Bitdefender

为什么安全团队需要 EDR 端点检测和响应

www.bitdefender-cn.com

目 录

端点保护，必不可少但能力有限

预防和阻止已经不够

总体而言，当前顶级安全厂商的端点保护解决方案已经非常出色。 与过去相比，现代的端点保护工具可以比以往阻止更多的恶意软件和更多类型的威胁。 顶级的安全厂商已经结合了人工智能（AI），机器学习（ML）和自适应启发式技术，远远超出了静态且易于绕过的“病毒特征库”防护。

现在，预执行前检测，执行时阻止，执行后终止是顶级端点保护产品的必备功能。 总的来说，误报更少，检测更快更精准，能对检测的内容和原因进行更好的解释。 但是，每个安全领导者都应牢记，端点保护有其不足之处。 当规划网络安全战略时，您应该详细了解。

端点保护的不足之处

在每次攻击开始之前，检测和阻止攻击，查杀所有病毒是任何安全团队都希望达到的理想状态，但是回顾历史，证明这是一个遥不可及的目标 。 防护率从未达到100%， “完美的安全”永远无法实现。 无文件攻击和浏览器攻击不会在硬盘中存储任何文件，许多高级的，多阶段，多向量攻击只会以某种方式展开，看起来像正常的行为，从而使检测它们变得异常困难，甚至无法阻止。 其中许多攻击只能在进行中或事后检测。 具体来说，端点保护的不足之处包括：

- **检测的太少，太迟了：**端点保护可能会进行检测，但仅在恶意软件已经部分或全部成功到达计算机时，才检测，且只告诉你已经阻止，要么就是没有检测到任何威胁，攻击成功，计算机失陷，威胁运行。
- **丢失关联的线索：**端点保护可能会生成许多警报，但是每个警报都是独立的，没有关联。 分析师看不到完整的事件或相关事件链。
- **出了问题，该怎么办？** 恶意软件可能已被端点保护阻止，但分析人员不知道该漏洞的严重程度，它是否存在于其他计算机上，或者是否需要清除其他任何内容。

为什么需要在防护堆栈中使用EDR

消除关键的安全漏洞

端点保护对于合规性以及消除外部恶意软件和常见威胁是必需的，但对于防御高级，复杂或针对性的攻击，还远远不够。 如果您拥有重要的知识产权，个人身份信息PII/个人健康信息PHI，客户或财务数据，那么EDR不再是奢侈的东西，现在已成为必需品。

对高级威胁的防护不足

端点保护通常无法提供针对高级威胁的足够防护。 复杂的攻击通常使用正常的行为，例如：打开文档，建立远程连接，从Internet下载资源等，但随后才表现出可疑或恶意行为。

缺乏警报分类和响应功能

端点保护会生成许多警报，但看不到攻击的所有元素。 尽管每个警报都代表端点保护阻止了威胁，但是安全团队可能需要采取后续措施，进行调查和采取纠正操作，而不是仅仅删除发现的恶意文件。 如果你使用端点保护方案，你从哪里开始着手?

发现漏洞后响应缓慢

端点保护提供很少的攻击预警信号，几乎没有有关威胁评估的详细信息。 用户可能会注意到计算机的行为异常，或者网络工程师可能会看到异常的流量模式或数据高峰，但是没有提供有关因果关系的详细信息。

无法识别根本原因并防止攻击再次发生

好的，您的端点保护解决方案已经阻止了恶意软件。 但是，还不是庆祝的时候。 您是否可以确定整个攻击是被阻止的还是仅某些攻击被阻止了？ 其余的攻击是否逃避了检测并攻击成功了？攻击的入口点是什么？ 它从哪里来的？ 我们如何关闭那条攻击链路，使攻击不再发生?

无法了解攻击者使用的TTP/入侵指标IOC

这是一次性事件还是在企业中的许多受害机器上都有这样的事件，会不会是系统性事件？ 是否已经多次发生相同或相似的攻击？ 攻击是否仍在组织中的其他计算机上进行？ 您能否在整个系统范围内使用入侵指标进行搜索?

有没有关于主动改善安全状况的建议？您如何改善安全状况并加强防护，以防止将来被入侵？ 您是否可以识别会给您的组织带来风险的操作系统配置错误，应用程序漏洞和人为风险因素？ 一旦确定，您是否可以根据改进指标来衡量和修正?

