Enterprise Strategy Group | 了解更重要的事实。™

ESG 白皮书

Managed Detection and Response：快速改进安全计划的途径

作者：首席分析师 Dave Gruber

2022 年 8 月

本 ESG 白皮书受 Dell Technologies 委托撰写，经 TechTarget, Inc. 许可分发。

目录

摘要

随着数字化转型加快、云采用效率提升、威胁环境日益复杂以及安全技能持续短缺，种种现状都使安全团队举步维艰。当前的安全解决方案无法跟上发展的步伐，这迫使许多组织优先考虑通过 SOC 现代化计划来改进技术和流程。有关零信任和扩展检测和响应 (XDR) 的行业大趋势展现了新的愿景；然而，许多组织在有效实施这些战略方面都遇到了困难。Managed Detection and Response (MDR) 服务可提供缓解措施，为众多组织提供所需的人员、流程和技术，以便在当下的动荡环境中巩固其安全计划。

简介

随着破坏性网络攻击风险不断升级，组织在核心业务方面投入的精力和预算被占据，只得通过加强网络安全计划来做出响应。对某些组织而言，使用内部资源构建整个安全计划是可行的，但对大多数组织而言，则需要第三方资源来帮助实现计划的快速发展和扩展。

安全运营 (SecOps) 负责监视和保护数字攻击面的各个方面，是所有网络安全计划的核心。SecOps 涉及的安全遥测和警报数量（包括网络、端点、云、身份、应用程序和数据）不断攀升，这使组织举步维艰，许多组织不得不求助于 MDR 服务提供商来提供缓解措施。

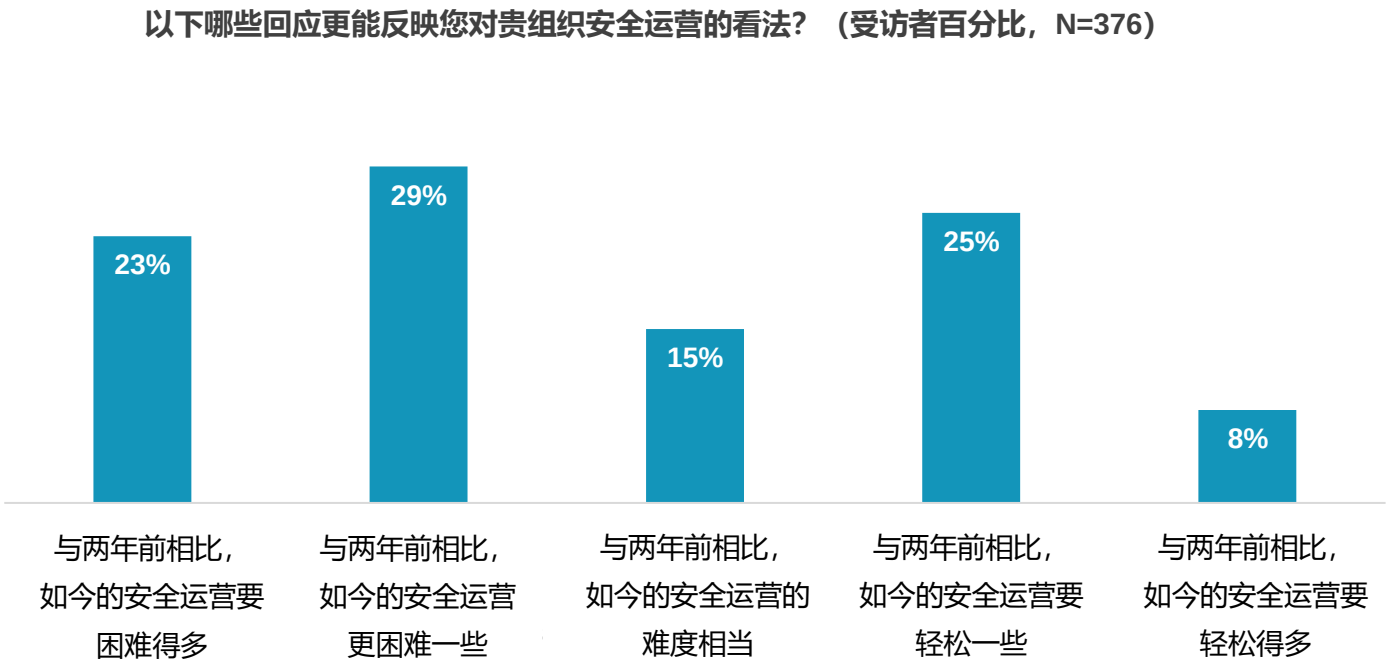
MDR 服务提供商已成为这些组织的关键机制，可提供一系列安全服务产品，如事件响应、全天候监控、计划管理和风险管理。Enterprise Strategy Group (ESG) 研究表明，对于规模和安全成熟度各异的组织，MDR 服务已成为他们的现代网络安全战略的主流。

