Bitdefender

Gravityzone

如何以精简团队搭建完善的网络安全体系

多数网络安全报告开篇都会警示新型威胁，但对于人员精简的安全团队而言，真正的挑战却在别处。报告中披露的触目数据令人警醒：过去十年，企业邮件诈骗（BEC）造成的经济损失高达 550 亿美元；企业邮件诈骗事件发生率飙升 66%；勒索软件出现在 44% 的网络入侵事件中，且年增长率达 37%。

这些数据虽能帮助企业董事会和高管层建立安全认知，但对于 IT 与安全部门负责人而言早已不是新鲜事，他们深知这类威胁的危害程度多年来一直在不断升级。真正的新挑战，在于企业数字业务版图的持续扩张，以及随之而来的攻击面不断扩大。

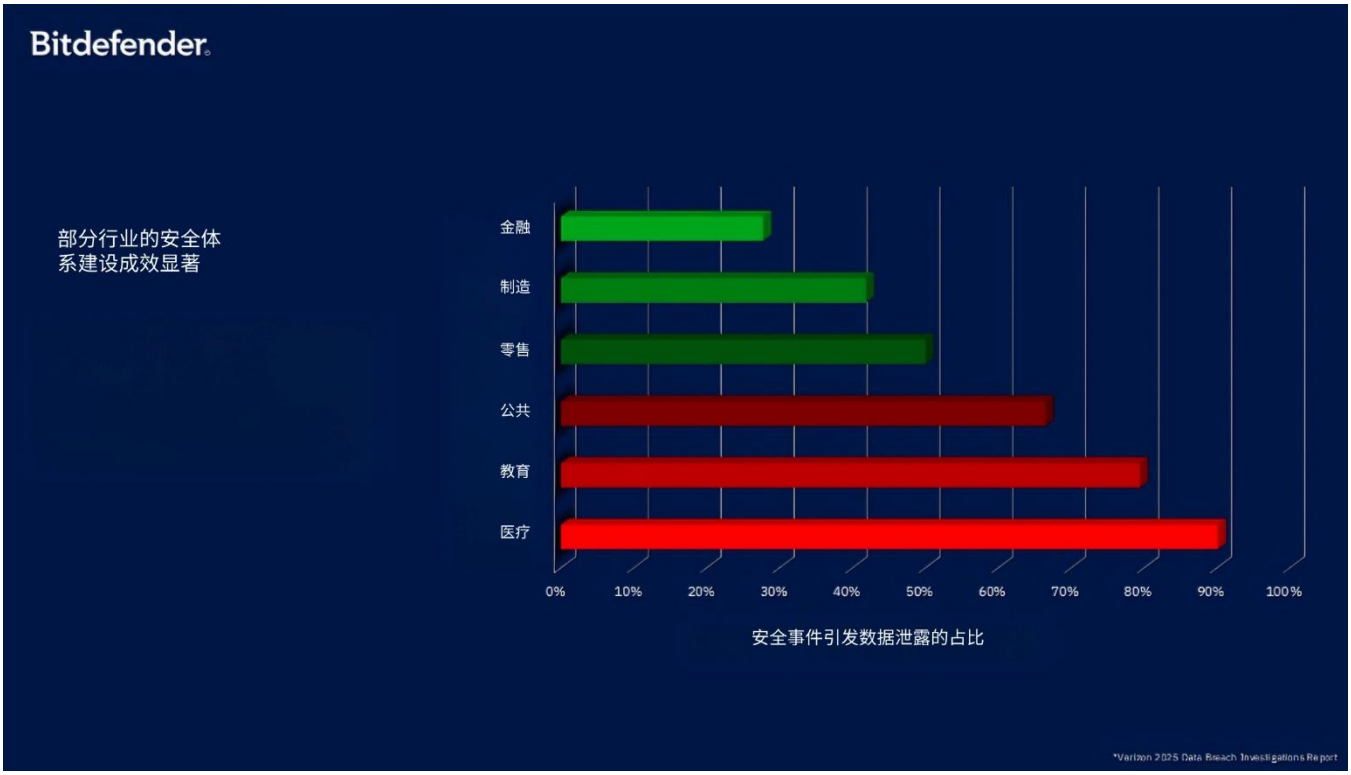
如果企业无法全面掌握内部、外部所有资产的情况 —— 包括影子 IT 系统、云应用，以及流入人工智能工具的各类数据，攻击者必然会趁机利用其中的漏洞发起攻击。企业员工与供应链同样属于攻击面的一部分，忽视这两方面的安全管理，会形成巨大的安全盲区。

