# 新增内容：Sophos Cloud Native Security

跨环境、工作负荷和标识中的完整多云安全覆盖


SOPHOS
Cybersecurity delivered.

## 一个集成云安全解决方案

随着向主机、容器、存储服务和基础设施即代码（Infrastructure as Code）等云技术转移，企业必须提高可见性以防范错误配置、恶意软件、勒索软件、入侵等。

Sophos Cloud Native Security云原生安全统一所需工具，提供这一可见性，并让您的云环境坚固，难以攻破，快速恢复。一个用于 Amazon Web Services、Microsoft Azure 和 Google Cloud Platform 的集成解决方案 Sophos Cloud Native Security，组合 Sophos Cloud Optix 和 Sophos Intercept X Advanced for Server XDR。

利用 Sophos Central console 控制台的单个管理视图，您可以追捕多云威胁，接收按优先级排列的事件侦测，受益于自动连接的安全事件以优化威胁调查与响应时间 – 全部在一个位置。

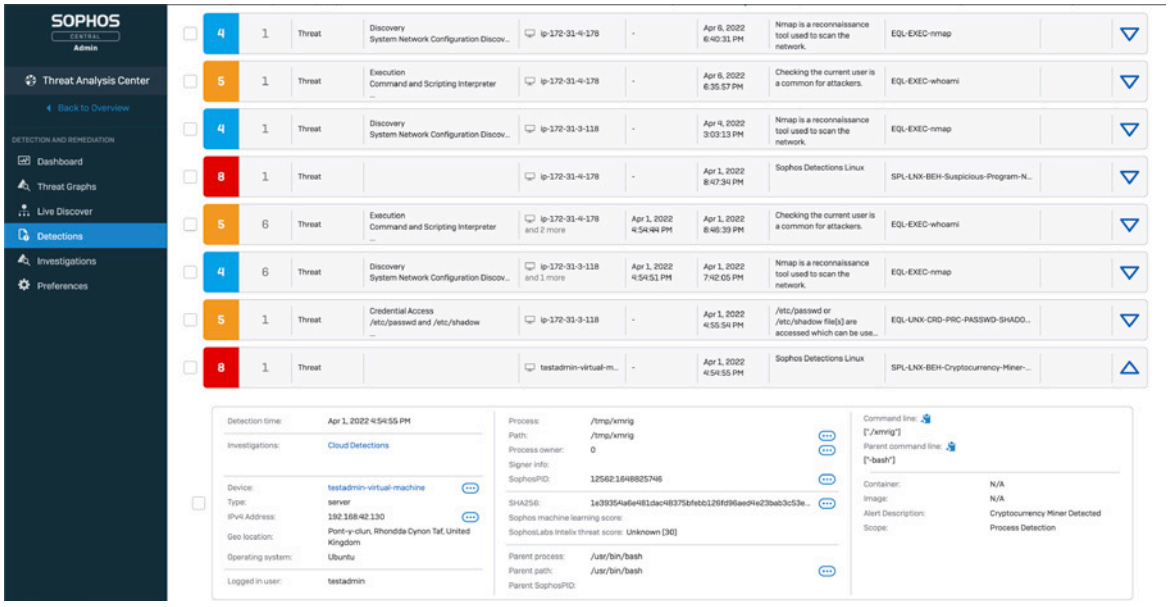
## Sophos Server Protection的最新进化

为了保护公共云中的服务器工作负荷，Sophos 扩展其值得信任的 Windows 防护以保护 Linux 部署 – 云端最普遍的操作系统之一。

今年早些时候，Sophos 云工作负荷服务器防护大幅提升 Linux 和容器功能，带来新的行为和漏洞利用攻击运行时威胁防护，识别复杂的 Linux 安全事件。

Sophos Cloud Native Security 提供保护现在的基础设施和数据所需的工作负荷防护功能，并且可在云端进化。

- 保护一切。云、数据中心、主机、容器、Windows 或 Linux。
- 通过代理或 Linux API 的轻量 Linux 和 Windows 主机防护，保证性能和运行时间。
- 无需部署内核模块，在运行时确定复杂 Linux 和容器安全事件。
- 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。
- 控制应用程序，锁定配置，监测关键 Windows 系统文件的更改。
- 利用扩展侦测与响应 (XDR) 简化威胁调查和响应，排定优先级并连接事件。




