograniczając dostęp do narzędzi takich jak PowerShell czy WMI, uniemożliwiasz napastnikom eskalację ataku i wtapianie się w normalną aktywność.
- ↳ **Neutralizacja powielania schematów ataków** – Ponieważ PHASR dostosowuje zabezpieczenia na każdym urządzeniu, atakujący nie mogą wykorzystywać jednego wzorca na wielu systemach.



Kluczowe funkcje Bitdefender GravityZone PHASR:

- ↳ **Spersonalizowane zabezpieczenia** – PHASR dostosowuje zabezpieczenia do zachowania użytkownika, ograniczając niepotrzebne, ale ryzykowne narzędzia.
- ↳ **Dynamiczna redukcja powierzchni ataku** – PHASR stale i autonomicznie dostosowuje się do zmian w zachowaniu użytkowników i nowych wektorów ataków, minimalizując wysiłek administracyjny.
- ↳ **Precyzyjna kontrola** – PHASR pozwala blokować nieużywane, ale ryzykowne aplikacje, a także wprowadzać szczegółowe ograniczenia w używanych programach, blokując tylko nietypowe zachowania.
- ↳ **Ochrona oparta na analizie zagrożeń** – PHASR wykorzystuje analizę zagrożeń Bitdefender, zapewniając skuteczność wobec najnowszych metod ataków.
- ↳ **Inteligentne grupowanie** – PHASR grupuje użytkowników o podobnych zachowaniach, umożliwiając skuteczne wdrażanie redukcji powierzchni ataku w całej organizacji.
- ↳ **Autonomiczne ograniczanie ryzyka** – Tryb Autopilot umożliwia adaptacyjne i samodzielne zmiany zabezpieczeń, podczas gdy tryb Direct Control dostarcza rekomendacje i wymaga decyzji administratora.
- ↳ **Zintegrowane zarządzanie ryzykiem i bezpieczeństwem** – PHASR płynnie integruje się z istniejącymi architekturami jako część platformy GravityZone XDR, zapewniając kompleksową widoczność ryzyka, priorytetyzację i neutralizację zagrożeń, a także prewencję, ochronę, wykrywanie i reakcję.



"Bitdefender konsekwentnie osiąga doskonałe wyniki w niezależnych testach, w tym MITRE Engenuity, i wprowadza innowacyjne funkcje, takie jak Deep Process Inspector i Advanced Reasoning. W 2024 roku firma zaprezentowała Proactive Hardening and Attack Surface Reduction (PHASR), przełomową technologię, która zmienia sposób stosowania i zarządzania zabezpieczeniami opartymi na głębokiej obronie w firmach."

IDC, IDC ProductScape: Worldwide Small and Medium-Sized Business Endpoint Protection Market, 2024-2025, dokument #US52830124, styczeń 2025

Dowiedz się, jak PHASR może aktywnie chronić Cię przed podstępными atakami:

[Skontaktuj się z nami i zamów demo](#)