ESG 展示

：为何 MDR 已成为现代网络安全战略不可或缺的一部分

日期：2022 年 8 月**作者：**Dave Gruber，ESG 首席分析师

摘要：检测和响应功能在网络安全计划中的重要性已经得到广泛认可。最大的问题是，面对数量成倍增加且复杂性超出大多数组织适应能力的威胁，如何更好地确保检测和响应及时、准确、可靠且一致。Managed Detection and Response (MDR) 是一种第三方托管服务，可帮助组织跟上时代步伐。

简介：MDR 的兴起

所有组织都面临着一个严峻的现实：网络安全威胁正在迅速增加，攻击面不断扩大，而用于检测和响应威胁的传统流程和工具已经不够用。威胁本身和实施威胁的不法分子都更加熟练、敏捷和密集，对移动数字目标进行攻击，给负责保护企业资产安全的安全和 IT 专业人员造成困难。

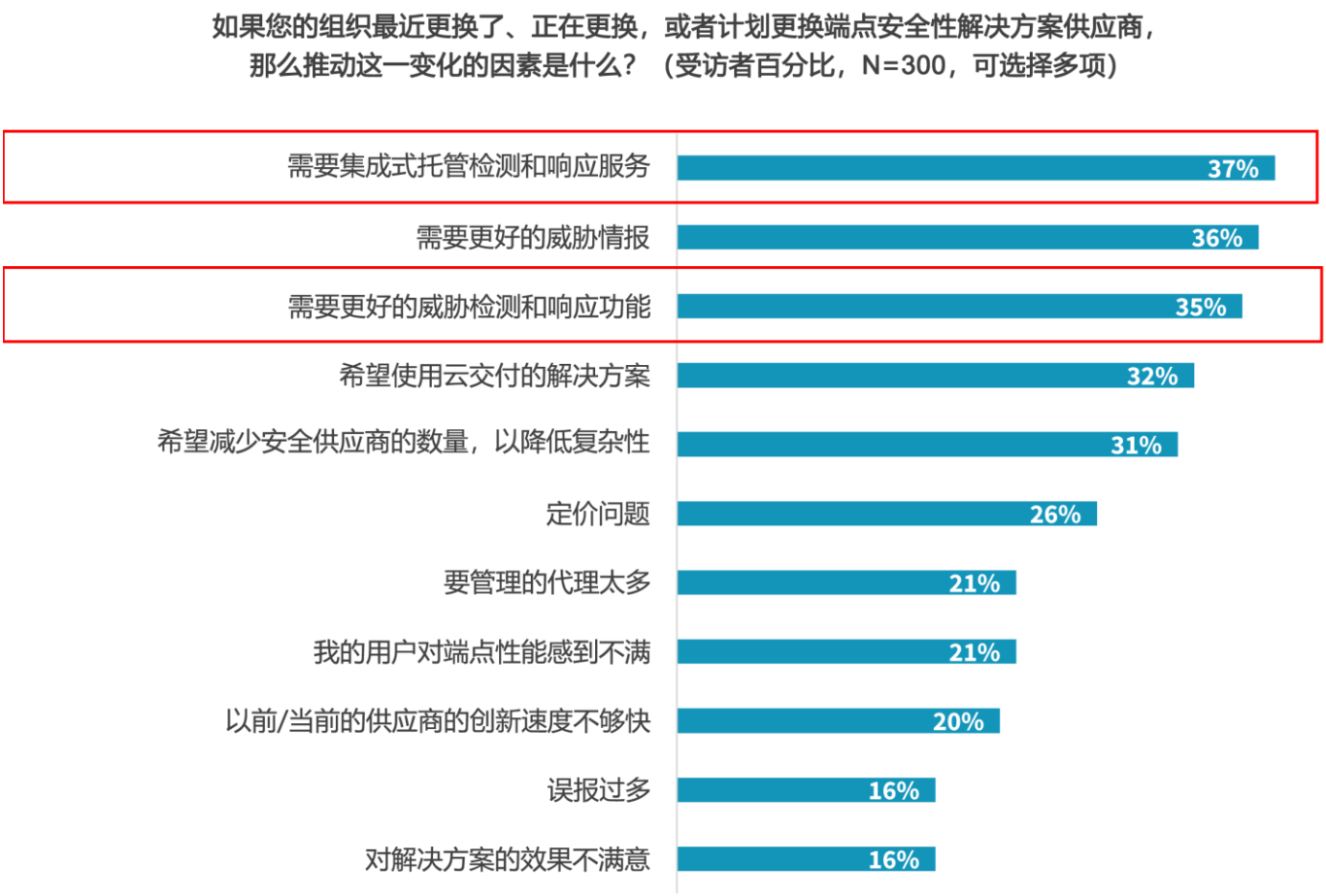
安全控制措施自然有不少，但大多都要求安全团队手动对持续出现的警报进行分类，以从误报中选出有效威胁，这会增加检测和响应工作的成本和复杂性。要构建更大规模的安全运营中心 (SOC)，就要为其安排更多的工具和安全工程师，这会带来高昂的成本，况且还要求组织在网络安全技能缺口巨大且日益扩大的现状下，寻找并雇用足够的安全专业人员。

