Sophos ZTNA

零信任网络访问

安全连接任何人、任何地方、任何应用程序。Sophos ZTNA 将用户透明连接到重要业务应用程序和数据，相比传统远程访问 VPN 提供更好的划分、安全和可见性。可以作为独立产品，以及与 Sophos Firewall 和 Intercept X 完全集成的 Synchronized Security 解决方案形式提供。

在零信任的世界中重获信任

Sophos ZTNA 采用零信任原则：不信任一切，核实一切。各个用户和设备成为自己的细分外围，不断验证和核实。它们不再处于具有通常所有默认信任和访问权的“网络”上。现在信任是要争取的 – 不是给予的。

支持员工远程办公

Sophos ZTNA 支持远程办公人员安全无缝访问需要的应用程序和数据，部署、注册和管理相比传统 VPN 容易得多。

细分应用程序

Sophos ZTNA 提供终极细分，这样无论您的应用程序位于本地设施、数据中心还是公共云基础设施，都可以提供安全应用程序访问。您还可以获得应用程序活动的状态、安全状态和使用等实时可见性。您还可以通过 Sophos ZTNA 控制多个 SaaS 应用程序的访问权，利用 IP 地址限制仅允许来自 ZTNA 网关的连接。

阻止勒索软件和威胁

有了 ZTNA，再也不用担心勒索软件和其他威胁在网络上通过被攻破的用户设备传播的可能。用户和设备只有对特定应用程序的，基于明确政策的访问权。这样消除 VPN 的一个主要挑战，即暗含信任和普遍网络访问权。

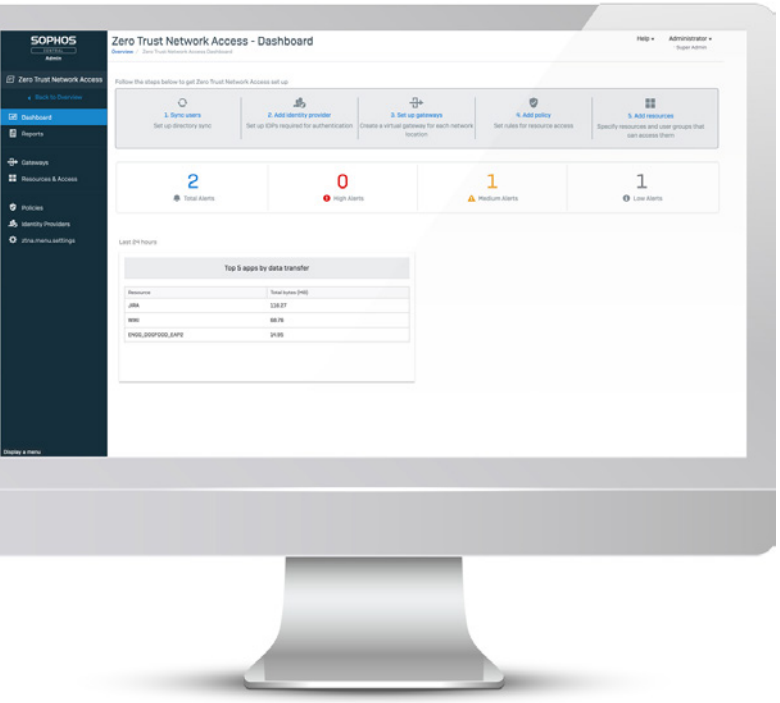
快速部署、调整和缩放

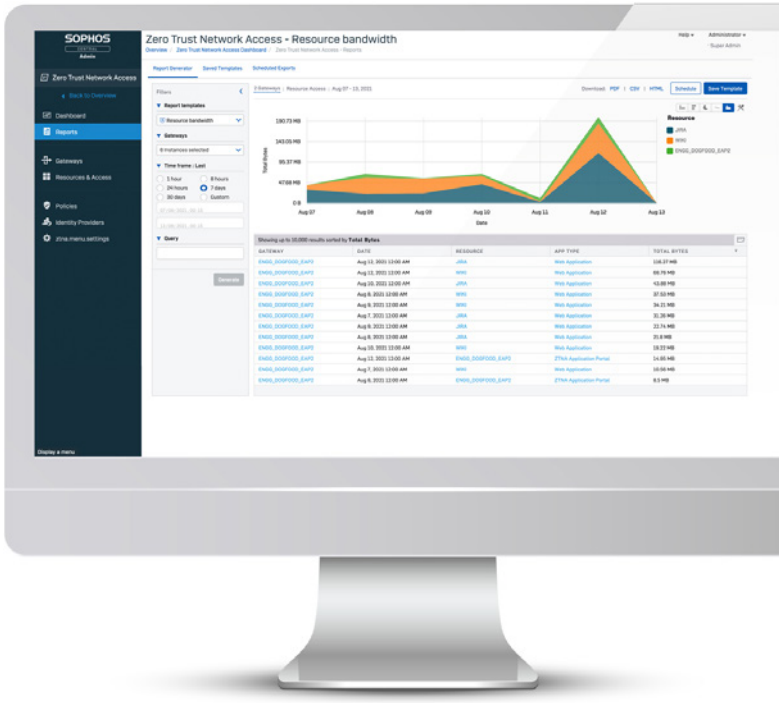
Sophos ZTNA 为动态变化、快速发展、快速移动到云端的现代网络而设计。这是一个精益干净的解决方案，可以快速轻松案例启动新应用程序，注册或停用用户和设备，获取应用程序状态和使用的重要信息。

