SOPHOS
Cybersecurity evolved.

保护任意位置组织的安全

任何位置。任何设备。任何资源。

Sophos 白皮书 2021 年 2 月

关于远程办公：据 Gartner 称，在新冠疫情结束后，74% 的组织希望部分员工远程办公[1]。同时，人们工作需要的各种资源也分布在多个位置：办公室的服务器；云应用程序，如 Office 365 或 Salesforce；私有或公共云环境，如 Amazon Web Services (AWS) 和 Microsoft Azure。

IT 团队的任务是保护所有用户和所有资源，无论身处何地。同时，犯罪分子一直在寻找更好更具破坏性的方法，从所有节点渗透进越来越虚拟化的组织。

要保护企业分布在任意位置的人员和资源，需要：

- 安全连接，这样用户可以从任何位置访问资源：家中、现场或办公室
- 保护用于连接的设备 — 台式机、笔记本、手机和平板电脑
- 保护用户需要访问的数据和载荷，无论是在云端还是本地网络中
- 简单管理，这样 IT 团队可以从任意位置管理分布式组织，不增加工作量

幸运的是，Sophos 支持所有这些方面。我们提供搭载先进保护功能的全套下一代安全产品。所有产品通过一个 Web 安全平台控制，降低每日管理开销，同时支持 IT 团队从任意位置管理组织安全。

通过这个解决方案概要，您可以了解 Sophos 如何满足每个要求，并了解客户采用 Sophos 网络安全系统保护组织安全后，带来的生产效率和防护优势。

安全连接

毋庸置疑，新冠疫情推动远程办公大幅增加。2020 年 5 月，62% 的美国人在家办公 (WFH)。但是，在新冠疫情之前远程办公室已经形成趋势，许多办公室员工已经习惯每周数天在家办公。在英国，过去十年的远程办公以 74% 的速度增加，而在澳大利亚，约三分之一的员工通常在家办公。

员工办公对于公司和员工来说是一种双赢方案：员工节约通勤时间和费用，同时提高灵活性和生产力。同时，企业降低成本和周转费用。但对于 IT 团队来说，长期远程办公带来更多安全挑战。无论员工从自己的起居室登录，拜访客户，还是在地球对面数千英里外的 Wi-Fi 热点处喝咖啡，网络和数据始终保持保护。

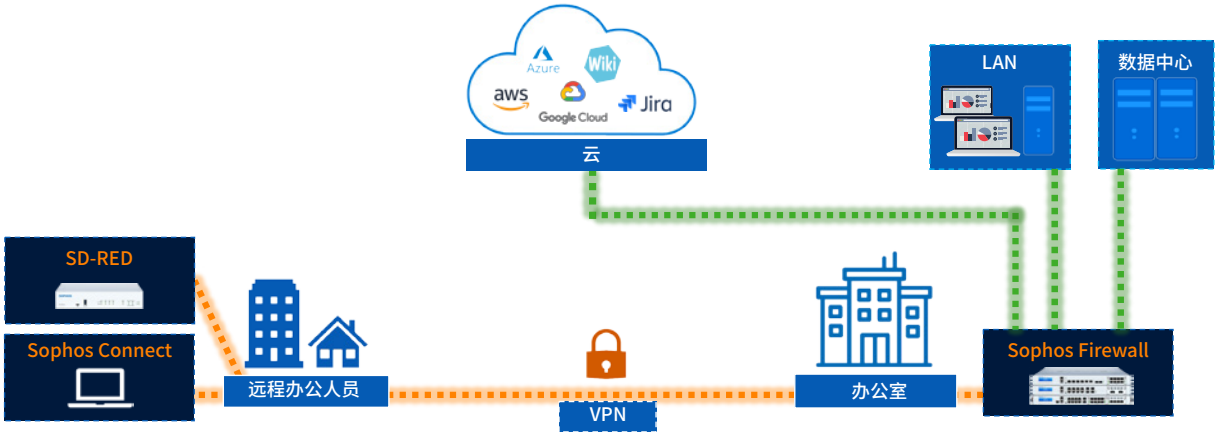
有了 Sophos，您的员工可以从任何位置快速高效安全连接并工作，我们提供基于 VPN 的传统方式和零信任网络访问 (ZTNA) 方式。

