Bitdefender

GravityZone PHASR 攻击面减少

引言：新形势下的终端安全挑战

随着攻击技术不断演进，网络威胁愈加隐蔽复杂。攻击者越来越多地利用合法工具，如 PowerShell、WMI、命令行脚本等发起“Living off the Land”（LOTL）攻击。这类攻击往往无需下载恶意程序，极易绕过传统防病毒机制，并在系统中长期潜伏。研究显示，超过70%的现代网络攻击已涉及 LotL 技术。

在此背景下，传统统一、静态的安全策略已难以应对复杂多变的终端风险。企业迫切需要一种能够动态识别、个性化防御、精细控制的新型防护方案。

GravityZone 攻击面减少概述

GravityZone PHASR 是一款面向终端环境的智能安全加固模块，可无缝集成至 Bitdefender GravityZone XDR 平台。PHASR 通过用户行为建模、风险工具分析与动态策略执行，持续收敛系统攻击面，防止攻击者借助系统原生工具完成横向移动、权限提升等操作。

通过深度行为学习与威胁情报驱动，PHASR 能够识别用户不必要但潜在危险的工具，并进行限制，而不干扰其实际业务需求。该方案兼顾了“安全性、可用性、易管理性”，是当前应对 LotL 攻击的理想之选。

产品主要优势

→ 有效对抗 LotL 攻击：在攻击早期阶段主动阻断对高危工具的滥用，防止隐匿攻击与横向移动。

→ 个性化防护体验：策略依据用户行为动态生成，避免“一刀切”限制，提升终端使用效率与安全性。

→ 自动化降低管理负担：智能化策略制定与执行，大幅减少管理员手动干预与配置成本。

→ 增强网络韧性：各终端策略独立，攻击者无法在多个设备间复用相同战术。

→ 无缝集成平台：作为 GravityZone XDR 的核心组件之一，实现安全防护、威胁检测、响应处置的统一可视化与协同作业。

核心能力

GravityZone PHASR 通过融合用户行为分析、智能策略引擎与全球威胁情报，构建了一套高度自动化、动态调整、精细可控的终端防护体系。不同于传统静态规则或一刀切的应用控制方式，PHASR 能根据用户角色与行为模式定制化实施攻击面收敛策略，从而在不影响业务连续性的前提下，实现对潜在威胁的精准拦截与风险最小化。

以下为其关键能力模块：

→ 个性化深度加固：根据每位用户的行为模式，识别其不需要但易被攻击者滥用的工具（如脚本解释器、远程调用组件），并安全限制。

→ 动态攻击面收敛：持续感知行为演变与威胁变化，策略动态调整，保障安全同时不过度干预业务流程。

→ 细粒度行为控制：不仅可以封禁整个程序，也能控制特定功能操作，如阻止 Office 宏、命令行参数调用等典型异常行为。

→ 威胁情报驱动防护：基于 Bitdefender 实时全球威胁数据更新本地策略库，确保对最新攻击技术的应对能力。

→ 智能用户聚类：自动将行为模式相近的用户归类统一管理，实现策略集中部署与差异化控制的平衡。

→ 自主/推荐双模式：自动驾驶模式：系统自主决策并执行攻击面收敛操作。管理员控制模式：由系统推荐策略，管理员确认后生效，保障可控性。

→ 统一安全与风险视图：与 GravityZone XDR 平台深度集成，实现威胁防护、事件响应、风险管理三位一体的安全运营体系。

免费试用

产品介绍：https://www.bitdefender-cn.com/free-trial.html

联系电话：4000-132-568

联系邮箱：sales@bitdefender-cn.com

关于Bitdefender

Bitdefender 是全球领先的网络安全公司，保护全球 5 亿多设备，覆盖 170 多个国家。其安全技术被全球超过220+公司集成并采用，深受客户与行业认可。

扫一扫 关注我们