

Sophos 针对 AWS 的威胁防护、监测和响应

透过结合自动化保护和针对 AWS 的 24/7 全天候托管式侦测和响应服务的单一网络安全套件, 加速您的业务并确保安全成为云端转型的推手。



Sophos Cloud Security

快速行动, 保持安全

优化安全和合规性姿态, 了解要优先处理的 AWS 服务提醒, 保持数据安全隐私, 阻止高级威胁, 是所有企业的高优先级任务, 但是如果如果没有专业的 AWS 平台技能, 这些目标难以实现。

Sophos 得到数以百万的用户信任, 提供强大而有效的网络安全解决方案, 这些方案采用专门设计, 可供任何企业访问和管理。Sophos 采用一个中央控制台管理的单个网络安全组合形式, 保护数据和 AWS 环境免于最新高级威胁和漏洞 - 帮助企业在公共云中快速行动, 保持安全。

24/7 全天候 AWS 资源保护和监测

作为 AWS 1 级托管安全服务提供商和高级技术合作伙伴, Sophos 与 AWS 合作开发了一个综合网络安全组合, 结合端点、云工作负荷和网络防护、漏洞扫描、库存可见性和合规性跟踪 - 通过人工智能和机器学习促进、改进和加快。

部署管理

我们灵活的方法意味着企业可以控制如何在云环境中部署和管理 Sophos 的 AWS 安全组合。

- 内部 IT 安全团队部署和管理 Sophos 防护。
- 允许 Sophos 为您接入经验丰富的 Sophos 托管安全合作伙伴。
- Sophos 专业服务团队可以帮助解决初始部署, 进行定期安全运行状态检查⁺。

亮点

- AWS 1 级托管安全服务提供商和高级技术合作伙伴
- 自动化 AWS 环境的威胁防护
- 主动防止错误配置和安全漏洞
- 发挥 AWS CloudTrail 和 Amazon GuardDuty 服务的更大价值
- 价格固定的网络安全组合
- AWS Marketplace 提供
- 利用有限预算的安全开支实现任何 AWS 合同承诺

Sophos 针对 AWS 的威胁防护、监测和响应组合

通过一个组合状态管理和合规性、防火墙、云工作负荷和端点防护、Amazon GuardDuty 和 AWS CloudTrail 的调查结果组合,更快响应与 AWS 相关的安全事件*;Sophos 托管式侦测与响应服务持续监测 AWS 环境,分析并分流安全事件。

状态管理和合规性

Sophos Cloud Optimix 帮助主动减轻企业遇到的未批准操作、漏洞和错误配置等风险。使用 AWS CloudTrail 和 Amazon GuardDuty 服务,Cloud Optimix 持续监测公共云基础设施。这为企业提供部署资源和 IAM 角色的可见性,发现 AWS 帐户和配置何时不符合安全与合规性最佳做法,包括 CIS Foundations 1.2、HIPAA、ISO 27001、PCI DSS 和 SOC2 标准。

网络 and 应用程序安全

Sophos 高可用性防火墙保护环境免于已知和新兴网络威胁,维持 Web 应用程序可用性。用一体式防火墙解决方案节约部署多个网络安全产品的的时间,包括 IPS、ATP、URL 过滤和 WAF 双向防火墙,保护面对 Web 的应用程序。将 Sophos 防护与 AWS Shield 服务结合,实时发现恶意流量,按照 AWS 最佳做法减小攻击面。

云工作负荷和端点防护

Sophos Intercept X with XDR 为端点、Amazon Workspaces 和云服务器实例提供自动高级威胁防护。保护用户、应用程序和数据安全,防范最新网络安全威胁,如漏洞和勒索软件,同时利用 XDR 提出 IT 运行和威胁追踪问题并解答,采取措施解决任何问题。

专业安全专家团队支持

自动防御最新高级威胁是第一步。Sophos 托管式侦测与响应服务团队接收这些 Sophos 产品的遥测数据,在 AWS 环境中实现 24/7 全天候威胁防护、监测和响应。这支经验丰富的团队能够发现隐秘迹象 - 可疑行为和事件 - 防止其威胁您的数据和系统。

通过 AWS Marketplace 现代化网络安全获取

Sophos 威胁防护、监测和响应组合通过 AWS Marketplace 提供,帮助客户改进获取流程,符合云速度,同时维持合规性,实现已有的任何 AWS 合同承诺。



* Sophos 组合需要激活 AWS CloudTrail 和 Amazon GuardDuty 服务,必须单独购买

† 专业服务运行状况检查取决于当地是否提供。请联系 Sophos 了解更多信息。

了解更多信息,或联系专家
www.sophos.com/aws-mssp

中国(大陆地区)销售咨询
电子邮件:salescn@sophos.com