Bitdefender

Gravityzone

买家指南

如何选择合适的安全平台

Bitdefender

安全平台是否适合你的企业?

人员精简的中型企业，其 IT 与安全团队面临的网络安全挑战，与那些坐拥充足预算、配备专业安全风险管理团队的大型同行及竞争对手并无二致。尽管企业的攻击面或许不及大型企业，但在过去数年中也必然大幅扩张，成为勒索软件及其他网络攻击者的主要目标。

而中型企业面临的业务挑战还远不止于此。威瑞森《2025 年数据泄露调查报告》指出，30% 的已报告数据泄露事件均牵涉第三方。供应链攻击的高发，迫使企业对商业合作伙伴展开严格的安全审核，要求对方证明其已建立完善的安全防护措施。若企业自身无法满足安全审核要求，不仅会将业务拱手让给竞争对手，即便侥幸通过，也会因安全态势审核导致的合作入驻流程延长，错失营收良机。

如何在竞争中保持优势，避免因资源和预算差距被对手超越?

安全平台或许正是破局之道 —— 它不仅能筑牢企业的安全防线，还能让企业向合作方清晰证明自身的安全防护能力。这不仅能加快企业的营收落地速度，若身处受监管行业，还能大幅降低合规审计的工作成本。

本选购指南将梳理六大核心步骤，助力企业判断安全平台是否为适配的选择：

1. 企业当前的安全体系处于何种状态?
2. 采用安全平台是否为正确的解决方案?
3. 如何甄选适配的安全平台?
4. 如何选择合适的平台供应商?
5. 如何最大化发挥所选平台的价值?
6. 验证平台选择的合理性

完成上述六大步骤并确认安全平台适配企业发展需求后，本指南的最后一部分将列出企业需向入围供应商提出的核心问题，确保最终选择能精准匹配企业的安全需求。

Bitdefender

1 企业当前的安全体系处于何种状态？
2 采用安全平台是否为正确的解决方案？
3 如何甄选适配的安全平台？
4 如何选择合适的平台供应商？
5 如何最大化发挥所选平台的价值？
6 验证平台选择的合理性

第一步：企业当前的安全体系处于何种状态

在调整安全体系之前，企业首先需要明确：是否需要做出调整？调整的原因是什么？

实现攻击面的全面可视，是了解企业整体安全态势的关键，市面上也有诸多技术方案能提供相关支持。企业或许已部署补丁管理方案和配置管理数据库，但受预算限制，网络威胁暴露管理平台（CTEM）这类企业级工具往往难以企及。即便有能力部署，这类工具也会增加安全体系的复杂度，给本就人员精简的 IT 与安全团队带来沉重负担。

核心术语定义

安全态势：企业信息安全防护的整体就绪状态，包括所有硬件、软件、服务及信息的状态可视性。

攻击面：网络攻击者可利用的、用以实现攻击目的的所有载体总和。

借助简化安全框架，开展自我评估

众多机构发布了安全框架和指导方案，助力企业了解自身安全现状、发现核心安全漏洞，其中包括国际标准化组织（ISO）、欧盟网络安全局（ENISA）、美国国家标准与技术研究院（NIST）。部分机构还专为中小及中型企业打造了简化版安全框架。

核心行动：梳理企业现有安全技术架构

无论是否参照标准化框架，在考虑更换或新增安全技术之前，企业的首要任务是梳理现有安全体系 —— 明确当前已部署哪些措施，用以保护核心资产及易被攻击者利用的初始接入点。

企业可从以下维度梳理安全防护覆盖情况：

- 终端：受管终端与非受管终端
- 身份认证：人工身份与非人工身份
- 云环境：云基础设施与 SaaS 应用
- 邮件：邮件网关与邮件平台
- 网络：网络边界与内部网络

Bitdefender

防护完善	防护存在漏洞
若上述维度均实现全面防护，说明企业安全基础良好。此时需评估现有防护措施的有效性，若为单点解决方案，还需分析将其整合至安全平台是否能实现价值提升。	若存在防护漏洞，需根据漏洞的风险等级确定整改优先级，综合考量漏洞被利用的可能性及一旦被利用可能造成的事件影响。随后需决定：是部署单点安全解决方案，还是通过安全平台满足防护需求。

Bitdefender

第二步：采用安全平台是否为正确的解决方案

将安全工具整合至统一平台并非全新理念。早在 2023 年，网络安全媒体 eSecurity Planet 就曾报道， Gartner 的一项调查显示，75% 的安全产品采购者正推进供应商整合，这一趋势也推动供应商将单点产品整合至统一安全平台。而推动这一整合的首要因素，是降低安全体系复杂度，而非直接削减成本。