日益严峻的安全运营挑战

根据 ESG 的研究（参见图 1），大多数组织都意识到，与两年前相比，如今的整个 SecOps 领域面临着更多困难。[1]

[1] 来源：ESG 完整问卷调查结果，“*SOC 现代化和 XDR 的作用*”，2022 年 8 月。除非另有说明，否则本白皮书中的所有 ESG 参考资料和图表均取自此项调查结果。

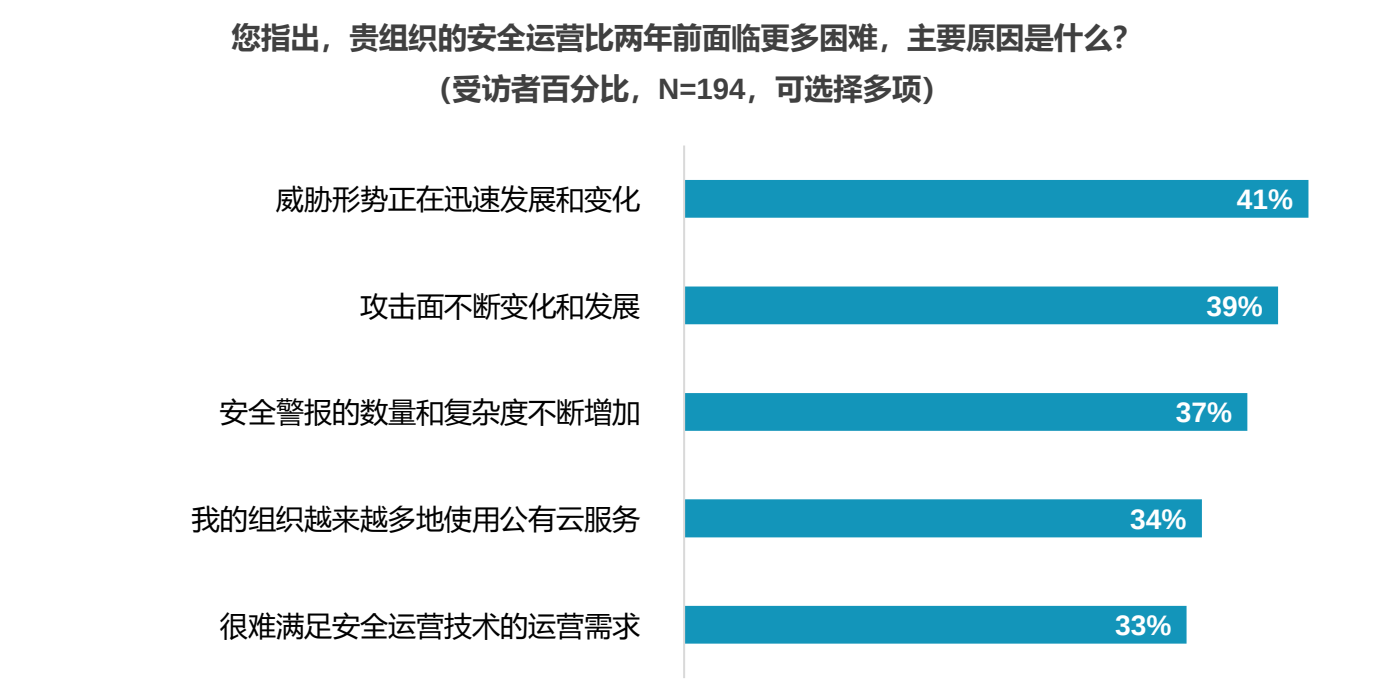
图 1. 超过一半的组织认为 SecOps 面临更多困难



来源：TechTarget, Inc. 旗下部门 ESG

如图 2 所示，ESG 研究还指出了使检测和响应比以往更加困难的其他挑战，例如攻击面的不断扩大、威胁环境的发展和多样性，以及云服务在更广泛的应用程序和应用场景中迅速采用。

图 2. SecOps 面临更多困难的五大原因



来源：TechTarget, Inc. 旗下部门 ESG

实现检测和响应计划的现代化

攻击面和威胁环境的规模和复杂性都在增长，与此同时，组织利用的安全控制措施也越来越多，这就生成了成千上万的警报和海量安全数据。为了支持警报和事件分类与调查，安全团队必须聚合、关联和分析这些数据，这通常需要大量的手动流程。但是，除了捕获和分析警报和安全数据之外，还需要采取更多措施。

安全团队需要重新思考总体计划运营，以进一步整合来自 IT 和业务线团队的资产和风险数据，专注于那些对组织目标构成更大风险的威胁。例如，从短期和长期来看，域管理凭据被盗可能会对组织的运营、财务和品牌声誉产生广泛的潜在负面影响。

越来越多的组织的安全负责人在重新思考相应战略后将日常运营活动转移给了第三方，以便将内部资源重新集中在更具战略意义的安全活动上。在内部安全资源专注于重新构建安全运营流程的同时，MDR 服务提供商会负责处理事件检测、分类和响应，并迅速采取措施来止损并减少潜在的运营业务中断。

