SOPHOS

不断发展的网络安全：SOPHOS如何为业务带来改变

通过五个客户案例研究来量化 Sophos 网络安全系统的实际保护和效率优势

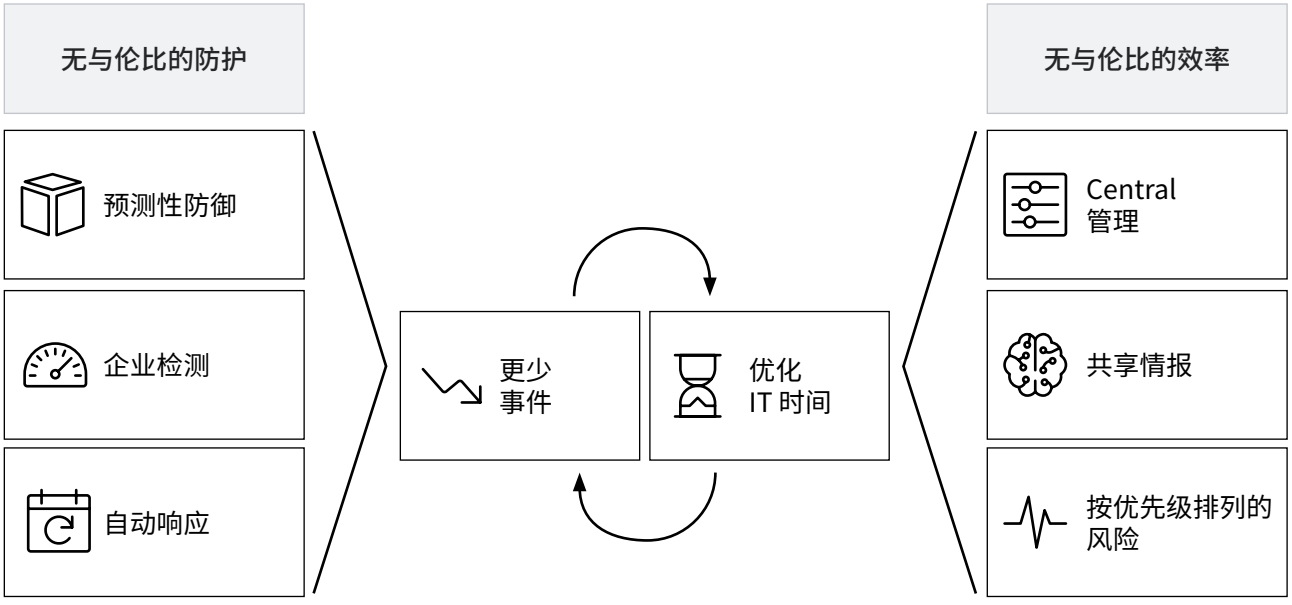
Sophos 白皮书 2020 年 6 月

简介

选择 Sophos 防护威胁，您将享受到全世界首个（也是最佳的）网络安全系统：

- **全套的下一代产品和服务。**我们可以满足您对于网络安全的所有需求：端点、移动和服务器防护；EDR；下一代防火墙；电子邮件；统一端点管理；等等。无论您运行的是完整的云应用、混合应用还是现场部署，我们都能为您提供保护。
- **无与伦比的防护** 得益于最新的技术以及我们世界知名的数据学团队、威胁追踪团队和 SophosLabs 团队的专业实力。企业级检测，可以阻止当前的高级攻击，人工智能支持的深度学习神经网络，可以预见性地阻止从未见过的威胁。Sophos 产品还提供实时配合，进一步提升您的防护。产品之间共享威胁健康和安全信息，自动响应事件。
- **单个管理平台。**通过我们的云管理平台 Sophos Central 来管理所有的 Sophos 防护工作。利用共享情报，提供按优先级排列的风险信息，而引导式调查则可以为每个场景提供建议措施。

