Bitdefender

Gravityzone

勒索病毒防护方案

Bitdefender

勒索病毒仍是当今企业面临的最顽固、代价最高的网络威胁之一。尽管企业多年来在网络安全工具和安全意识培训上投入巨资，却依然以惊人的频率沦为攻击受害者。

Verizon《2025 年数据泄露调查报告》显示，勒索病毒攻击事件年增长率高达 37%，这意味着攻击者的手段进化速度，已远超许多企业的防御迭代速度。对于 IT 与安全部门负责人而言，这一数据也警示着：传统的、碎片化的防御体系早已无法满足安全需求。

这一困境的部分根源，在于勒索病毒善于利用企业攻击面中各类防护漏洞。企业团队的漏洞补丁延迟、系统配置失误、资源过度分散，都会让攻击者有机可乘。这也解释了为何拥有成熟合规体系的大型企业（如金融等强监管行业的企业）防御效果更佳，而小型企业和精简型 IT 团队往往难以达到同等防护水平，进而成为攻击者的主要目标。

但好消息是，有效的勒索病毒防御并非大型企业的专属权利。通过合理搭配预防、检测、响应与风险管理手段，即便是精简型 IT 团队，也能搭建起企业级的勒索病毒防护体系。

勒索病毒防护痛点与Bitdefender解决方案解析

现代攻击者会不断变换攻击手法，利用企业系统漏洞发起进攻。对于配备精简型 IT 安全团队的企业而言，关键是要掌握如何在勒索病毒攻击链的每个阶段开展有效防御。

初始入侵与预防阶段

有效的勒索病毒防护策略，首先要应对不断扩大的企业攻击面，以及现代攻击者极快的攻击节奏。有些攻击者会在潜入企业系统数周后才发起攻击，但更多攻击者会在获取访问权限后的数小时内就发动攻击。对于依赖人工操作、碎片化防御的精简型 IT 安全团队而言，根本无法跟上这样的攻击速度。正因如此，预防优先的防御策略至关重要，唯有从源头阻止攻击者潜入企业系统，才能筑牢第一道防线。

如今许多勒索病毒团伙会利用扫描工具，大规模识别并利用企业系统漏洞，这也让定向攻击和机会性攻击的界限变得模糊。一个被忽视的补丁、一处配置失误，都可能迅速成为攻击者发起大规模入侵的突破口，这让精简型 IT 团队在这一阶段的防御工作倍感吃力。

以下是Bitdefender在初始入侵阶段为企业提供的多重防护手段：

→ 攻击者会持续扫描企业环境中的漏洞，GravityZone 外部攻击面管理（EASM）功能可精准识别攻击者可能利用的漏洞，包括暴露的资产和影子 IT 系统；

→ 攻击者常将恶意代码隐藏在看似无害的文件中，GravityZone 沙箱分析器会在安全环境中运行高风险文件，挖掘其隐藏的恶意行为；

→ 勒索病毒攻击往往始于钓鱼邮件，GravityZone 高级邮件安全功能可拦截可疑邮件，阻止其进入用户收件箱，同时精准阻断勒索病毒、钓鱼攻击和企业邮件诈骗行为；

一旦攻击者成功突破这一阶段的防御，通常会试图在企业系统中建立立足点，进一步推进攻击流程。

Bitdefender

攻击扩散与检测阶段

成功实现初始入侵后，攻击者的目标将从 “潜入” 转为 “在企业网络中建立多个立足点”，进而尝试访问更多系统、植入持久化访问程序、试探提升控制权的方法。

以下是Bitdefender针对攻击扩散与检测阶段核心痛点的解决方案：

→ 攻击者常会试图攻陷域控制器，以实现勒索病毒的广泛部署，或让企业无法访问核心系统。GravityZone XDR 可检测针对域控制器的异常行为，即便拥有高权限账户的操作存在异常，也能被精准识别，避免这类行为成为漏网之鱼；

→ 勒索病毒团伙会主动搜寻企业敏感数据，并试探企业防御能力，评估其网络安全就绪状态。GravityZone 网络流量分析作为 XDR 的核心组件，通过集成遥测数据与分析能力，及时发现攻击者的侦察行为，助力企业快速响应；

