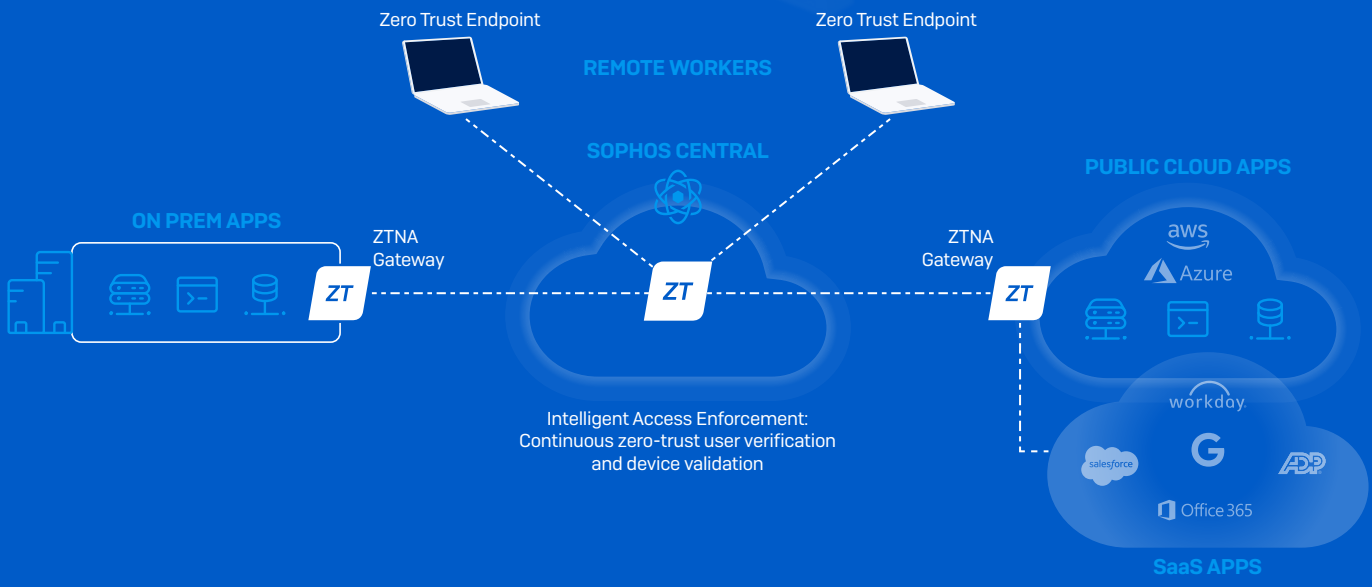
SOPHOS

Sophos ZTNA Deployment Checklist

Deploying Sophos ZTNA is a quick and easy thanks to being cloud-delivered and cloud-managed through Sophos Central, the world's most trusted cybersecurity management platform. Utilize this checklist to ensure you have the necessary supporting technologies available for a smooth deployment.



Your Quick-Start Deployment Checklist:

- ✓ You have a desire to micro-segment the managed applications inside your network and hosted in AWS, providing secure access for your remote users.
- ✓ You have a supported hypervisor platform or cloud provider for the ZTNA gateway(s).
- ✓ You have a modern Identity Provider – Azure or Okta. Azure can be free in many cases for basic IDP support and quickly integrates with on-premises Active Directory.
- ✓ You have Windows 10, or macOS for thick application access or wish to offer clientless browser-based access to web applications on all platforms.
- ✓ Optionally, you wish to integrate device health into access policies using Sophos Synchronized Security with Intercept X.

Detailed Considerations:

Identify all your managed applications: Identify applications you wish to micro-segment and provide secure remote access to. Sophos ZTNA requires that these applications be hosted on premises, in your datacenter, at a hosting provider, or in the Amazon Web Services (AWS) Public Cloud. Sophos ZTNA can also control access to SaaS applications that offer IP address control restrictions.

Determine your gateway strategy: Sophos ZTNA gateways facilitate the secure connection on the application end. ZTNA Gateways are required at the network gateway of each application hosting location. For example, if you have applications hosted in two different data centers and in AWS, you will require three ZTNA gateways.

Two types of gateways are available and can be mixed in a hybird manner:

- Cloud Gateway – lightweight gateway deployed on-prem that connects automatically to the Sophos Cloud via regional Sophos cloud points of presence. This solution offers the ultimate streamlined deployment without requiring any firewall configuration and makes the applications more invisible and secure as a result.
- On-Premise Gateways provide a private data plane connection directly between your endpoints and applications. This solution will be best for those customers who have concerns about latency via the cloud points of presence.

Regardless of which option you choose, Sophos ZTNA gateways are free to deploy as many as you need. Platform support is outlined in the table below. Ensure you have these platforms available for your Gateway deployment.

Define your Identity strategy: You will require an Identity Provider (IDP) that is supported by Sophos ZTNA for authenticating your users. The list of providers is outlined in the table below. Sophos ZTNA will work with most multi-factor authentication (MFA) solutions that integrate with the supported IDPs. You can utilize on-premises Active Directory to import a directory tree into Sophos Central for user-based policy authoring, but this is not sufficient as a remote access IDP solution.

Determine your user count: ZTNA licensing is extremely simple - based on users - so just tally the number of users that require secure application access. To make client deployment easy, the Sophos Client is easily deployed from Sophos Central alongside our Intercept X endpoint agent, but can also be deployed independently alongside any other desktop AV product.

Consider your device health strategy (optional): This is an optional added layer of security for controlling access to applications based on device health or compliance. Initially, Sophos ZTNA supports Sophos Security Heartbeat for device health and compliance. This requires Sophos Intercept X which is also managed through Sophos Central offering a single-pane-of-glass for managing all your cybersecurity needs. Intercept X shares device health status with Sophos ZTNA which can be used in application access policies.

Sophos ZTNA Supported Platforms

Supported Platforms	Current	Planned
Identity Providers	Microsoft Azure and Okta	Additional IDPs based on demand
ZTNA Gateway Platforms	VMware ESXi 6.5+, Hyper-V, and AWS	Azure, Nutanix, and GCP
ZTNA Client Platforms	Windows 10 1803 or later, macOS 11 (Big Sur) or later	iOS and Android
ZTNA Device Health	Sophos Security Heartbeat (Intercept X)	Windows Security Center Additional posture assessment attributes are planned

Sophos ZTNA Cloud Gateway Points of Presence (PoPs)

If deploying Sophos Cloud Gateways, points of presence are available in the following regions:

- Europe (Ireland and Frankfurt)
- North America (Ohio and Oregon)
- Asia Pacific (Mumbai and Sydney)

Sophos ZTNA Licensing

- Sophos ZTNA is licensed simply by the number of users.
- Sophos ZTNA gateways are free to deploy as many as you need.
- Sophos Central management is included at no extra charge.
- Sophos ZTNA works better together with Sophos Intercept X and Sophos Firewall (but also works perfectly alongside any endpoint or firewall product)

Additional Resources

Take advantage of the following resources to further plan your Sophos ZTNA deployment.

- Sophos ZTNA Documentation
- Sophos ZTNA Community Resources

Try Sophos ZTNA free for 30 days at
sophos.com/ztna

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

23-01-10 EN (DD)

SOPHOS