Sophos Central 控制台中的 Sophos XDR Linux 运行时威胁侦测示例。

## Cloud Workload Protection 部署选项

Sophos Central Management - 轻量 Linux 代理为安全团队提供所需的关键信息，在一个位置调查并响应 Windows 和 Linux 行为、漏洞利用攻击和恶意软件威胁。此部署选项监测主机，允许团队从一个面板管理 Sophos 解决方案，在威胁追踪、修复和管理之间无缝切换。

API 集成 - Sophos Linux Sensor 是为性能微调的高度灵活的部署选项。Sensor 利用 API 在主机或容器环境中集成丰富运行时威胁侦测与现有威胁响应工具。提供更高层级的控制，创建仅包含满足特定安全使用案例所需运行时行为侦测的自定义规则集。

除了 Sophos Linux Agent，Sophos Linux Sensor 还提供：

- 更多侦测：访问其他应用程序和系统漏洞利用攻击侦测
- 配置和调节：修改默认侦测允许和阻止列表的选项
- 资源调节：帮助优化主机资源利用的配置选项

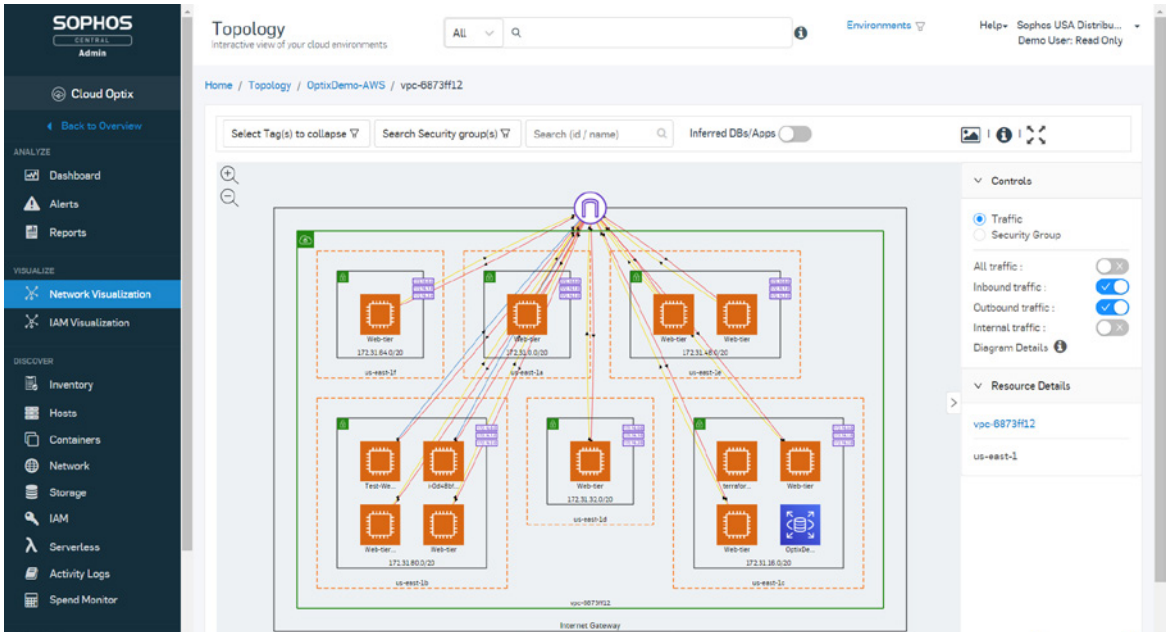
# 了解您需要保护内容的更多信息

减少 AWS、Azure 和 GCP 环境中的整个攻击面，不仅仅是防护和侦测云工作负荷威胁。所以 Sophos Cloud Native Security 将安全工具包整合为一个工具，包含云安全状态管理、Kubernetes 安全状态管理、基础设施即服务安全、云基础设施权限管理和云开支监测。