VPN

使用易于部署的免费 **Sophos Connect VPN 客户端**和 **Sophos Firewall**，将员工远程连接到主办公室和云资源。Sophos Connect 全球拥有超过 140 万用户，在 Windows 和 macOS 设备上诶远程用户提供企业网络或公共云资源的安全访问。

为了实现终极远程连接，**Sophos SD-RED** (Remote Ethernet Device) 是一款简单即插即用型设备，可以配合 **Sophos Firewall** 将分支办事处、远程地点和个人连接到主网络（无论物理还是云端）。

它提供始终开启的专用或拆分通道 VPN，易于部署和管理，选项灵活。它体积非常小且便携，非常适合需要随时随地访问安全连接的高管和其他人员。



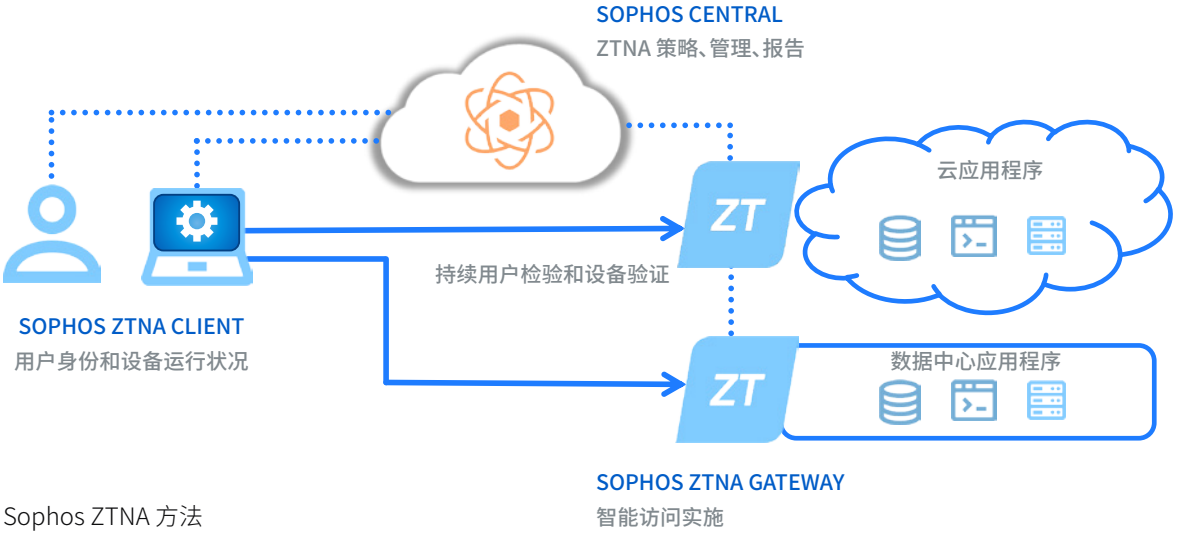
通过 Sophos Firewall 和 Sophos Connect VPN 及 SD-RED 保护远程连接安全

ZTNA

多年来，VPN 技术成功帮助员工远程连接，在疫情之初带来巨大帮助，支持企业在数天内快速切换为安全远程办公。但是，许多企业开始需要的功能已经超出 VPN 设计能力。

Sophos Zero Trust Network Access (ZTNA) 是远程访问 VPN 很好的替代品，可以帮助用户从任意位置直接透明连接企业资源。同时，还持续验证用户身份 — 通常采用多因素身份验证和身份提供机构 — 验证设备的运行状况和合规性，增强您的安全。