→ 攻击者常利用 PowerShell、WMI/WMIC、PsExec 等合法工具隐藏攻击行为，增加检测难度。GravityZone 在 XDR 中集成了身份威胁检测与响应（ITDR）功能，可精准区分这类偏离正常用户行为的操作，即便攻击者躲在可信工具背后，也能被识别。

GravityZone 具备强大检测能力的核心秘诀，是定制化机器学习模型。与依赖通用模型不同，GravityZone 会为每个企业的环境单独训练专属模型，深度学习企业系统的行为模式，即便攻击者引发的异常十分细微，也能被精准捕捉，及时发现攻击者的踪迹。这一能力能为企业团队争取更多的可疑行为响应时间，控制潜在损失，让企业更快开展威胁遏制工作。

响应与遏制阶段

一旦检测到勒索病毒威胁，企业必须迅速采取行动，在攻击升级前将损失降至最低。对于精简型 IT 团队而言，有效的勒索病毒防护策略，需要将自动化响应与人工辅助响应能力相结合。

以下是Bitdefender在响应与遏制阶段为企业提供的支持：

→ 攻击者常会通过权限提升、未授权系统修改等持久化手段维持对企业系统的访问，GravityZone 会持续监控这类行为，并立即切断攻击者的访问权限；

→ 精简型 IT 团队在应对威胁时，往往难以在响应速度和判断准确性之间找到平衡。GravityZone 的 EDR、XDR 与 MDR 功能提供自动化遏制能力，可在终端、服务器和网络中快速实现威胁遏制；

→ 安全团队常常难以将碎片化的攻击告警梳理成清晰的事件时间线，GravityZone 提供实时攻击可视化功能，以图形化方式呈现完整的攻击链，帮助团队明确攻击起点、传播路径及造成的影响。

GravityZone 将预防、检测、响应能力深度融合，助力企业大幅缩短攻击者的潜伏时间，更高效地阻断勒索病毒攻击，将原本可能演变为全面危机的勒索病毒攻击，转化为可轻松应对的普通安全事件。

Bitdefender

一体化安全平台的核心价值

依靠单一的一体化平台抵御攻击，远比使用多款独立工具的防护效果更佳。但遗憾的是，许多宣称能提供 “一站式解决方案” 的供应商，其产品往往存在明显短板：要么缺乏真正的预防能力，要么操作过于复杂，精简型团队难以有效使用。优质的安全平台，应能提供全面的防护能力，且不会产生额外的隐性运营成本。

Bitdefender在设计 GravityZone 时，就将解决这一行业痛点作为核心目标，确保这款一体化安全平台能适配精简型 IT 团队面临的复杂场景与实际需求。GravityZone 可自动关联各类安全信号，构建完整的攻击画像，无需安全分析师手动从多款工具中搜集线索、拼凑证据；同时大幅降低对人工检测的依赖，让企业能在威胁升级前精准识别真实的安全风险。

这款平台让精简型 IT 团队，也能拥有曾只有大型企业才能享有的、由专业安全团队支撑的检测与响应能力，同时彻底摆脱管理多款碎片化工具带来的沉重运营负担。

将安全工具整合至一体化安全平台，能为企业带来立竿见影的显著成本节约；从长期来看，团队可减少在系统配置和工具管理上的时间投入，将更多精力放在事件调查、风险降低等高价值安全工作上，进一步为企业节省成本。此外，工具整合还能简化企业各部门的安全培训工作，降低授权许可与设备维护成本。

为精简型 IT 团队简化检测与响应流程

对于精简型 IT 安全团队而言，时间是最宝贵的资源。但传统的安全防护方式，常让分析师淹没在原始日志中，被大量告警信息压得喘不过气，不得不花费大量时间手动梳理事件脉络，才能开展后续的响应工作。这一过程不仅令人挫败，还会大幅延长攻击者的潜伏时间，让其有更多机会对企业造成严重破坏。

GravityZone 通过自动化检测与信号关联，为团队减轻这一工作负担。它不会将每条告警孤立看待，而是收集所有安全信号，梳理成一份清晰、易懂的完整事件报告；同时通过自动化过滤误报信息，结合场景化的精准洞察，直接为分析师指明问题根源。

