SOPHOS

端点安全买家指南

随着网络威胁越来越复杂，物色合适的端点解决方案的压力也在增加。然而，端点安全市场已经充斥着众多不同的解决方案和没有实际证据支持的营销宣传，这使得为您的组织做出明智的决策变得日益困难。

本指南通过详细介绍端点防护解决方案的关键功能以及您需要防范当今复杂威胁的功能特色，来为您提供清晰的指导。拥有这些深入见解，您将更好地为您的组织做出决策。

当今的安全威胁态势

我们对 14 个国家中 3000 名负责 IT/ 网络安全的领导者进行的独立调查，结果显示，当今的现实是一种双速赛道的网络安全系统，当中攻击敌手和防御者的发展速度各有不同。在多重逆境的作用下，防御者滞后，而攻击敌手却不断加速。

网络犯罪经济的演化

近年来，威胁态势的一个最显著变化是网络犯罪经济已经演变成一个行业，具备一套支持性服务网络和成熟的专业操作方法。

随着信息科技公司转向“即服务”产品，网络犯罪生态体系同样如此。这降低了潜在网络罪犯的准入门槛，并使威胁行为者能够加速攻击的数量、速度和影响。

因此，攻击敌手现在可以大规模执行各种复杂的攻击。94% 的组织在过去一年中遭受了网络攻击。尽管勒索软件是最广泛报告的攻击类型，但组织也经历了许多其他类型的威胁，包括：[1]

27% 恶意电子邮件	**27%** 网络钓鱼（包括鱼叉式网络钓鱼）	**26%** 数据外流（攻击者所为）
24% 网络勒索	**24%** 商务邮件受骇	**21%** 移动恶意软件
18% 加密货币挖矿	**24%** 拒绝服务 (DDoS)	**14%** 擦除程序

请阅读我们的报告《2023 年网络安全现状：对攻击敌手的业务影响》以了解更多信息。

勒索软件仍然困扰着组织

在勒索软件方面，有 59% 的组织表示他们在过去一年中遭受攻击。

2020年	2021年	2022年	2023年	2024
51%	37%	66%	66%	59%

去年您的企业受到过勒索软件攻击吗？
是的。n=5,000 (2024)，3,000 (2023)，5,600 (2022)，5,400 (2021)，5,000 (2020)。

虽然 2024 年报告的攻击率相比 2023 年有所减少，但勒索软件引起的数据加密仍然很高，在 70% 的攻击中，攻击敌手成功加密了数据。

与以往相比，勒索软件引起的成本也达到了前所未有的高度，多个组织报告的平均恢复成本为 273 万美元，较 2023 年的 182 万美元有所增加。[2]

请阅读我们的年度报告《2024 年勒索软件现状》，了解组织在 2024 年面临的实际情况，包括攻击频率、成本和根本原因。

1 The State of Cybersecurity 2023:《攻击敌手带来的业务影响》，Sophos - 这项独立研究在 2023 年 1 月和 2 月进行，调查了来自 14 个国家的 3000 名负责 IT/ 网络安全的领导者。

《2024 年勒索软件现状》，Sophos - 这是一项于 2024 年 1 月至 2 月进行的独立研究，涵盖 14 个国家的 5000 名负责 IT 和网络安全的领导者。

传统方法导致不佳的安全结果

近年来，许多组织面对的商业环境改变了。最终用户可能在办公室工作、远程办公，或者不断在客户和合作伙伴之间移动。公司数据不再仅仅保存在本地，它可以分布在本地、云端和最终用户设备上；同时可以在本地和远程进行访问，以满足地理位置分散的员工的需求。因此，继续坚持传统的网络安全方法通常导致差强人意的安全结果。

