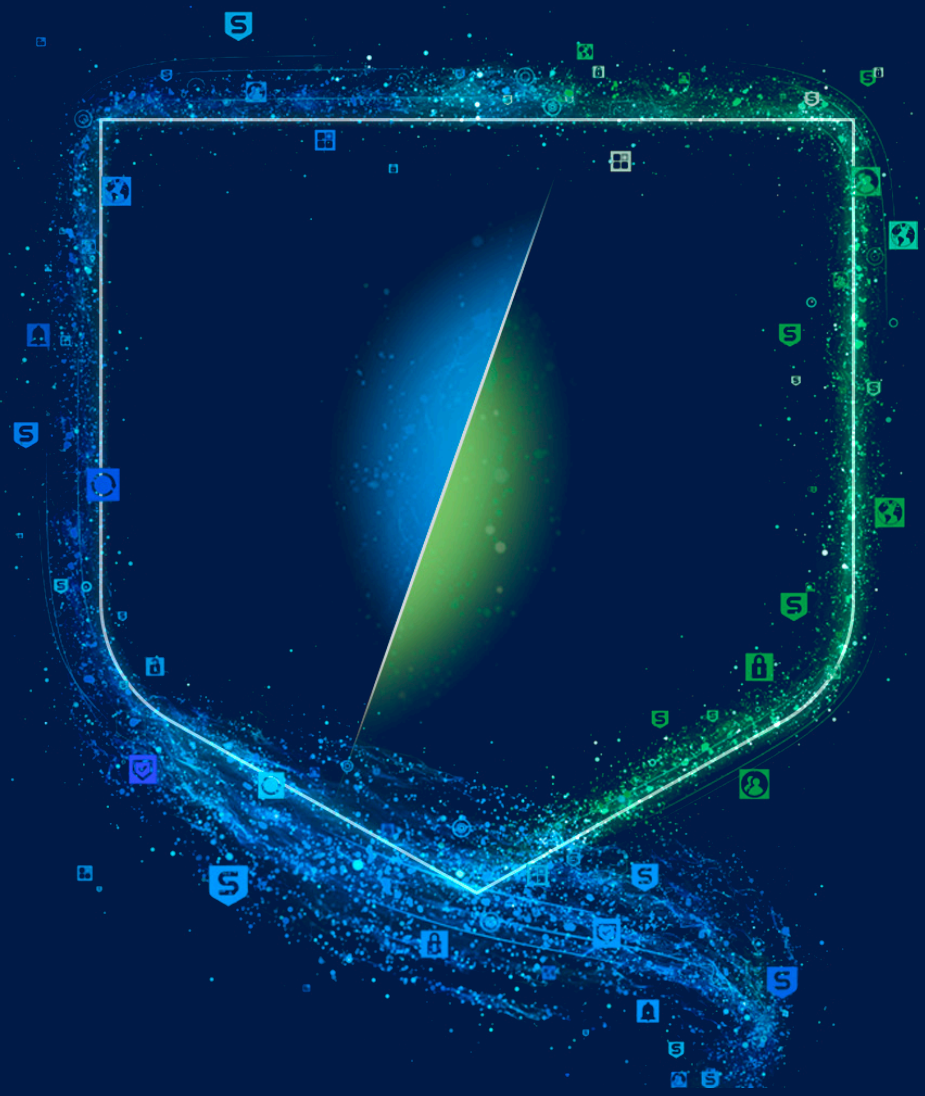
SOPHOS

Sophos AI 驱动的网络防御

强大且经过实战验证的产品和服务，结合了 AI 技术与人类专家的专业知识，通过 Sophos 自适应 AI 原生平台提供。



SOPHOS

自 2017 年以来，Sophos 一直致力于推动 AI 在网络安全领域的应用的前沿，将 AI 技术与人类网络安全专业知识相结合，旨在阻止各种威胁，无论它们来自何处。安全分析师能够更迅速地做出明智决策，而组织则可以放心运营，信赖 Sophos 强大且经过实战验证的 AI 解决方案能够为其提供有力支持。

我们将深度学习和生成式 AI 能力融入到解决方案中，有效解决客户面临的最关键问题，并通过业内最大的 AI 原生平台提供。凭借超过 600,000 个多样化的客户环境中的攻击数据进行训练，Sophos 自适应 AI 原生平台为客户提供无与伦比的防御能力，并进一步增强防守者的应对能力。