Sophos 网络安全团队**提升您的防护**，同时**降低总体拥有成本 (TCO)**。建立一个良性循环，使无与伦比的防护和无与伦比的效率得以不断地互相强化。



信任圈可以帮助您显著提高 IT 团队的效率，减少威胁 – 所有这些都无需增加人手。

为客户带来改变

为了衡量 Sophos 网络安全系统在真实客户环境中的影响，我们采访了北美、欧洲和亚洲的五名 Sophos 客户。每个客户的场景各不相同，具有各自的组织结构、挑战和业务要求。但是，所有客户都具有一个共同点：

客户表示，如果不采用 Sophos 下一代网络安全系统的话，他们需要**加倍**安排安全人手，才能保持相同的防护水平。

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。使用 Sophos 的结果包括：

- IT 安全人手减少 50%
- 用于日常网络安全管理的时间减少 90%以上
- 用于发现问题的时间减少 90%以上
- 安全事件数量减少 85%
- 显著减少整个企业的停机时间

客户 A：美国医疗提供商

- 4,500 名员工
- 80 名 IT 人员，其中 3 名专门负责网络安全
- Sophos 产品：Intercept X Advanced with EDR、XG Firewall、Intercept X for Server Protection（Windows、Linux 和虚拟机）

客户 A 是一名地区性医疗提供商，其服务包括门诊和住院治疗、医疗、疗养院和一系列专业服务。

为业务带来改变

- **IT 安全资源要求减小 50%**
  客户目前雇用三名专业网络安全人员。他们计算，如果不使用 Sophos，将需要额外雇用三名全职安全分析师，专门负责事件响应。

  在采用 Sophos 之前，团队必须完成大量手动工作，识别网络上发生的情况，大量时间用在了识别事件上。Sophos 现在主动为他们识别问题，并在 95% 的情况下自动解决问题。这样，团队就可以将重心放在解决需要人为干预的 5% 问题上了。

- **日常安全管理减少 90%以上**
  IT 安全经理每天用 30 分钟时间浏览日志，研究值得关注的内容。在采用 Sophos 之前，他通常需要整整一天才能获得相同程度的信息和信心。利用 Sophos，将所有数据整合在一个管理平台中，以一致的格式显示，便于识别和响应问题。这样就减轻了每天的工作负担，不需要跨多个来源对应数据来确定可疑还是不可疑、恶性还是良性。

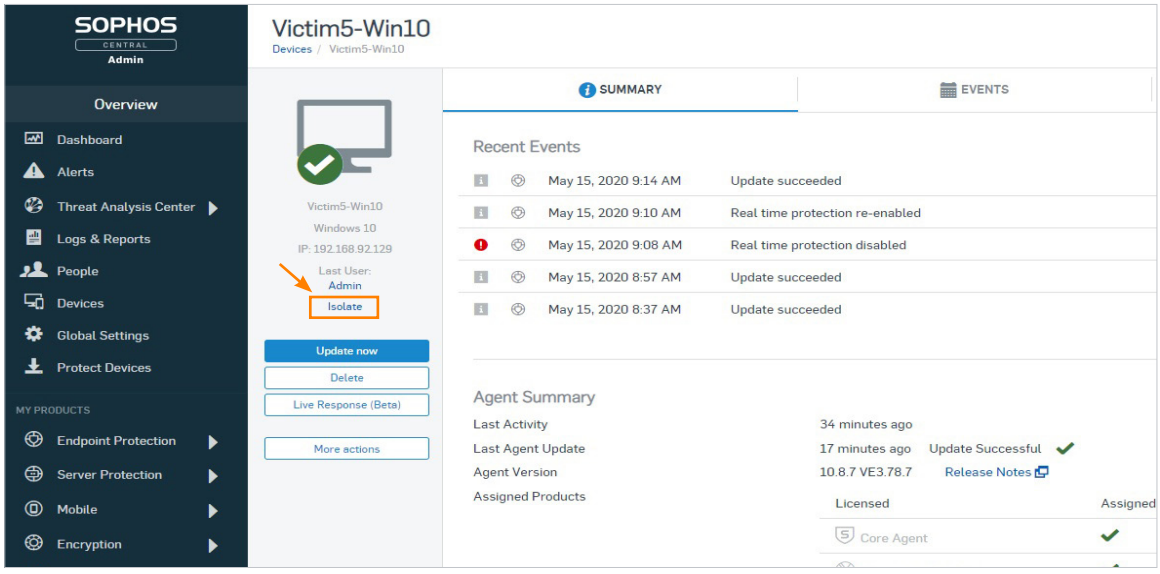
- **安全事件减少 85%**
  作为医院，他们保管大量的敏感个人可识别信息 (PII) 以及支付信息，因此成了网络罪犯的目标。在采用 Sophos 之前，他们平均每天遇到 3 起值得进一步研究的事件。有了 Sophos 以后，这一数字下降到平均每三天一起。

