

云安全状态管理解 决方案帮助 Sophos 控制其云资产

Sophos 为全球超过 3,000 个用户和 400,000 的客户保护基础设施与数据。Sophos 内部 IT 与安全团队为企业每日安全运营使用多个 Sophos 产品。现实环境是一个宝贵的试验场, 为公司提供宝贵信息, 激励 Sophos 产品系列的不断改进和提高。

Sophos
Abingdon, UK
行业
国际安全软件提供商

网站
www.sophos.cn
用户数量
3,000+

Sophos 解决方案
Sophos Cloud Optix

“有了 Sophos Cloud Optix, 我们极大减少了提醒疲劳, Sophos Cloud Optix 内置的强大人工智能关联数据, 向我们展示真正有意义和可操作的信息。”

Ross McKerchar
CISO
Sophos



挑战

- 获得整个云资产的可见性
- 防止过度提醒产生倦怠反应
- 从一个集中位置管理云帐户和云安全
- 重新确认已有安全控制措施按预期工作

Sophos 为全球超过 3,000 个用户和 400,000 的客户保护基础设施与数据。Sophos 内部 IT 与安全团队为企业每日安全运营使用多个 Sophos 产品。现实环境是一个宝贵的试验场, 为公司提供宝贵信息, 激励 Sophos 产品系列的不断改进和提高。

Sophos 如何在整个公共云环境中实现无人能及的可见性?

Sophos IT 和 Sophos Cybersecurity 团队为整个云资产寻找可见性、安全和合规性工具, 资产包括超过 200 个公共云帐户, 采用 Amazon Web Services (AWS) 的 Amazon Elastic Compute Cloud (Amazon EC2) 和 Microsoft Azure。Sophos CIS 全球运营经理 Andy Joel 和 Sophos 资深红队主管 Dave Davison 主持评估工作, 对多个产品的概念评估进行深度验证。

他们评估的一些工具包括只有有限安全功能的云管理解决方案。其他解决防那缺乏可缩放性—虽然具有精心设计的单面板管理控制台, 但在任何给定时间只能处理个位数的帐户。“环顾市场上的现有产品, 企业存在一个重要误区, 他们往往认为云管理解决方案包含云安全, 但事实并非如此。加入一组简单配置检查并不意味着云安全。在现代不断变化的环境中, 坏人利

用自动化和人工智能进行攻击, 您需要成熟解决方案分析网络流量和用户活动日志, 主动获悉潜在攻破。对我们来说, 这就是 Cloud Optix”, Davison 表示。

团队发现, 唯一真正满足所有要求的解决方案是 Sophos Cloud Optix。在 Sophos, 业务迅速运转变化, 产品团队不断创建新的云帐户用于开发。对于 Joel 来说, 该工具解决了一个最大的鼓励: 对所有高流动生产环境的可见性, 并确保其安全。

直观且易于使用的集中管理中枢提供高动态 Sophos 云资产的全面视图, 包含仪表板和云基础设施可视化, 加上通信流量; 提醒摘要与详细信息; 合规性状态。

“Sophos Cloud Optix 为我们提供了整体资产的最高级可见性, 远远超出大多数云管理工具所声称的水平”, 他解释。Sophos Cloud Optix 提供所有云环境内企业资产的自动发现。通过网络拓扑可视化和持续资产监测, 安全团队可以快速响应并弥补安全风险。



Sophos Cloud Optix 如何帮助改进安全流程，同时提供额外保证？

一个 Sophos Cloud Optix 示例是最近发现一些用户帐户没有启用多重身份验证，这与公司政策直接冲突。尽管 Sophos 设有启用多重身份验证的流程，仍然发生了此政策违规行为。通过 Sophos Cloud Optix, Joel 发现该流程并没有完全按预期工作，因此相应调整。

“如果您没有环境的完整连续可见性，将发现不了潜在可疑、恶意或不合规行为。Sophos Cloud Optix 帮助我们洞悉一切，保护一切，采取合理措施”，Joel 表示。

部署 Sophos Cloud Optix 的另一个发现是，Sophos 在整个云资产中有少量高优先级提醒和零个关键提醒，包括 Sophos Central 管理平台的生产帐户。Joel 指出，“对于设计和建立生产环境的人

来说，这是最好的证明。Sophos Cloud Optix 带给我们信心和保证，让我们相信在合理的位置采取了所有合理控制，并且安全预期工作。”

Sophos Cloud Optix 提醒与竞争对手技术的区别是什么？

Davison 还指出，竞争对手往往有数以千计的提醒，令安全团队焦头烂额，Sophos Cloud Optix 则不同，利用人工智能驱动监测、侦测和安全分析。所有这些实现了一套按优先级排序且相关的“智能提醒”，既准确，又可以采取操作。它帮助 Sophos 团队更快补救安全风险，将自动提醒排序与上下文信息相结合，避免提醒疲劳，帮助安全团队关注最相关的内容。


“我发现，一些供应商尝试说服客户，提醒数量越多越好，但事实并非如此。我们不希望筛选数以百计的优先项。我认为 Sophos Cloud Optix 在这个方面真正抓到了精髓。关键提醒往往才是我们希望处理的”，他表示。

自定义配置提醒和修复的灵活性是 Sophos 这类企业的另一个重大优势，这类企业有许多不同小组—每个小组具有自己的安全要求—产生云载荷。例如，某个提醒在一些帐户中分类为“关键”，而在其他帐户中分类为“中等”。

Sophos CISO Ross McKerchar 进一步说明这一点：“有了 Sophos Cloud Optix, 我们极大减少了提醒疲劳，其他解决方案以量取胜，海量没有区分的提醒令安全团队焦头烂额。Sophos Cloud Optix 内置的强大人工智能关联数据，向我们展示真正有意义和可操作的信息。这让我们极为准确了解安全状态和风险等级，通过自动流程优先安排并主动修复。这是安全人员针对安全人员打造的安全产品。如果我们没有这项技术，我们也会希望使用它。”

在不断变化的云环境中，Sophos Cloud Optix 如何帮助保持持续合规性？

合规性是 Sophos Cloud Optix 为 Sophos 满足的第三个要求。通过现成模板、自动化、自定义策略和协作工具，解决标准外部合规性法规和内部治理问题，在企业所有云帐户中确保一致最佳做法。在云端创建载荷后，确定适用的合规性流程和实施方式通常是一个挑战。Davison 和该团队期望在不久的将来使用 Sophos Cloud Optix, 降低公共云环境中的治理、风险以及合规性的成本与复杂性。



“在现代不断变化的环境中,坏人利用自动化和人工智能进行攻击,您需要成熟解决方案分析网络流量和用户活动日志,主动获悉潜在攻破。”

Dave Davison
资深红队主管
Sophos

免费试用所有 Sophos
Cloud Optix 功能。
www.sophos.cn/cloud-optix