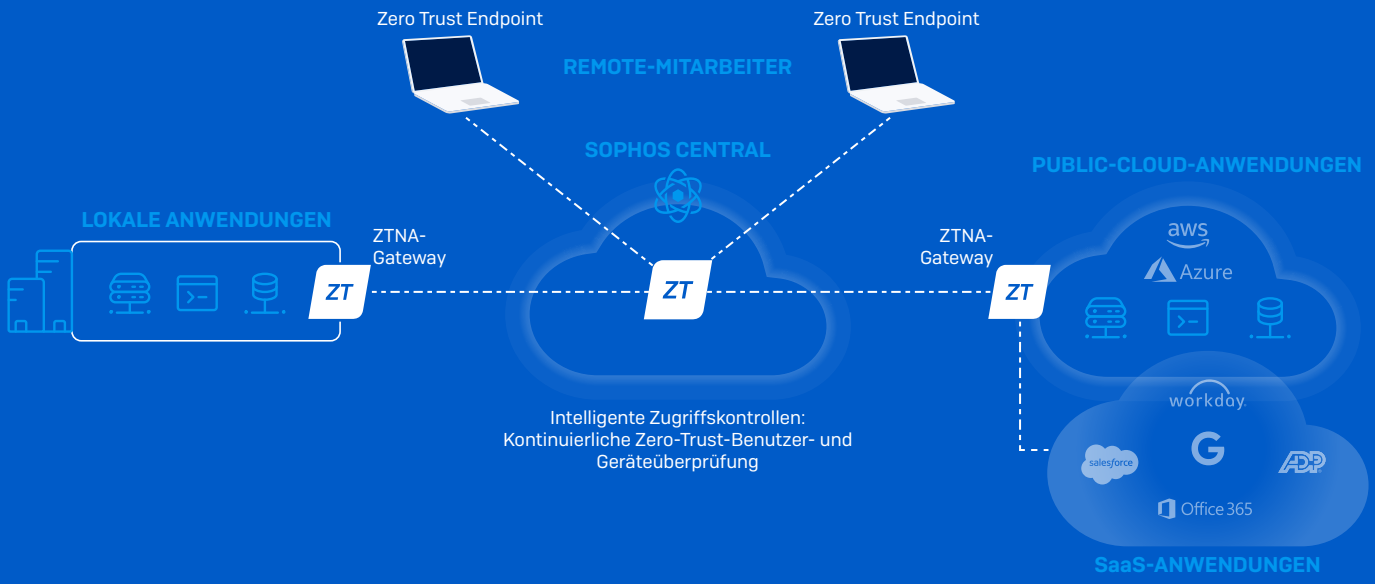
SOPHOS

Sophos ZTNA Bereitstellungs-Checkliste

Sophos ZTNA lässt sich schnell und einfach bereitstellen, da Bereitstellung und Verwaltung über die Cloud in Sophos Central erfolgen – der Cloud-Security-Plattform, der weltweit die meisten Kunden vertrauen. Nutzen Sie diese Checkliste, um sicherzugehen, dass Sie über alle unterstützenden Technologien verfügen, die für eine reibungslose Bereitstellung benötigt werden.



Ihre Quick-Start Bereitstellungs-Checkliste:

- ✔ Sie möchten die in Ihrem Netzwerk verwalteten und in AWS gehosteten Anwendungen mikrosegmentieren, um Ihren Remote-Benutzern einen sicheren Zugriff zu ermöglichen.
- ✔ Sie verfügen über eine unterstützte Hypervisor-Plattform oder einen Cloud-Anbieter für das/die ZTNA-Gateway(s).
- ✔ Sie haben einen modernen Identity Provider (IDP) – Azure oder Okta. Azure lässt sich schnell in das lokale Active Directory integrieren und kann in vielen Fällen für IDP-Basissupport kostenlos genutzt werden.
- ✔ Sie verfügen über Windows 10 oder macOS für den Zugriff auf Thick-Anwendungen oder möchten clientlosen, browserbasierten Zugriff auf Webanwendungen auf allen Plattformen anbieten.
- ✔ Optional können Sie unter Verwendung von Sophos Synchronized Security mit Intercept X den Gerätestatus in Zugriffsrichtlinien integrieren.

Wichtige Punkte:

Ermitteln Sie alle Ihre verwalteten Anwendungen: Legen Sie fest, welche Anwendungen Sie mikrosegmentieren und für welche Sie einen sicheren Remote-Zugriff bereitstellen möchten. Zur Nutzung von Sophos ZTNA müssen die Anwendungen lokal, in Ihrem Rechenzentrum, bei einem Hosting-Anbieter oder in der Amazon Web Services (AWS) Public Cloud gehostet werden. Mit Sophos ZTNA können Sie auch den Zugriff auf SaaS-Anwendungen steuern, die Beschränkungen von IP-Adressen erlauben.

Definieren Sie Ihre Gateway-Strategie: Sophos ZTNA-Gateways erleichtern die sichere Verbindung auf Anwendungsseite. ZTNA-Gateways sind am Netzwerk-Gateway des Hosting-Standorts jeder Anwendung erforderlich. Wenn Ihre Anwendungen beispielsweise in zwei verschiedenen Rechenzentren und in AWS gehostet werden, benötigen Sie drei ZTNA-Gateways.