其他组织则希望 MDR 提供商在总体计划制定方面提供指导，并引入专家和经验证的安全运营流程来优化结果。

随着 XDR 变迁进一步在实现检测和响应计划现代化所需的措施方面明确愿景和路线图，其他组织希望利用 MDR 提供商来帮助实施 XDR 级解决方案。

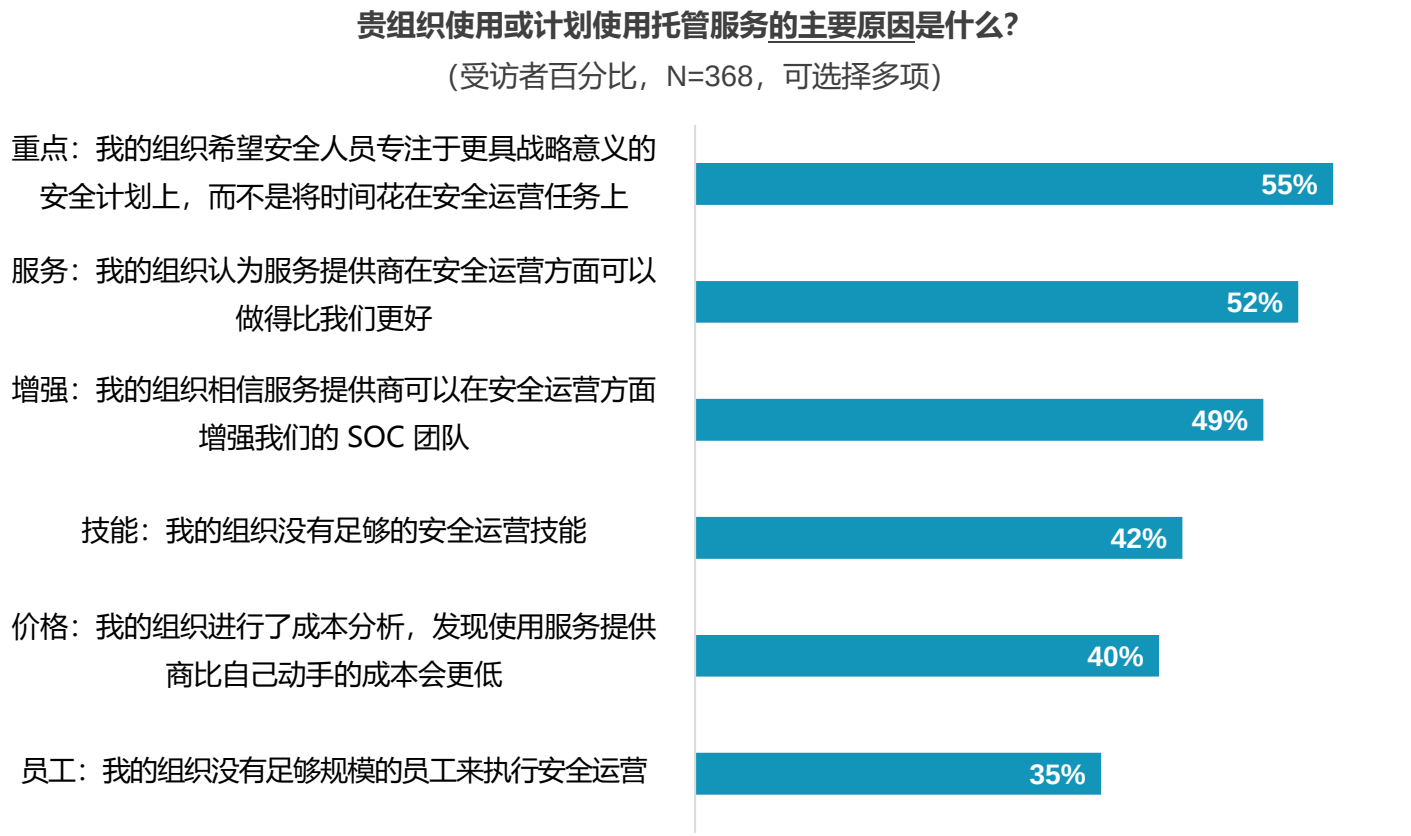
MDR 应用场景

虽然许多 MDR 提供商都提供广泛的安全服务，但起初通常从可监测、分类和调查警报的核心检测和响应服务开始。MDR 提供商的运营模式各不相同，因此安全负责人必须仔细研究他们的各项组织要求，寻找可帮助他们实现特定目标的 MDR 提供商。例如，一些安全负责人选择将其安全运营完全外包，让 MDR 提供商提供全面的攻击面覆盖、威胁监视和修复。在此模式中，MDR 提供商通常提供实现服务所需的技术堆栈、流程和安全专家。对于其他组织而言，MDR 服务是内部安全运营职能的延伸，为主要负责技术堆栈和运营流程的内部团队增加非工作时间覆盖或增添额外的安全专家。这些只是众多使用 MDR 服务的应用场景中的两个示例。

因此，MDR 不是“一刀切”的解决方案。相反，它通常表示一组可自定义的功能，可满足单个组织的需求。

不同的组织将根据其内部资源和技能，为检测和响应的不同方面选择 MDR 合作伙伴。ESG 研究探讨了其中的主要原因，如图 3 所示。

图 3. 组织为何选择 MDR 合作伙伴



来源：TechTarget, Inc. 旗下部门 ESG

MDR 参与的关键价值驱动因素

制定安全计划时需要同时关注效率和有效性，而 MDR 服务可以对这两项产生积极影响。

- **运营改进和效率。**MDR 可帮助组织通过多种方式（如基础架构、人员和管理）降低安全运营的总成本。它还可解决“警报疲劳”问题，并提高误报显著降低的可能性。
- **提高了网络安全的有效性和降低了风险。**MDR 可帮助组织阻止已经存在的威胁，改进对潜在威胁和高级持续性攻击的检测，激活主动威胁搜索，并将更强的控制转化为机制以识别和预防未来攻击。