## 获得多云可见性、管理和合规性

在一个控制台中，通过 AWS、Azure、GCP、Kubernetes、基础设施即代码和 Docker Hub 环境中的无代理可见性与修复工具提高效率。

- 通过按需资产库存和可导出的网络拓扑可视化，了解更全面的信息。
- 在一个视图中集成云提供商安全服务，包括 Azure Advisor、Azure Sentinel、AWS Security Hub、Amazon GuardDuty、AWS CloudTrail、AWS IAM Access Analyzer、Amazon Detective、Amazon Inspector、AWS Systems Manager 和 AWS Trusted Advisor。
- 通过 Sophos 工作负荷防护代理和防火墙部署的自动资产发现与可视化，阻止影子 IT。
- 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。
- 利用自动对应到您环境的政策，持续监测和维持安全与合规性标准，和以支持审计要求的报告来节约数周工作。政策包括 CIS Foundations Benchmark、ISO 27001、EBU R 143、FEDRAMP FIEC、GDPR、HIPAA、PCI DSS、SOC2 和 Sophos 最佳做法。
- 在一个屏幕并排跟踪多个 AWS 和 Azure 服务的云开支，改善可见性。接收建议，优化 Sophos 的云提供商开支，或与 AWS Trusted Advisor 或 Azure Advisor 服务集成。
- 风险评估和颜色编码提醒显示详细修复步骤，减少提醒疲劳，并高效发现快速获胜和关键问题。