- **研究事件的时间减少 90%以上**
  在采用 Sophos 之前，彻底研究事件需要约 3 个小时，包括在本地访问受影响的计算机。现在通过 Sophos Central 平台，最多只需 15 分钟就能远程完成所有操作。

  以前团队需要停用网络适配器，然后实际访问设备，来研究和解决问题，最后手动重新连接。他们还需要适应用户的工作流程；例如，等待医生没有治疗患者，访问该系统进行治疗前。通过 Sophos Central 控制台隔离设备的功能，支持团队可以远程研究问题，不会影响用户和系统可用性。

  研究时间缩短，以及远程管理所有内容的功能，还极大减少了对医院内其他用户的干扰。

- **调查过程中持续保护**
  以前需要把设备从网络断开，进行手动干预，离线时无法获得保护更新。有了 Sophos 后，当 IT 团队隔离设备来研究问题时，设备保持在线，继续接收保护更新。



客户 B：印度教育服务提供商

- 700 名员工
- 总部位于班加罗尔，在印度各地和东南亚地区设有当地经理
- Sophos 产品：Intercept X Advanced with EDR、Intercept X Advanced for Server、XG Firewall

客户 B 为印度和东南亚地区的大学院校提供教育服务。他们通过班加罗尔总部的中央 IT 团队，以及派驻现场的当地 IT 经理团队，保护数以万计的学生的安全。

为业务带来改变

- **日常安全管理需要的资源减少 50%**
  以前他们雇用四名工程师管理日常安全。自从采用 Sophos 后，只需两名工程师负责整个公司的安全。
- **识别需要研究的高风险领域的时间减少 94%**
  在采用 Sophos 之前，需要占用客户 3 到 4 个小时来识别需要重点关注进一步研究的重要问题。现在只需 10 到 15 分钟，就可以在 Sophos Central 中识别整个企业内的安全问题。
- **识别网络恶意通信来源的时间减少了 98%**
  以前的网络安全实施，需要 2 天（或更长时间）来识别网络上导致性能或安全问题的设备。现在只需 15 分钟就可以发现问题并开始处理。
- **用于管理固件更新的时间减少了 95%**
  以前的网络安全实施还带来可用性和风险问题，因此每次软件更新需要 3 到 4 小时。现在有了 Sophos，每次更新只需 10 分钟。每年 20 到 25 次更新，相当于每年节约 75 小时更新时间（两个完整工作周）。

客户 C：美国临床试验提供商

- 150 名员工，分布在 4 个地点
- 两名 IT 员工，负责所有方面，包括网络安全
- Sophos 产品：Intercept X Advanced with EDR、XG Firewall、Central Device Encryption

客户 C 是私人企业，提供新药物法规认证所需要的临床试验数据。业务性质决定其保存了大量敏感个人信息。

为业务带来改变

- **IT 资源要求减少 50%**
  该客户仅用 2 人团队管理所有 IT 事宜。目前每天用一个小时浏览日志和研究值得关注内容。如果不使用 Sophos，他们表示仅管理日志一项，就需要额外雇用 1 到 2 名安全工程师。
- **处理潜在问题的时间减少 33%**
  以前，遇到设备安全问题时，他们的解决方案是重新映像计算机，需要 90 分钟到 2 小时。现在他们可以进行深度研究，包括系统隔离、彻底威胁追踪、完整安全扫描和最终修复，只需约 1 小时，无需重新映像。Sophos 方法带来的另一个优势是，只要研究结束，用户就可以恢复生产力；而使用重新映像的话，重置计算机配置和自定义设置还会损失时间。