Verizon《2025 年数据泄露调查报告》显示，60% 的网络入侵事件都与人为因素相关，30% 则牵涉第三方合作方。Bitdefender的研究还发现了一个令人担忧的近期趋势：在 84% 的网络安全事件中，攻击者都会盗用设备中已安装的合法工具实施攻击。这类行为并非利用系统漏洞，无需通过补丁修复，而工具本身的合法属性，让其滥用行为的检测工作面临巨大挑战。

Verizon的研究还指出，企业平均需要 32 天才能修复网络边界设备的漏洞，这让企业在漫长的修复期内始终暴露在安全风险中。这一现象也凸显了安全可视性不足的严重后果：无法及时发现的漏洞，自然也无法得到快速修复。对于人员精简的团队而言，即便资源有限，如何实现全面的安全可视性、缩短企业的风险暴露窗口，才是当下最核心的挑战。

哪些企业的网络安全工作做得更好？

不同行业中，升级为实际数据泄露事件的安全事故占比差异显著，这一差异也反映出各行业在安全投入和安全体系成熟度上的不同。



金融、制造、零售、公共部门、教育、医疗健康行业的安全事件转化为数据泄露的比例依次递增（金融行业最低，医疗健康行业最高）。

受严格监管且通常拥有充足安全预算的金融机构，数据泄露发生率最低，制造业紧随其后。这表明，构建体系化的安全管理方案、投入专属的安全资源，能显著降低安全事件升级为数据泄露的概率。与之形成鲜明对比的是，公共部门、教育、医疗健康等高度依赖公共资金的行业，在网络安全管理方面面临的困境则严峻得多。

从企业规模维度分析这一数据可以发现，大型企业的安全表现明显更优：员工规模超 1000 人的企业，因安全事件引发数据泄露的概率，比员工不足 1000 人的企业低近 20%。

这一数据传递的核心结论十分明确：那些通过制定安全政策、部署技术工具、开展员工培训等方式，重视并投入网络安全建设的企业，在遭遇安全事件时的应对能力更强；反之，资源有限或安全体系成熟度较低的企业，抗风险能力更弱，安全事件也更易升级为造成严重损失的数据泄露事故。

那么问题来了，这些网络安全工作做得好的企业，究竟采取了哪些有效举措？其他企业又该如何借鉴？

Bitdefender

全攻击生命周期的企业安全防护

网络安全建设成效显著的企业，均构建了基于风险管理与合规框架的成熟安全体系，并实现了全攻击生命周期的安全防护覆盖。

Bitdefender

以下为各环节的核心价值与工作重点：

1. 预防

作为安全防护的首个环节，核心是实现企业攻击面的全面可视，识别潜在安全风险、评估系统漏洞。唯有清晰掌握自身的防护对象与风险点，才能主动降低企业面临的威胁暴露概率。

2. 保护

在该环节，团队需部署自动化安全工具，在攻击行为实施前对其进行拦截，最大限度降低企业系统被入侵的可能性。

3. 检测

企业需明确，没有任何系统是绝对坚不可摧的。因此需投入技术资源，部署能快速识别突破预防措施的攻击行为的工具，从而控制潜在损失。

4. 响应

当安全事件发生时，优秀的企业能够快速遏制威胁扩散、调查事件原因、恢复受影响的系统，并采取补救措施防止同类事件再次发生。

检测与响应环节的处理速度至关重要。安全团队会通过监测平均检测时间（MTTD）、平均遏制时间（MTTC）、平均响应时间（MTTR）等指标，持续优化安全运营工作。

主动预防是安全防护的核心关键

核心结论十分明确：做好主动预防环节的工作，是降低安全事件升级为数据泄露事故的关键因素。

通过对预防、防护、检测、响应全攻击生命周期进行高效管理，即便遭遇网络攻击，企业的抗风险能力也能得到大幅提升，数据泄露发生率也会显著降低。

这也为安全部门负责人提出了一个重要问题：你是否在通过上述指标衡量安全运营团队的工作表现？是否能实现企业全攻击生命周期各环节的安全可视？厘清这些问题，能帮助企业发现安全体系中的漏洞，找到最关键的防护强化方向。