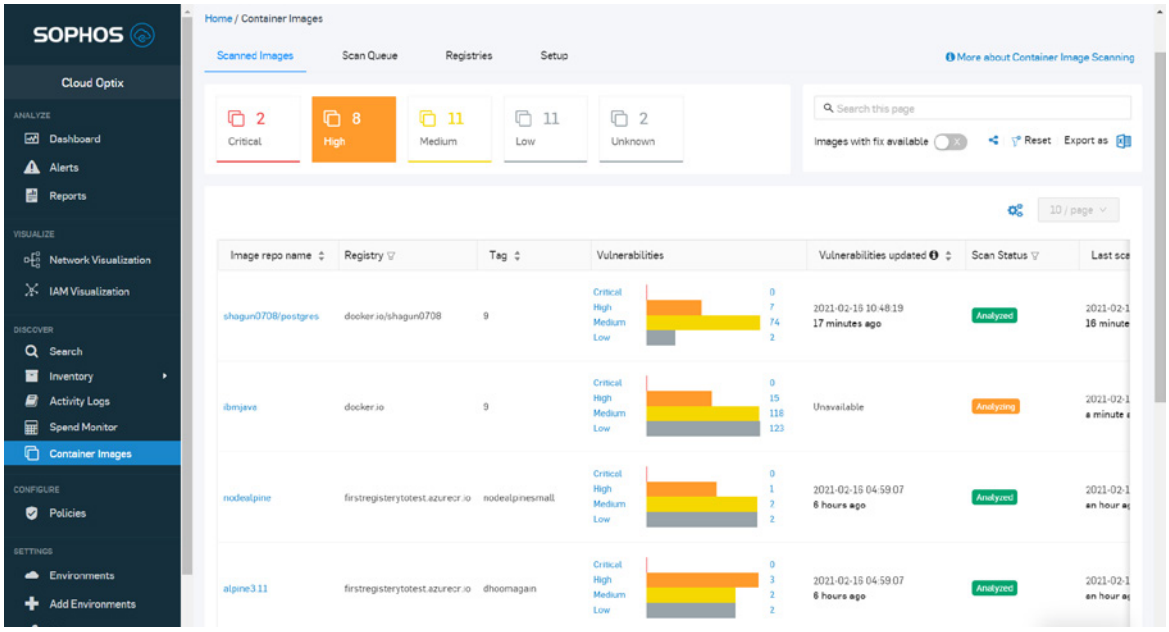



Sophos 用于 AWS 的网络拓扑可视化和安全组分析示例。

## 减小风险而不失去 DevOps 速度

实现快速安全开发，在开发管线任何阶段的集成安全配置与合规性检查。

- 自动侦测 Terraform、AWS CloudFormation、Ansible、Kubernetes 和 Azure Resource Manager 模板文件中的错误配置、嵌入式密钥、密码和密钥。
- 防止部署带有操作系统弱点的容器，识别可用修复。支持 Amazon ECR、ACR、Docker hub 注册表、基础设施即代码环境和生成管线中的镜像。
- 无缝集成 GitHub 和 Bitbucket，在 Sophos Central 接收按需扫描结果，或者使用 REST API 在任意开发阶段扫描 IAC 模板和容器镜像。

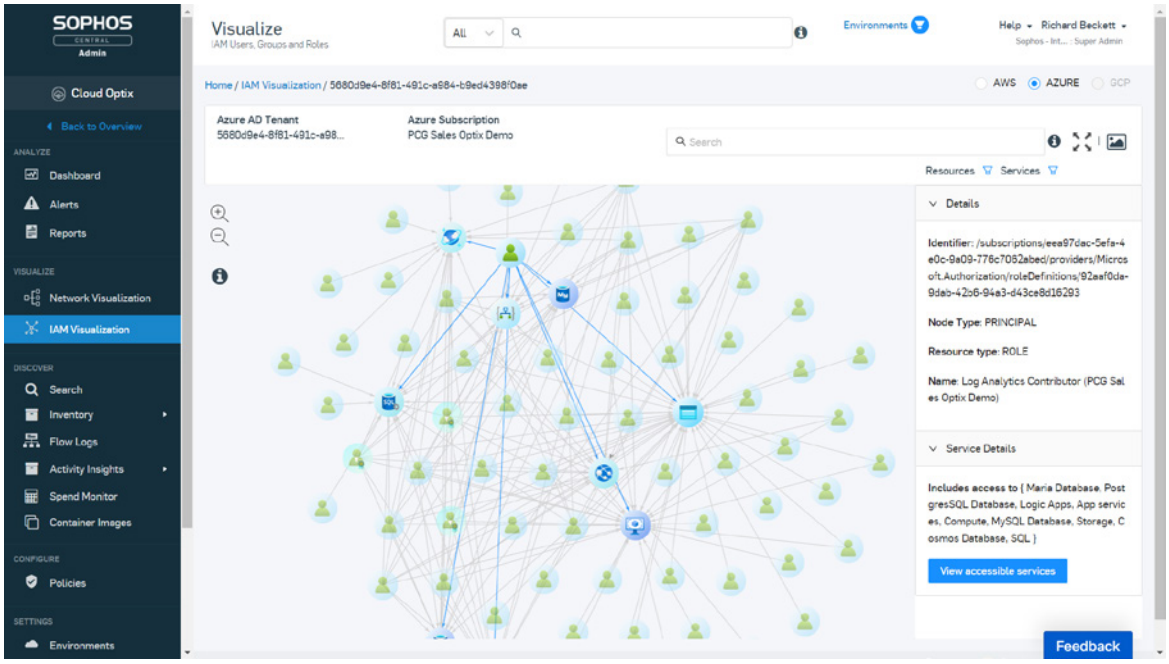



Sophos 容器镜像扫描弱点评估结果汇总。

## 实施最低权限原则

借助我们的帮助在被利用前管理标识，利用多云环境的云基础设施权限管理，实施最低权限。

- 确保所有 ID 仅执行其任务所需的操作，不能执行任何其他操作。
- 确定异常用户访问模式和位置，找出凭据误用或盗窃。
- 标示出用于存取环境的孤立、非托管和过期 Microsoft Azure IAM 角色，获得环境访问权。
- 可视化相互交织的复杂 AWS IAM 角色，快速突出显示并阻止权限过高的 IAM 角色。
- 利用 SophosAI 关联 AWS 环境用户行为的不同高风险异常，阻止泄漏。

