SOPHOS

通过 Sophos MDR 加强 Microsoft Defender

通过由全球最值得信赖的 MDR 服务提供商的24/7全天候人工主导的威胁侦测和响应以加强 Microsoft Defender，来降低网络风险，提高安全投资的效率和影响力，并进一步提升高可保性。

引言

端点安全是一种不可或缺的保护层，但它无法阻止所有威胁。如今，老练的攻击敌手越来越多地采用隐蔽的战术、技术和程序 (TTPs)，以避免被安全技术阻挡，包括利用未修补的漏洞、盗用凭据和滥用合法的 IT 工具。

为了阻止高级勒索软件攻击和入侵，必须为 Microsoft Defender 补强全天候人工侦测和响应。然而，微软安全技术所产生的海量警报，加上威胁环境的复杂性，使得安全操作对大多数公司来说是一项耗费资源的艰巨任务。

因此，越来越多的组织转向全球最值得信赖和评级最高的托管式侦测和响应 (MDR) 服务提供商 Sophos，以加强 Microsoft Defender。Sophos 的分析师全天候监控、排优先序并响应微软的安全警报，采取即时行动来阻止已确认的威胁。他们还利用 Sophos 的专有侦测技术、威胁情报和人工主导的威胁捕猎来侦测和阻止超越 Microsoft Defender 范围的威胁。

Sophos MDR 旨在与您现有的 IT 和安全投资以及内部资源配合使用，满足您的现况需求。无论您是希望通过额外的专业知识来补充内部团队，还是通过全面的“办公时间外”覆盖范围来扩展网络防御，或者完全外包威胁侦测和响应，Sophos MDR 都可以帮助您实现卓越的网络安全成果。

通过 Sophos MDR 加强 Microsoft Defender

✓ 降低网络风险

- 阻止高级勒索软件攻击和入侵，包括绕过 Microsoft Defender 的人为威胁

✓ 提高安全投资的效率和影响力

- 释放 IT 资源以用于战略计划交付
- 降低发生重大事件恢复成本的可能性
- 从现有的投资中获得更多回报

✓ 提高可保性

- 获得对您降低的网络风险有所认可并回报的改进的保险方案

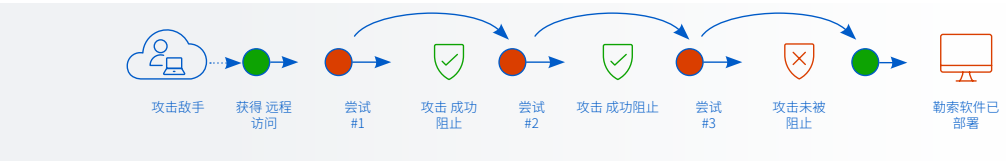
攻击敌手不是强行闯入，而是堂堂登入

现实情况是，仅凭技术解决方案（包括 Microsoft Defender）无法阻止所有网络攻击。活跃攻击敌手（Active adversaries）是指那些根据安全技术和防御者的行动实时调整自己的战术、技术和程序（TTP），并通过实际操作键盘来逃避侦测的威胁行为者。

此类攻击往往带来毁灭性的勒索软件和数据外泄事件，是最难阻止的攻击。它们也变得非常普遍，有 23% 的中小型组织报告称，在过去一年中，他们的组织经历了一次涉及活跃攻击敌手的攻击。有 30% 的 IT /网络安全领导者将活跃攻击敌手视为 2023[1] 年最令他们担忧的网络威胁之一，这反映出这些攻击的潜在破坏性。

仅依靠安全技术来阻止活跃攻击敌手是不够的。这些技术娴熟且难缠坚持不懈的威胁行为者采用多种创新方法来实现他们的目标，其中包括：

- 利用安全弱点渗透到组织内部并在网络内部进行横向移动，包括窃取凭证、未修补的漏洞和安全工具配置错误
- 滥用防御者为避免触发侦测而使用的合法的 IT 工具，包括 PowerShell、PsExec 和 RDP
- 对手根据安全控制实时修改他们的攻击，通过不断转向新技术直到找到实现目标的方法。