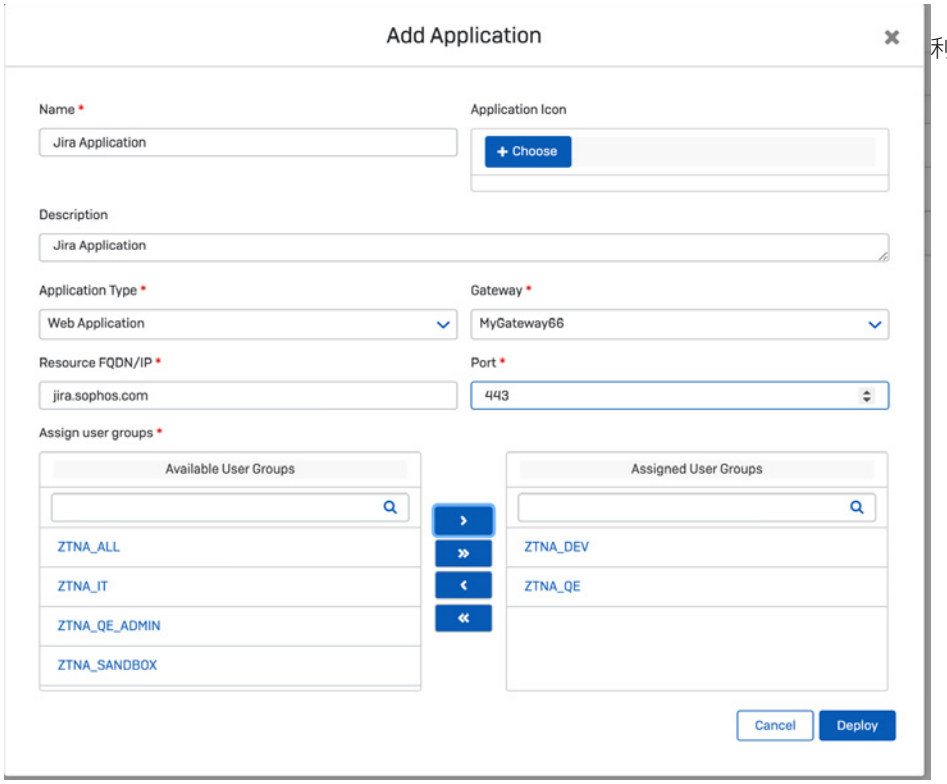
Sophos ZTNA 确保设备已注册，处于最新状态，正确保护，启用加密。然后利用这些信息，根据可自定义的策略作出决定，确定用户对关键联网应用程序的访问权和权限。



Sophos ZTNA 方法

利用 Sophos ZTNA，您可以：

- 增强网络防御。Sophos ZTNA 为您提供颗粒化程度非常高的控制：可以根据单个企业策略和适合的风险等级，分别控制任何用户、任何设备、任何应用程序。不再仅仅根据存在于网络上就隐含信任个人，而且在允许访问前不断评估身份和设备运行状况，从而提升防护并减小网络内横向移动的风险。
- 提高效率。由于 Sophos ZTNA 通过 Sophos Central 平台管理，很容易注册新用户，从而可以适应多变的工作环境。此外，对于最终用户更加透明，相比 VPN，连接体验流畅，“就是好用”。



利用

Sophos ZTNA 轻松添加应用程序

无论选择何种方法，Sophos 获奖的安全产品都将帮助您保护任意位置任意设备上的员工安全。

保护设备

去年 51% 的企业受到勒索软件攻击，在 73% 的攻击中，攻击者成功加密数据[2]。

令人警惕的统计数据，加上保护所有设备 — 台式机、笔记本、企业和个人设备 — 以及 Windows、macOS、Linux、Android、Chromebook 和 iOS 各种操作系统的需要，面临的网络安全危机不断加剧。

Sophos Intercept X 为所有设备和平台带来全球最佳防护。多层技术在攻击链多个点阻止攻击者，包括：

- 勒索软件防护，阻止未经授权加密文件、硬盘和引导区记录，恢复至安全状态
- 深度学习人工智能，利用数以百万的文件分析威胁，阻止已知和未知恶意软件，阻止其执行
- 防漏洞供给技术，阻止对手技术和免文件及基于脚本的攻击
- 基础特征码防护，阻止已知威胁

此外，Sophos Intercept X 保护任何平台上的任何设备 – 这样您的员工可以在选择的任何设备上安全工作：

- 运行 Windows 和 macOS 的台式机与笔记本电脑
- Windows 和 Linux 服务器
- 云提供商的虚拟桌面环境
- 运行 Android、iOS 或 Chromebook 的移动设备

端点侦测与响应 (EDR)