亮点

- 零信任：不信任一切，核实一切
- 集成 Sophos Intercept X
- 单一代理，单一控制台解决方案
- 终极远程访问 VPN 替代
- 细分并保护您的网络应用程序安全
- 适用于网络内外任何位置
- 云管理，云交付
- 对最终用户透明
- 卓越的应用程序可见性和洞察力
- 将设备运行状况集成在访问政策中
- 简单按用户每年订购授予许可，免费网关

SOPHOS





云交付，云管理

Sophos ZTNA 从一开始设计旨在实现简单、集成、安全的零信任网络访问。Sophos ZTNA 采用云交付和云管理，集成在全球最受信任的网络安全云管理和报告平台 Sophos Central 中。

从 Sophos Central 不仅可以管理 ZTNA，还可以管理 Sophos 防火墙、端点、服务器防护、移动设备、云安全、电子邮件防护等。您可以随时随地在任何设备上登录并管理您的 IT 安全。

单一代理，单一控制台，单一供应商

Sophos ZTNA 独有集成整个 Sophos 网络安全生态体系，让您的工作轻松很多。您可以获得 ZTNA 和下一代端点防护的单一代理解决方案。您还可以在 Sophos Central 中获得单面板管理控制台，获取前所未有的所有 IT 安全产品的信息。

客户表示赞同：全集成 Sophos 网络安全解决方案节省时间的优势巨大，就好像 IT 团队人手翻倍一样。

独有集成：ZTNA 和下一代端点防护

Sophos ZTNA 是唯一紧密集成下一代端点产品 – Sophos Intercept X 的 ZTNA 解决方案，在防护、部署和管理方面具有明显优势。

- 端到端防护：通过最强大的机器学习和下一代端点技术，保护您的应用程序访问全球，保护端点和网络不受外泄和威胁（如勒索软件）影响。
- Synchronized Security同步安全：集成 ZTNA 和端点，一致共享状态和运行状态信息，自动隔离受威胁系统以防止威胁移动或盗窃数据。
- 单一代理，单一控制台，单一供应商的便捷性。