Es stehen zwei Arten von Gateways zur Verfügung, die hybrid kombiniert werden können:

- Cloud Gateway – leichtgewichtiges Gateway, das lokal bereitgestellt und automatisch über regionale Sophos Cloud Zugangspunkte mit der Sophos Cloud verbunden wird. Diese Lösung ermöglicht eine unkomplizierte Bereitstellung ohne Firewall-Konfiguration und macht Anwendungen so unsichtbarer und damit sicherer.
- Lokale Gateways stellen eine direkte Verbindung auf privater Datenebene zwischen Ihren Endpoints und Anwendungen her. Diese Lösung eignet sich vor allem für Kunden, die Bedenken hinsichtlich der Latenz über die Cloud-Zugangspunkte haben.

Egal für welche Option Sie sich entscheiden: Sie können im Rahmen Ihrer ZTNA-Benutzer-Lizenzierung so viele Sophos ZTNA-Gateways bereitstellen, wie Sie benötigen. Entnehmen Sie bitte der Tabelle auf der folgenden Seite, mit welchen Plattformen die Gateways kompatibel sind. Stellen Sie sicher, dass diese Plattformen für Ihre Gateway-Bereitstellung verfügbar sind.

Definieren Sie Ihre Identitätsstrategie: Zur Authentifizierung Ihrer Benutzer benötigen Sie einen Identitätsanbieter, der von Sophos ZTNA unterstützt wird. Eine Liste dieser Anbieter finden Sie in der Tabelle auf der folgenden Seite. Sophos ZTNA ist mit den meisten Lösungen für eine mehrstufige Authentifizierung (MFA), die sich in die unterstützten IDPs integrieren lassen, kompatibel. Sie können Ihr lokales Active Directory verwenden, wenn Sie eine Verzeichnisstruktur nach Sophos Central importieren möchten, um benutzerbasierte Richtlinien zu erstellen. Als IDP-Lösung für den Remote-Zugriff ist dies jedoch nicht ausreichend.

Ermitteln Sie Ihre Benutzerzahl: Die ZTNA-Lizenzierung ist kinderleicht. Sie erfolgt auf Basis der Benutzerzahl – ermitteln Sie also einfach, wie viele Benutzer einen sicheren Anwendungszugriff benötigen. Der Sophos Client kann problemlos über Sophos Central gemeinsam mit unserem Intercept X Endpoint Agent bereitgestellt werden. Darüber hinaus ist jedoch auch eine unabhängige Bereitstellung mit beliebigen anderen Desktop-Antivirus-Produkten möglich.

Integrieren Sie den Gerätestatus in Ihre Zugriffsrichtlinien (optional): Dies ist eine optionale zusätzliche Schutzschicht, die es ermöglicht, den Zugriff auf Anwendungen auf Basis des Gerätestatus oder der Compliance zu steuern. Für diese Funktionalität nutzt Sophos ZTNA den Sophos Security Heartbeat. Hierzu ist Sophos Intercept X erforderlich, das ebenfalls über Sophos Central verwaltet wird. Sie erhalten also eine zentrale Oberfläche zur Verwaltung Ihrer gesamten Cybersecurity. Intercept X tauscht den Gerätestatus mit Sophos ZTNA aus, sodass dieser in Zugriffsrichtlinien für Anwendungen einfließen kann.

Sophos ZTNA – unterstützte Plattformen

Unterstützte Plattformen	Aktuell	In Planung
Identitätsanbieter	Microsoft Azure und Okta	Zusätzliche IDPs nach Bedarf
ZTNA-Gateway-Plattformen	VMware ESXi 6.5+, Hyper-V und AWS	Azure, Nutanix und GCP
ZTNA-Client-Plattformen	Windows 10, Version 1803 oder höher, macOS 11 (Big Sur) oder höher	iOS und Android
ZTNA-Gerätestatus	Sophos Security Heartbeat (Intercept X)	Windows-Sicherheitscenter – weitere Posture-Assessment-Attribute in Planung

Sophos ZTNA Cloud Gateway Points of Presence (PoPs)

Zur Bereitstellung von Sophos Cloud Gateways sind Zugangspunkte in den folgenden Regionen verfügbar:

- Europa (Irland und Frankfurt)
- Nordamerika (Ohio und Oregon)
- Asien-Pazifik (Mumbai und Sydney)

Sophos ZTNA-Lizenzierung

- Sophos ZTNA wird nach der Benutzerzahl lizenziert.
- Sie können im Rahmen Ihrer ZTNA-Benutzer-Lizenzierung so viele Sophos ZTNA-Gateways bereitstellen, wie Sie benötigen.
- Die Verwaltung über Sophos Central ist ohne Aufpreis enthalten.
- Sophos ZTNA wurde für den gemeinsamen Einsatz mit Sophos Intercept X und der Sophos Firewall optimiert, kann jedoch auch mit anderen Endpoint- oder Firewall-Produkten genutzt werden.

Weiterführende Informationen

Nutzen Sie zur weiteren Planung Ihrer Sophos ZTNA-Bereitstellung die folgenden Ressourcen:

- Sophos ZTNA – Dokumentation
- Sophos ZTNA – Community-Ressourcen

Testen Sie Sophos ZTNA 30 Tage kostenlos unter
sophos.de/ztna

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

23-01-10 DE (DD)