最具破坏性的网络威胁通常涉及人主导的攻击，往往利用合法工具和进程，如 PowerShell。亲自动手进行的实时黑客攻击使攻击者能够随时修改战术、技术和方法 (TTP)，绕过安全产品和协议。进入受害者网络后，攻击者可以横向移动，窃取数据，部署勒索软件，安装恶意软件和后门用于未来攻击。

阻止此类人主导的攻击需要人主导的威胁追踪。**Intercept X with EDR**（端点侦测与响应）可以提供您需要的工具，从用于管理 Intercept X 端点防护的控制台执行威胁追踪。

这是首个为安全分析师和 IT 管理员设计的 EDR。其他 EDR 工具通常需要专业人员或者自己的内部安全操作中心 (SOC)，Sophos EDR 使用简单，同时不牺牲执行强大分析的能力。

有了 Intercept X with EDR，您可以研究可疑迹象和威胁，通过现成可自定义的强大 SQL 查询改善 IT 健康。常用用例包括：

- Chrome 运行缓慢。识别安装的未经授权 Chrome 扩展
- 网络活动检查。查找失败登录尝试和来自 PowerShell 的活跃通信
- 软件查询。检查是否已从设备移除敏感文件和/或没有超出软件许可用途
- 网络钓鱼研究。找出单击可疑链接的用户以及其是否下载文件

此外，您可以利用命令行工具远程访问设备修复问题，如重新启动设备、终止活跃进程、运行脚本或程序、编辑配置文件、运行鉴证工具以及安装/卸载软件。

托管检测与响应 (MDR)

如果没有时间、能力和专业技术自行运行威胁追踪与调查，**Sophos Managed Threat Response** (MTR) 服务为您提供帮助。

Sophos MTR 是由威胁追踪专家和响应专家组成的团队，以全托管服务形式提供 24/7 全天候监测、侦测和响应能力。他们主动追踪并验证潜在威胁和事件—阻止其产生危害。

他们还关联来自 Sophos 防护解决方案的数据，找出威胁迹象。和其他托管侦测与响应服务不同，Sophos 不仅通知您问题；我们还确定并采取最合适操作消除威胁。

移动设备

员工使用个人设备办公时，IT 团队面临保护公司数据同时不侵犯用户隐私的挑战。我们的统一端点管理解决方案 **Sophos Mobile** 保护 iOS、Android、Chrome OS、Windows 10 和 macOS 设备。允许您以最小工作量保护任何个人和企业设备，非常适合 BYOD（自带设备）场景。

Sophos Mobile 支持您：

- 阻止移动威胁。获得行业领先的移动恶意软件、网络钓鱼、中间人攻击等防护，全部由 Intercept X 支持
- 保护企业数据安全。根据需求，选择全设备或仅容器管理
- 减少管理工作量。灵活的自助门户允许用户注册自己的个人 macOS、Windows 10 或移动设备，重置密码，获取帮助 – 无需 IT 介入