AI 水平设定

AI 是一个简短的缩写，涵盖了广泛的不同规模和用途的技术。尽管生成式 AI 模型，如谈到 AI 时人们通常举出的 Microsoft Copilot 和 Google Gemini，但它们只是其中的一部分。
在 Sophos，我们利用多种 AI 模型来加速网络安全，并根据具体的安全目标选择最合适的模型。

类型

深度学习 AI（应用）

利用人工神经网络来识别模式并做出决策，模拟人类大脑的工作方式。它将所学内容应用于执行任务。

示例：

Sophos URL 安全模型
侦测恶意 URL、钓鱼网站及其他基于网络的威胁。

部署于：
Sophos Endpoint、Sophos Firewall、Sophos Email、Sophos Mobile

生成式 AI（创作）

基于现有数据的结构和模式创造 (生成) 全新的内容。

示例：

Sophos AI 个案摘要工具
提供易于理解的威胁活动摘要，并推荐后续步骤。

部署于：
Sophos XDR、Sophos MDR

大小

大规模 AI 模型

帮助用户执行广泛的任务。

示例：

Microsoft Copilot、Google Gemini
这些大型语言模型 (LLM) 能够帮助用户完成非常多种的任务。它们经过大量的公开数据的训练。

小型 AI 模型

为特定、专门的使用场景设计、训练和构建。

示例：

Sophos Android 深度学习模型
基于 Sophos 专有的 Android 数据进行训练，专门侦测 Android 平台上的恶意软件。

部署于：
Sophos Mobile

AI 应用于您防线中的每个部分

Sophos 解决方案中超过 50 个（并且数量持续增长）深度学习和生成式 AI 模型，能够提供快速、有效的防护，不论网络威胁在何时何地操作。我们的 AI 驱动的网络安全减少暴露风险，自动阻止威胁，并帮助安全分析师更快做出明智决策。

Sophos 产品和服务中的 AI 应用示例

缓解威胁风险
减少受攻击的暴露面

SOPHOS MANAGED RISK
利用 Tenable 漏洞优先级评级 (VPR) AI 模型预测 CVE 在 28 天内被利用的可能性

自动阻止威胁
防止攻击执行

SOPHOS ENDPOINT
多个深度学习模型防护已知和前所未见的攻击，包括 Microsoft Office 方案、PDF 和富文本格式 (RTF) 文件中的威胁

SOPHOS FIREWALL
通过 SophosLabs Intelix 提供的 AI 驱动的零日威胁情报

SOPHOS ENDPOINT & FIREWALL
Web 保护模型侦测恶意 URL、钓鱼网站及其他基于网络的威胁

SOPHOS EMAIL
深度学习驱动的自然语言处理 (NLP) 识别冒充企图

SOPHOS MOBILE
Android 深度学习模型基于专有 Android 数据进行训练，专门侦测 Android 平台的恶意软件

捕猎、调查和响应
识别并消除威胁

SOPHOS XDR、SOPHOS MDR
AI 生成的威胁评分帮助分析师排工作处理优先序

SOPHOS XDR, SOPHOS MDR
AI 个案摘要提供清晰的侦测概述和建议的后续步骤

SOPHOS MDR
AI 驱动的个案分流加速调查进程，并消除重复个案

SOPHOS XDR、SOPHOS MDR
AI 指令分析通过检查创建侦测的指令，提供对攻击者行为的洞察

SOPHOS XDR、SOPHOS MDR
AI 搜索让分析师使用自然语言来快速搜索数据，加速调查过程

通过 Sophos 自适应 AI 原生平台提供

Sophos Central 是个自适应 AI 原生平台，提供无与伦比的保护，并增强防御者的能力。动态防御、经过实战验证的 AI，以及一个开放且集成丰富的生态系统汇聚于业界最大的 AI 原生平台。

Sophos Central

动态

- 防护措施会根据全球超过 600,000 个多样化客户环境中的攻击情报不断更新。
- 自适应防御会自动响应威胁。
- AI 模型通过 300 名安全运营专家的实时输入不断增强。

开放

- 与 Sophos 产品、其他厂商的产品或两者的组合兼容，跨多个操作系统环境。
- 集中数据和集成工作流优化安全任务，提升人类生产力，加速安全成效。

最大

- 广度：利用来自全球 600,000 多个不同规模和行业客户的攻击遥测数据。
- 深度：使用来自跨 IT 环境的数据，包括 Sophos 和非 Sophos 技术，以及运行 Windows、iOS 和 Linux 操作系统的设备。