这是其他地方都没有的优胜组合。

单一代理部署

Sophos ZTNA 紧密集成 Sophos Intercept X 下一代端点防护，支持单一代理部署选项。

只需单一代理部署，您就可以获得全球最好的端点和勒索软件防护能力，以及终极应用程序安全和划分。

还支持免客户端访问基于浏览器的应用程序。

可缩放的应用程序网关

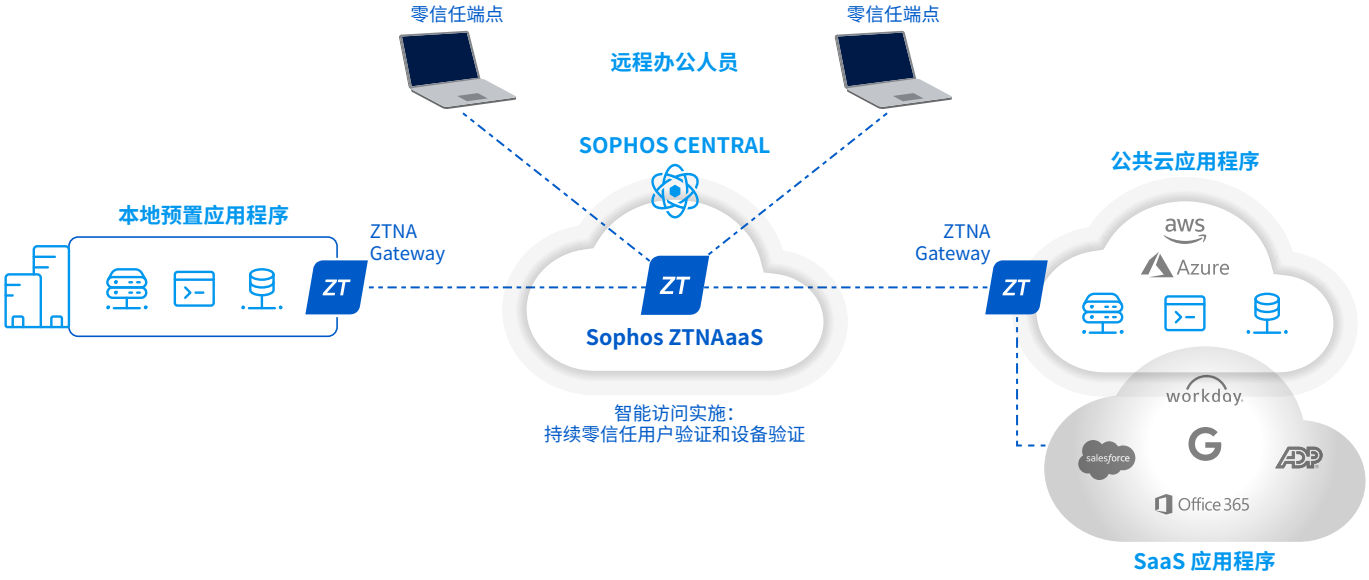
Sophos ZTNA 网关可以免费轻松部署在需要的任何位置。作为虚拟设备，您可以轻松部署高可用性网关，并随着企业增长缩放。

同步设备运行状况

Sophos ZTNA 充分发挥 Sophos Synchronized Security 的优势，利用 Sophos Intercept X 端点和 Sophos Central 与 ZTNA 之间的 Security Heartbeat™，访问设备运行状态，并确定活跃威胁与攻破迹象，从而实现即时响应，显示网络内外被攻破或不合规设备的访问权。

集成身份识别

对于零信任，身份识别就是一切。Sophos ZTNA 持续核实用户身份，支持最流行的 IDP 解决方案，包括 Microsoft Azure 和 Okta。当然，您也可以利用偏好的多重因素身份验证 (MFA) 解决方案，集成这些 IDP 防范凭据盗窃或被攻破的设备。



Sophos 零信任端点

运行无代理或使用与 Sophos Intercept X 集成的 Sophos ZTNA 代理，提供终极的具同步安全的零信任端点解决方案。如果需要，Sophos ZTNA 还可配合您的现有端点防护产品。

Sophos Central

轻松实现 ZTNA 即服务，提供快速部署，精细化政策控制，及来自云端的深入可见性和报告功能。与主流身份标识提供商集成，通过持续用户验证和设备验证，为应用程序支持智能访问实施。

Sophos ZTNA 网关

作为 Hyper-V、VMware 和 Amazon Web Services 上的虚拟设备提供，免费轻松部署。它让公共互联网无法看到您的应用程序，同时为验证用户及其验证设备提供到其开展作业需要的应用程序的安全连接。

Sophos ZTNA 功能汇总

- 安全访问：针对本地设施或公共云基础设施上的业务应用程序
- 应用程序：所有免客户端模式基于浏览器的 Web 应用程序；胖应用程序，如 SSH、VNC、RDP 以及其他通过 ZTNA 客户端的
- 访问政策：基于用户组的政策，基于 Synchronized Security 运行状况的访问政策
- 通过 Sophos Central 报告、监测、记录和审计应用程序状态、访问及使用
- 最终用户访问已标记的应用程序的用户门户

技术规格

支持的平台	当前
身份识别提供商	Microsoft Azure 和 Okta
ZTNA 网关平台	VMware ESXi 6.5+、Hyper-V 2016+、AWS；即将推出：Sophos Firewall v20 （适用于所有硬件、虚拟和云平台）
ZTNA 客户端平台	Windows 10 1803 或更高版本，macOS 11 (Big Sur) 或更高版本；所有支持无代理的 Web 应用程序访问的平台平台
ZTNA 设备运行状况	Sophos Security Heartbeat (Intercept X)

网关规格	
建议的 VM	2 核 / 4GB
多节点集群	多达 9 个节点带负载平衡，实现性能、容量和业务连续性
节点容量和缩放	一个节点 10,000 个代理连接，一个集群（最多 9 个节点）最多 90,000 个代理连接

如何购买

Sophos ZTNA 采用每个用户每年订阅的方式授予许可。ZTNA Gateway 可根据需要免费部署任意数量。

要了解更多信息，请访问：
www.sophos.com/ztna

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

23-06-28 DS-ZHCN (PC)

SOPHOS