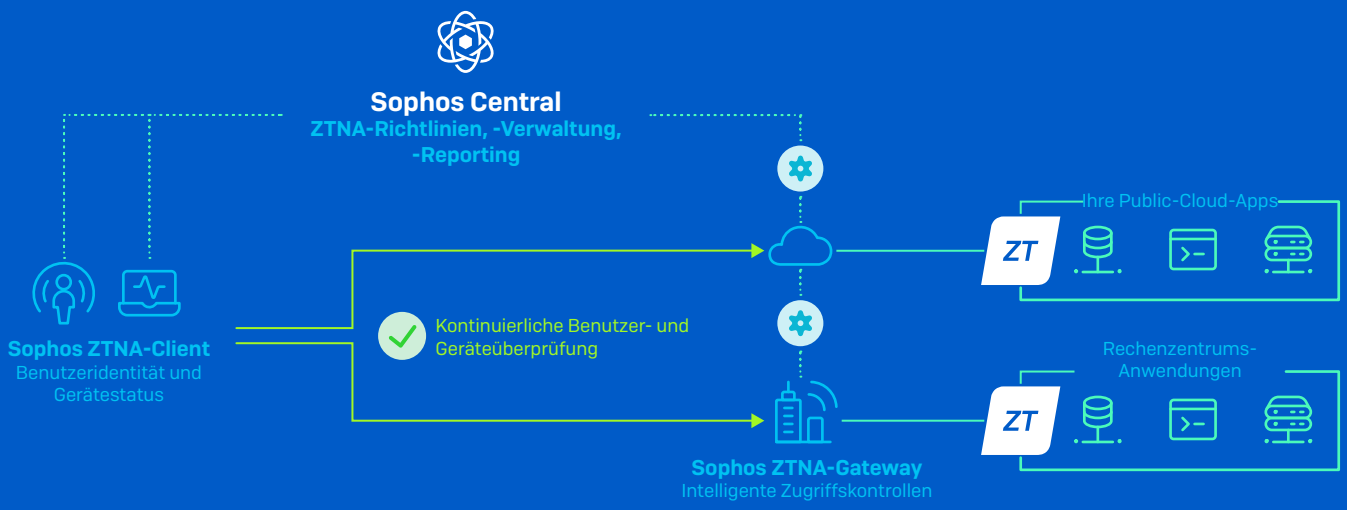
SOPHOS

Sophos ZTNA Bereitstellungs-Checkliste

Durch die Integration in Sophos Central – unsere Cloud-Security-Plattform, der weltweit die meisten Kunden vertrauen – ist Sophos ZTNA vollständig cloudfähig. Die Lösung lässt sich damit schnell und einfach in der Cloud bereitstellen und verwalten. Stellen Sie anhand dieser Checkliste sicher, dass Sie über die erforderlichen unterstützenden Technologien für eine reibungslose Bereitstellung verfügen.



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 Identitätsanbieter (Identity Provider, IDP) wie 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 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 vor Ort, in Ihrem Rechenzentrum, bei einem Hosting-Anbieter oder in der Amazon Web Services (AWS) Public Cloud gehostet werden. Der Zugriff auf im Internet gehostete Anwendungen von Drittanbietern (SaaS) wie Salesforce.com oder 0365 kann mit Sophos ZTNA nicht kontrolliert werden, da diese Anwendungen öffentlich zugänglich sind.

Definieren Sie Ihre Gateway-Strategie: Sophos ZTNA-Gateways steuern den Zugriff auf Anwendungen und ermöglichen eine kontinuierliche Benutzer- und Geräteüberprüfung. 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. Sie können eine beliebige Anzahl von Sophos Zero-Trust-Gateways kostenlos bereitstellen. Entnehmen Sie bitte der Tabelle auf der folgenden Seite, mit welchen Plattformen ZNTA-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 greift Sophos ZTNA auf den Sophos Security Heartbeat zurück. 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+ und AWS	Azure, Hyper-V, Nutanix und GCP
ZTNA-Client-Plattformen	Windows	macOS, iOS, Android
ZTNA-Gerätestatus	Sophos Security Heartbeat (Intercept X)	Windows-Sicherheitscenter – weitere Posture-Assessment-Attribute in Planung

Sophos ZTNA-Lizenzierung

- Sophos ZTNA wird nach der Benutzerzahl lizenziert.
- Sie können eine beliebige Anzahl von Sophos ZTNA-Gateways kostenlos bereitstellen.
- Die Verwaltung über Sophos Central ist ebenfalls 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
www.sophos.de/ztna

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

21-08-18 DE (DD)

SOPHOS