主动攻击敌手攻击策略示例

恶意行为者通过模仿授权用户并利用组织防御中的弱点，可以避免触发难以区分合法用户和攻击者的自动侦测技术。

对于防御者而言，当今资金雄厚的攻击敌手也在不断创新和发展其业务模式进一步加剧所面临的挑战。最近，网络犯罪即服务模式的迅速增长，包括勒索软件即服务和网络钓鱼即服务，降低了潜在威胁行为者的准入门槛，同时使得大规模执行更加容易，并提高了攻击的质量。

这些威胁态势的发展导致因勒索软件引致的数据加密率达到了历史最高水平，网络犯罪分子在超过四分之三 (76%) 的攻击中成功加密了数据[2]。

勒索软件的现实

- 66% 的组织在去年受到勒索软件攻击
- 76% 的勒索软件攻击导致数据加密
- 在数据加密的攻击中，30% 的攻击还导致数据被窃取
- 攻击的根本原因#1：利用漏洞 (36%)
- 攻击的根本原因#2：凭据泄露 (29%)

1 网络安全现状2023：攻击敌手对业务的影响，Sophos。

2 勒索软件研究现状 2023，Sophos。

全天候的威胁侦测和响应：现代网络安全必备

好消息是，通过将技术和专业人员结合起来，我们能够阻止先进的、由人工主导的攻击。每当攻击敌手采取行动时，都会产生一个信号。通过将人类专业知识、先进的由人工智能驱动的机器学习模型和扩展式侦测和响应 (XDR) 工具相结合，安全分析人员可以利用来自安全和 IT 技术的信号，侦测、调查并消除最先进的人工主导的攻击，从而防止勒索软件攻击和数据泄露。

虽然全天候威胁侦测和响应现在是任何网络安全堆栈的关键部分，但大多数组织在有效交付上面临着挑战，使其容易受到攻击。缺乏专业知识和资源不足是两个最常见的障碍。

挑战#1：缺乏专业知识

威胁侦测、调查和响应是一项高度专业化的活动，需要深入了解攻击技术和调查策略，并熟练掌握防御者使用的工具。很少有组织内部拥有这种复杂（且昂贵）的技能组合，93% 的组织承认他们觉得执行必要的安全操作任务具有挑战性：

- 71% 的受访者认为从杂讯中识别信号具有挑战性(即了解要调查哪些信号/警报)
- 71% 的受访者难以获得足够的数据来识别信号是恶意的还是良性的
- 75% 的受访者表示，确定事件的根本原因（即攻击者如何进入组织）具有挑战性

当你看到防御者从他们的网络安全工具收到的数据时，挑战的艰巨性就一目了然了。此表包含 Microsoft Defender 事件和事件类别的非尽录列表。

了解警报只是威胁侦测和响应过程的一部分：防御者随后需要应用环境深入资讯和威胁情报，以便能够完全理解威胁并确定最佳行动方案。

事件标题	事件类别
点击可疑网址	初始访问
与 3CXDesktopApp.exe 进程关联的恶意文件或网络连接	恶意软件
创建新用户账户	存留
TS_BL_可疑事件日志清除或使用 Wevtutil 进行配置	避开防御
进程权限升级	权限提升
试图关闭 Microsoft Defender Antivirus 保护	避开防御
侦测到与威胁行为者 Storm-0867 相关的文件或网络连接	凭据访问
TS_BL_Script 引擎连接到互联网	指挥控制
潜在的人为恶意活动	可疑活动
通过 Office Binaries 下载TS_BL_Malicious负载	执行
侦测到新兴威胁活动组织 DEV-0867	凭据访问
侦测到新兴威胁活动组织 Citrine Sleet	恶意软件