EDR 商业驱动

以下是需要在您的防护武器库中添加EDR的主要商业驱动因素：

- 您无法确保100%防护高级入侵，以防止入侵者留在您的系统中
- 一旦发现潜在的入侵指标，您无法终止可疑活动或隔离受感染的计算机
- 您缺乏可操作的情报来采取行动，也没有循序渐进的建议来指导如何处理已识别的入侵行为
- 您缺乏集中的威胁数据库，无法跨系统进行协调的攻击分析和补救
- 您不了解基础架构面临的系统性风险，也不知道如何主动改善安全状况

EDR 产品类型

端点检测和响应提供单独的价值，并具有自己的优点，与端点保护相辅相成。 将这两种解决方案串联起来防护，可以防范规避防御的的最复杂攻击。 Bitdefender提供了丰富的EDR安全产品套装：

- 端点保护EPP集成EDR，Ultra Security旗舰版
- 独立的EDR套装，轻量级的解决方案，可与任何第三方端点保护解决方案兼容
- XDR，Ultra +网络流量安全分析
- MDR，外包式网络安全运营。MDR服务包含XDR，和Bitdefender安全分析师提供的7*24专业服务，持续监视网络的安全状态，主动猎杀网络威胁。

您如何评价您的端点保护工具?

所有端点保护解决方案都各有利弊，需要权衡利弊。 哪个陈述最能描述您的端点保护状况?

- 我对我的端点保护解决方案感到满意，但是我意识到它在调查和修复方面的局限性
- 我对当前的端点保护解决方案不满意，但是我现有的合同仍然有时间
- 当前的端点保护解决方案很糟糕，需要立即替换

如果您符合上述三种陈述，我们建议您立即升级到Bitdefender EDR，它未来带来了前所未有的安全能力，而且比您想象的更简单，更具成本效益。

独立的EDR

在以下情况下，安全领导者可能会认为独立EDR是端点保护的宝贵补充：

- 安全分析师缺乏对端点和网络上可疑和恶意活动的了解
- 现有的端点保护解决方案缺少EDR，XDR或MDR
- 需要与现有端点保护解决方案兼容，需要事件检测和报告功能
- 寻求具有轻量级代理且易于部署和管理的事件响应平台
- 希望简化安全工作流程，以进行威胁取证和端点补救

Bitdefender EDR

Bitdefender EDR提供了预防，检测，调查，响应和安全加固的组合。 它利用最新的尖端技术提供更高的可见性，收集和关联威胁信息，同时采用人工智能分析和自动化功能来帮助检测可疑事件。

攻击者及其相关战术、技术及流程TTP可见性

Bitdefender EDR提供了高级攻击检测和响应功能。 传统端点保护产品缺乏TPP的可见性。无法主动采取特定的补救措施，也没有集成应对这些攻击所需的工具。

MITRE ATT&CK 技术

MITRE ATT&CK是全球安全行业的标准，Bitdefender EDR集成了MITRE ATT&CK技术，可查看针对攻击的每个阶段的检测到的事件和单个警报，包括：执行，持久化，提权，防御逃避，访问凭据，发现，横向移动，收

集，命令和控制，以及泄露数据。 当EDR 与MITER ATT＆CK技术的结合使用时，您就可以清楚地看到完整的攻击画面，并了解覆盖范围的“空白”区域。

IOC/IOA搜索和关联

您通过什么样的迹象来查看机器是否受到攻击或感染？ 安全团队可以在EDR平台种查询整个组织中的各个攻击指标（IOA）和危害指标（IOC），以搜索受感染的计算机，这些计算机可能不会向其用户或安全管理员生成任何被入侵的外部证据。

根本原因分析和完整攻击可视化

从初始电子邮件攻击媒介到第一个客户端感染，提权，发现，横向移动，数据收集和泄露的完整逐个动作的播放。

防止再次被入侵

检查成功攻击（和部分成功）的攻击路径，并高亮攻击路径，你可以快速关闭这些入口和访问点，以便将来再次发生相同或相似的攻击。

一键解决警报分类和优先级

EDR可帮助安全团队快速识别事件并确定优先级，以进行操作和补救，通常采用一键操作来结束可疑进程，隔离恶意文件，将攻击者域名列入黑名单等。

减轻运营负担

Bitdefender EDR，易于部署，易于使用，无需专业的安全技能，也能轻松掌握，并且占用系统资源极低，大大减轻了客户的运营负担。该产品灵活，可扩展，可满足各种不同类型客户的安全需求，例如独立的EDR, 端点保护集成EDR， XDR，MDR等。

缩小网络安全技能差距

通过易于遵循的内置工作流程来帮助组织弥合网络安全技能的鸿沟，高效的安全响应能阻止持续的攻击并清除已造成的任何损害。 威胁朔源，和攻击根本原因分析，最大程度地提高了客户的响应能力。

