SOPHOS
Cybersecurity evolved.

Sophos 自适应网络安全生态体系

Sophos 自适应网络安全生态体系 (ACE) 是一个旨在优化防御、侦测和响应的丰富体系。这个体系可以保护互连业务系统的新现实，防御不断变化的结合自动化与真人黑客的网络攻击。

Sophos ACE 利用自动化和分析师，以及 Sophos 产品、合作伙伴、客户和开发人员的意见，打造能够持续改进的防护，形成不断学习和进化的良性循环。最出色的一点在于，可以从小处开始，不断发展壮大。从 Sophos 端点或防火墙技术开始，奠定坚实的基础。

变化的蓝图

网络安全蓝图不断发展，近年来业务环境和攻击性质都发生了天翻地覆的变化。

业务变化：互连性

企业不断寻找提高生产力和效率的方式，因此形成了高度互连的供应链，以及相应提供支持的基础设施和技术。将数据和应用程序迁移到云端，可以带来许多优势，如随时随地工作，降低运营成本，提高性能和可缩放性，促进全球数字供应链的发展。

与此同时，新冠疫情迅速加快了向居家/远程办公的转变，打破企业外围的概念。应该假定，可以在任何地方找到人、应用程序、设备和数据。

这些相互连接而分散的系统为我们提供很好的服务，但同时也带来了新的安全挑战。许多企业难以绘制网络的范围，只能保护连接到网络的各个系统。

在规模机会的引诱下，智能自适应对手一直针对这些系统。最近（但不是唯一）的一个证据是 2020 年 12 月的 SolarWinds 攻击，受到影响的受害者包括大型技术供应商和小型企业，也包括最高水平的公共领域实体。

攻击转变：从自动向可操作

处理网络安全时，很容易忽略一个重要而被低估的事实：在关键系统和数据战斗中，防御者处于上风。

报道新安全外泄事件的每日头条消息起到了一个重要用途：作为警示案例，提醒我们采取预防措施和保持警惕。但这些案例是规则的例外情况。企业每天成功防御数以千计的外泄尝试并没有头条报道。

不仅网络安全效果极大提高，而且最新工具和托管安全服务比以往更加容易获取，更加经济。所有人都可以获得防勒索软件、漏洞攻击防御、行为侦测和防网络钓鱼等技术。

这些功能得到人工智能和机器学习的促进、改进和加速，正在解决 MITRE ATT&CK 框架中的已知对手的战术、技术和程序，以及从未见过的新攻击。这些改进通过弥补漏洞、封闭路径、拦截技术，让一些攻击的成本超出攻击者已经适应的水平。安全的改进非常显著，过去的“攻击者只需要成功一次”的说法已经不再成立。要挣钱，攻击者需要在一次攻击中成功多次。

事实上，这种情况已经将攻击者的方法从自动恶意软件，向结合自动和手动黑客的更全面方法转变。对手的主要目的是保持不被发现，最好的方法是像员工一样行动 – 使用本地工具、本地设备和典型流量模式。

这些成熟的攻击需要大量人力投入，对受害者造成的成本最高。攻击者能够利用对受害者环境的深入了解造成最大破坏 – 并要求最大回报。

IT 安全向安全运营转变

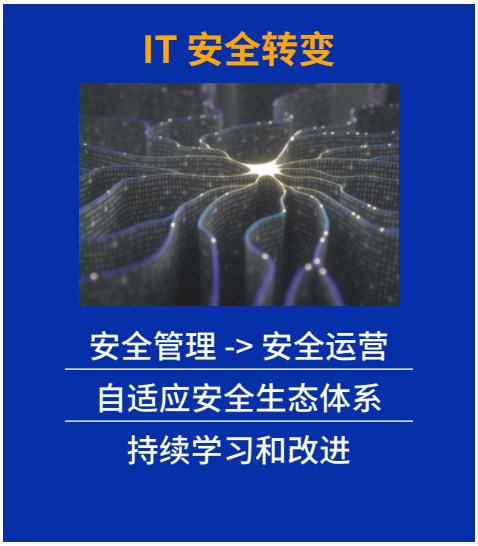
此类企业和攻击转变需要 IT 安全的进化。企业面临智能对手，在不断推进过程中不断改变目标，需要 IT 安全团队制定对策，提高胜率。

首先，需要从**安全管理向安全运营**的步骤改变。以前“设置以后就不管”的安全策略已经过时；因为攻击者转向手动操作，IT 安全也需要追踪和侦测可疑行为与事件，防止其成为外泄。

安全团队需要尽可能在攻击链早期发现可疑行为，为防御者提供在破坏前响应的能力。再隐秘的攻击者也会留下痕迹，安全团队需要找到并追踪痕迹，早早阻止攻击。现在不是从噪声中找出信号的问题，而是在变为更强信号前识别关键弱信号的问题。信号越强，距离外泄越近。利用合适的工具，可以主动侦测并修复 IT 问题，避免对手能够发现并用于攻击。