减少单点安全工具的数量，不仅能缩小企业攻击面，加之安全平台通常具备深度集成和告警关联能力，企业还能大幅缩短攻击响应与遏制的时间。

不过，安全平台的普及程度仍存争议，尤其是对于拥有充足安全预算和专业团队的大型企业而言。

对于人员精简的中型企业，降低安全体系复杂度是重中之重，但同时绝不能以牺牲安全态势为代价。在掌握自身安全现状、明确理想安全状态后，企业需综合权衡单点解决方案与安全平台两种模式的利弊。

下载参考：Bitdefender解决方案指南 —《如何以精简团队搭建完善的网络安全体系》

安全平台的核心优势	
消除体系碎片化	实现预防、防护、检测、响应的一体化管理，降低全网络攻击生命周期内、企业所有数字与非数字资产的安全风险。
降低运营复杂度	工具数量减少，直接缩小攻击面，降低配置失误概率及潜在漏洞产生的可能性。
提升运营效率与产能	单一操作界面简化管理与运营流程，缓解控制台操作疲劳，让各项安全工作得以高效、便捷开展。
优化事件响应能力	多工具深度集成提升威胁可视性与告警关联度，减少误报，缩短攻击遏制与响应时间。
简化合规管理流程	单一数据源生成标准化报告，大幅降低审计工作负担。
降低总拥有成本	减少采购、日常维护、技术支持及人员培训成本，实现运营效率提升。

安全平台的潜在不足	
单一供应商依赖风险	过度依赖单一供应商会集中风险，若供应商出现服务中断或商业变动，可能导致企业安全服务水平下降。
潜在单点故障	平台若发生故障，可能引发企业整体安全防护体系的瘫痪。
供应商锁定效应	若所选平台无法满足企业未来发展需求，切换至其他供应商的过程可能会十分繁琐。
功能覆盖漏洞	没有任何一款安全平台能满足企业所有的安全需求，部分专项功能的适配性可能不及同类单点产品。
初期部署与迁移成本高	迁移至新平台需要投入较高的实施成本，且需要一定时间才能实现价值落地

Bitdefender

1 企业当前的安全体系处于何种状态？

2 采用安全平台是否为正确的解决方案？

3 如何甄选适配的安全平台？

4 如何选择合适的平台供应商？

5 如何最大化发挥所选平台的价值？

6 验证平台选择的合理性

第三步：如何甄选适配的安全平台

市面上的安全平台种类繁多，企业可通过自问以下核心问题，筛选出符合自身需求的平台：

该平台是否为大型企业安全运营中心（SOC）量身打造？	这类平台通常围绕安全信息与事件管理系统（SIEM）、安全编排自动化与响应平台（SOAR）打造，部分还整合了网络检测与响应（NDR）功能，能为复杂业务环境的企业提供卓越的功能支持，但需要专业的安全风险管理团队才能发挥其最大价值。
该平台是否新增了无意义的复杂度？	企业用不到的功能会增加体系复杂度、扩大攻击面，非但无法降低风险，反而可能让风险攀升。
该平台是否因功能繁多而定价过高？	企业需明确自身的核心需求，供应商会持续新增功能以体现价值，但企业无需为无用功能买单。
该平台是否提供灵活的授权模式？	企业通常无需在初期就全盘采购平台的所有功能，但若选择该平台，需确保能随着安全体系的成熟，灵活新增集成化功能。
该平台是否具备强大的AI人工智能自动化能力？	人员精简的 IT 与安全团队需要全方位的技术支持，自动化不仅是实现快速响应的关键，还能为事件调查与系统恢复提供全程指导。
该平台是否能覆盖企业的核心资产？	平台需实现对终端、网络、云环境、身份认证及邮件的全面安全防护。
供应商是否提供托管检测与响应（MDR）服务？	MDR 服务是重要补充，能确保企业在需要扩充团队时，获得熟悉该平台的安全运营专业人员支持。

Bitdefender

优选以终端检测与响应（EDR）为核心的 XDR 平台

对于人员精简的中型企业，以 EDR 为核心打造的扩展检测与响应（XDR）平台，能在安全防护与体系复杂度之间实现最佳平衡。
企业也可考虑由 NDR 及 SIEM、SOAR 等通用安全运营中心工具演进而来的平台，以下将对比各类平台的核心优劣。