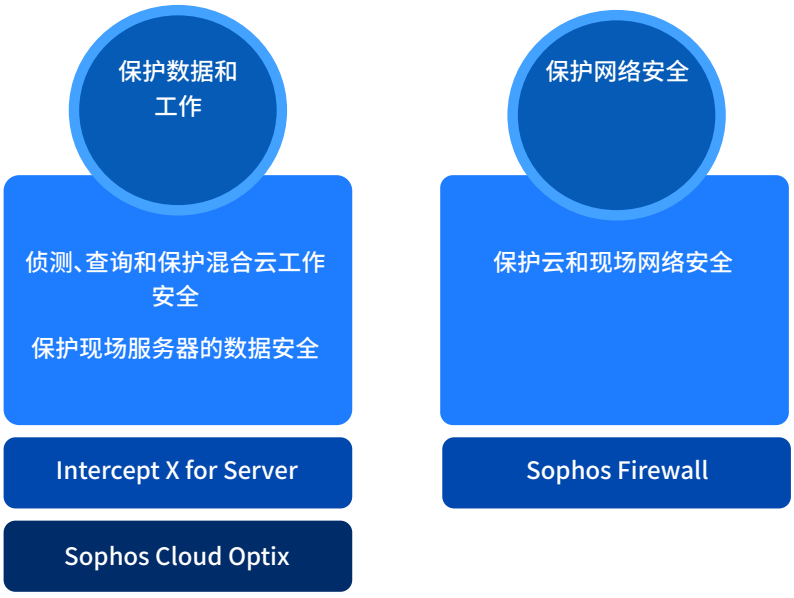
保护资源安全

根据企业需求，您可能在现场运行服务器，使用云应用程序，或者在 AWS、Azure 或 GCP 的私有和公共云环境宿主资源。更有可能的是，以上都做。

云在大多数企业日常运营中的地位正迅速变得越来越重要。因此，网络罪犯非常关注云带来的机会，过去 12 个月，70% 使用公共云的公司遇到云安全事件[3]。

要保护任意位置的资源安全，您需要做两件事：

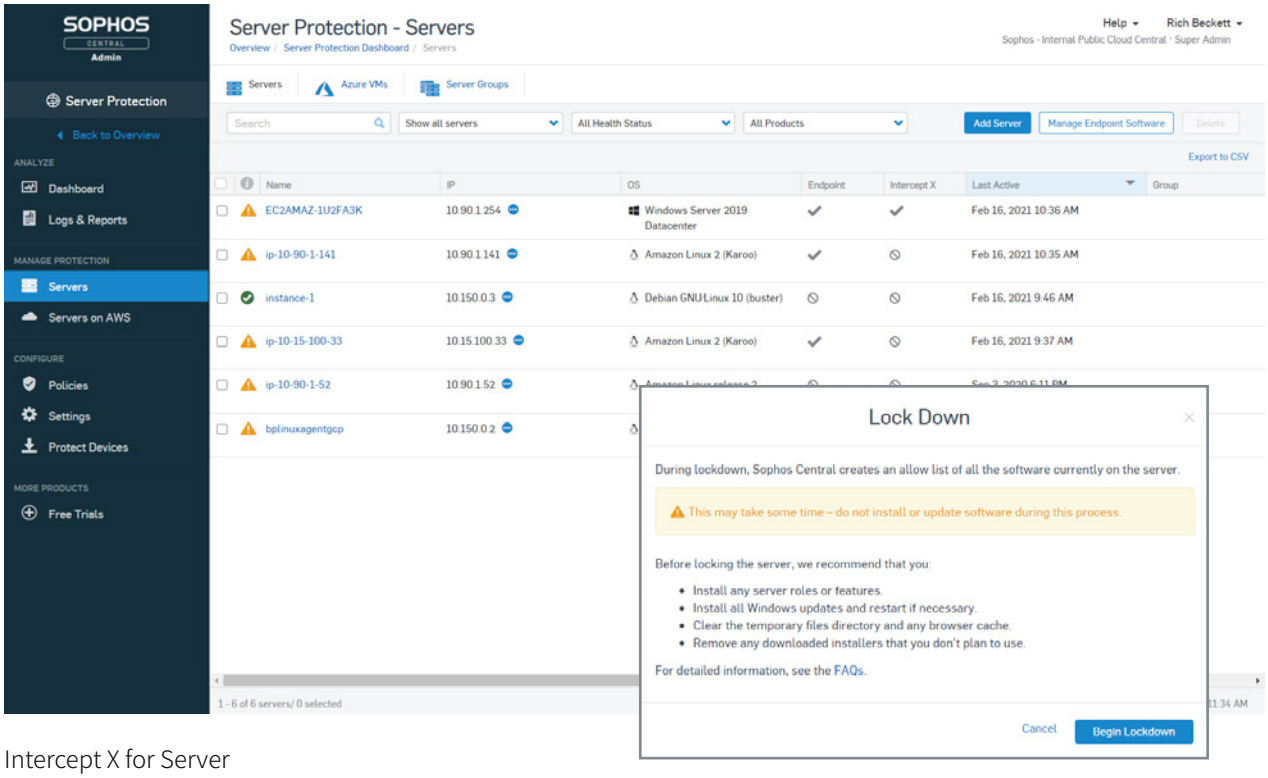
1. 保护数据和工作本身
2. 保护数据和工作所在的网络，阻止入侵者进入



保护数据和工作

数据和工作是您最重要的资产。**Sophos Intercept X for Server** 保护云、现场或混合工作环境。它可以保护 Windows 和 Linux 虚拟机及虚拟桌面免于最新威胁。