双赢：人类专业知识与 AI 技术的结合

我们的团队是 AI 驱动的网络安全解决方案的核心，将他们的专业知识融入到开发过程的每一个环节。

- Sophos X-Ops，跨部门网络安全工作组，拥有深厚的**威胁分析和攻击敌手行为**知识，帮助识别 AI 如何、何时能够产生最大效果。
- Sophos AI 团队运用广泛的 **AI 专业知识**来设计、构建并维护 50 多个专门用于网络安全的 AI 模型。
- 凭借 30 多年**的网络安全工程专业知识**，我们确保 AI 模型能够成功集成到 Sophos 产品和服务中，以及安全功能的推出。

通过 AI 部署获得的经验不断推动我们的人类专业知识进步，帮助我们持续优化模型，发现新的应用，并推动技术进步。

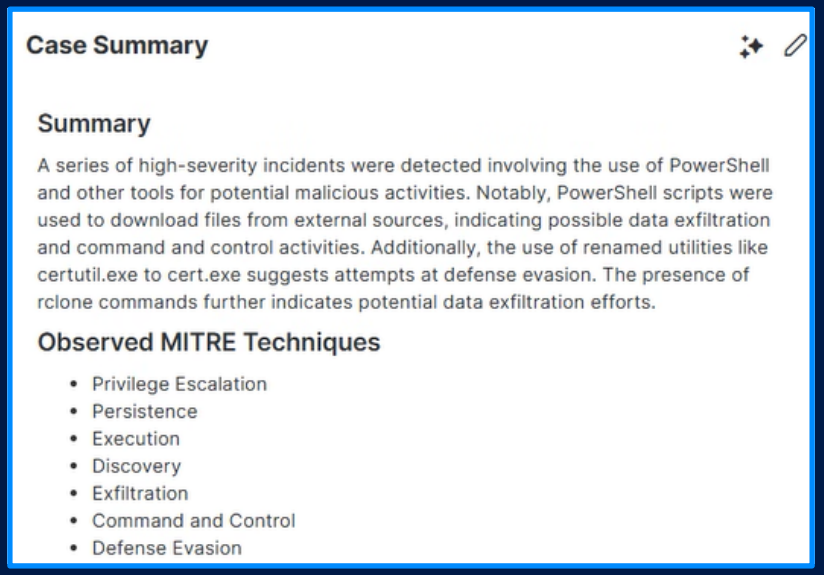
Sophos AI 使用案例

通过生成式 AI 加速安全运营

Sophos 扩展式侦测与响应 (XDR) 强大的生成式 AI 功能让安全分析师更迅速地消除攻击敌手威胁，从而提升分析师和企业的信心。

- **AI 个案摘要**提供简洁明了的侦测概述和后续步骤建议，帮助分析师快速做出明智决策。
- **AI 指令分析**通过分析生成侦测的命令，洞察攻击者行为。
- **AI 搜索**以自然语言搜索来加速日常任务的处理，降低安全操作的技术难度。
- **AI 个案助手**为分析师在处理个案时提供支持和建议，帮助资深和新手分析师更迅速地应对对手（2025 年第一季度推出）。