在企业互连程度如此高的情况下，安全同样需要如此。IT 安全团队需要从未集成的安全点产品向**自适应安全系统**转变，尽可能自动阻止，同时允许操作员搜索和侦测较弱信号（例如可疑行为和事件）防止其外泄。

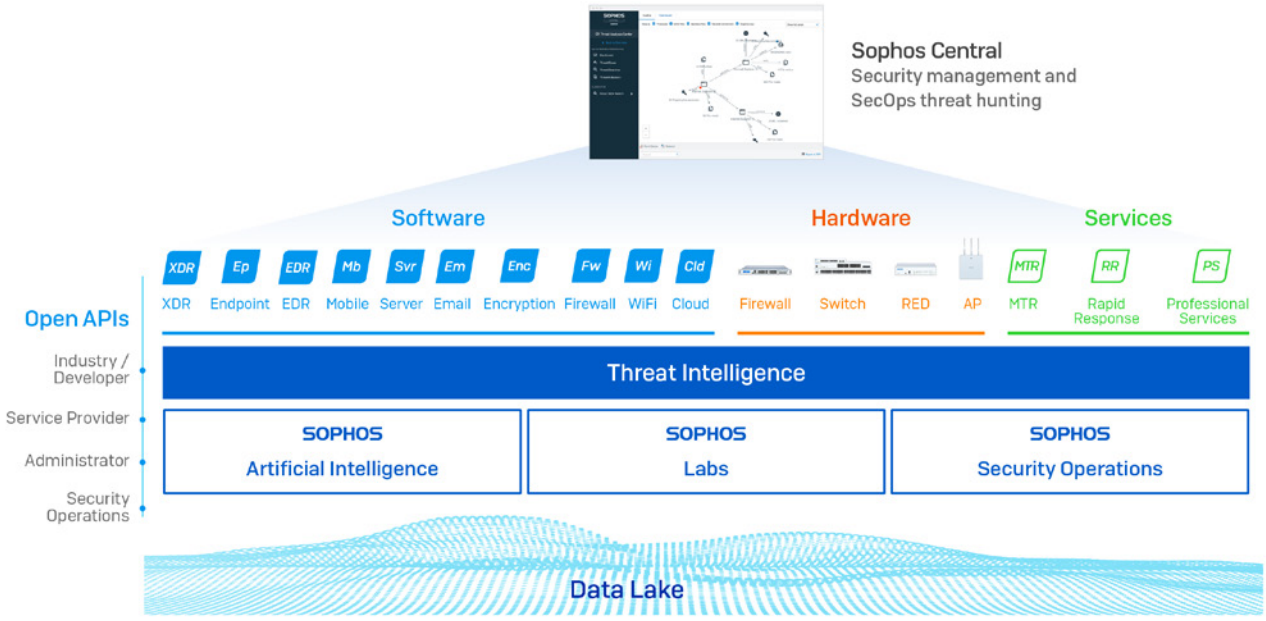
业务环境和攻击始终在发展。IT 安全的未来是能够实现唯一反馈回路的系统，从而**不断学习和提高。**操作团队发现的新信息和事件可以自动化，改进防御，减少进入系统的新攻击数量。同样，随着自动软件的发展，操作员可以更快找出可疑行为和事件，从而减少事件。这种良性循环不断提高企业及其连接业务的整体安全。



Sophos 自适应网络安全生态体系

好消息是这个系统已经存在。Sophos 的自适应网络安全生态体系 (ACE) 可以解决这个新的现实。利用自动化和分析师，从安全管理向安全运营转变。自动化可以更快分析和应对行为与事件，同时人类分析师更擅长关联多个可疑信号并解释其含义。

Sophos ACE 旨在保护业务和网络的互连性。它可以保护任何位置的系统和数据，不断学习改进，防范技术和攻击的未来改变。



Sophos ACE 从 SophosLabs，Sophos 安全运营（通过托管威胁响应服务，对数以千计算客户环境进行先进威胁追踪的人类分析师），以及 Sophos Artificial Intelligence 小组的集合**威胁情报**开始。这些实时智能功能不断改进我们全球领先的**软件**与**硬件**产品中的下一代技术。

单个集成 **data lake 数据湖**将我们所有产品和威胁情报来源的信息，与实时分析相结合，支持防御者主动找出可疑信号，防止攻破。同时，**开放 APIs** 支持客户、合作伙伴和开发人员打造与系统交互的工具和解决方案。一切通过 **Sophos Central 管理平台**管理。所有安全在一个位置，获得无与伦比的效率。