一些 IT 安全团队面临的最常见问题包括：

- **技能短缺 -** 寻找熟练的 IT 员工仍然困难。缺乏经验意味着员工可能无法判断安全警报是恶意的还是无害的。
- **杂讯过多 –** 来自多个不同系统的过多警报使操作员应接不暇，不知道如何把要调查的信号 / 警报的排优先级，可能会错过攻击的迹象。
- **数据孤立 –** 威胁信号和警报仅限于特定技术，阻碍 IT 团队全面了解情况并及时处理恶意警报或事件。
- **缺乏集成 –** 安全工具之间或与业务的 IT 基础设施之间缺乏集成，增加了复杂性。
- **手动流程 -** IT 团队花费大量时间来关联事件、日志和信息以了解发生的情况。这些措施延迟了对攻击的识别和应对。
- **被动响应 –** 由于上述原因，许多 IT 团队往往处于劣势，只有在威胁造成损害后才进行响应，而不是在攻击链的早期就加以制止。
- **专注于灭火 -** 日常阻止威胁的功夫会妨碍长期的改进。当 IT 团队在应对紧急情况时，通常没有机会识别事件的根本原因，或者记录攻击和采取的措施的准确信息。这会阻碍解决结构性问题的努力。
- **分布式数据 -** 用户和设备随处可见。因此，数据无处不在，既在本地、云端和设备上，又能够在本地和通过远程访问解决方案进行访问。

应对这些挑战的一种方法是部署一流的端点防护解决方案。

端点防护要素

端点安全解决方案应该为您服务并与您一起工作，根据攻击来调整您的防御措施。至少，现代端点安全解决方案应该采用预防为主的方法，即：

减少威胁暴露 — 阻止恶意内容和基于 web 的威胁，控制对应用程序、网站、外围设备等的访问。

阻止恶意活动 — 防止恶意编码人员和勒索软件攻击者为实现其目的所使用的漏洞利用攻击和技术，识别这种特定活动并在它成为问题之前加以阻止。

促进自适应和自动响应 — 您的防御应该自动应对威胁并适应不断变化的攻击者行为。这不仅可以扰乱攻击者，还可以提醒您的团队他们的存在，并为您的团队争取宝贵的响应时间。

充当威胁猎人的渠道（无论是内部还是托管）— 富含安全深入信息的高质量信号可以大大加速威胁侦测和响应。输入质量越好，分辨率就越快。

实现最佳的安全结果

到此我们已经概述了端点防护解决方案在功能层面上应该具备的功能，那么从更广泛的角度来看其如何为您的组织带来益处就至关重要了。强大的端点防护应该致力于提供最佳的安全结果。

降低网络风险

强大的端点防护可以降低您的网络风险，保护您免受大量网络威胁的侵害。

预防为先的方法

攻击越早被阻止，以后需要做的工作（如有的话）就越少。卓越的端点防护采用多层防护来抵御针对计算机、笔记本电脑、移动设备和服务器的网络威胁和攻击。端点防护保护这些设备及其数据防范恶意软件、病毒、勒索软件和其他恶意活动的危害。

识别安全状态的漂移

安全状态会随着时间的推移而发生变化，原因有很多。在最近的一个与厂商无关的调查中，安全工具配置错误是 IT 管理人员所认为是 2023 年最大的安全风险。[2]

寻找端点安全解决方案，可以持续评估您的安全状态并优化您的配置。这种自动化的方法对于实现强大的安全状态、降低网络风险以及减轻手动操作的繁琐工作至关重要。

简化管理

集中式管理控制台允许 IT 管理员从单个位置监视和管理所有端点的安全设置、政策、排除项目和威胁警报。这简化了安全管理，降低了错误配置的风险，确保了一致的防护。一些集中式管理控制台更进一步，通过自动检查您的安全状态并标记可能危及其的活动或政策更改来提高安全性。

加速侦测和响应

如果环境中出现攻击敌手，分秒必争。采用以预防为主的方法的高质量端点防护可以减少杂讯并提供高保真度的警报。端点侦测和响应 (EDR) 以及扩展式侦测和响应 (XDR) 技术可用于调查这些警报。

一些解决方案更进一步，利用人工智能 (AI) 和威胁情报来自动排序侦测的优先级。这些解决方案确保您的团队知道在哪里集中精力，并加速人为领导的威胁响应。

提高 IT 效率

64% 的企业希望他们的 IT 团队花更少的时间应对紧急的网络攻击问题，而更多时间用于战略性问题。[3] 自动化且易于使用的端点防护有助于 IT 团队实现这一目标。

