SOPHOS
Cybersecurity delivered.

使用 MDR 服务的五大理由

引言

随着网络威胁的数量、复杂程度和影响不断增加，企业正越来越转向托管式侦测与响应 (MDR) 服务，侦测并消除单纯技术解决方案无法防御的高级攻击。事实上，Gartner 预测，到 2025 年，50% 的公司将使用 MDR 进行威胁监测、侦测和响应[1]。

但是，市面上雨后春笋的防御解决方案让人难以了解 MDR 的确切含义，MDR 与您的更广泛的网络安全生态体系的适合程度，以及使用 MDR 服务可以带来的好处。本指南为这些问题作出解答，提供选择 MDR 服务时要考虑的问题的实用指南。

Sophos MDR

Sophos MDR 是全球最值得信任的 MDR 服务，保护超过 11,000[2] 家企业抵御最高级的威胁，包括勒索软件。Sophos MDR 得到 Gartner Peer Insights™[3] 最高评分，以及在服务中端市场的 MDR 服务的 2022 G2 Grid® 得到顶级供应商认可 ，您的网络防御可以放心。

定义 MDR

要了解 MDR 的好处，以及 MDR 服务需求增长背后的推动力，务必了解什么是 MDR — 什么不是 MDR。

托管式侦测与响应服务 (MDR) 是一项由专家交付的全托管 24/7 全天候服务，他们擅长侦测和响应单纯技术解决方案无法阻止的网络攻击。

不要将 MDR 与 EDR（端点侦测与响应）和 XDR（扩展式侦测与响应）混淆。虽然 MDR、EDR 和 XDR 都支持和实现威胁捕猎，但 EDR 和 XDR 是允许分析师捕猎`和调查潜在威胁的工具；而借助 MDR，安全供应商的分析师可以捕猎、调查并代表您消除威胁。

顾名思义，EDR 工具处理端点防护技术的数据点，而 XDR 工具在跨广泛 IT 堆栈（包括防火墙、电子邮件、云和移动安全解决方案）中扩展其数据来源，来提供更大的可见性和更多信息。Sophos 使用我们行业领先的 EDR 和 XDR 解决方案提供 MDR 服务。

MDR 不负责日常网络安全管理，例如部署安全技术，更新政策，打补丁或安装更新。托管式服务提供商 (MSPs) 为寻找此方面支持的企业提供 IT 安全管理服务。

哪些人使用 MDR 服务

无论是 IT 资源有限的小公司，还是有内部 SOC 团队的大型企业，所有行业所有类型的企业都使用 MDR 服务。真正的问题是：企业如何使用 MDR 服务?MDR 响应模型有三种：

- MDR 团队代表客户完全管理威胁响应
- MDR 团队与内部团队合作，共同管理威胁响应
- MDR 团队提醒内部团队，提供修复指南

Sophos 支持所有三种方法，根据需要满足不同客户要求。

1 Gartner Market Guide for MDR 2021
2 截止 2022 年 8 月。
3 截止 2022 年 8 月 1 日过去 12 个月的评论。Gartner Peer Insights 内容由个人最终用户根据自己对平台列出的供应商的体验作出的意见，不构成事实声明，也不表示 Gartner 或其子公司的观点。Gartner 不为本内容介绍的任何供应商、产品或服务背书，不对其内容的准确性或完备性作任何明示或暗示保证，包括对适销性或特定用途适合性的任何保证。
4 Sophos 在 2022 G2 Grid® 服务中端市场的 MDR 服务中被评为顶级供应商。