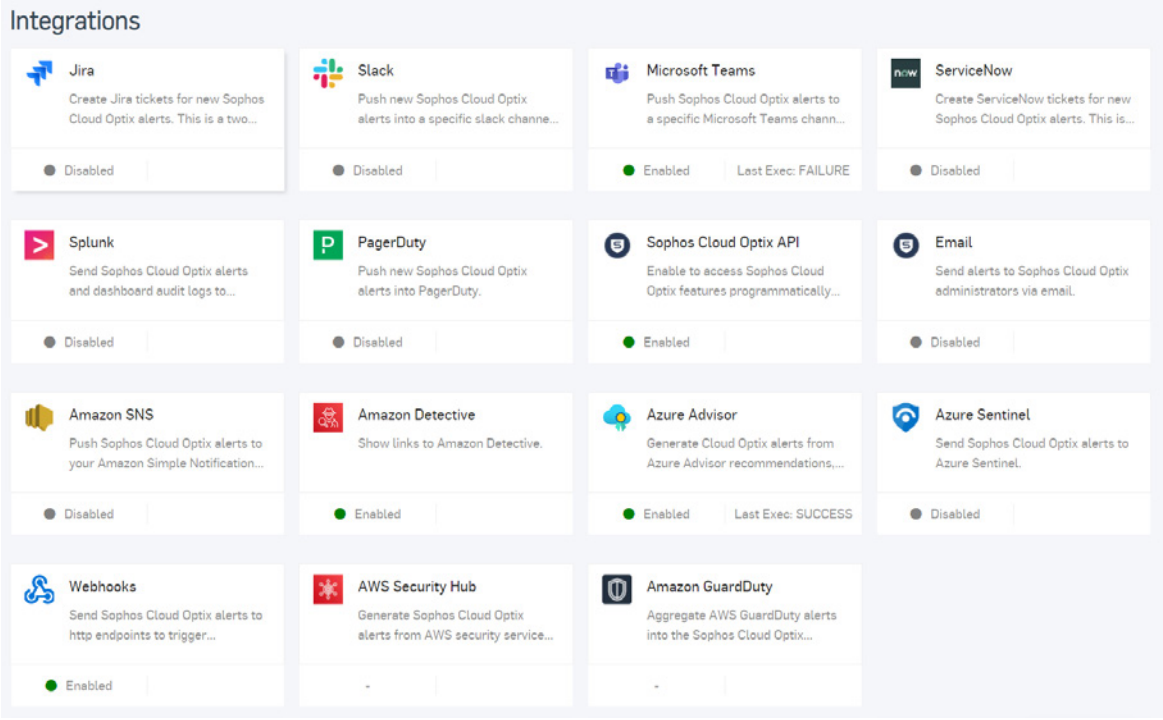



Sophos IAM 对 Microsoft Azure 可视化示例。

## 简化 SecOps 和改善协作

将云环境安全状态提醒与流行的 SIEM、协作、工作流和 DevOps 工具集成，提高企业内的敏捷性。

- 安全运行：与 Splunk、Azure Sentinel 和 PagerDuty 集成，接收安全和合规性事件的即时通知。
- 协作工具：向 Slack、Microsoft Teams 或 Amazon Simple Notification Service (SNS) 发送即时提醒，针对特定主题进行协作。
- 工作流管理：从 Sophos Central 创建 JIRA 和 ServiceNow 票据，将警示响应内建到标准工作流程中，并利用双向整合避免出现重复工作单的情形况。