三类主流安全平台核心指标对比

对比维度	以 EDR 为核心的 XDR 平台	以 NDR 为核心的 XDR 平台	SIEM & SOAR 平台
部署方式	可作为终端安全方案的一部分轻松部署，多数支持云端 / 本地控制台双选项	在网络中部署硬件或虚拟设备，支持直连或 SPAN 端口接入，多数支持云端 / 本地控制台双选项	多数支持云端 / 本地控制台双选项
集成与覆盖	以 EDR 为基础，通过代理、连接器和 API 获取网络、身份认证、云环境、邮件的补充信号，在供应商生态内实现全面覆盖，捕捉高价值核心信号（如身份认证相关）	以 EDR 为基础，为各网络段增设探测节点，第三方工具的数据接入能力取决于供应商	需完成复杂集成，将终端、网络、身份认证、云环境、邮件等所有资产和安全执行点的日志数据接入 SIEM，SOAR 剧本的创建数量取决于企业业务环境的复杂度
价值落地时间	终端初期部署便捷，仅需短期被动学习即可建立行为基线	需根据网络架构部署相应数量的探测节点，价值落地时间受其影响	取决于业务环境复杂度、监控资产的日志采集量、所需的调优工作及剧本数量
攻击可视性	实现终端攻击的全面可视（多数攻击者会通过攻陷终端获取敏感信息），其他资产的可视性取决于所使用的代理、连接器和 API	可清晰可视非受管终端的攻击行为（如工业控制系统遭破坏），能在攻击抵达受管终端前，检测到受感染非受管设备的横向移动企图	配置优化后，可实现告警关联及全环境深度洞察，提前发现初始接入、横向移动及受攻陷资产的异常情况
防护能力	主流 EDR 平台均内置终端防护功能，可在攻击执行前实现拦截	可通过网络探测节点检测横向移动行为，其他资产的可视性取决于所使用的代理、连接器和 API；NDR 可根据部署方式阻断部分攻击	依赖第三方终端防护平台（EPP）及其他安全措施，实现终端、邮件、网页等场景的攻击拦截
检测能力	依托开箱即用的深度 EDR 能力实现终端核心检测，包括人工智能行为分析，同时结合其他代理、连接器和 API 的信号进行关联分析，提升检测精准度	依托深度数据包检测和人工智能行为分析实现网络核心检测，同时结合其他代理、连接器和 API 的信号进行关联分析	关联规则高度可定制且功能强大，但需要手动配置、调优并持续维护

检测效能 / 精准度	检测效能优异，误报率低，结合补充信号丰富场景信息后，精准度更高	通常误报率较高、告警信息繁杂，需要大量调优工作才能保证检测精准度	检测效果取决于采集的数据质量，需大量调优工作保证检测精准度
响应能力	支持自动化、指导性的攻击遏制，通过终端隔离、进程终止等简易操作，将对业务的影响降至最低	对业务的影响取决于部署方式；终端响应选项有限，依赖代理及与 EPP 的集成效果	SOAR 具备强大的编排 / 自动化能力，但需要创建剧本，并与 SIEM 及其他外部工具完成集成
易用性	不同供应商的产品体验差异较大，理想平台应包含可视化面板、标准化工作流、操作指导，且能提供查询工具，支持深度事件调查	与 EDR 平台类似，此外 NDR 平台向来告警信息繁杂，需要专业人员进行事件分析与响应	需专业人员搭建并维护与企业所有资产、安全执行点的集成；使用 SIEM 需掌握查询技术，使用 SOAR 需具备剧本创建能力以实现响应自动化
总拥有成本	主流终端防护产品均内置 EDR 功能，仅需为连接器、代理、API 接入支付少量额外成本；多数提供云端控制台，无需投入昂贵的基础设施；管理成本低，多支持生成人性化报告，无需专业安全运营人员即可实现快速事件响应	需在本地部署并维护硬件 / 虚拟设备；多数提供云端控制台，减少基础设施及部署成本；NDR 的事件分析与响应需要高薪聘请专业安全运营人员	需投入基础设施、存储成本，且需要专业安全运营人员进行调优和日常维护；若能与企业现有复杂环境深度集成，可实现现有安全工具的投资回报率提升

Bitdefender

1 企业当前的安全体系处于何种状态？

2 采用安全平台是否为正确的解决方案？

3 如何甄选适配的安全平台？

4 如何选择合适的平台供应商？

5 如何最大化发挥所选平台的价值？

6 验证平台选择的合理性

第四步：如何选择合适的平台供应商

上述分析已明确：对于人员精简的中型企业，以 EDR 为核心的安全平台是最佳选择。接下来，企业在筛选入围供应商时，不仅要考量平台的检测与响应能力，还需关注优质 XDR 平台所具备的增值功能 —— 这类功能能让平台的价值超越单纯的 XDR 工具，为企业带来更多赋能。