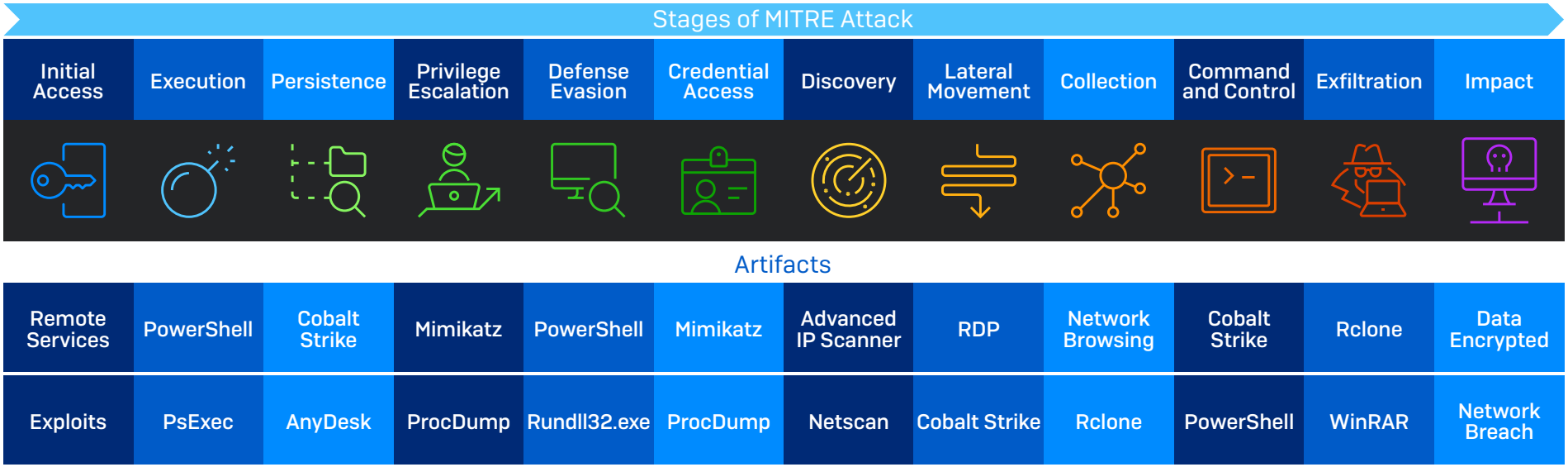
对人为主导的威胁侦测与响应的需求

现实情况是单纯技术解决方案无法防御所有网络攻击。为了避免被网络安全解决方案发现，恶意黑客在攻击中越来越多利用合法 IT 工具，利用失窃凭据和访问许可，利用未打补丁的漏洞。通过模拟授权用户和利用企业防御漏洞，恶意黑客可以避免触发自动侦测技术。

下图详细说明 Sophos 前线威胁猎手在 2021 年发现的，攻击者在 MITRE ATT&CK 链每个阶段使用的工具。可以看到，敌手频繁滥用 IT 团队经常使用的工具，如 PowerShell、PsExec 和 RDP。自动技术难以区分使用此类工具的合法 IT 人员，与使用失窃凭据利用此类工具的攻击者。

阻止此类高级“离地”攻击需要结合技术与人类经验。攻击者每次采取行动时，都会产生一个信号。将人类专业知识与强大的防护技术和基于人工智能的先进机器学习模型相结合，安全分析师可以侦测、调查甚至消除最高级的人为主导的攻击以避免数据外泄。

虽然威胁捕猎、调查和响应可以完全在内部利用 EDR 和 XDR 工具执行，但使用 MDR 服务也有很多优势，无论是与内部团队一起还是作为全外包服务。



Mitre 攻击链每个阶段使用的主要工具。主动攻击敌手指南 2022，Sophos

防护技术在现代防御中仍然起到关键作用

虽然人为主导的托管式侦测与响应是网络防御的重要一层，但高质量防护技术仍然很关键。端点、网络、电子邮件和云安全技术在现代防御中继续起到关键作用 — 合适的解决方案可以提高 MDR 服务的效果和影响：

- 自动防护技术允许防御者领先于日益增加的攻击量，因为敌手利用自动化、人工智能和恶意软件即服务技术扩散其威胁。Sophos Endpoint Protection 在威胁影响到企业前99.98%自动加以阻止。
- 威胁猎手面临的一个最大实际挑战是杂音：信号非常多，可能难以找出有意义的。出色的防御技术减少分析师需要调查的提醒数量。高质量防御技术允许威胁猎手专注于更少更准确的侦测结果，加速人主导的威胁响应。
- 人类分析师利用侦测结果和防御技术的信号，确定并调查可疑活动。侦测质量越高，环境信息越多，调查和响应速度越快，效果越好。