卓越的端点解决方案能自动阻止和清除大多数威胁。这释放了 IT 容量，使 IT 团队能够更好地优先处理业务有关工作。诸如 XDR 等技术有助于减少信号疲劳，为重要项目腾出更多时间。

这种提高的效率最终让 IT 团队能够从被动的网络安全模式转向主动的模式。这让团队有更多时间在威胁造成长期问题之前找到它们。这反过来也降低了网络风险。

《2024 年勒索软件现状》，Sophos - 这是一项于 2024 年 1 月至 2 月进行的独立研究，涵盖 14 个国家的 5000 名负责 IT 和网络安全的领导者。

3 网络安全现状2023：击敌手引起的业务影响，Sophos - 对 14 个国家的 3000 名负责 IT/网络安全的领导者进行的独立研究，于 2023 年 1 月和 2 月进行。

提高网络安全投资回报率

强化的网络安全能够保护组织免受重大安全事件的财务和运营风险。

投资于卓越的端点防护至关重要。有效的预防要远比事后补救便宜得多。强大的端点防护可以预先阻止大多数威胁，降低遭受攻击和处理相关成本的机会。

此外，一流的端点防护解决方案可以与您现有的安全投资进行集成和通信，以扩展您的防护范围，减少复杂性，并使您现有的防护技术（如电子邮件、防火墙、网络、身份和云等）比以往更加智能和高效。

所有这些都可以提高您的网络安全投资回报率，同时降低您的总体拥有成本。

优化网络保险状态

近年来，网络保险费用大幅上涨，保单申请变得更加复杂和耗时。保险公司要求加强网络控制——实际上，过去一年购买保险的组织中，95% 表示其防御质量直接影响其保险状态 [4]。

优化您的保险状态的关键在于将网络风险降至最低。 投资于强大的防御，包括 24/7 全天候的安全服务和领先的侦测和响应工具，可以带来多重保险利益 :

1. 更容易获得网络保险覆盖（即提高可保性）
2. 有助于降低保费和加强保险条件
3. 降低索赔的可能性，从而减少相关的更高保费
4. 降低发生事件后不获赔付的风险

一流的端点防护技术可作为侦测和响应能力的通道，所以确保您的备选厂应商提供这些功能。现在，对于大多数网络保险公司和组织而言，端点侦测和响应 (EDR) 已经是获得保险覆盖的前提条件，而没有此功能的组织通常很难获得保险。

网络保险公司认为那些用于优化侦测和响应以把网络事件风险减到最低的服务是“黄金标准”。尤其是使用托管式侦测和响应 (MDR) 服务的组织通常被保险公司视为“一级”客户，因为它们代表了最低风险水平。

话虽如此，请寻找能够提供从端点防护解决方案无缝升级到 24/7 全天候全面管理的威胁捕猎、侦测和 / 或事件响应服务的厂商，而这些服务与现有产品和第三方安全控制集成在一起。

5 前沿网络防御在网络保险采用中的关键作用 - Sophos。

评估端点安全：十大问题

既然您对一流的端点安全解决方案有了更清晰的了解，以下是一些应向潜在厂商提出的建议问题。

1. 该产品采用多层预防为主的方法？还是依赖于侦测为主的方法？该技术的核心特定功能是什么？
2. 该产品是否具备侦测和自动纠正安全状态漂移的功能？它能够标示出会增加风险的政策设置更改吗？
3. 该产品是否可以自动响应网络威胁？是否可以自动清理威胁并响应事件？
4. 该产品是否在侦测到人为 " 手按键盘 " 攻击时具有自动调整的防御机制？
5. 该产品是否具有强大的反勒索和防漏洞利用的能力，包括对远程勒索攻击的实时防护？这些功能是否默认启用？这些功能是否需要在您的环境中激活和培训后才能正常工作？
6. 需要多少个控制台来管理该产品？控制台是云托管的，还是需要在本地安装？
7. 该产品是否允许在同一管理控制台和端点 / 服务器上使用相同代理来实现流畅的过渡到 EDR/XDR？
8. 产品的 XDR 功能是否集成并整合了原生和第三方安全控制的警报，以提供对我的环境的全面了解？
9. 产品是否提供了升级路径，使您可以无缝过渡到 24/7 全天候全面管理的威胁捕猎、侦测和事件响应服务，而这与我的现有产品和第三方安全控制进行集成？
10. 厂商是否有第三方测试组织、分析师和客户见证，证明他们的端点防护方法的有效性？