Bitdefender

安全工具繁杂引发的运营难题

工具繁杂是现代企业网络安全运营面临的最突出挑战之一，这一问题不仅会推高安全投入成本，还会大幅增加运营复杂度。IBM 的研究显示，企业平均会使用 83 款不同的安全解决方案；52% 的安全从业者认为，工具繁杂是阻碍安全运营工作高效开展的最大因素。

企业常用的安全工具主要包括以下类别：

- 攻击面管理工具：用于监控各类企业资产；
- 防护工具：如终端、邮件、网页、网络安全防护工具等；
- 检测技术工具：部署于企业所有入侵风险点与资产节点；
- 安全事件与事件管理平台：对其他工具发出的告警信息进行分析研判；
- 响应与恢复工具：助力遏制、分析攻击行为，并对攻击造成的损害进行补救。

企业部署繁杂的安全工具，本意是实现全攻击生命周期的防护覆盖，让每款工具各司其职。但遗憾的是，工具数量过多会引发运营内耗、推高成本，还需要专业度极高的安全运营人才 —— 这类人才不仅薪资成本高，招聘和留存也存在较大难度。更关键的是，每新增一款工具，都会扩大企业的攻击面，增加因配置失误被攻击者利用的风险。

上述研究结论也印证了工具整合与精简的重要性：简化复杂的安全运营环境，既能降低企业的运营风险、提升防护效果，也能从长期角度降低安全投入成本。

平台化方案破解工具繁杂难题

解决工具繁杂、运营复杂问题的理想方案，是搭建一体化网络安全平台。理论上，该平台可将多种安全功能整合至单一的集成环境中，实现全攻击生命周期内预防、防护、检测、响应环节的流程简化，从而降低运营复杂度、节约成本。

当然，全功能整合的理念也存在一定局限性，没有企业能够（也不应）将所有工具和流程都强行纳入单一平台。拥有充足预算和庞大安全运营团队的大型企业，通常会部署数十款专业安全工具，能够承担由此带来的复杂度；对这类企业而言，工具的落地使用基本不存在问题，即便多工具运营会造成效率损耗、扩大攻击面，其专业的人员团队也能进行有效管理。

而对于 IT 与安全团队人员精简的中型企业而言，平台化方案的价值则尤为突出。这类企业中，工具繁杂会引发巨大风险：配置失误、响应延迟、防护覆盖漏洞等问题，都可能快速升级为重大安全事件。合适的一体化平台能够整合核心安全功能、淘汰冗余工具、实现集中化管理，让小团队也能拥有与大型企业安全运营团队相当的工作效率和防护规模。

降低复杂度、整合核心安全能力，是一体化平台的核心优势。借助这一方案，中型企业无需依赖庞大的专业安全团队，也能实现全面的企业安全防护；同时，平台能实现全攻击生命周期的安全可视，自动化完成核心安全工作，简化检测与响应流程。

尽管一体化平台并非放之四海而皆准的解决方案，但对于被工具繁杂、资源不足问题困扰的企业而言，精心选择的平台能让混乱的安全运营环境变得流程化、高效化、易管理。简言之，这类平台能以更低的运营复杂度，为企业提供企业级的安全防护能力。

Bitdefender

GravityZone：极简运营的安全防护方案

针对工具繁杂、运营复杂、网络安全成本持续攀升等痛点，Bitdefender研发了 GravityZone 安全平台。该平台兼具各类专业安全工具的防护优势，且无需企业投入高额的运营成本，也无需组建庞大的安全专业团队。