这五个要素（威胁情报、下一代技术、数据湖、API 和中央管理）可以协同打造能够不断学习和改进的自适应网络安全生态体系。由于综合生态体系的性能非常强大，可以按需要量使用。许多客户从端点防护或防火墙开始，然后以自己的速度展开。

去年将许多安全运营中心转化为虚拟 SOC。安全专家可以从任何位置管理 Sophos ACE，为企业提供找出最佳全球安全人才的能力。或者，我们的专家可以采用服务形式为您管理威胁侦测和响应。

Synchronized Security 的发展

Synchronized Security，即 Sophos 产品通过 Security Heartbeat™ 共享实时信息并自动响应事件的功能，多年来已经成为我们防护的奠基石。2015 年推出时，Synchronized Security 在市面上独一无二，我们继续提供任何安全供应商与更深入跨产品信息的最深入集成。

> “Sophos 继续以防火墙和端点安全产品之间的 XDR 功能领跑市场。”
>
> Gartner
> Gartner Magic Quadrant for Enterprise Network Firewalls，
> 分析师：Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 2020 年 11 月 9 日

Sophos 自适应网络安全生态体系以 Synchronized Security 的自动化和集成为基础，进一步扩展 Sophos 网络安全体系。

更高可见性

没人知道下次攻击来自哪里，人类操作员无法做到监控一切。您需要能够监控一切的系统，帮助您快速应对刚出现的威胁。所以我们扩大生态体系，加入更多技术，包括新的 Sophos 扩展侦测与响应 (XDR) 和我们的 API。Sophos 产品可以发现并记录环境中的所有可疑事件、行为和侦测，方便您掌握需要的信息。

更多数据

数据湖组合并关联所有传感器的信息，提供更深入的跨产品信息。操作员可以直接用 Sophos Intercept X with EDR 和 Sophos XDR 查询数据湖，发现整个环境中的可疑行为和事件 – 阻止问题变为外泄。

更多情报

随着托管威胁响应 (MTR) 服务的快速发展，我们能够增加来自专家威胁追踪的实时数据，补充侦测数据。同时，我们继续改进 SophosLabs 的 AI 模型和威胁侦测输入。

更多集成

SophosLabs、Sophos AI 和 Sophos Security Operations 协同工作，集成专业知识，为所有客户带来福利，形成一个良性循环。例如，PowerShell 是一个具有很多不错用途的合法工具，但也被攻击者广泛滥用。MTR 操作员根据现实经验，培训 AI 模型区分“好”PowerShell 用途和“坏”PowerShell 用途。然后用 AI 学习更新整个系统，提高客户防护。

Sophos 自适应网络安全生态体系解决方案在行动

Sophos ACE 是一个在现实场景中不断提高和扩展防护的在线系统。2021 年 3 月，一个名为 Hafnium 的组织利用 Microsoft Exchange 的 ProxyLogon 漏洞进行攻击。这是一个零日漏洞，攻击者利用 Exchange 设计中的固有弱电，避免触发任何直接侦测。

得知漏洞后，Sophos 托管威胁响应 (MTR) 服务立刻更新传感器检测，加入与 ProxyLogon 相关的行为。利用数据湖已有的信息，Sophos MTR 立刻获取需要的所有输入，发现并纠正与该漏洞有关的恶意行为。