考虑到这一点，我们现在看一看使用 MDR 服务的各组织所报告的 5 大好处。

1. 提升网络防御

使用 MDR 提供商相比纯内部安全运营计划的主要优点之一，是提升针对勒索软件和其他高级网络威胁的防护。

使用 MDR，可以获得提供商分析师的广泛而深入的经验。MDR 供应商遇到的攻击数量和种类超过任何一个组织，其掌握的专业知识是内部几乎无法做到的。

MDR 团队每天还调查和响应事件，因此威胁捕猎工具的使用明显更熟练。这使得他们可以在过程的所有阶段更加快速准确响应 — 从辨识重要信号，到调查潜在事件和消除恶意活动。

作为大型团队的一份子工作，还支持分析师分享其知识和洞见，进一步加快响应速度，Sophos MDR 团队关联我们遇到的每个威胁或独特黑客的相关执行脚本。在调查过程中确定对手后，我们的团队无需在攻击时执行广泛研究，而可以参考相关执行脚本，然后直接开展行动。

执行脚本持续更新，分析师在每次活动中记录重要信息，例如：

- 常见或者特定攻击或威胁黑客特有的 TTP（战术、技术和过程）
- 相关 IOC（入侵迹象）。
- 与开放漏洞关联的漏洞攻击的已知概念证明。
- 处理具体攻击或威胁黑客时的有用威胁捕猎查询。

MDR 服务的另一个优势是可以将一个客户的情报应用于符合相同目标档案的其他客户，从而主动防御该群体内的类似攻击。Sophos MDR 团队主动调查客户资产的场景示例包括：

- 以特定方式针对特定行业的一个客户。
- Sophos X-Ops 提供以某个行业或组织为目标的重要攻击的情报。
- 在安全领域中发生重大事件，我们希望确定是否影响到我们的任何客户。

如果分析师发现任何可疑信号，可以快速调查并修复情况，创建对目标组的团体免疫性。

在客户环境中应用学习成果的能力，以及当中更广更深的经验，使得 Sophos MDR 团队可以提升企业防御至超过其自行可达到的水平。

“Sophos MDR 的有形回报包括侦测需要调查的高风险威胁的时间缩短 90%，识别攻击来源和威胁类型的时间缩短 95%，还有提高的侦测准确性。”
Chitale Dairy，印度

“入侵测试人员对于找不到方法入侵感到震惊，此时我们认识到可以绝对信任 Sophos 服务。”
University of South Queensland，澳大利亚

“有了 Sophos MDR，我们大幅缩短了威胁响应时间。”
Tata BlueScope Steel，印度

“我们实时接收任何威胁的通知。”
Bardiani Valvole，意大利

2. 释放 IT 处理能力

威胁捕猎耗时且不可预测。对于艰难处理多个任务和优先级的 IT 专业人员来说，难以跟上挑战：79% 的 IT 团队承认，他们无法完全掌握审核日志以确定可疑信号或活动 。

考虑到攻击对企业的潜在影响，发现可疑情况时，您需要放下一切工作，从而可以立刻调查威胁和采取行动。工作的紧迫性可能阻止团队将精力集中在更加有战略性 — 往往也更有趣的 — 挑战。

使用 MDR 服务，您可以释放 IT 能力，支持业务尤关的活动。使用 Sophos MDR 的企业一致称使用我们服务显著提升 IT 效率，反过来让他们更好地支持企业目标。

“自从实施 Sophos 以后，我们成功腾出了大量运行时间，让我们的团队可以集中精力于提高学生满意度的工作。”
London South Bank University，英国

“Sophos MDR 快速修复或移除威胁并提醒我们注意的能力解放了我们，让我们集中精力于高价值任务。”
Tomago Aluminium，澳大利亚

“有了 Sophos MDR，我们可以支持培养企业的其他方面，例如漏洞管理、打补丁和安全意识。”
The Fresh Market，美国

“Sophos 保持领先于最新网络活动和威胁，这样我们可以专注于为客户和艺术家提供安全的世界级服务。”
CD Baby，美国

5 2022 年 1 月-6 月对 5,600 名 IT 专业人员的独立调查。由 Sophos 委托，并由 Vanson Bourne 执行。

3. 24/7 全天候安枕无忧

由于恶意黑客分布在全球各地，攻击可能出现在任何时刻。您的 IT 团队最不可能在线的时候，例如晚上、周末和假日，攻击的敌手最活跃。因此，威胁侦测与响应是全天候任务；如果您仅在办公时间工作，您的企业将暴露在风险下。

