SOPHOS
Cybersecurity delivered.

在环境、工作负荷和身份识别中实现完整多云架构安全覆盖

在云工作负荷、云环境和权限管理中集成网络安全工具，在 Amazon Web Services、Microsoft Azure 和 Google Cloud Platform 中为企业提供最佳可见性、安全和合规性成效。

了解您需要保护内容的更多信息

随着向主机、容器、存储服务和基础设施即代码等云技术转移，需要更大可见性以防范错误配置、恶意软件、勒索软件、入侵等。

尽量减少侦测和响应时间的能力

Sophos Cloud Native Security 是一个集成解决方案，阻止恶意软件、漏洞利用攻击、错误配置和异常行为攻破您的云安全。提供强大的扩展式侦测与响应 (XDR) 功能，安全团队可以轻松侦测和追捕多云威胁，接收优先事件侦测，从自动连接的安全事件获益，优化调查和响应时间。

最大化网络安全投资

将云配置和合规性管理、云工作负荷保护和云权限管理加入一个软件套件中，优化您的网络安全控制和预算。

- 通过按需资产库存和网络拓扑可视化，了解更全面的信息。
- 阻止并修复主机、容器、Kubernetes、无服务器、存储和数据库服务以及网络安全组的配置风险。
- 通过在安全漏洞出现前快速识别过高权限 IAM 角色、高风险用户行为以及凭据盗窃迹象，实施最低权限原则。
- 在开发管线的任何阶段集成网络安全，进一步调离攻击者，发现操作系统弱点、错误配置、嵌入式机密讯息、密码和密钥。
- 在运行时确定复杂 Linux 主机和容器安全事件，而不部署内核模块。
- 保护您的 Windows 主机和远程工作人员防范勒索软件、漏洞利用攻击和从未见过的威胁。
- 利用自动对应环境的政策，持续监测和维持安全与合规性标准。
- 在一个屏幕监测并优化多个 AWS 和 Azure 服务的云开支。

云采纳继续增加

2022 年企业将支出总共

4820 亿美元

用于云服务，2020 年为 3130 亿美元[1]。

[1] Bernard Marr, “The 5 Biggest Cloud Computing Trends In 2022.” Forbes, 2021 年 10 月 25 日

在环境、工作负荷和身份识别中实现完整多云架构安全覆盖

适合您的网络安全

将云环境安全状态提醒与流行的 SIEM、协作以及您已经采用的工作流工具集成，提高企业内的灵活性。

集成 Splunk、Azure Sentinel 和 PagerDuty 以接收影响其安全状态的安全和合规性事件即时通知，SOC 团队可以提高效率。

集成 Slack、Microsoft Teams 和 Amazon Simple Notification Service (SNS)，确保跨组织团队可以高效协作，修复安全和合规性事件。从 Sophos 控制台创建 JIRA 和 ServiceNow 票据，将安全和合规性事件解决轻松嵌入日常流程。

灵活的云安全方法

我们灵活的方法意味着您控制如何在云环境中部署和管理 Sophos Cloud Native Security。利用您自己的安全团队或 Sophos Managed Threat Response 服务，24/7/365 全天候监测您的环境，响应潜在威胁，搜索攻破迹象，阻止复杂威胁将您的数据和系统作为目标。

立刻开始使用 Sophos

无论是自己使用、通过 Sophos 合作伙伴或通过 Sophos MTR 服务，使用 Sophos 直观云安全和修复工具，都可以最妥善地应对当今的安全事件。

查找 Sophos 解决方案

www.sophos.cn/cloud

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

© 版权所有 2022。Sophos 有限责任公司 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 公司的注册商标。所有其他产品和公司名称均是其各自所有者的商标或注册商标。

2022-7-8 DA-ZHCN (DD)

SOPHOS