这一能力能让团队快速掌握：攻击事件的发生过程、触发原因、起源位置，以及哪些系统正面临风险。对于人员编制有限的中小团队而言，这一功能的价值不言而喻 —— 它能将原本需要数小时的人工调查，转变为近乎实时的快速响应。

Bitdefender

依托风险管理与补丁管控，提升企业安全态势

稳固的企业安全态势，建立在主动识别并修复漏洞的基础上，让攻击者无漏洞可钻。GravityZone 的风险管理、高优先级影响安全修复（PHASR）、集成化补丁管控等功能，为企业提供了实现这一目标的高效工具，助力企业减少风险暴露，加快漏洞修复速度。

→ GravityZone 外部攻击面管理 (EASM)

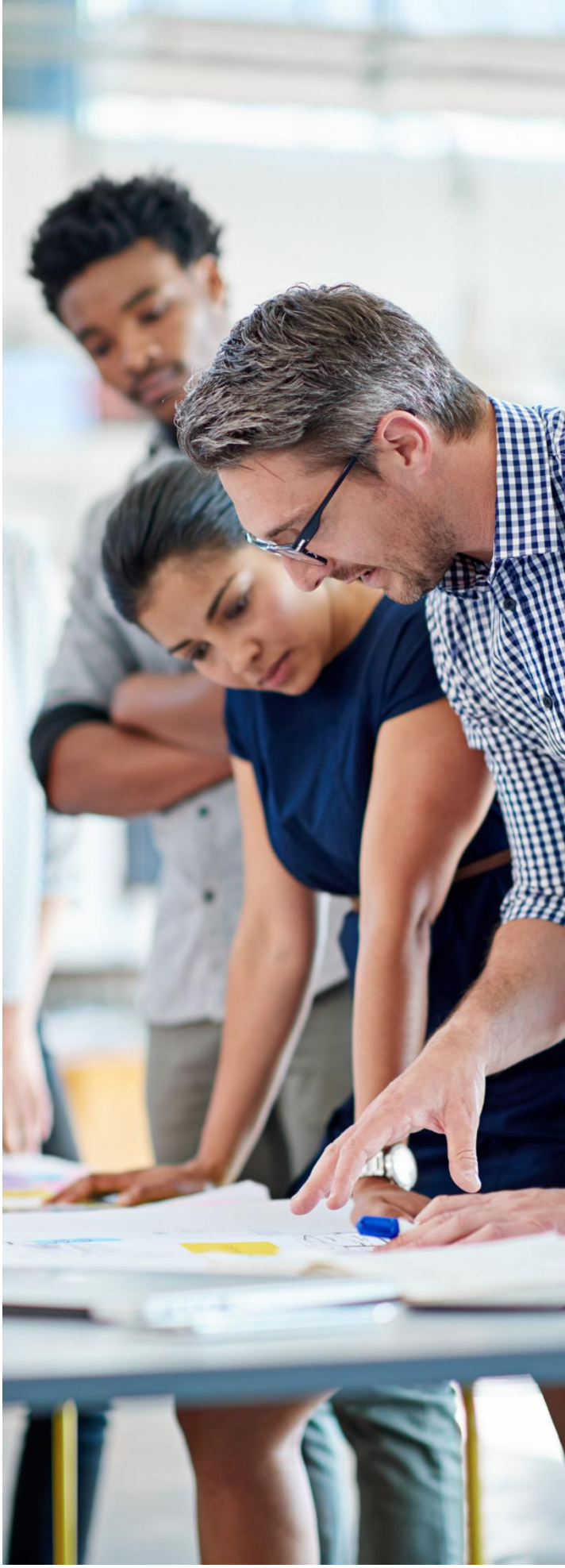
主动识别、监控并保护企业所有面向互联网的资产，防止被攻击者利用。该功能可清晰展示企业所有公网暴露 IP、自治系统号报告、即将过期或已过期的证书、存在漏洞的公共服务及开放端口，让企业能从攻击者的视角审视自身安全状况；同时还能识别与企业域名相似的恶意域名，发现针对企业的仿冒和欺诈行为。

→ GravityZone PHASR 主动攻击面收敛 大幅缩减企业攻击面，进一步强化安全态势。该功能可识别用户层面的安全风险，限制未使用的应用程序及非典型但高风险的应用程序运行，最高可将企业攻击面缩减 95%；同时能有效抵御攻击者利用 “合法工具（LOTL）” 的攻击手法，即通过 PowerShell 等合法工具隐藏行为、躲避检测的攻击。