MDR 服务提供 24/7 全天候覆盖，让人放心和安心。对于 IT 团队，这意味着 — 名副其实 — 晚上能够安枕无忧。他们可以放松，知道 MDR 提供商 — 而不是他们 — 将在晚上负责，这样可以重新获得自己的个人时间。

对于高管和客户，24/7 全天候专家覆盖和保持随时高网络就绪，能提供强大的保证，他们的数据和企业本身得到充分保护。

“有 Sophos MDR 团队作后盾，让我晚上可以安枕无忧，因为我知道可以得到 24/7 全天候保护。”
Vancouver Canucks，加拿大

“Sophos 团队充当我们的守门员，用他们的技能在背后守护我们，让我们放心。”
Inspire Education Group，英国

“现在我们对我们安全设立的可靠性、健全性和全面性更有信心。”
Aligned Automation，印度

“有了 Sophos MDR，业务变得更有韧性。”
McKenzie Aged Care Group，澳大利亚

4. 提高专业技术，而非增加人员

威胁捕猎是一个非常复杂的操作。此领域的人才需具备特定而独特的技能组合，威胁猎手需要的典型特征包括：

- **创意和好奇心** – 寻找网络威胁就像大海捞针，威胁猎手往往用数天时间运用多种方法挖掘以寻找威胁。
- **网络安全经验** – 威胁捕猎是网络安全中最高级的作业，因此必须具备该领域的现场经验和基础知识。
- **威胁态势知识** – 了解最新威胁趋势是寻找并消除未知威胁时的必备条件。
- **对立性思维** – 像黑客一样思考在对抗现在人为主导攻击很关键。
- **技术编写能力** – 威胁猎手需要在调查过程中记录所有发现。因此，传递此类复杂信息的能力是从捕猎得出结论的关键条件。
- **操作系统 (OS) 和联网知识** – 这两个领域的出色工作知识至关重要。
- **编写代码/脚本的经验** – 需要帮助威胁猎手生成程序，自动执行任务，解析日志，执行数据分析任务，以协助和推进其调查。

此列表是罕见的能力组合，IT 领域明显的技能短缺加剧这一点，对于大多数企业来说，招募威胁捕猎专家是一件难事。

MDR 服务为您提供专业知识。Sophos 有数以百计的专家分析师，为全球客户提供持续 MDR 服务。Sophos MDR 支持客户扩大其安全运营能力，而无需增加人手。

“现在我们扩大了现有安全做法，无需建立自己的内部能力。”
Hammondcare，澳大利亚

“Sophos 帮助我们跟上网络威胁不断扩大的数量和成熟度，无需扩充我们的安全运行团队。”
Tourism Finance Corporation of India Limited，印度

“Sophos 为我们节约了招聘 5 名负责这项工作的新员工的开支。”
AG Barr，英国

5. 提高网络安全 ROI

管理 24/7 全天候威胁捕猎团队的代价高昂。要提供全天候覆盖，您需要至少 5 到 6 名网络安全人员轮班工作。MDR 服务发挥经济效益，提供具成本效益的方法来保护您的企业，进一步降低您的网络安全预算。

此外，通过提升您的防护，MDR 服务还极大减少遇到高昂的数据外泄的风险，避免处理大型事件的经济负担。2021 年中型企业修复勒索软件攻击的平均成本达到 140 万美元，在防御的投资是理智的经济决策。

如果您使用还提供端点 – 和其他网络安全产品的 MDR 供应商，可以整合至单个提供商，简化供应商管理工作，得到显著的 TCO 优势。

最后，选择可集成您当前安全技术的供应商，可以增加现有投资回报。Sophos 提供跨供应商的 MDR 方法，支持您将现有安全产品用于威胁侦测、调查和响应，增加 ROI。有了 Sophos MDR，您可以使用我们的世界级工具、非 Sophos 工具或者二者组合。