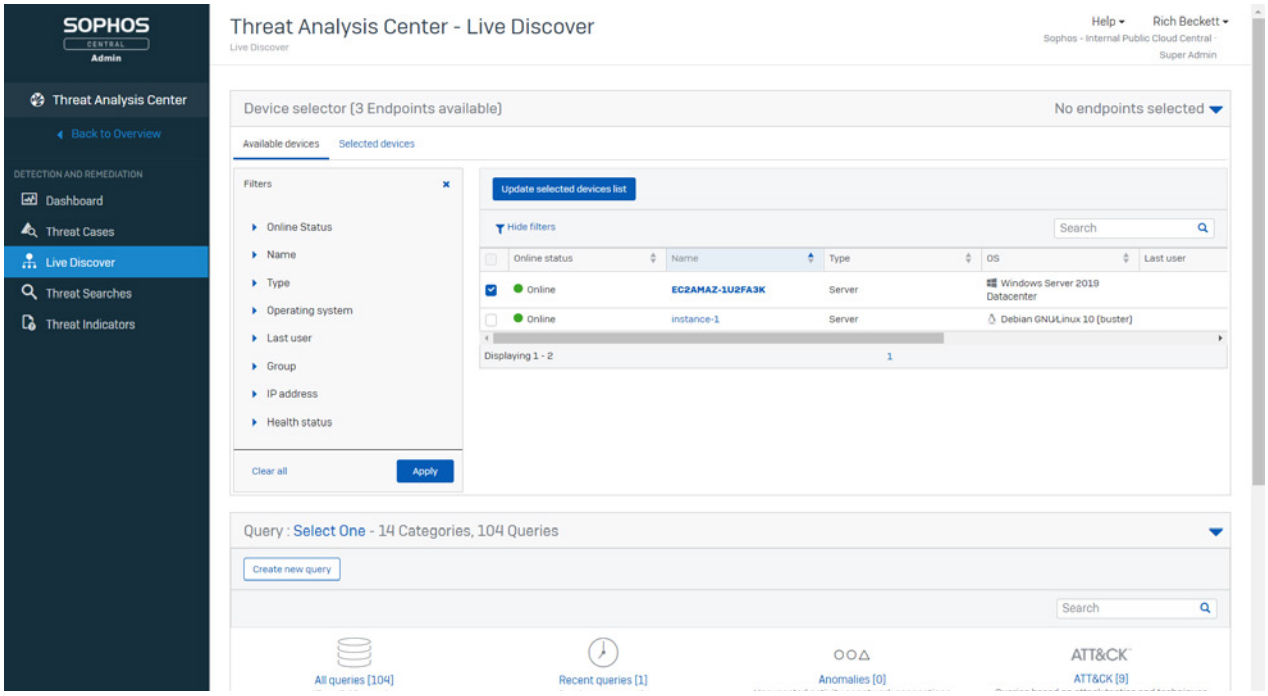
- 阻止高级供给。包括勒索软件、基于漏洞的供给以及从未见过的恶意软件
- 锁定服务器工作。控制可以和不可运行的应用程序，获取任何未经授权更改尝试的通知。
- 中央管理所有内容。从一个控制台部署和维护所有内容，包括云工作和现场服务器组成的混合场景



Intercept X for Server

利用 **Intercept X for Server with EDR**，您可以将 EDR 调查扩展到服务器，无论现场还是云端。这样您可以：

- 执行关键 IT 操作和威胁追踪工作。发现性能问题，了解安装位置和安装内容，追踪可疑行为
- 自动侦测云工作。留意关键云服务，包括 S3 bucket、数据库和免服务器功能
- 侦测不安全的部署。依赖人工智能持续监测云环境和异常通知