Sophos 安全防护解决方案

现在让我们看看 Sophos 的端点防护方法。Sophos Endpoint 针对高级网络攻击提供无与伦比的保护。严密的勒索软件防护和全面的深度防御方法，在威胁影响系统之前就能阻止最广泛的威胁。强大的 EDR 和 XDR 工具使您的团队能够快速准确地搜索、调查和响应威胁。

以预防为主的方法

Sophos Endpoint 采用全面的方法来保护所有端点，而非依赖于单一的安全技术。通过在前期阻止更多威胁，资源有限的 IT 团队需要调查和解决的事件就更少。

减少威胁暴露

Sophos Endpoint 采用全面的方法来保护所有端点，而不依赖于单一的安全技术。它可以阻止恶意 web 内容和基于 web 的威胁，还能让您控制对应用程序、网站和外围设备的访问。

阻止基于 web 的威胁和控制 web 访问

现实中有许多基于 web 的威胁。组织经常使用下一代防火墙来保护在办公室工作的用户防御网络钓鱼、恶意网站和其他基于 web 的威胁。虽然这可以保护在办公室网络上的端点，但端点也可以在家里、在路上、在咖啡馆等地方使用，而防火墙无法保护它们。

Sophos Endpoint 通过分析文件、网页和 IP 地址来阻止访问网络钓鱼和恶意网站。不论在任何位置，它都可以确保端点持续受到对网络威胁的防护。

此外，SophosLabs 和 Sophos MDR 团队提供实时威胁情报，以保护 Sophos 客户防御新兴威胁。

控制 web、外围设备和应用程序

Sophos 允许您限制端点的活动。这些控制通常与组织的可接受使用政策一起使用。

第一个控制是监控和 / 或阻止访问网站的类别（赌博、社交媒体等）。Sophos Endpoint 允许您监视和阻止网站的类别，而在办公网络内外都在执行。

控制对可移动媒体或其他外围设备的访问还可以进一步减少攻击面。想想用户连接打印机或 USB 存储设备、或者通过 USB 端口给手机充电的情景。这些操作是否被允许？这个功能不仅可以阻止攻击媒介将恶意代码传递到端点上，还可以帮助阻止公司数据的泄露。

应用程序也是另一个需要考虑的类别。通过应用程序控制，您可以阻止在工作设备上运行的应用程序或浏览器插件。在考虑数据外泄方面，您可以考虑使用 OneDrive 或 Google Drive 等云存储应用程序。或者，思考一下像 torrent 程序、TOR 浏览器等应用程序，是否应该允许在您的端点上使用。存在着各种各样的 web 浏览器插件，其中许多具有合法和有益的用途，而其他一些则没有。

阻止恶意活动

下一层的防御涉及使用人工智能、行为分析、反勒索软件、防漏洞攻击和其他技术，以在威胁升级之前快速加以阻止。

Sophos 采用 AI 优先的防护，首先对可执行文件进行 AI 分类。它利用一个经过数百万个良性和恶意可执行文件训练的模型。该模型可以迅速而有效地根据可执行文件的属性去识别恶意可执行文件，而无需任何特定的特征码。

严密的勒索软件保护

Sophos Endpoint 是本地和远程勒索软件防护的最强大零接触端点防御系统。它配备了先进的 CryptoGuard 技术，能够侦测到任何来源的加密迹象。这种通用方法可以阻止新的变种以及本地和远程的勒索软件。它实时检查文件内容的更改，以侦测恶意加密，并阻止在其他设备上运行的远程勒索软件通过网络加密文件。被勒索软件加密的文件将自动恢复到未加密状态，无论文件的大小或类型如何。这将最大限度地减少对业务生产力的影响。此外，它还可以保护主引导记录 (MBR) 防御某些勒索软件攻击中使用的加密。