GravityZone 的研发从源头就确立了三大核心目标：

1. 实现全威胁 / 攻击生命周期的全面防护

平台围绕预防、防护、检测、响应全环节，为企业提供一站式安全防护能力，确保企业能在攻击的各个阶段开展有效防御，即便遭遇安全事件，也能大幅降低数据泄露的概率。

2. 简化安全运营工作

通过简化安全运营流程，助力企业团队高效达成安全防护目标，同时将运营风险降至最低。将核心安全功能整合至单一集成环境，大幅降低了传统多单点工具管理模式下的运营复杂度、成本与工作负担。

3. 依托成熟可靠的前沿安全技术s

平台以Bitdefender实验室为核心技术底座。凭借 16 余年的人工智能技术创新积累，该实验室每日分析超 50 万个新型威胁变体，打造了一套完善的预防与防护技术体系，助力人员精简的企业团队高效落地端到端的网络安全防护。

Bitdefender的安全技术已通过数百次独立机构测评验证，核心成效包括：99.3% 的威胁响应率、安全耐力测试满分、100% 的攻击链可视性，以及行业最高的 93% 可执行报告率，同时告警信息发送量处于行业最低水平。

Bitdefender

GravityZone 如何强化全攻击生命周期的安全防护

GravityZone 将预防、防护、检测、响应能力整合至单一平台，助力人员精简的 IT 与安全团队在全攻击生命周期内降低安全风险、提升运营效率。

预防环节

平台通过实现企业全攻击面的持续可视，强化企业的风险降低策略。它能精准识别系统漏洞、配置失误、高风险操作行为与高价值防护目标，助力企业根据风险严重程度和潜在影响，优先开展补救工作。

测试数据显示，Bitdefender的主动加固与攻击面缩减技术（PHASR）能将特定类型的攻击行为减少 95%。

同时，平台能将企业资产与监管框架进行匹配，生成合规评分、识别合规漏洞并提供可执行的改进建议，助力企业强化合规管理工作。其自动化报告功能既能体现风险管理体系的投资回报率（ROI），也能为审计工作提供依据，让企业管理层直观看到企业安全态势的改善效果。

防护环节

企业可借助 GravityZone 的多层防护技术，对所有资产和入侵风险点的威胁进行自动化拦截。从源头阻止攻击者侵入企业系统，既能降低安全事件的发生概率，也能减轻安全团队的应急响应负担。

独立测评证实，GravityZone 防护效果优异、检测精准，且误报率极低。某比特梵德客户反馈，部署该平台后，与终端相关的安全事件数量下降了 80% 至 90%。

防护作为主动防御的第二道防线，能最大限度降低数据泄露概率，让安全团队在为企业提供全面防护的同时，将精力聚焦于更高优先级的工作。

检测环节

即便攻击行为突破了企业的主动预防措施，GravityZone 也能通过关联分析所有威胁载体和资产节点的告警信息，快速检测出攻击行为；同时，平台能识别受管与非受管设备中的异常行为、横向移动攻击与凭证盗用行为。

平台会对各类安全信号和告警信息进行分级与关联分析，并以人性化的可视化形式呈现安全事件，助力团队快速开展响应与遏制工作；对高价值和高风险资产的场景化可视，能提升决策效率，而自动化的攻击路径分析则能大幅缩短事件调查与解决的时间。

> 某客户表示，借助 GravityZone 的安全洞察，其安全事件的调查与解决时间缩短了 50%。

这套全方位的检测方案，能让企业实现威胁的早期发现与快速响应，从而控制攻击造成的损失与业务中断影响。

响应环节

安全团队必须具备快速遏制、调查并补救攻击行为的能力。GravityZone 支持一键操作，可实现终端隔离、恶意进程终止与系统恢复；同时，平台能开展事后事件分析，挖掘事件根本原因、梳理攻击路径，为后续的补救工作提供依据，防止同类事件再次发生。此外，平台的全面报告功能，既能满足监管机构的事件上报要求，也能实现与企业利益相关方的透明化沟通。