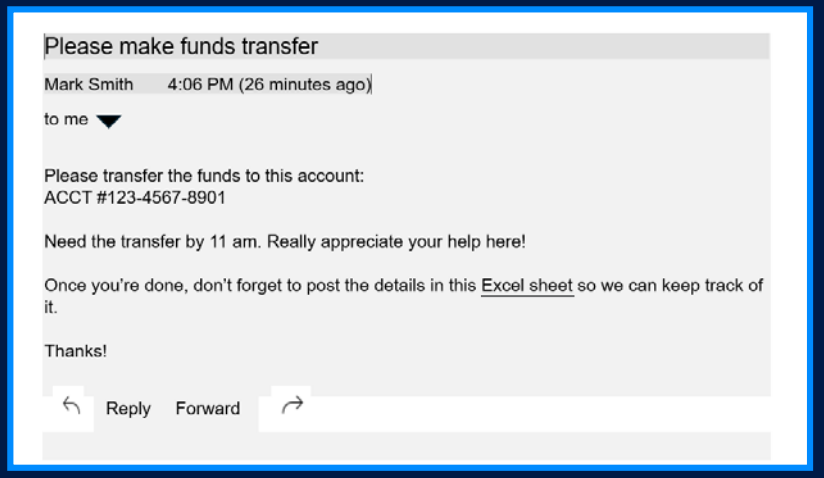
Sophos 生成式 AI 功能可选择启用，您可完全掌控。



通过深度学习防止企业电子邮件欺诈

Sophos Email 中的深度学习驱动的自然语言处理 (NLP) 技术能识别冒充行为，企图引导用户误信欺诈或钓鱼邮件为合法邮件。

Sophos Email 利用 AI 分析邮件的主题和内容，从语气和措辞中识别可疑对话。冒充行为会被自动拦截，攻击被防止，管理员会收到通知。



值得信赖的经验

自 2017 年以来，我们一直在成功地使用 AI 加速网络安全。选择 Sophos，您可以安心专注于业务，抱有信心 AI 为您的组织带来的是回报而非风险。

风险	SOPHOS 的方法
组织未能从 AI 投资中获得预期的收益。	**以结果为导向的 AI** 凭借多年的 AI 专业知识，我们知道如何实现实际的影响。
开发、训练和部署不当的 AI 解决方案可能造成实际损害。	**以安全为先的流程** 我们强大的开发流程让客户放心使用 Sophos AI。
厂商专注于 AI 本身，而非它带来的益处。	**切实的好处** 我们强大且经过实战验证的 AI 驱动解决方案通过更快消除威胁，并帮助分析师做出明智决策，带来实质性的优势。

Sophos AI 团队

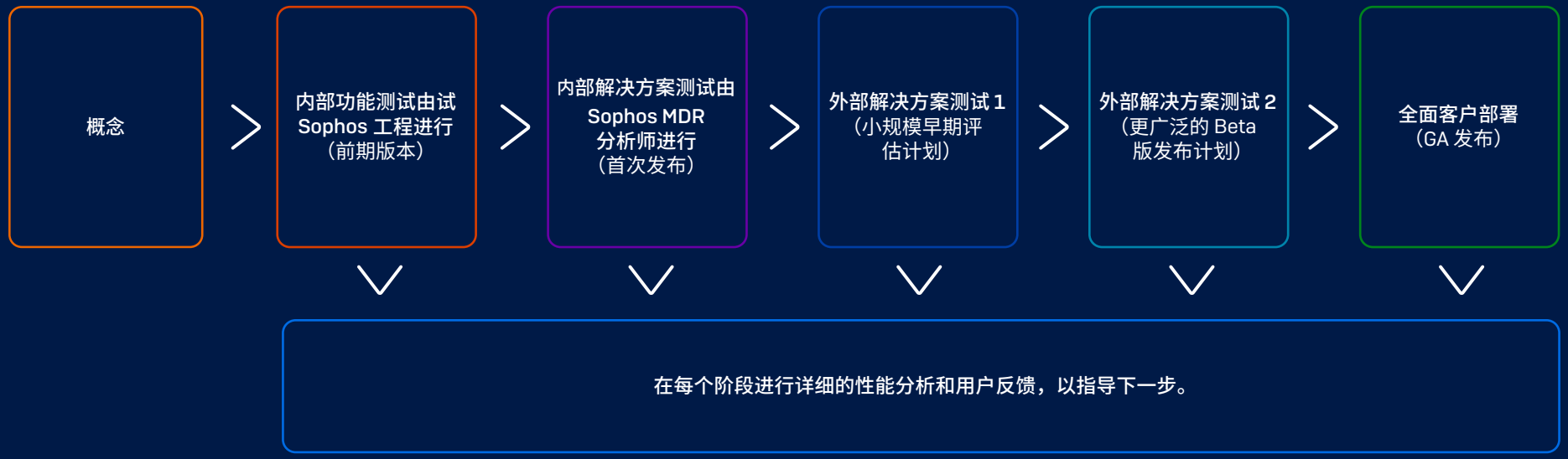
Sophos AI 团队由专家组成，他们深知如何运用 AI 来加速实现正面的网络安全成效。
这个全球专门小组专注于两大领域：

- 在 Sophos 的解决方案中开发和应用 AI
- 推动 AI 在网络安全领域的创新研究

Sophos AI 团队通过公开报告和活动分享其研究成果。请访问 **Sophos AI 博客**，查看其最新发布。

强大的生成式 AI 开发流程

生成式 AI 在网络安全中的好处与其潜在的风险并存。Sophos 为所有生成式 AI 工具部署严格的流程，从概念到全面部署。在每个阶段进行详细的性能分析和用户反馈，以指导下一步的开发过程。



与 Sophos 在 AI 潮流中安全航行

欲了解更多关于 Sophos AI 驱动的网络安全解决方案，以及它们如何帮助您实现目标的信息，
请访问 **www.sophos.com** 或与您的 Sophos 合作伙伴或代表联系。

SOPHOS

2025-01-14 SB-ZHCN (MP)