防漏洞利用攻击

防漏洞利用攻击技术阻止攻击者依赖的行为和技术，以入侵设备、窃取凭据和分发恶意软件。Sophos 为所有应用大规模部署了基于设备的崭新反漏洞利用方法。开箱即用，Sophos 在 Windows 提供的基本防护的基础上搭建，提供最少 60 种专有的、预先配置而经过调优的漏洞缓解措施。其结果是，Sophos 通过阻止攻击链中使用的各种技术，可保障您的组织防御无文件攻击和零日攻击的威胁。

适应性防御

这些额外的动态防御是行业首创的，提供了一种适应攻击环境的自动化防护升级。Sophos Endpoint 会阻止那些在日常环境中本质上并不是恶意，但在攻击环境中却具有潜在危险的操作。这一功能可以动态响应和中断主动攻击，即使攻击者在没有引起警觉，也没有使用恶意代码的情况下取得立足点。

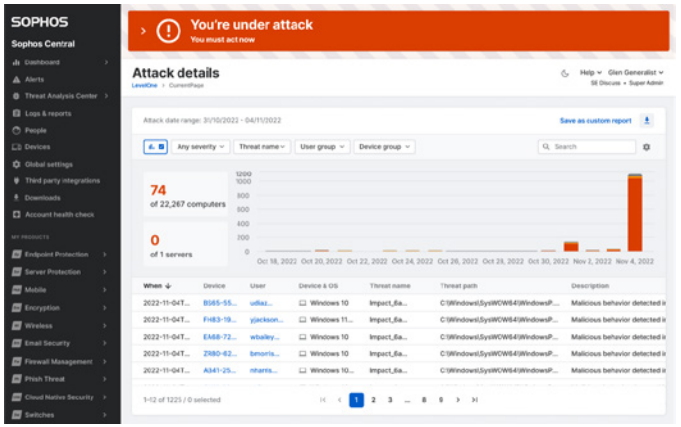
	行为防护	自适应攻击防护	紧急攻击警告
范围	单个设备	单个设备	单个设备
优势	行为引擎可阻止主动攻击敌手的攻击的早期阶段	提高防护的敏感度以预防损害	向客户发出需要立即响应的攻击警报
触发	行为规则	侦测到黑客工具集	侦测到高影响的主动攻击敌手迹象，包括组织级的相关性和界限值
类比	“开启防御！”	“升起防御！”	“红色警戒！”

Adaptive Attack Protection 自适应攻击防护

自适应攻击防护是在侦测到人为手按键盘攻击时，动态启用端点上的加强式防御措施。这样可以消除攻击者进一步行动的能力，最小化攻击面，阻碍和隔离攻击，并争取宝贵的响应时间。

紧急攻击警告

紧急攻击警告会在侦测到您环境中多个端点或服务器上有攻击敌手活动时，发出额外的高影响指标来提醒您发生严重跨资产攻击。这是一种红色警戒情况，表示您正在受到攻击！自动化技术会告知您发生的情况，提供攻击的背景内容和详细信息。您可以使用 Sophos XDR 进行响应，寻求合作伙伴的协助，或与 Sophos Incident Response 事件响应团队合作以帮助应对威胁。



降低网络安全总拥有成本

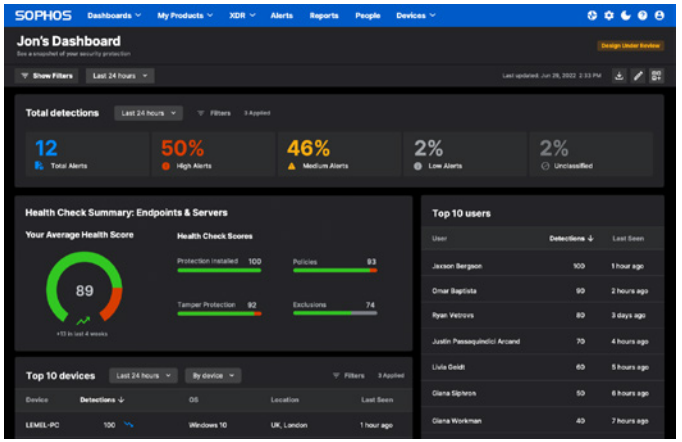
大多数 IT 和安全团队都面临资源不胜负荷的挑战。自动化和节省时间精力是 Sophos Endpoint 的关键主题。任何可以自动化、减少或从 IT 和安全团队的工作负担中剔除的任务都能让这些团队更专注于其他业务工作。