来自 Microsoft Defender 的案例创建侦测示例

挑战 2：资源不足

威胁侦测、调查和响应是一项耗时的活动。这一点可以通过以下数据加以说明：在拥有 100-3000 名员工的组织中，侦测、调查和响应警报的中位数时间为 9 小时，在拥有 3001-5000 名员工的组织中为 15 小时。

处理安全警报消耗了大量的 IT 工作时间，而这项工作的紧急性可能会妨碍团队专注于更具战略性的挑战。此外，由于攻击敌手可能在白天或晚上的任何时间进行攻击，威胁侦测和响应需要全年无休地进行，以发挥最大的影响力。许多（如果不是大多数）组织都在艰难力求取得所需的资源。

解决方案：通过托管式侦测和响应 (MDR) 服务来补强防御

由于 52% 的 IT /网络安全领导者表示网络威胁对于他们的组织来说过于先进，无法单独解决，他们越来越多地寻求专业的托管式侦测和响应服务提供商（如 Sophos）来补强和扩展内部能力。

定义 MDR

托管式侦测和响应 (MDR) 是一项全面托管的全天候服务，由专注于侦测和响应技术解决方案无法阻止的网络攻击的专家提供。

扩展式侦测和响应 (XDR) 是一个平台，将来自多个来源的安全数据统一起来，以孤立的单一解决方案无法实现的方式自动化和加速威胁侦测、调查和响应。

Sophos MDR 分析师利用 Sophos XDR 平台代表您寻找、调查和消除威胁。他们利用来自防火墙、电子邮件、云和移动安全解决方案等整个 IT堆栈的信号，加速威胁侦测和响应。

通过 Sophos MDR 加强 Microsoft Defender

Sophos MDR 为 Microsoft Defender 环境提供经过验证的全天候威胁侦测和响应服务。Sophos 的分析师全天候监控、优先处理并响应微软的安全警报，采取即时行动来阻止已确认的威胁。他们还利用 Sophos 的专有检测技术、威胁情报和人工主导的威胁搜索，侦测和阻止超出 Microsoft Defender 范围的人工威胁。

我们发现的越多，行动就越快。Sophos MDR 利用 Microsoft E3 和 E5 授权许可证中包含的额外 Microsoft Security 事件源以及来自第三方防火墙、云、电子邮件、身份辨识和网络侦测与响应 (NDR) 投资的信号，以加速威胁侦测和响应。

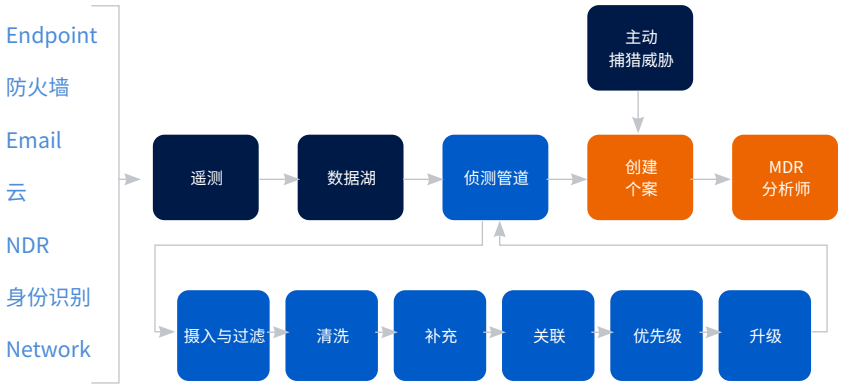
Microsoft Defender 用户可以通过全天候的服务电话随时与 Sophos 安全运营专家联系，并在 Sophos Central 平台上获得关于威胁活动的详细报告。

Sophos MDR 适用于 Microsoft Defender，并与 Microsoft 的Security Event源兼容

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- MS O365 Security & Compliance Center
- Microsoft Azure Sentinel
- Office 365 Management Activity (统一审核日志)