如何考量现代 MDR 解决方案提供商

请注意，总的来说，MDR 解决方案并不是新鲜事物。事实上，它已经存在了一段时间，并拥有出色的成功记录。但是，许多“1.0 代”MDR 解决方案是为不同的时代设计和实施的：数据和威胁更少、检测更简单。下一代 MDR 解决方案以及部署和管理它们的第三方必须面对更广泛、更深入、更复杂的一系列挑战，这些挑战使检测和响应比以往时候更加重要和困难。

在评估 MDR 解决方案时，组织应寻找以下功能：

- 全天候监视事件和日志，按量、位置和类型提供有关可疑活动和警报的快速、高可见性信息。
- 持续且可扩展的网络监视和威胁分析。
- 针对上下文响应选项的 AI 驱动型建议。
- 监管合规性报告。
- 与内部团队直接联系的“人力”安全顾问。
- 基于威胁检测、分类、调查和取证的详细实时分析。
- 漏洞评估、优先级排序和缓解指导。

在考虑能够提供一些、大部分甚至全部外包 MDR 功能的大量潜在服务提供商时，组织应寻找能够具备以下能力的合作伙伴：

- 上下文威胁情报。
- 丰富的遥测功能。
- 经验证在组织地理覆盖范围、垂直市场和法规概况方面具有出色的业绩记录。
- 展示出威胁搜索功能。
- 长期致力于基于云的 MDR，在多云和混合云环境、零信任和云安全责任共担模型方面具有全面的能力。
- 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。

Dell Technologies 的 MDR 方法

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 Dell Technologies 子公司 Secureworks 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。

Taegis XDR 的功能可通过戴尔庞大的安全分析师和工程师团队的专业知识和技能得到更大限度提升，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 为基于订阅的托管服务，这大大减少了组织寻找并招募安全专业人员来处理更多威胁、攻击和警报的需求。戴尔 Managed Detection and Response 可高效且有效地补充和扩展组织的内部功能。这样一来，内部 SecOps 人员便可以将更多时间和精力集中在其他安全相关任务上。

成功案例：MDR 的实际应用情况

ESG 与戴尔 MDR 客户的 IT 和安全负责人进行了交流，深入了解了具体的应用场景、运营模式和成果。

示例 1：中型地方政府

地方政府的 IT 和网络安全资源很少达到私营企业的水平，但这并不意味着他们不会遇到同样的问题。在此示例中，美国西南部州某中等规模县难以在应对和克服越来越多的安全威胁的同时将支出严格控制在预算范围内。

新的 IT 总监上任后，他立即意识到他的小型团队面临着不断发展的威胁环境，并发现了他们的检测和响应能力中的潜在漏洞。“我们的安全态势不够完善，而且我们必须在不增加工资的情况下扩展我们的能力，这是一个对行政决策者高度敏感的主题，”他说。“但我知道，我可以呼吁他们在财政上保持节俭，同时指出解决我们的漏洞的必要性。”

他首先着手评估该县现有的端点安全供应商，当时该供应商推行了 90 天“免费试用”软件升级，以改进检测和响应能力。但是，他发现相应软件缺乏满足其需求的功能，并且该供应商的沟通方式不符合预期，因此他决定采用更全面的 MDR 解决方案。