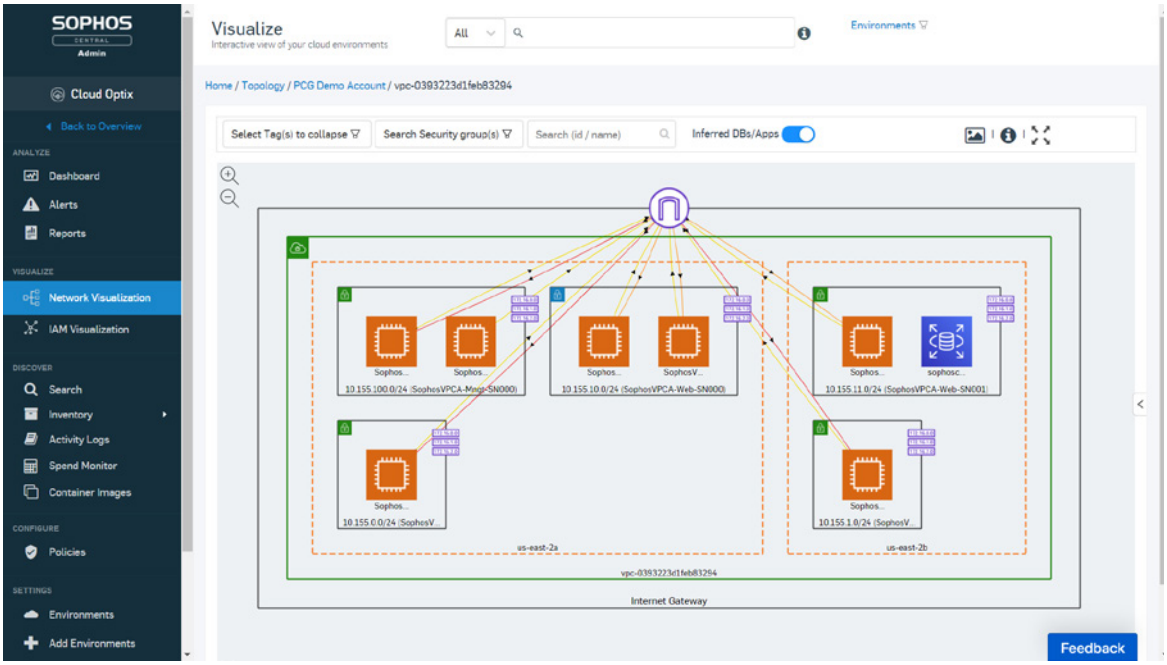


将 EDR 调查扩展到服务器

数据和工作防护的一面是防护，另一面是可见性。您需要持续清楚了解运行的内容，配置云提供商服务以阻止安全攻击的能力。

我们的云安全状态管理解决方案 **Sophos Cloud Optix** 可以提供保护企业安全需要的可见性，包括：

- 多云可见性。详细云资源库存，包括服务器、容器、存储、网络以及用于 AWS、Azure 和 GCP 的 IAM
- 基于风险确定优先级为安全任务和过高权限 IAM 访问持续分析配置
- 合规性管理。通过现成模板、自定义策略和协作工具，持续监测合规性
- 集成安全。找出 Sophos Firewall 和 AWS 上的工作保护
- 云成本优化。在一个屏幕管理 AWS 和 Azure 开销



Sophos Cloud Optix

虽然云环境安全提醒很有用，利用 Amazon GuardDuty 等服务带来巨大价值，但海量通知很容易让人不知所措。这样几乎无法辨认真正需要处理的通知。

Sophos 利用 Sophos Cloud Optix 保护用于宿主网络安全平台 Sophos Central 的 Amazon Web Services 环境。我们自己的安全团队从 Cloud Optix 得到的一个重要优势是能够关注重要内容。

“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。”