Sophos Central 提供了一个基于云的管理平台，用于管理各种 Sophos 产品（包括端点、服务器、移动设备、防火墙、交换机、接入点、电子邮件和云等）。从一个位置，您可以创建和管理政策、查看侦测和警报、调查和应对潜在威胁，以及在 Sophos 产品中执行其他操作。

Sophos 的推荐防护技术已默认启用，这确保简易设定，和让您立即获得了最强大的防护设置，无需进行复杂的调整。如果需要也可作精细的控制。

识别安全状态的漂移

组织的安全状态随着时间的推移可能会偏离合规性或最佳配置。配置不当的政策设置、排除规则和其他因素都可能对您的安全状态构成风险。Sophos 的 Account Health Check 帐户系统健康检查能够识别安全状态的漂移和高风险的错误配置，让您可以通过简单的点击即可解决这些问题。

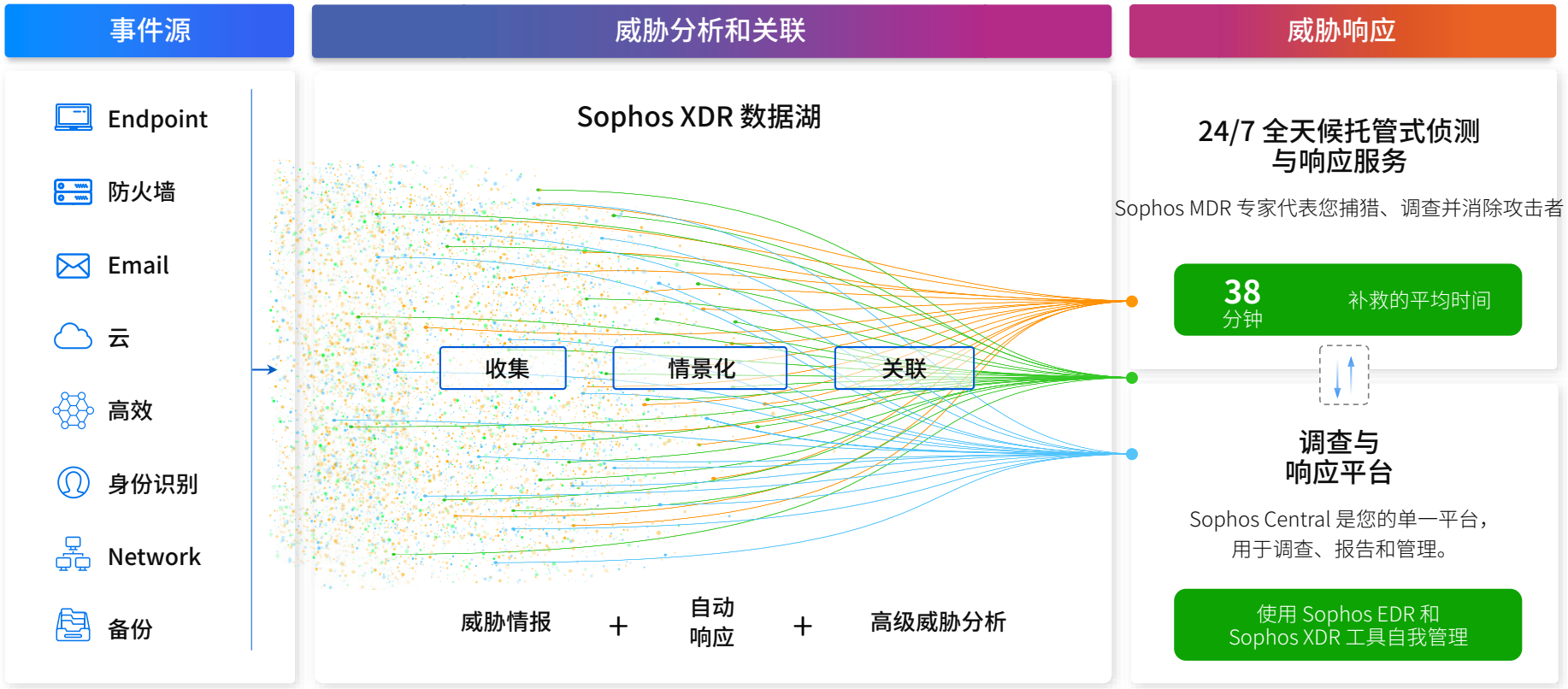


Synchronized Security 同步安全

Sophos 解决方案组合协作效果更佳。Sophos Endpoint 与 Sophos Firewall、Sophos ZTNA 以及其他产品共享状态和健康信息，以提供对威胁和应用程序使用情况的额外可见性。Synchronized Security 同步安全将在执行清理时自动隔离受骇设备，然后在威胁被消除后恢复网络访问，无需管理员干预。

加速侦测与响应：EDR, XDR 和 MDR

Sophos 采用预防为主的方法，自动地在最前端尽可能多地阻止和清除威胁，这意味着 IT 和安全团队需要在后续进行的高质量侦测调查就更少。



Sophos 的预防、侦测和响应方法。

Sophos 端点侦测与响应 (EDR)

Sophos 将强大的侦测和响应能力与 Sophos Endpoint 的万稳固的以预防为主方法整合，使您能够跨越端点和服务器捕猎、调查和响应可疑活动。通过 AI 驱动的分析来优先处理侦测，帮助您确定最佳的关注点。操作员可以远程访问设备以调查问题、安装和卸载软件以及修复任何问题。

Sophos 扩展式侦测与响应 (XDR)