Sophos MDR Security Event Flow

我们获得专利的 Security Event Flow是 Sophos MDR 服务的关键要素。Sophos 数据湖摄入来自整个安全环境（包括 Microsoft Defender）的遥测数据，然后通过我们的侦测管道进行处理，将大量的微软和第三方警报转换为可用的优先级深入资讯，使我们能够有效地进行调查和响应。



Sophos MDR Security Event Flow

摄入和过滤 - 摄入遥测数据和过滤掉不需要的杂讯

清洗 – 将数据转换为规范化的模式，并映射到 MITRE ATT&CK® 框架

充实 – 添加额外的第三方威胁情报和业务背景信息

关联 – 基于实体、MITRE ATT&CK 分类和时间的集群警报

排优先级 – 对警报和集群进行评分，按优先级排序

升级 – 应用逻辑将集群升级到案例以进行调查

Sophos MDR 全球七个安全运营中心 (SOC) 提供全天候覆盖

威胁由全球团队的威胁侦测和响应专家调查和修复，这些专家分布在北美（印第安纳州、犹他州、夏威夷）、欧洲（英国/爱尔兰、德国）和亚太地区（印度、澳大利亚）的七个全球安全运营中心 (SOC) 中。Sophos MDR 拥有超过 500 名专家，覆盖整个威胁环境，包括恶意软件、自动化、人工智能和补救专家，其专业知识的广度和深度几乎无法在内部团队复制。

世界领先的侦测和响应时间

Sophos MDR 借助独特的人力、技术和威胁专业知识的结合，实现了世界领先，仅为 38 分钟的事件响应时间，进而推动出色的网络安全成果：

- 平均侦测时间 (MTTD)：1 分钟
- 平均调查时间 (MTTI)：25 分钟
- 平均响应时间 (MTTR)：12 分钟

谁在使用 Sophos MDR

各行各业的数千家组织都在使用 Sophos MDR 服务，从 IT 资源有限的小公司到拥有内部 SOC 小组的大企业。三种最普及的 Sophos MDR 响应模型是：

- Sophos MDR 完全代表客户管理威胁响应
- Sophos MDR 与内部团队合作，共同管理威胁的响应
- Sophos MDR 支持和补充内部团队，提醒他们注意需要关注的事件，并提供威胁深入信息和补救指导

威胁案例：利用 Microsoft Defender 侦测命令和控制

行业
专业服务

总部
美国

员工
750 人

服务层级
Sophos MDR for Microsoft Defender

Sophos MDR 集成的遥测数据源

✓ Endpoint	X 身份识别
✓ 防火墙	X 云
X Email	✓ Network

什么是命令与控制？

Command-and-Control 命令与控制（也称为 C&C 或 C2）是攻击者用来在受害者网络里与受其控制的系统进行通信并发送命令的技术。

攻击者可以通过各种方式在目标环境和攻击者基础设施之间建立命令与控制通道，包括通过网络钓鱼电子邮件、社交工程、恶意软件、浏览器插件漏洞等途径。攻击敌手通常利用常见的资源和模拟预期的网络流量，以避免被侦测和怀疑。