参考第三方测评，确认检测精准度

MITRE ATT&CK"

验证平台的检测效能与精准度

上述对比可见，部分 NDR 平台的告警信息繁杂，其实 EDR 平台也存在这一问题。因此企业的核心考量不仅是平台的威胁检测能力，更包括其区分 “异常行为” 与 “威胁行为” 的能力。若人员精简的 IT 与安全团队需要手动处理数百条告警，进行关联分析和优先级排序，那么在团队完成遏制前，安全事件极有可能升级为数据泄露事故。

企业应优先选择经验证、具备高精准度检测能力的平台，即检测结果准确、误报率低的平台，可参考 MITRE ATT&CK 框架的测评结果。

实现全攻击生命周期的防护覆盖

部分 XDR 供应商认为，安全事件的发生是必然的，因此将核心精力放在检测与响应环节。但对于没有安全运营中心、团队人员精简的企业而言，这一理念并无实际价值。企业的核心目标是：尽可能阻止威胁演变为安全事件，避免给团队带来繁重的响应工作。

参考第三方测评，
验证平台防护效能

AV comparatives

AV-TEST The Independent IT-Security Institute Magdeburg Germany

在攻击执行前拦截尽可能多的威胁

企业的首要且最易落地的举措，是选择防护能力最优的平台 —— 在攻击执行前拦截尽可能多的威胁。建议优先选择在第三方效能测评中表现始终优异的供应商。

Bitdefender

将主动预防作为核心防护策略

曾几何时，能帮助企业了解并管理攻击面、安全态势及漏洞的预防技术，是中型企业难以企及的。如今，部分 XDR 供应商通过在平台中集成这类核心预防能力形成差异化竞争。而那些聚焦大型企业的供应商，默认客户已部署相关单点解决方案。因此，中型企业应优先选择专为自身优化的 XDR 平台。

这类平台能为企业安全体系带来实实在在、可量化的价值：

- 主动降低攻击成功的风险；
- 量化企业持续开展的风险降低工作成效；
- 向企业管理层直观展示安全态势的改善情况；
- 降低安全事件的发生概率，减轻 IT 与安全团队的响应负担；
- 显著降低合规达标与持续合规的成本和工作难度；
- 降低网络安全保险的采购成本与审核难度。

企业应选择这样的平台：并非简单捆绑合规管理、攻击面管理、漏洞管理、补丁管理功能，而是将这些功能与风险分析、终端加固等攻击面缩减工具深度集成。

集成是发挥这类工具价值的关键，企业需警惕那些仅通过收购获得技术、却只简单更换操作界面的供应商。

确保差异化功能不新增无意义复杂度

企业甄选平台的核心目标，始终是简化安全运营、降低安全风险。因此在评估入围供应商时，企业需时刻牢记这一目标，警惕新增功能可能偏离核心需求。但同时也需明确：增值功能并不等同于复杂度，企业需在二者之间找到平衡，优先选择为中型企业优化各类新增功能的平台。

Bitdefender

第五步：如何最大化发挥所选平台的价值

确保所选供应商能为企业团队及安全体系提供赋能与支持，是发挥平台价值的关键。

托管检测与响应（MDR）服务是重要的增值服务，能为人员精简的 IT 与安全团队提供补充支持，通过强化企业整体安全体系降低风险。企业首先需明确自身是否需要 MDR 服务，其核心价值包括：

- 借助供应商安全运营中心的专业能力，实现 XDR 平台投资回报率的最大化；
- 突破人员编制限制，解决专业人才招聘与留存的难题；
- 为人员精简的 IT 与安全团队提供所需支持，让团队将精力聚焦于高投资回报率的工作；
- 显著降低合规达标、持续合规及网络安全保险采购的成本与工作难度。

关注供应商的差异化服务能力

企业可选择具备灵活服务模式的 XDR 平台供应商，支持后续新增 MDR 服务。需注意的是，并非所有的配套服务都同等优质，即便企业暂不订阅 MDR 服务，也应提前评估供应商的 MDR 服务能力。

值得关注的差异化服务包括：

- 提供专业优化建议，助力企业完善预防性安全管控措施、缩减攻击面；
- 支持直接对接专业的网络威胁情报团队，开展个性化、专属的威胁研究；
- 定期开展威胁狩猎，主动发现企业环境中的新型威胁，以及躲避防护、正在悄悄推进攻击的网络攻击者；
- 并非仅作为告警聚合工具，而是能凭借预先获批的操作权限，代表企业快速响应、遏制攻击，将业务影响降至最低；
- 开展事件根本原因分析，助力企业快速恢复系统、恢复正常业务运营

Bitdefender

1 企业当前的安全体系处于何种状态?