“幸运的是，我们安排戴尔提供了虚拟 CSO（首席安全官），这样一来，县负责人便了解了在检测和响应场景中使用托管服务方法的好处。”他补充称，戴尔团队补充了该县的小型内部安全团队和 IT 专业人员，而不是替代他们。“他们是我们团队的延伸，他们可与我们的团队顺畅地合作。”

以 Microsoft Exchange Web 电子邮箱为目标的一场全球黑客活动凸显了这一安排的好处，因为包括该县在内的众多组织都使用了这个主流平台。“Microsoft 在发现攻击后立即开发并发送了修补程序，但此次攻击的零日可能

是在一个月之前，”该县 IT 总监说。“当时戴尔虚拟 CSO 在下班后联系了我们，戴尔 MDR 团队随即介入。他们给我们发送了脚本来检查服务器，我们很快发现其中一台服务器遭到入侵。”

“戴尔（及其 Secureworks 合作伙伴）非常擅长他们的工作。在应对攻击期间，我们每天都会进行两三次通话。”他补充称，事件响应团队与该县工作人员一起查看了调查结果，向他们展示了表明遭到攻击的代码片段和其他迹象以及入侵的证据。

最后，他们提供了许多技术和非技术建议，这不仅解决了攻击带来的潜在影响，而且还在更广泛的范围和更长时间内增强了该县网络安全状况。

“我们的经验告诉我们，寻找增强型检测和响应服务的方法是找到可靠、成熟、值得信赖且拥有这方面经验的 MDR 专家，而不是通过低成本的方法来升级 EDR 软件，”他说。“不仅是在处理攻击后果期间，而且在定期与他们合作时，我都会有一种暖心的感觉，因为我们有优秀的团队在帮助我们确保安全。”

示例 2：中型学区

各学区过去在 IT 方面的投资通常不足，特别是网络安全方面。但是，随着针对学区的勒索软件和其他网络攻击不断增加，当地公共教育官员正竭力想出更好、更可靠、更经济实惠的方法来防范漏洞。

例如，美国一个中型学区发现自己受到勒索软件的攻击，其所有技术驱动型运营都停止了。该学区有 8,500 名学生和教职员工，21 个设施，拥有合理规模的 IT 配置，包括 100 台物理服务器和另外 63 台虚拟服务器，这些服务器连接着 11,000 多台供学生和员工使用的设备。显然，该学区有许多不法分子可能利用的切入点，他们需要一个可以快速行动的合作伙伴。

明确勒索软件攻击的存在且必须立即应对攻击后，学区的 IT 团队联系了戴尔 Managed Detection and Response 团队。“在攻击的第二天，戴尔就派出了 10 人来帮助我们，”学区 IT 主管表示。“我们高度信任戴尔的团队，他们立即接管了工作。”

幸运的是，该学区最终收获了积极的成果。“在我们系统中超过 600 万个文件中，我们只丢失了 6 个，”IT 主管指出。“我们甚至未向威胁实施者支付赎金。我们是安全度过勒索软件攻击并继续安全可靠地开展工作的真实案例。

“与戴尔合作是一次积极的体验。我们的现场安全分析师在与戴尔人员交谈后总是很满意，我们目前的立场比我们与戴尔 Managed Detection and Response 团队合作之前提升了 95%。”

更重要的事实

随着破坏性网络攻击风险不断升级，破坏核心业务目标的信息共享和预算，组织必须加强网络安全计划。虽然应用场景各不相同，但大多数组织都在利用 MDR 服务提供商来扩展其计划。

MDR 服务提供商提供了一种方法来克服在制定成功的安全计划时面临的许多公认的挑战，此类计划包括安全专家、经验证的流程以及可扩展且易于部署的安全技术。

Dell Technologies 汇集了一系列紧密集成的技术、经验丰富的安全专家和最佳实践，来帮助组织近乎实时地检测和响应威胁。如本白皮书中的案例分析所示，Dell Technologies 已帮助各行各业具备不同资源配置的众多组织缓解了新兴威胁对整个企业的影响。

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