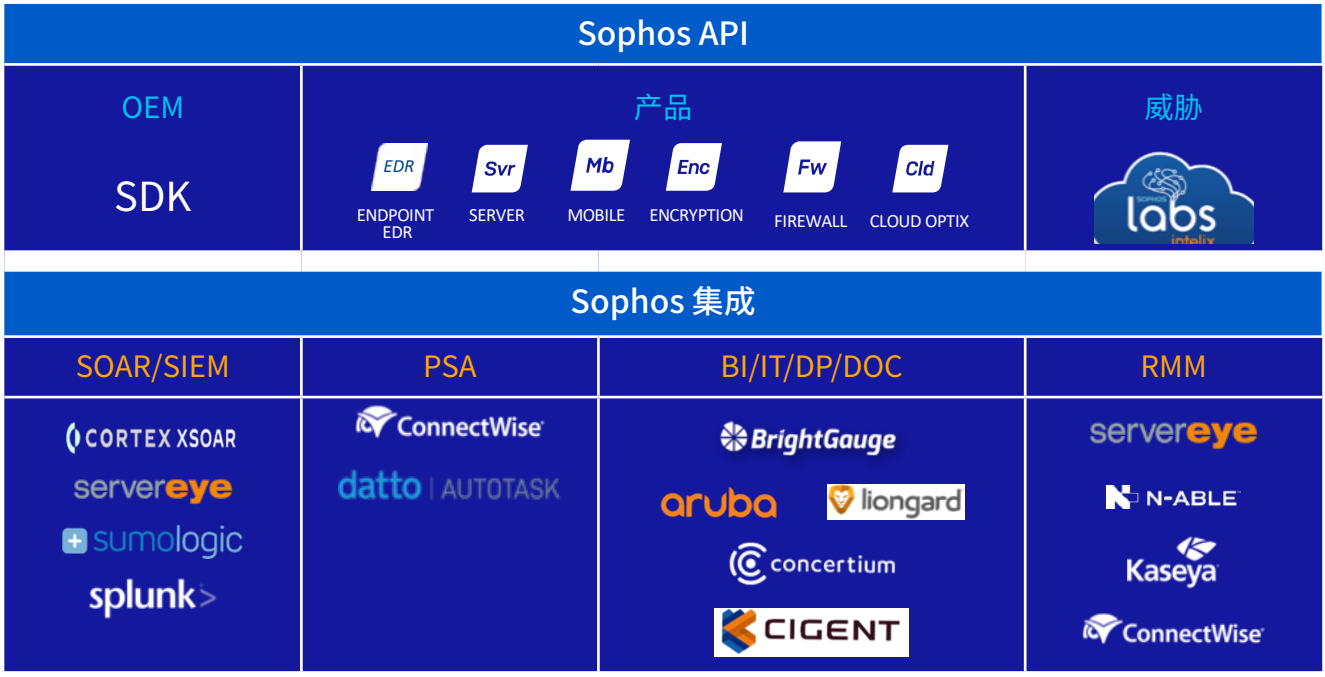
此外，他们将威胁追求技能与 Sophos EDR 技术结合，发现与攻击有关的新伪像或威胁指标 (IOC)。这些指标直接与 SophosLabs 共享，后者利用其发布与 Exchange 漏洞有关的更多 IOC，为所有 Sophos 客户提供更多防护。

具有强大集成和开放 API 的开放平台

在互连的世界中，网络安全务必与更广泛的业务环境集成。网络安全具有多方面，Sophos 自适应网络安全生态体系支持多种安全需求，包括：

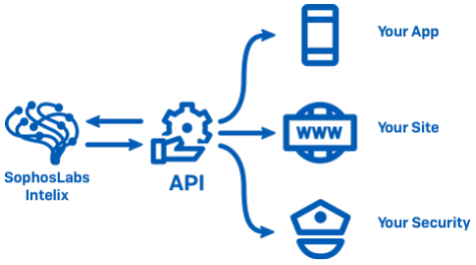
- MSSP – 支持为客户提供先进网络防御
- 渠道合作伙伴 – 简化业务流程
- ISP – 允许其确保提供的互联网服务的安全
- 中小型企业 – 促进创建自定义工具，控制并实现安全

混合 API 和集成已经就位（未来还有更多）Sophos ACE 每天已经处理超过五百万个 API 请求。



API 展示：SophosLabs Intelix™

Intelix 是一套简单而快速响应的 RESTful API，支持应用程序识别、分类和防御威胁，提高其安全。Sophos 生态体系客户、合作伙伴和开发人员可以利用这些 API 进行云威胁查找、静态文件分析和动态文件分析。可以访问 https://www.sophos.com/zh-cn/labs/intelix.aspx，了解 SophosLabs Intelix API 的更多信息。



Sophos ACE：带来真实业务影响

Sophos 自适应网络安全生态体系带来的优势。组合下一代技术：来自 SophosLabs、Sophos AI 和 Sophos Security Operations 的威胁情报；集成、自适应、始终学习的系统；通过 Sophos Central 平台中央管理，给防护和效率带来巨大影响。

下一代技术 + 安全威胁信息 + 集成自适应系统 + 集中式管理

同时运行 Sophos Firewall 和 Sophos Intercept X 的客户已经告诉我们，如果没有 Sophos 网络安全系统，他们现在的安全人手需要加倍，才能维持相同的防护水平。他们还告诉我们，他们遇到的安全事件减少了，可以更快地发现和响应出现的问题。Sophos ACE 建立在此基础上，进一步转型网络安全 TCO 以及防护。

开始使用

Sophos 网络安全生态体系非常灵活，入门就和部署一个 Sophos 防护产品或服务一样简单。企业直接从 Sophos AI、SophosLabs 和 Sophos Security Operations 的组合威胁情报专业知识获益。您可以随时扩大生态体系，符合您的业务需求。最受欢迎的起点包括：

用于端点或服务器的 Sophos Intercept X（提供增加 EDR 或 XDR 功能的选项）

Sophos Firewall – 硬件、软件或虚拟

Sophos Managed Threat Response (MTR) 服务

要了解更多，请与 Sophos 代表交谈，查看我们的网站，或开始免费试用。

Gartner Magic Quadrant for Enterprise Network Firewalls，

分析师：Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 2020 年 11 月 9 日

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。

了解更多勒索软件以及 Sophos 如何帮助您保护企业安全的信息。

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。

2021-04-26 (SB-NP)

SOPHOS