2 采用安全平台是否为正确的解决方案?

3 如何甄选适配的安全平台?

4 如何选择合适的平台供应商?

5 如何最大化发挥所选平台的价值?

6 验证平台选择的合理性

第六步：验证平台选择的合理性

即便是拥有专业安全团队的大型企业，也在推动工具整合以降低体系复杂度。这就导致部分聚焦大型企业的供应商，将一系列松散集成的单点产品包装为安全平台，这类平台功能臃肿，中型企业往往因时间、人员、技术能力限制，无法发挥其价值。

市面上不乏适配中型企业的安全平台，但企业需谨慎选择，重点考量以下四点：

- 平台是否能实现全威胁生命周期的安全防护 —— 涵盖预防、防护、检测、响应全环节?
- 平台是否能简化安全运营，为企业的工具整合策略提供支持，降低运营风险?
- 平台是否具备灵活性，既能支持企业当前的迁移工作，又能随着安全体系的成熟新增功能，匹配企业业务发展需求?
- 平台供应商是否能提供所需的支持服务，助力人员精简的企业团队，随着安全体系的成熟一同成长?

参考第三方测评，验证选择合理性

这是企业甄选安全平台的最后一步。

企业应重点参考同类型企业的案例与测评，大型企业的正面评价参考价值有限 —— 毕竟二者的业务环境和安全体系相去甚远。高德纳同行洞察平台（Gartner Peer Insights）是优质的第三方测评来源，该平台还会为各领域表现优异的供应商颁发客户之选奖项。

企业也可参考Gartner市场指南、魔力象限等行业分析师报告，但需警惕排名陷阱：这类排名往往基于企业级功能评估，并非为中型企业量身打造。不过，供应商能入选这类报告，也能证明其行业认可度与实力。

Bitdefender

向安全平台供应商提出的核心问题

通用问题	↳ 平台是否能通过预防、防护、检测、响应核心工具，降低企业全攻击生命周期的风险 ↳ 平台是否能实现对终端、身份认证、云环境、网络、邮件所有资产的防护? ↳ 平台的部署与管理对企业团队而言是否简便易操作? ↳ 平台将通过哪些方式降低企业的总拥有成本? ↳ 平台的授权模式具备怎样的灵活性?
预防能力相关问题	↳ 平台是否能报告并展示企业的风险降低成效，以及合规达标情况? ↳ 平台是否能识别不合规项，并提供可执行的改进建议以弥补漏洞? ↳ 平台是否集成了以下工具的核心预防能力: - 网络资产攻击面管理（CAASM） - 持续威胁暴露管理（CTEM） - 云安全态势管理（CSPM） - 外部攻击面管理（EASM） ↳ 平台是否能根据风险的严重程度和潜在影响划分优先级，提供可执行的洞察、建议及指导性补救措施? ↳ 平台具备哪些攻击面缩减能力？例如补丁管理、终端加固等。
防护能力相关问题	↳ 在第三方技术测评中，平台的防护效能与检测精准度表现如何? ↳ 供应商的威胁研究团队具备哪些专业资质? ↳ 平台的防护能力覆盖哪些资产?

Bitdefender

检测与响应能力相关问题	↳ 平台能从企业基础设施的哪些资产中采集告警信息？ ↳ 平台是否能可视化展示企业内易被攻击者盯上的资产？ ↳ 平台内置了哪些自动化功能，助力告警的关联分析与优先级排序？ ↳ 在检测效能、精准度及告警量相关的第三方测评中，平台表现如何？ ↳ 企业在响应安全事件时，可采取哪些措施将业务影响降至最低？ ↳ 平台提供哪些根本原因分析工具？ ↳ 平台是否支持生成人性化报告，并具备深度查询能力？
MDR 服务相关问题	↳ 供应商为提升企业安全态势提供的建议详细程度如何？ ↳ 企业是否能直接对接供应商的威胁研究团队？ ↳ 供应商为企业环境开展威胁狩猎的频率是多少？ ↳ 供应商是否能代表企业开展响应工作？其采取的操作是否精细化，能将企业业务影响降至最低？ ↳ 供应商是否会开展事件根本原因分析？ ↳ 供应商是否提供网络安全质量保证服务？

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