Sophos 副总裁兼首席信息安全官 Ross McKerchar

保护网络安全

要保护资源，您还需要保护资源运行所在的网络。**Sophos Firewall** 为现场、AWS 和 Azure 环境提供无人能及的保护和可见性。

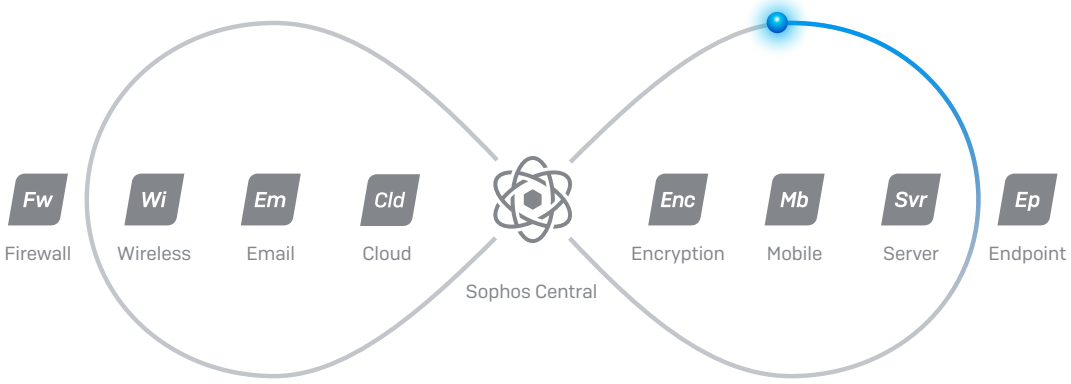
- 集成多层防护阻止最高级的威胁
- 强大的一体式解决方案，实现 WAF、IPS、ATP、URL 过滤，基于路径的路由和国家级拦截，提供各种报告，包括有关用户和网络活动的完整信息
- 云应用程序可见性，影子 IT 发现，以及自动威胁响应
- 能够加强云工作对黑客攻击的防御能力，如 SQL 注入和跨站点脚本，同时通过反向代理身份验证为用户提供安全访问
- 作为独立和高可用性解决方案运行的灵活性

为了简化云部署，全部在一个预先配置好的虚拟机镜像中提供。

简化管理

利用 Sophos，可以通过一个 Web 平台管理所有安全：Sophos Central。再也不用切换控制台来保护企业安全；全部在一个地方进行。您还可以轻松进行跨产品调查，轻松关联来自多个服务的数据。

由于 Sophos Central 宿主在云端，非常适合分布式 IT 团队。我们的全球用户超过 400,000 名，所以请放心，您使用的是全球最受信任的网络安全平台。



Sophos Central 还支持 Sophos 产品共享实时威胁健康和安全信息，共同自动响应威胁，我们称之为 Synchronized Security。优点包括：

- 自动事件响应。如果某个 Sophos 产品侦测到可疑内容，如恶意软件感染或设备不合规，将与网络安全系统的其他产品共享此信息。其他产品可以在数秒内自动响应该事件。例如：
  - Sophos Firewall 即时隔离被感染的设备，阻止威胁传播，阻止横向移动。
  - 如果侦测到受威胁邮箱，Intercept X 自动扫描端点，限制电子邮件携带的威胁造成影响。
  - Sophos Wi-Fi 限制不合规设备的网络访问权，禁止恶意和不安全设备进入您的无线网络。
- 独有情报。IT 团队对网络的可见性和控制增加，包括能够：
  - 按名称而不是 IP 地址识别被感染项，加速安全调查。
  - 识别网络上的所有应用程序。平均 43% 的网络流量以“未分类状态”通过，因此 IT 团队不知道其好坏或恶意。通过 Synchronized Security，Sophos Firewall 和 Intercept X 共同自动识别并分类网络上的所有应用程序。

无与伦比的防护。无与伦比的效率。

运行 Sophos 网络安全系统带来下一代防护，一个管理平台，产品之间共享威胁情报，以及自动事件响应。这些功能共同为 IT 团队带来巨大的效率和生产力提升。

事实上，运行 Sophos Intercept X 和 Sophos Firewall（通过 Sophos Central 管理）的客户一致表示，他们**的 IT 团队效率提高一倍，**安全事件减少 **85%。**

“自动侦测并纠正大多数安全事件的工具，帮助我们的小型 IT 团队管理公司安全，阻止威胁。”

软件服务提供商首席技术官

保护任何位置安全。任何设备。任何资源。

向灵活的远程办公过渡，增加云使用，没有回头路。它们简化生活，同时给 IT 团队带来新的挑战，给坏人创造新的机会。保护这种新环境安全需要安全连接、安全资源和安全设备，无论身处何地，并且不增加 IT 开销。

Sophos 提供强大可信任的解决方案，帮助您解决这些现代挑战。联系 Sophos 代表，讨论您的要求，或者启动非强制性免费试用，试用任何产品。

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2.脚注 2020 勒索软件现状，Sophos

3.脚注 2020 云安全现状，Sophos

中国（大陆地区）销售咨询
电子邮件: salescn@sophos.com

210215 WPZHCN (MP)

SOPHOS