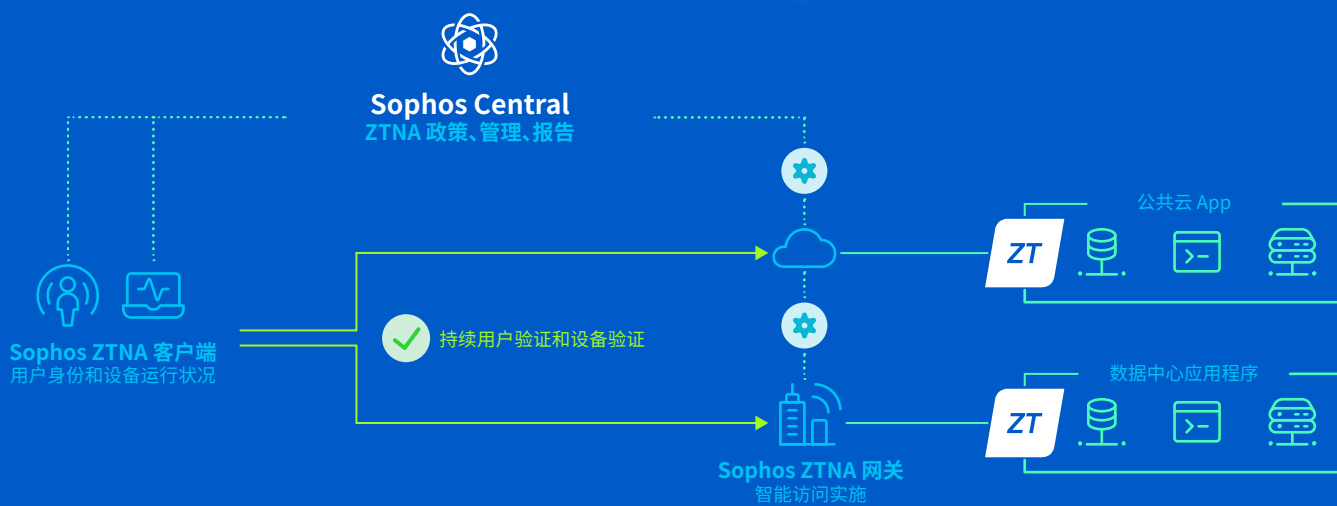




Sophos ZTNA 部署核查清单

通过全球最值得信任的网络安全管理平台 Sophos Central 云交付和云管理,可以方便快捷地部署 Sophos ZTNA。利用这份核查清单,确保您获得必要支持技术,实现顺利部署。



快速入门部署核查清单：

- ✓ 您希望细分网络内和 AWS 中宿主的托管应用程序，这些应用程序可以帮助远程用户进行安全访问。
- ✓ 您有支持 ZTNA 网关的 hypervisor 管理程序平台或云提供商。
- ✓ 您有现代身份提供商 – Azure 或 Okta。Azure 在许多情况下对于基本 IDP 支持是免费的，可以快速集成本地 Active Directory。
- ✓ 您有 Windows 10，可以密集访问应用程序，或者希望为所有平台的 Web 应用程序提供无客户端浏览器访问。
- ✓ 您可能希望使用 Sophos Synchronized Security with Intercept X，在访问政策中集成设备运行状况。

详细注意事项：



确定所有托管应用程序：确定要细分的应用程序，提供安全远程访问。Sophos ZTNA 要求这些应用程序位于本地、数据中心、托管提供商或者 Amazon Web Services (AWS) 公共云。Sophos ZTNA 无法控制对第三方互联网托管 (SaaS) 应用程序 (为面对公众而设计的应用程序，如 Salesforce.com 或 O365) 的访问。



确定网关策略：Sophos ZTNA 网关控制应用程序访问，提供持续用户身份验证和设备验证。每个应用程序托管位置的网络网关需要 ZTNA 网关。例如，如果您在两个不同数据中心和 AWS 中托管应用程序，则需要三个 ZTNA 网关。Sophos 零信任网关免费部署任意数量。下表概要介绍 ZTNA 网关平台支持。确保您有这些平台可用于网关部署。



部署您的身份识别策略：您将需要 Sophos ZTNA 支持的身份识别提供商 (IDP) 验证您的用户身份。下表概要介绍提供商列表。Sophos ZTNA 可以配合集成支持 IDP 的大多数多重形式身份验证 (MFA) 解决方案。您可以利用本地 Active Directory 在 Sophos Central 中导入目录树进行基于用户的政策创作，但不足以达到远程访问 IDP 解决方案的程度。



确定您的用户数量：ZTNA 授权许可非常简单 - 根据用户 - 仅计算需要安全应用程序访问的用户数量。要轻松部署客户端，从 Sophos Central 以及 Intercept X 端点代理轻松部署 Sophos Client，也可以在任何其他桌面 AV 产品独立部署。



考虑设备运行状况策略 (可选)：这是根据设备运行状况或合规性控制应用程序访问的可选额外安全层。最初，Sophos ZTNA 支持 Sophos Security Heartbeat 用于设备运行状况和合规性。这需要从 Sophos Central 管理的 Sophos Intercept X，为管理所有网络安全需求提供一个面板。Intercept X 与 Sophos ZTNA 共享设备运行状态，可以用于应用程序访问政策。

Sophos ZTNA 支持的平台

支持的平台	当前	计划
身份识别提供商	Microsoft Azure 和 Okta	其他按需 IDP
ZTNA 网关平台	VMware ESXi 6.5+ 和 AWS	Azure, Hyper-V, Nutanix 和 GCP
ZTNA 客户端平台	Windows	macOS, iOS, Android
ZTNA 设备运行状况	Sophos Security Heartbeat (Intercept X)	Windows 安全中心 计划其他状态评估属性

Sophos ZTNA 授权许可

- Sophos ZTNA 按用户数量授权许可。
- Sophos ZTNA 网关免费部署任意数量。
- 免费提供 Sophos Central 管理。
- Sophos ZTNA 与 Sophos Intercept X 和 Sophos Firewall 组合时效果更佳 (但也可完美配合任何端点或防火墙产品)

更多资源

利用以下资源进一步计划 Sophos ZTNA 部署。

免费试用 Sophos ZTNA
30 天

www.sophos.cn/ztna