- **可以明显更快发现问题，威胁风险减小 88%**
  有了 Sophos 网络安全系统，IT 团队可以在可疑事件出现数分钟内识别需要研究的新问题。在 Sophos 之前，需要一整天浏览日志找出需要研究的问题。响应时间的缩短极大地减少了威胁。
- **改善用户行为**
  有了 Sophos，用户现在知道 IT 团队可以快速解决问题和事件，不会导致停机或额外工作。因此，IT 团队报告用户现在更加愿意报告问题或顾虑（如单击了电子邮件中的潜在恶意链接）。

客户 D：塞尔维亚公共服务提供商

- 300 名员工
- 10 名 IT 员工，其中 4 名专门负责网络安全
- Sophos 产品：Intercept X Advanced、Intercept X Advanced for Server、XG Firewall、Sophos Email、Sophos Mobile

客户 D 是一家业务范围覆盖塞尔维亚首都贝尔格莱德的公共领域企业。该客户是 Sophos 的长期忠实用户，已经升级至通过 Sophos Central 管理的下一代产品。

为业务带来改变

- **用于日常安全管理的时间减少 50%**
  现在他们每天用 30 分钟进行安全管理，在 Sophos Central 管理控制台中检查提醒、日志、用户、设备、流量和应用程序，确保一切正常。以前，这一日常安全管理工作需要至少两倍的时间来确定要解决的高优先级问题，和采取的措施。
- **相比其他供应商，用于日常安全管理的时间减少了 90%以上**
  客户预计，根据以前的经验，使用其他供应商的产品时，日常安全管理需要一整天，而使用 Sophos 只需 30 分钟。
- **零重大安全事件**
  客户已经使用 Sophos 很多年，最近 8-10 年没有出现过重大安全事件。这并不是说没有遇到过威胁；而是 Sophos 产品在后台快速安静解决问题，用户甚至没有意识到。

客户 E：斯洛文尼亚法规认证机构

- 150 名员工，其中三分之一远程办公，三分之二在总部
- 2 名 IT 人员负责包括网络安全在内的各方面的工作，加上外部供应商支持主要项目
- Sophos 产品：Sophos Endpoint Protection、Intercept X Advanced for Server、XG Firewall、Sophos Mobile、Sophos Device Encryption

客户 E 是一家公共领域机构，负责确保产品符合所需的标准。该客户是 Sophos 长期忠实用户，已经升级至通过 Sophos Central 管理的下一代产品。

为业务带来改变

- **用于日常安全管理的时间减少 50%**
  他们每天用 15-30 分钟进行安全管理：检查防火墙，查看提醒，清理电子邮件隔离区等。以前他们用时至少是两倍。效率增加的原因包括能够在一个位置管理所有安全产品，无需在应用程序和服务器之间切换。
- **零重大安全事件**
  客户已经记不起使用 Sophos 以来的重大安全事件。

结束语

正如客户证词所证明的那样，Sophos 的网络安全方法带来了切实的保护和效率的提升，帮助您显著地提高 IT 团队的效率，减少威胁 – 所有这些都无需增加人手。

不同的客户有着不同的业务环境、资源和挑战，但他们一致表示，运行 Sophos 网络安全系统后，IT 安全工作量减少 50%。用于日常网络安全管理的时间减少 90%以上，安全事件数量减少 85%。

要更多了解 Sophos 的网络安全解决方案和开始无义务免费试用，请访问

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

© 版权所有 2020。Sophos Ltd. 保留所有权利。
英格兰和威尔士注册编号 2096520，The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos Ltd. 的注册商标。本文提到的所有其他产品和公司名称是其各自所有者的商标或注册商标。

200612 WPZHCN (NP)

SOPHOS