管理云端安全状态管理警示的 Sophos 主要整合功能范例。

## 增强您团队的合作伙伴关系

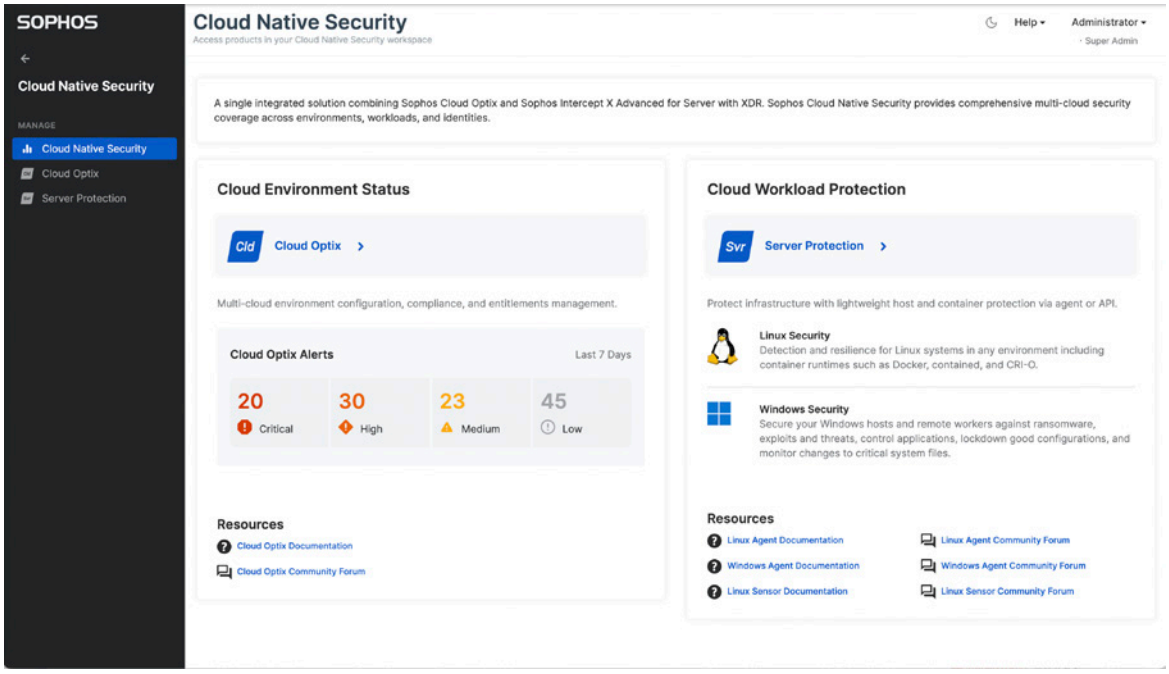
用您的方式管理防护 — 利用您自己的安全团队，借助 Sophos 合作伙伴，或者通过 Sophos Managed Threat Response (MTR) 服务，确保 24/7 全天候监测和响应。

Sophos MTR 是 Sophos Cloud Native Security 的完美补充。此托管威胁响应服务可与您的团队合作，24/7/365 全天候监测环境，响应潜在威胁，寻找攻破迹象，提供事件详细分析，包括发生的情况、地点、时间、方式和原因，阻止复杂威胁攻破您的数据和系统。

## Sophos Cloud Native Security 可用性

这一新的组合向所有客户提供，可以从 Intercept X Essentials for Server、Intercept X Advanced for Server 和 Intercept X Advanced for Server with XDR 升级。

在 Sophos Central 中激活后，客户和合作伙伴将在左侧导航中找到新的“CNS”项。它链接到新的 Cloud Native Security 汇总仪表板，提供 Sophos Cloud Optix 和 Intercept X Advanced for Server with XDR 产品访问。




Sophos Central 管理控制台中的 Sophos Cloud Native Security 仪表板的示例。

## 立即免费试用

注册即可享受 30 天免费试用
www.sophos.cn/cloud

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com



22-07-06 ZHCN (DD)