侦测

Microsoft Defender 生成了一个关于与恶意 IP 地址通信的警报。

微软警报会自动与 Sophos XDR 数据湖中的事件进行关联，以断定攻击是否被客户的防火墙阻止，并且是否影响了多个端点。

调查

Sophos MDR 分析师确认，与 Microsoft Defender 警报相关的恶意连接已被阻止，并且眼前的威胁已被控制。

使用 SophosLabs Intelix 来识别此攻击的攻击家族、入侵指标 (IOC) 以及攻击者使用的已知 IP 地址和域名。

最初的微软警报增加了这一威胁情报，因此可用于根本原因分析。

响应

被入侵的设备被隔离，并且攻击被控制住。

Sophos MDR 确认初次访问是通过电子邮件钓鱼进行的。进行调查以确定钓鱼电子邮件的构成，并确保没有其他用户账户被入侵。

Sophos 提供了减少未来成功钓鱼攻击可能性的建议。

客户优势

无论您是想补充和支持内部安全运营团队，还是希望在没有自己建立 SOC 的运营负担下获得全天候的专家领导的侦测和响应，Sophos MDR 都可以提供帮助。使用 Sophos MDR 加强 Microsoft Defender 的组织可以获得更好的成效，包括降低网络风险，提高安全投资的效率和影响力，以及提高可保性。

使用 Microsoft + Sophos MDR 阻止高级威胁：

由专家团队进行全天候监控和响应
Sophos MDR 分析师全天候监控、排优先序并响应 Microsoft Defender 的警报，采取立即行动来阻止已确认的威胁

侦测和阻止绕过 Microsoft Defender 的威胁
利用 Sophos 的专有侦测技术、威胁情报和人工主导的威胁捕猎提供额外的防御层

增强可见性并情景化 Microsoft Defender 警报
集成包含在您的 E3 或 E5 授权许可证中的其他 Microsoft Security 事件源

立即与安全运营专家取得联系
Sophos MDR 分析师提供全天候的电话支持，并在 Sophos Central 平台提供有关威胁活动的详细报告

降低网络风险

使用 Sophos MDR 加强 Microsoft Defender 的主要优势之一是提高对勒索软件和其他高级网络威胁的保护。

Sophos 分析师具备丰富的经验和熟练运用遥测和威胁捕猎工具的能力，这在内部团队几乎无法复制。这使得他们能够快速准确地在过程中的所有阶段作出反应，从识别重要信号到调查潜在事件和消除恶意活动。

Sophos MDR 保护的组织数量超过任何其他提供商，使我们能够提供无与伦比的“社区免疫力”。通过将一位客户的防御情报自动应用于所有具有类似特征的其他客户，我们能够主动预防该社区的类似攻击。

★★★★★

“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

提高安全投资的效率和影响

Sophos MDR 可以提高您的人员和安全工具的效率和影响力。

威胁侦测和响应消耗大量的 IT 资源。Sophos MDR 负起了这一负担，释放宝贵的 IT 资源用于战略项目交付。同时，可全天候与 Sophos 安全运营专家电话联系，以及通过 Sophos Central 平台取得的威胁活动详细报告，加快内部团队的响应速度和准确性。

通过利用现有的微软和第三方安全工具的遥测技术来加速威胁侦测和响应，Sophos MDR 提升您的防御能力，同时增加您现有投资的回报。

此外，修复勒索软件攻击的平均费用现在达到 185 万美元，而84% 的勒索软件受害者表示攻击导致了业务/收入的损失[2]，因此投资 Sophos MDR 等服务可以降低网络安全的总体拥有成本 (TCO)。

★★★★★

"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威胁的能力解放了我们的人力，让我们集中精力于高价值任务。"

Tomago Aluminium，澳大利亚

提高可保性

Sophos MDR 让组织能够实现许多关键的网络控制，这些控制对于获得保险覆盖和优质保单优惠至关重要，包括全天候的侦测和响应、网络事件响应计划、日志记录和监控等等。

客户报告称，他们获得保险覆盖的机会，以及肯定和奖励其减低的网络风险的保险政策的机会有所提升。

★★★★★

"我们决定采用 Sophos XDR 和 MDR，这对于我们成功降低网络安全保费起到了重要的作用；这与我们最初被告知的保费减了一倍。这是一个显示出真正的价值的巨大胜利，...我实际上收到了首席财务官的一封感谢信，感谢我们团队所做的努力，而 MDR 在其中起到了重要的作用。"