将快速的威胁遏制与详尽的取证分析相结合，能最大限度减少企业的业务停机时间、经济损失和声誉风险，确保团队在遭遇安全事件时，仍能维持企业的业务连续性。

Bitdefender

MDR 托管检测与响应服务

托管检测与响应服务能为企业提供 7×24 小时的安全运营支持，助力企业突破资源与专业能力的限制。企业可选择借助该服务补充现有安全团队的能力，也可将安全运营工作完全外包给Bitdefender的专业团队，从而减少专业人才的招聘与培训成本。

Bitdefender 的 MDR 服务入选 Gartner《托管检测与响应市场指南》，并在其用户评价平台获得 4.8/5 的平均评分。

Bitdefender 的 MDR 服务不止于发出告警 —— 专业团队会代表企业主动响应并遏制攻击行为，同时为企业内部团队提供专业指导，助力其提升安全能力，包括定制化改进建议、威胁狩猎支持，以及前瞻性的战略洞察，帮助企业应对不断演变的网络威胁。

借助 MDR 服务，人员精简的 IT 与安全团队能实现与大型企业同行、竞争对手相当的安全防护水平，同时因企业环境得到持续监控而拥有更强的安全信心。

某客户表示，自建安全运营中心（SOC）的成本，是使用该服务的 5 倍；另有客户反馈，Bitdefender的 MDR 服务为其节约了 40% 的运营成本。

Bitdefender 实验室：核心技术支撑

Bitdefender的所有产品与服务，均以Bitdefender实验室研发并维护的创新安全技术为核心支撑。这些技术不仅为 GravityZone 平台提供动力，还被超 200 家科技厂商和服务提供商授权应用于其自有产品中。

实验室的技术性能与防护效果持续通过第三方独立机构验证，Bitdefender也在各类测评中始终保持高评分，累计参与超 450 次公开测评并取得优异成绩。

Bitdefender近半数员工投身研发工作，技术创新则依托与高校的合作展开，聚焦神经网络、量子计算、深度伪造等前沿领域；同时，实验室与全球执法机构保持紧密合作，已与欧洲刑警组织、欧洲司法组织、国际刑警组织等 32 家机构建立合作关系。

这些多方验证与合作，确保 GravityZone 始终处于威胁预防、防护、检测与响应领域的前沿，为Bitdefender的客户提供领先的安全防护能力。

Bitdefender

以精简团队实现企业级安全防护

GravityZone 专为人员精简的 IT 团队打造，在实现全面的企业级安全防护的同时，实现了运营效率的优化。

总结来看，企业部署 GravityZone 后，能实现五大核心价值:

1. **全网络攻击生命周期的风险显著降低**

平台提供全方位的预防、防护、检测与响应能力，其安全性能已得到验证 —— Bitdefender的产品与服务入选Gartner、Forrester、IDC 等机构发布的 20 余份最新分析报告

2. **快速实现价值落地**

平台部署流程便捷、上手快速，能让企业立即掌握自身安全风险情况，从而合理规划漏洞补救与风险缓解工作的优先级。在高德纳同行洞察平台，GravityZone 的集成与部署能力获得 4.6/5 的高分评价。

3. 提升精简团队的运营效率与工作产能

平台拥有单一且直观的操作界面，具备丰富的自动化功能。基于这一特性，普通 IT 人员能快速完成基础网络安全工作，而高级功能则可由专业安全人员按需使用。某高德纳同行洞察平台的客户反馈，切换至Bitdefender方案后，其日常安全管理工作的耗时减少了 70%。

4. 降低总拥有成本

通过工具整合与运营优化，企业对高成本专业安全团队的依赖度大幅降低。某客户实现了 120% 的投资回报率，另有客户在不降低防护效果的前提下，将运营成本削减了 50%。

5. 为企业发展提供可拓展的安全投资方案

灵活的模块化授权模式，加上持续的研发更新，让平台能随新型威胁的演变不断升级；同时，企业可根据自身安全体系的成熟度，逐步增加所需的功能模块。

上述价值充分证明，GravityZone 能全面提升企业全攻击生命周期的安全态势，同时为企业带来可量化的投资回报率和运营成本降低效果。

欢迎访问Bitdefender中国官网，了解 GravityZone 如何为企业打造定制化的安全防护方案，以极简运营消除安全复杂度、降低安全风险，且该方案在各类独立机构测评中始终保持领先。

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