管理和降低组织风险

Bitdefender EDR技术还可以帮助客户评估并最大程度地降低总体组织风险（特别是在系统配置错误，操作系统漏洞，应用程序漏洞和人为风险等方面），从而向安全团队准确显示出现风险的位置，并为快速缓解这些风险确定必要的任务优先级。

EDR vs. SIEM 工具

EDR针对安全团队进行了优化

EDR是端点保护和SIEM系统之间的“中间地带”。 SIEM工具功能强大，在大型企业中发挥着重要作用，但它们也很昂贵（要不断获取人员，进行运营和维护），通常它们无法进入中小型企业，不太适合中小型客户。

SIEM通常将重点放在特定的事件，离散事件或指标上，而不是为了支持完整的事件，攻击或活动，或事件之间的因果联系，进程或关系而设计的，这要由熟练的分析师来得出自己的结论，数据到底包含什么。 提示事件关系的数据可视化必须手动构建，从而导致团队中分析结果的差异。

SIEM不可操作。 它们汇总了单向数据馈送的结果，而没有返回原始系统的路径。 无法进行更新，也不能从SIEM工具中采取任何直接措施来执行修复。 新事件只会在旧事件之上发布。 这为熟练的分析人员提供了丰富的原始信息，以根据他们的技能和经验进行搜索，关联和得出自己的结论。

EDR专门用于检测和响应事件。 它会自动将单个警报升级为全面的事件，显示攻击各个阶段的因果链，然后直接从控制台执行调查和修复。 此外，EDR是“为所有人服务的”，即使缺乏安全技能的中小型企业的安全团队，也能轻松进行检测和响应。

EDR	安全信息与事件管理
专门用于显示端点安全事件	汇总通用安全事件和日志
双向数据流回原始系统	仅来自原始系统的单向数据流
预先建立的安全响应仪表盘	分析师必须建立自己的仪表板
清晰的因果链接，攻击链可视化	没有内置的攻击链可视化
自动化事件分类和优先级	事件严重程度取决于分析师的解释
安全响应工作流程和建议	分析师确定响应步骤和顺序
由安全响应者直接采取行动	无法由安全响应者采取行动
对中小型安全团队进行了优化	最适合大型安全团队

表 1: EDR 和 SIEM 工具对比

为什么EDR是更好的选择

EDR是中小型企业和大型安全团队进行检测和响应的最佳选择，而SIEM保持了纯“大数据”调查的优势，并为训练有素的大型安全团队提供了跨多个输入源的警报关联。

- EDR围绕事件而不是警报进行设计，将相关事件升级为综合视图
- EDR包含现成的，可操作的，以安全为中心的仪表盘，有助于快速响应事件
- 事件响应者可以直接在EDR控制台内直接采取补救措施
- 分析师可以在整个企业的IOC和IOA之间执行相关的查询和关联
- 安全团队可以使用清晰的攻击链可视化执行根本原因分析
- 管理员可以衡量和降低端点操作系统，应用程序和人为因素等多个维度的系统性风险
- 事件响应者可以快速分类警报并确定其优先级，然后按照明确的补救措施说明进行操作

超越 EDR

端点保护对于合规性和避免病毒，勒索软件等是必不可少的，但具有内置的局限性。 端点检测和响应更适合处理复杂的多阶段，多向量攻击，这些攻击是专门为逃避检测而设计的。

对于专注于安全成果而非工具的组织， MDR是理想的选择。MDR可确保您获得最佳安全性，并且由安全厂商种经验丰富的安全专家7X24负责安全运营，帮你监视和维护安全。

未来发展

NDR网络检测和响应利用传统端点和IoT设备生成的网络流量分析将EDR提升到一个新水平，以全面了解当前威胁环境。 更进一步，XDR扩展检测和响应可跨多个企业安全控制（电子邮件，端点，服务器，云工作负载和网络）自动收集并关联数据，从而可以更快地检测到威胁，安全分析师可以缩短调查并缩短响应时间。 这种统一的安全平台可提供跨网络，云，端点和应用程序的数据模式和事件的完整可见性，同时应用人工智能和自动化来检测，分析，搜寻和解决整个企业中的高级威胁。 目前Bitdefender的安全产品产品组合有独立的EDR, 集成端点保护的EDR，XDR， MDR等，我们仍然在持续研发，改进和优化产品，NDR即将到来。

关于 Bitdefender

Bitdefender是全球网络安全的领导者，为150多个国家的5亿用户提供尖端的端到端网络安全解决方案和先进的威胁防护。全球超过38%的安全公司使用Bitdefender的技术。典型客户包括：奇虎360，腾讯，百度，阿里巴巴，Microsoft，Cisco， IBM，软银，诺基亚，TeamViewer，华为，电讯盈科，中国金融认证中心，阿斯利康，FireEye，Cybereason等等。Bitdefender连续10年在国际权威测评机构AV-Test和AV-Comparatives的测试中排名第一。