Bob Pellerin，美国 Fresh Market 首席信息安全官

2 2023 勒索软件现状，Sophos。

世界上最值得信赖的 MDR 服务

Sophos 是全球领先的 MDR 提供商，为比其他供应商更多的组织提供保护，针对勒索软件、数据泄露和其他技术无法阻止的威胁。

Sophos MDR 保护着全球各行各业数以千计的组织，让我们拥有对不同行业面临的威胁具有无与伦比的深度和广度的专业知识。我们利用这些广泛的遥测数据来创建“社区免疫力”，将我们保护一个组织时获得的知识应用于所有具有类似特征的客户，提升每个人的防御能力。

当然，最重要的是我们为客户提供的网络安全成果。Sophos 是 Gartner® Peer Insights™ 上评级最高、评论最多的 MDR 解决方案，在 2023 年 6 月 14 日的 300 条评论中获得了 4.8/5 的评分，97% 的客户表示他们会推荐我们。

Sophos 还被 G2 Grid® 报告评为托管式侦测和响应的领导者之一，并在 G2 的整体、中端市场和企业细分市场中被评为 MDR 的领导者。

最受信任

超过 17000 个组织使用 Sophos MDR [2023 年第二季度]

评级最高

独立客户评级为 4.8/5

评论最多

在过去 12 个月中，Gartner Peer Insights 上有 300 条独立客户评价

要了解更多关于 Sophos MDR 以及它如何帮助 Microsoft Defender 用户降低网络风险、提高安全投资的效率和影响力，并提高可保性，请访问 www.sophos.com/mdr

了解更多 Sophos Endpoint Protection

Sophos Intercept X Endpoint Protection 与您紧密合作，在攻击发生时调整您的防御策略。

它拥有强大的多层保护功能，能够在攻击链的各个阶段提供针对勒索软件和复杂威胁的卓越保护，包括基于行为的勒索软件回滚和默认启用的 60 个漏洞缓解措施，无需额外的微调。

我们创新的Adaptive Attack Protection 自适应攻击保护能够动态应对人为发起的攻击，自动部署额外的防御措施，阻止攻击敌手并为防御人员争取时间做出响应。

运行 Microsoft Defender 的 Sophos MDR 服务用户可以随时切换到 Sophos Endpoint protection，为您提供完全的灵活性，并让您的安全部署不过时。

✓ 连续 13 次被 Gartner 评为领导者
自 2008 年以来，Sophos 一直在 Gartner 的 EPP 魔力象限报告中被评为领导者

✓ 在 Gartner Peer Insights中获得顶尖评级
独立客户评级为 4.8/5

✓ G2 适用于企业、中型市场和中小型企业的领导者
完全基于客户评论

✓ 100% 防护得分 - SE 实验室
企业和小企业安全方面的 AAA 评级

要了解更多信息并启用免费试用，请访问
www.sophos.com/endpoint

Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31 December 2022
GARTNER 是 GARTNER, Inc. 和/或其附属公司在美国和国际上的注册商标和服务标志，Magic Quadrant 和 PEER INSIGHTS 是 GARTNER, Inc. 和/或其附属公司的注册商标，并在此获得许可后使用。保留所有权利。
对于研究出版物中描述的任何供应商、产品或服务内容，以及建议技术用户仅选择具有最高评分或其他头衔的供应商，Gartner 不承担任何责任。Gartner的研究发表作品由Gartner研究企业的意见组成，不应被解释为对事实的陈述。Gartner 对于此项研究不做任何担保，明示或者暗示，包括任何用于商业用途或者某个特定目的的承诺。
Gartner Peer Insights 内容包含个人终端用户基于自身经验的意见，不应被解释为事实陈述，也不代表 Gartner 或其附属公司的观点。Gartner 不为本文件所述的任何供应商、产品或服务表示认可，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。

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。凭借备受验证的下一代功能，我们可通过由人工智能和机器学习驱动的产品有效地保护您的业务数据。

2023-06-27 (WP-NP)

SOPHOS