→ GravityZone 补丁管理 实现终端与服务器软件更新、安全补丁的自动化部署，提升企业系统的抗风险能力。该功能减少了补丁跟踪、测试、部署的人工操作，最大限度缩短企业因未及时打补丁而产生的漏洞暴露窗口 —— 这也是攻击者最常利用的突破口。

→ GravityZone XDR 实现企业全环境检测与响应能力的一体化，让精简型 IT 团队无需具备深厚的安全专业知识，也能快速识别并遏制攻击。

这些功能协同作用，助力精简型 IT 安全团队实时跟踪企业全环境的风险评分，监控安全态势的持续改善；同时还能帮助企业向内部及监管机构，清晰展示合规要求的达成情况。



Bitdefender

第三方独立测评的重要性

第三方独立测评能客观反映安全方案的实际效能，既凸显其优势，也揭露潜在短板；行业分析师报告与第三方测试数据，能为企业提供平台在实际场景中表现的真实、确凿证据。

选择在第三方独立测评中表现始终优异的勒索病毒防护方案，能让企业确信，所采用的技术能有效检测、预防并响应勒索病毒威胁。平台在威胁检测、攻击链可视性、可执行报告等维度的优异表现，足以证明其能快速识别威胁，并为团队提供清晰的洞察，助力高效响应。

AV-Comparatives 与 MITRE 是两家值得信赖的独立测评机构，其测评结果能客观反映安全方案的效能、效率与投资回报率；同时，高德纳、弗雷斯特等顶级行业分析机构发布的权威测评报告，也能帮助企业客观了解市面上各类防护方案的优劣。

经过第三方独立验证的安全技术，能为企业降低选择风险与运营不确定性，这对于精简型 IT 安全团队而言尤为重要。团队无需再花费时间验证告警的真实性，可直接聚焦于威胁响应，实现更快速、更有效的防御效果。

为精简型 IT 安全团队打造的现代化勒索病毒防护方案

随着勒索病毒的不断进化，攻击手法愈发精密，企业的勒索病毒防护方案也必须与时俱进。对于精简型 IT 团队而言，核心挑战是在全面防御与资源有限之间找到平衡，同时避免团队陷入告警疲劳。

Bitdefender GravityZone 专为解决这一挑战而生，将企业全环境的预防、防护、检测、响应能力融为一体。其多层级扩展预防能力、集成化遥测数据、自动化事件分析与风险管理功能，大幅减少人工操作，提升威胁响应速度，全面强化企业安全态势。

对于中型企业的精简团队而言，GravityZone 意味着更快速、更精准的威胁检测、更简化的安全运营流程，以及可量化的风险管理能力提升，且无需承担管理多款独立工具的复杂成本。GravityZone 的防护效能在历次第三方独立测评中均表现优异，让企业能安心依靠这款经过实践验证的技术，筑牢勒索病毒防御防线。

立即免费试用 Bitdefender GravityZone，亲身体验其全功能能力，见证它如何为企业简化安全运营工作。

Bitdefender

联系Bitdefender中国
联系电话：4000-132-568
联系邮箱：sales@bitdefender-cn.com

微信扫一扫，关注我们

关于Bitdefender

Bitdefender 是全球领先的网络安全企业，为全球客户提供一流的威胁预防、检测与响应解决方案。作为全球5亿消费者、企业与政府机构的网络安全守护者，Bitdefender是行业内最值得信赖的专家之一，致力于消除网络威胁、保护用户隐私、数字身份与数据安全，助力企业构建网络安全韧性。
Bitdefender在研发领域持续大力投入，旗下实验室每分钟发现数百个新型威胁，每日验证数十亿次威胁查询；企业在反恶意软件、物联网安全、行为分析、人工智能等领域开创了多项突破性创新技术，其技术被全球 200 余家知名科技品牌授权使用。
Bitdefender成立于 2001 年，业务覆盖全球 170 余个国家和地区，在全球多地设立办公机构。

罗马尼亚欧洲总部
Orhideea Towers
15A Orhideelor Road, 6th District,
Bucharest 060071

中国办公室
北京 . 上海 . 深圳