为何说 EDR 不足以保护企业

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Why EDR is not sufficient to protect your organization		
原文作者	查克·埃弗里特（Chuck Everette）	**原文发布日期**	2022 年 3 月 18 日
作者简介	查克·埃弗里特是 Deep Instinct 网络安全宣传总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/03/18/edr-tools/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	企业的安全策略应以预防性方法（而非只能在威胁出现时进行应对的被动方法）为中心。基于此，企业可以检测和阻止意图进入其系统的恶意软件，从而阻止其在系统中执行。这样一来，企业就能在恶意软件执行之前消灭它，大大降低发生攻击的风险。这也意味着 SOC 团队可以更有效地使用 EDR 和 XDR 工具来调查和修复其他问题，而不必一直担心会发生严重的攻击。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

为何说 EDR 不足以保护企业

查克·埃弗里特

2022 年 3 月 18 日

端点检测和响应（EDR）工具是当今大多数网络安全防御措施的基石。该技术在调查威胁方面发挥着重要作用，但是很多企业错误地将 EDR 作为其抵御攻击的第一道防线。

现实情况是，“假设发生攻击”的思维方式意味着 EDR 通常为时已晚。越来越多的恶意软件和攻击技术能够规避 EDR 解决方案，尤其是勒索软件和零日漏洞。

因此，企业不能仅依靠 EDR 来保护其环境免受最新威胁。那么，他们应该怎么做呢？

EDR 通常为时已晚

EDR 最大的缺点在于，它是一种反应式方法。传统的 EDR 工具依赖于行为分析，这意味着威胁已经在端点上执行，要想“在威胁造成任何损害之前阻止它”就得争分夺秒。发现恶意意图或活动后，EDR 会对其进行阻止，然后安全团队将介入进行补救和清理。

在安全人才缺乏的情况下，SOC 的工作效率对于保护企业非常重要。但是，典型的 EDR 解决方案会产生大量告警和误报，妨碍 SOC 团队执行更有价值的任务（如修补和强化系统）。

此外，严重的威胁很容易淹没在这些“噪音”中，导致它们不会被发现，在系统中停留更长的时间。

因此，每个端点的可见性对于保护企业都至关重要。然而，企业通常不知道是否所有端点都进行了检测，这会在企业系统中留下漏洞。此外，“自带设备”（BYOD）和远程办公等趋势使得企业更难保护所有的设备。

企业需要全面了解连接到其网络的每个端点。但是，大多数企业都做不到这一点。事实上，Deep Instinct 的一项调查发现，只有 1%的企业认为他们所有的端点都受到了保护。

仅依赖反应式方法是不够的

一些速度最快的恶意软件，在端点上执行不到一秒就能够感染端点。例如，勒索软件在被检测和阻止之前就有可能加密系统，恶意软件可能会迅速在系统中留下投放器和组件，而

这些投放器和组件不会被发现。

随着影子经济的日益发达，攻击者更容易获得高级恶意软件和零日漏洞。“勒索软件即服务”（RaaS）就是一个很好的例子，它模仿合法 SaaS 产品的结构，为犯罪分子提供低成本的访问权限，以执行强大的勒索软件攻击。此外，活跃的恶意软件交易导致变种不断出现，每天都会出现数十万个新版本。

“预防优先”战略的必要性

鉴于此，企业需要采取“预防优先”的方法来阻止更多攻击。

尽管 XDR 解决了 EDR 的许多问题，但它仍然是一种反应式模型。该模型容易遭受高级、未知恶意软件的攻击，并且容易产生大量安全告警。事实上，除非严格管理监控，否则监控的增加会导致大量告警生成，使 SOC 团队更难应对。

企业的安全策略应以预防性方法(而非只能在威胁出现时进行应对的被动方法)为中心。基于此，企业可以检测和阻止意图进入其系统的恶意软件，从而阻止其在系统中执行。这样一来，企业就能在恶意软件执行之前消灭它，大大降低发生攻击的风险。这也意味着 SOC 团队可以更有效地使用 EDR 和 XDR 工具来调查和修复其他问题，而不必一直担心会发生严重的攻击。

要想领先于快速发展的网络威胁，企业的安全解决方案需要更迅速地采取行动。通过深度学习技术的自我学习特性，企业可以在未知恶意软件哈希值的情况下了解攻击的特征，进而预测和预防未知威胁。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com