对于寻求更全面威胁侦测和响应能力的组织，Sophos XDR 使您能够在整个安全环境中搜寻、调查和应对可疑活动和多阶段攻击。这是由安全分析师为安全分析师而设计的，是业内唯一将本机 Sophos 和第三方安全控制的遥测数据整合在一起以加速侦测和响应的安全运营工具。Sophos XDR 提供与端点、防火墙、网络、电子邮件、身份辨识、生产力、云和备份解决方案的广泛生态系统的开箱即用集成，使您能够从现有安全工具中获得更多投资回报。

Sophos 托管式侦测与响应 (MDR)

针对没有足够资源来内部管理威胁侦测与响应的组织的需求，Sophos MDR 是由经验丰富的威胁猎手和事件响应人员组成的精英团队提供的 24/7 全天候服务。Sophos MDR 利用来自 Sophos 和第三方安全控制的遥测数据来侦测和消除最精细最复杂的威胁。

Sophos XDR 和 Sophos MDR 都能满足您的需求，它们可以与您现有的技术投资（包括电子邮件、防火墙、网络、身份和云等）集成，帮助您从现有投资中获得更高的回报。

Sophos Incident Response Service Retainer 长约服务

Sophos Incident Response Services Retainer 是年度订购服务，通过预先同意的服务条款，让端点、EDR 和 XDR 客户能够快速联系事件响应专家团队，以迅速阻止主动攻击并让您恢复正常运营。

为什么选择 Sophos

Sophos 是先进网络安全解决方案的全球领导者和创新者，包括 MDR、事件响应以及端点、网络、电子邮件和云安全技术，有助于组织抵御网络攻击。作为最大的纯网络安全厂商之一，Sophos 帮助全球超过 600,000 家企业和超过 1 亿用户抵御主动攻击对手、勒索软件、网络钓鱼、恶意软件等。这无与伦比的对威胁形势的可视度，提供了无与伦比的威胁情报，用于增强 Sophos 产品和服务的防御能力，从而惠及所有的客户。

独立测试

受信任的第三方测试帮助组织对其技术堆栈和安全投资做出明智的决策。然而，随着攻击数量和复杂性的增加，只有当这些测试反映出组织的真实世界情况时，才能获得有意义的结果。