联系我们以获取更多信息和产品演示

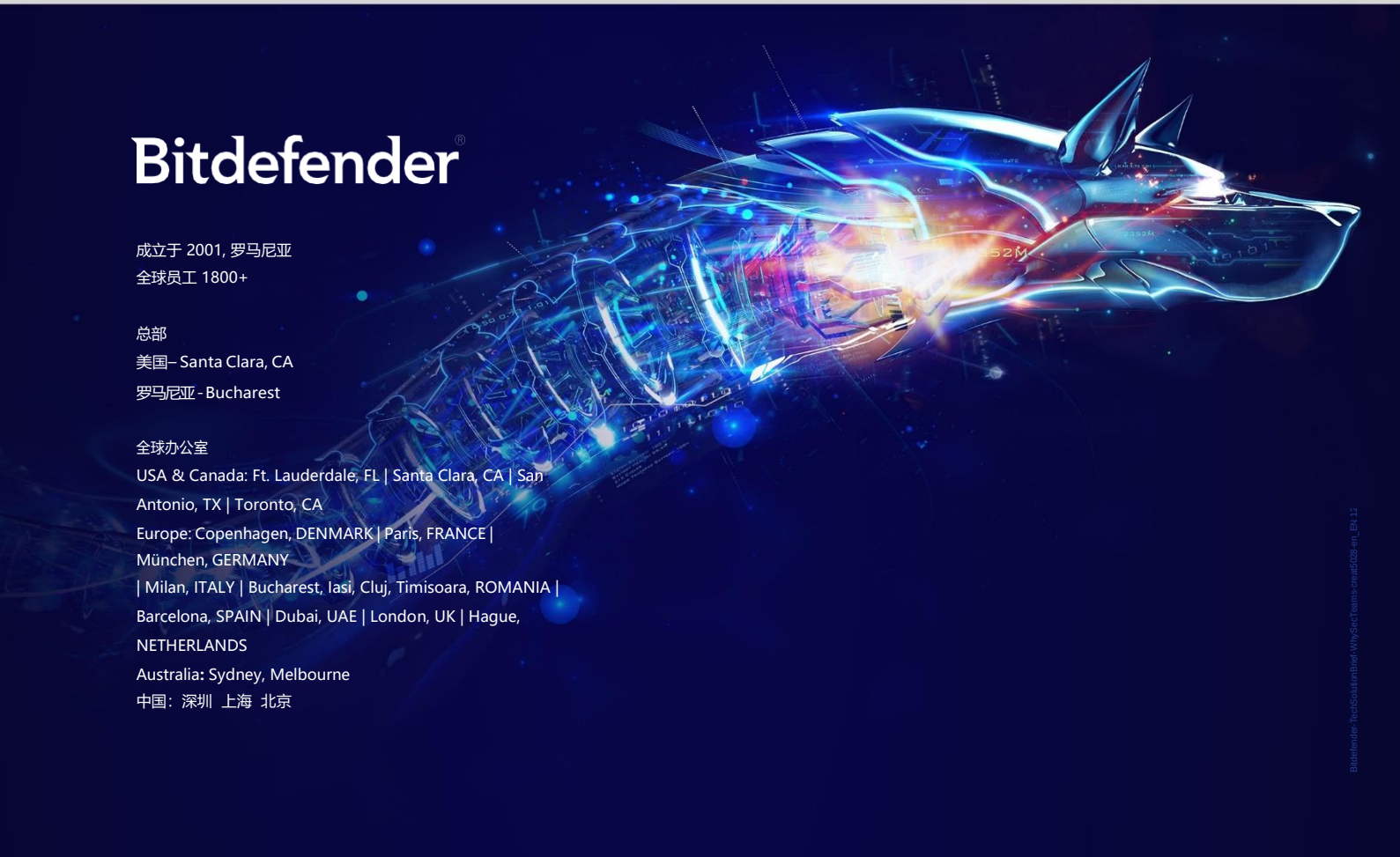
请联系我们以安排独立EDR，Ultra（端点保护+EDR），XDR， MDR等产品的深入产品演示和讨论，索取产品白皮书和PPT等。

联系电话：4000-132-568

申请试用：http://www.bitdefender-cn.com/trial.html

关注Bitdefender公众号

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX



Bitdefender®

成立于 2001, 罗马尼亚
全球员工 1800+

总部
美国– Santa Clara, CA
罗马尼亚 - Bucharest

全球办公室
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne
中国：深圳 上海 北京