由于需要重新制定网络安全计划，组织越来越频繁地求助于托管检测和响应服务提供商。

由于需要重新制定网络安全计划，组织越来越频繁地求助于托管检测和响应服务提供商来优化流程，填补资源和技能缺口和实现安全运营工具现代化。ESG 研究表明，许多组织将 MDR 与端点安全性关联起来，对集成式 MDR 服务的需求是促使组织更换其端点安全性解决方案供应商的一个重要因素（参见图 1）。[1]

[1] 来源：ESG 完整问卷调查结果，“*端点安全性趋势*”，2021 年 12 月。本展示中所有的 ESG 研究引用和图表均来自此项调查结果。

图 1。更换端点安全供应商的驱动因素



来源：TechTarget, Inc. 旗下部门 ESG

但是，随着安全团队扩展检测和响应计划，升级到更全面的扩展检测和响应 (XDR) 解决方案，MDR 产品为组织提供了更新技术和运营模式的方法，可提供更全面的攻击面覆盖和高级威胁检测。组织需要新的方法，将全天候监视、实时全球威胁情报、自动化和高级机器学习分析等功能相结合并处理海量安全遥测数据，从而为快速检测和威胁搜索提供支持。随着 XDR 不断发展和成熟，MDR 服务可以帮助各种规模和安全成熟度的组织实施检测和响应，从而减轻高级威胁的危害。随着组织重新定义从数据中心到边缘再到云的网络安全边界的范围和规模，这一点尤为重要。MDR 整合了人员、流程和技术，以满足分布式企业扩展威胁检测和响应应用场景的需求。

MDR 采用的主要驱动因素

随着 MDR 服务使用的不断普及，安全团队能够扩展覆盖范围，缩小人员配备缺口和强化总体计划目标。应用场景各不相同，但基本驱动因素都不乏：

- 威胁环境：网络攻击的数量以及这些攻击日益增加的复杂性，给组织带来了巨大的压力，要求组织能够更快、更明确地检测和响应。

- 攻击者意图：攻击者在规划和实施攻击方面变得更加智能、更持久、甚至更具战略性。如今已经形成了一个强大的"犯罪生态系统"，不法分子会分享策略，甚至就攻击展开协作。
- 成本：构建和扩展 SOC 需要巨额的资本支出 — 通常是七位数的支出，有时甚至更多。
- 网络安全技术更新：对于在内部执行全部或大部分安全运营活动的组织，必须更频繁地更新网络安全控制堆栈。其中包括从第一代端点检测和响应迁移到更全面的 XDR/MDR 框架。
- 技能不足：经常讨论的网络安全技能不足是一个长期存在的问题。无法在内部正确部署网络安全职位往往会导致检测和响应目标面临挑战，从而使资产面临风险。

网络攻击不会区分对象。中小型组织因员工、预算有限以及之前可能遭遇过各种类型的攻击，会面临一定的风险。即使是规模较大的组织也需要额外的人员配备、可扩展控制以及战略方面的高管级咨询，才能检测和响应不断变化的威胁环境。