SE Labs

SE Labs 是行业中为数不多的能够模拟网络犯罪分子和渗透测试人员当前使用的现代攻击工具、战术、技术和程序 (TTPs) 的安全测试机构之一。

Sophos 在 SE Labs 端点安全测试中，在企业和中小企业 (SMB) 类别中始终获得 AAA 评级。

SE Labs

MITRE ATT&CK Evaluations

Sophos 在 2024 年 MITRE ATT&CK® Evaluations 的企业产品类别中表现卓越。这一佳绩展示出我们为安全团队提供有关敌手行为的深度背景信息 – 发生什么、为何、如何发生 – 的能力。Sophos 在 Windows 和 Linux 勒索软件攻击场景中，实现了 100% 覆盖敌手活动的“technique”(技术) 级别，这是可能获得的最高评级。

MITRE ATT&CK Evaluations 是全球最受尊崇的独立安全测试之一，这主要归功于其对真实世界攻击场景的精心构建和模拟、结果的透明度以及参与者信息的丰富性。

MITRE | ATT&CK® Evaluations

奖项和分析报告

Gartner

✓ 获评为 2025 Gartner Magic Quadrant 端点防护平台的领导者之一，这是连续 16 次荣获的殊荣。

✓ 在 2022、2023、2024 和 2025 年的 Gartner® Peer Insights ™ 客户之声报告中，荣获端点防护平台 (EPP) 类别的“客户之选”奖。

IDC

✓ 在 2024 年 IDC MarketScape 中小型企业的全球现代端点安全市场研究报告中获评为领导者之一

G2

✓ 唯一一家在 G2 2025 春季整体 Grid® 报告中获评为端点防护套件、EDR、XDR、防火墙软件和 MDR 类别的领导者的厂商。

SE Labs Awards 2025

✓ 在 SE Labs Awards 2025 中，荣获企业端点和小型企业端点类别的胜出者。

客户评价

★★★★★

“Sophos Endpoint Protection 最有价值的功能是其进阶威胁防护，因为 Sophos 利用机器学习、行为分析和基于特征码的侦测等先进技术的组合来侦测和阻止恶意威胁。”

软件开发人员 | 金融（非银行）| 阅读 Gartner Peer Insights 上的完整评论

★★★★★

“针对高级网络安全威胁的单一管理平台解决方案。”

网络管理员 | 教育 | 阅读 Gartner Peer Insights 上的完整评论

★★★★★

“我的经历在行业角度来说是令人满意的。它减少了攻击面并防止攻击在我们组织的网络内传播。凭借其反勒索软件和深度学习人工智能，它可以在攻击影响系统之前就加以阻止，这是其巨大的优势。”

信息通信技术安全办公室 | 广播媒体 | 阅读 G2 评论上的完整评论

★★★★★

“Sophos 是一款极其用户友好且强大的端点解决方案。”

IT 运营经理 | 中型市场组织 | 阅读 G2 评论上的完整评论

★★★★★

“Sophos Endpoint 有助于减少我们面对攻击者的脆弱性，并确保我们客户的系统防御不良行为者的侵害，让我们高枕无忧。”

系统管理和备份与恢复经理 | 企业组织 | 阅读 G2 评论上的完整评论

结束语

网络安全具有高度对抗性，且变化迅速。攻击者不断改进他们的技术来绕过防御，因此安全厂应商和组织必须相应地进行调整。

要做到这一点，关键是使用以预防为主的安全工具。这些工具提供自动化和自适应的防御措施，以阻止或减缓攻击者，为您争取更多时间来响应网络攻击。

同时，了解在端点安全解决方案中要寻找什么以及什么是最佳的安全成效，可以帮助您做出明智的决策。这样，您的组织将能够获得对抗当今网络攻击的最佳防护。

在 Sophos，我们致力于保护组织防御当前和新兴威胁。我们的解决方案旨在帮助组织实现最佳的安全成效。如需了解更多信息，请随时联系我们。

要了解有关 Sophos Endpoint 以及它如何提供针对进阶攻击的无与伦比的防护，请访问
www.sophos.com/endpoint

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。

2025-07-16 ZHCN-WP (NP)

SOPHOS