“Sophos 提供了相当于 6 名全职员工的覆盖和工作量，而成本不到一名员工。”
Detmold Group，澳大利亚

“将我们的所有安全产品汇聚在一个平台下，为我们省钱而且提高效率。”
Independent Parliamentary Standards Authority，英国

“Sophos MDR 物有所值。即使每年阻止一起重大事件，也是 10 倍的回报，甚至更多。”
Hammondcare，澳大利亚

“我们每周节约 15 小时，生产力是之前的 2.6 倍。”
Tourism Finance Corporation of India Limited，印度

6 2022 勒索软件现状，Sophos。31 个国家 5,600 名 IT 专业人员的独立调查

选择 MDR 服务时要考虑的要点

不同提供商的 MDR 服务各有不同。评估服务时要考虑很多因素 — 务必研究下面四个方面。

1. **提供的支持和互动程度**

   您希望 MDR 供应商完全管理威胁响应，和您的团队共同管理，还是提醒您的团队从而其可以采取措施?确定您倾向的支持和互动程度，了解供应商比较如何。

   Sophos 充当客户 IT 团队在需要的能力方面的延伸。从全托管 24/7 全天候支持，到支持内部团队的指挥，我们都能满足您的所有需求。

2. **威胁经验的宽度和深度**

   更广泛、更深入应对网络威胁的经验，带来更好的防御。了解供应商 MDR 分析师可以获取的经验水平，如何在客户资产应用其共同经验。

   此外，研究供应商 MDR 团队背后的安全专业知识深度，为帮助分析师排定优先级和调查提醒所提供的环境信息的质量。

   Sophos MDR 保护全球超过 11,000 家企业，服务医疗、教育、制造、零售、科技、金融、政府、服务等众多行业。广泛而深入的经验让我们可以为客户提供无与伦比的防护。

   Sophos MDR 的后盾是 Sophos X-Ops 团队。凭借超过 30 年的恶意软件专业知识和世界领先的人工智能能力，Sophos X-Ops 提供深度信息和分析，帮助 MDR 代理快速确定并消除攻击。

3. **日常客户体验**

   有效的 MDR 供应商会成为您自己团队的延伸 —确保在签订合同后这是您希望合作的供应商。与现有客户交流，了解他们的体验，在独立评价站点查看客户反馈。

   Sophos MDR 是截止 2022 年 8 月 1 日在 Gartner Peer Insights 上评价最多而评分最高的 MDR 提供商，平均分为 4.8/5*。在<270><271此处阅读独立客户证明。

4. **遥测广度和深度**

   攻击敌手不会采用单一技术路线 — 您的 MDR 供应商的威胁捕猎也不应如此。分析师对环境的可见性越大，他们可以越好地侦测和响应恶意活动。向供应商询问其安全集成，在您的 IT 环境集成信号的广泛性。

   Sophos MDR 提供整个 IT堆栈的丰富集成，包括与端点、网络、云、电子邮件和 Microsoft 365 技术的本机和第三方集成。我们的跨供应商方法支持分析师获得整个客户环境的广泛可见性，反过来提升威胁侦测、调查和响应。

总结

随着网络威胁继续进化，MDR 正迅速成为所有规模企业必需的防护。与值得信任并获得证明的 MDR 供应商合作，能够带来很多好处 — 无论您需要完全外包威胁捕猎还是补充或增强您的内部服务：

1. 提升网络防御。
2. 释放 IT 能力。
3. 24/7 全天候安枕无忧。
4. 提高专业技术，不增加人员。
5. 提高网络安全 ROI。

有关 Sophos MDR 的更多信息，请联系 Sophos 合作伙伴或访问 www.sophos.cn/mdr

www.sophos.cn/mdr

Sophos 为所有规模的企业提供行业领先的网络安全解决方案，实时保护其防御高级威胁，如恶意软件、勒索软件和网络钓鱼。凭借成熟的新一代功能，产品在人工智能和机器学习的支持下，可以有效保护业务数据安全。

2022-09-16 ZHCN-WP (DD)

SOPHOS