应如何考量 MDR 服务和 MDR 服务提供商

所有评估 MDR 服务的组织都有一些重要且棘手的要求，包括：

- 上下文威胁情报：实现实时威胁情报和检测，包括关联多个指标来识别威胁或消除误报。
- 主动式应用场景：支持主动搜索已知威胁。
- 丰富的遥测：进行深入的取证调查和复杂的分析，这对于识别新的威胁尤为重要。
- 修复：提供特定于上下文的 AI 驱动型修复指导。
- 降低风险：漏洞评估和管理。

在选择 MDR 服务提供商时，组织应寻找能够提供特定、经过展示的功能的合作伙伴，包括：

- **24/7** 全天候覆盖：全天候提供持续监视。
- 假设情景规划和咨询。
- 服务提供商提供的人力专业知识和经验。
- 面向高管和董事会成员的指导。
- 能够确保治理成效、合规性和业务连续性。

此外，组织还应向潜在的 MDR 合作伙伴询问有关服务级别目标的问题。这些功能包括从发出警报到启动调查的平均反应时间、从启动调查到向组织提供事件分析的平均响应时间，以及从启动调查到完全解决问题的平均解决时间。

Dell Technologies 的 MDR 方法

识别、评估 MDR 服务提供商以及与他们合作时，组织不仅需要关注他们当前在检测和响应威胁方面的需求，还应关注这些需求在未来可能的演变和扩展方式。虽然没有组织能够准确预测网络安全威胁的未来状况，但组织应寻找经验证可基于创新技术、经验证的流程以及员工展现出的专业知识，随时间推移扩展其服务的 MDR 合作伙伴。

Dell Technologies 的 Managed Detection and Response 方法结合了灵活、智能且可扩展的技术与经验丰富的网络安全专业人员。我们基于订阅的服务旨在为组织提供成本可预测性，并使他们可在必要时无缝迁移到更高级别的服务。

戴尔 Managed Detection and Response 的技术平台是 Taegis XDR，这是一种完全托管的云原生服务，由戴尔的 Secureworks 业务部门开发。Taegis XDR 可在分布式和多样化的攻击面范围内检测、分析和处理经过全面审查的威胁，以帮助保护从大型跨国企业到相对小型企业的各种组织。

戴尔庞大的安全分析师和工程师团队的技能进一步加强了 Taegis XDR，他们掌握的知识来源于数十年来帮助组织抵御已知和未知威胁所积累的专业知识。这种组合提供了一种高效的方法来统一整个 IT 体系结构中的检测和响应方式，这在很大程度上是通过其持续更新的威胁情报数据库实现的。戴尔 Managed Detection and Response 还可监视、分析和识别恶意行为，以缩短平均检测和响应时间。

戴尔 Managed Detection and Response 还可监视、分析和识别恶意行为，以缩短平均检测和响应时间。

最后，由于戴尔 Managed Detection and Response 是一项托管服务，它可大幅减少组织为已经负担过重的内部 IT 和安全运营团队寻找和招募安全专业人员的需要。戴尔 Managed Detection and Response 旨在以经济高效且具有战略意义的方式补充和扩展组织自身的能力。

更重要的事实

随着组织对威胁检测和响应计划进行现代化改造，快速扩大的攻击面、反复的勒索软件攻击以及总体来说更复杂的威胁环境正在推动对 XDR 和 MDR 的投资和相应发展势头。虽然组织的安全策略各不相同，但他们都需要更广泛地了解攻击面，以及聚合、关联和分析来自提供保护的各种安全控制措施的海量安全数据，这是获得控制权的重要一步。

在安全团队利用 MDR 提供商来加强技能、流程和安全技术方面，Managed Detection and Response 服务既有效又随时可用。ESG 的研究表明，投资 XDR 的组织需要配套的 MDR 服务来帮助他们实施和运营这些解决方案。这意味着要与在提供安全解决方案和服务方面都有着经验证的业绩记录的解决方案提供商合作。随着时间的推移，这可以帮助 IT 和安全团队制定和扩展其安全计划。

ESG 建议了解 Dell Technologies 等公司提供的 MDR 解决方案，这些解决方案可提供人员、流程和技术来帮助组织实现这些目标。

Enterprise Strategy Group 是一家综合性技术分析、研究和战略咨询公司，为全球 IT 社区提供市场情报、切实可行的见解和走向市场的内容服务。

www.esg-global.com contact@esg-global.com 508.482.0188