Sophos ZTNA

Zero Trust Network Access

Sophos ZTNA verbindet Mitarbeiter von überall aus sicher mit Ihren Anwendungen. Neben einer besseren Segmentierung sorgt Sophos ZTNA auch für mehr Sicherheit und Transparenz als traditionelles Remote Access VPN. Sophos ZTNA ist eine Einzellösung, kann aber auch als integrierte Synchronized-Security-Lösung zusammen mit der Sophos Firewall und Intercept X genutzt werden.

Deutlich mehr Sicherheit mit Zero Trust

Sophos ZTNA basiert auf dem Zero-Trust-Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Einzelne Benutzer und Geräte werden zu ihrem eigenen mikrosegmentierten Perimeter, der ständig validiert und verifiziert wird. Sie befinden sich nicht mehr „im Netzwerk", hinter dessen Mauern jedem implizit vertraut und Zugriff gewährt wird. Vertrauen muss ab sofort verdient werden und wird nicht mehr vorausgesetzt.

Optimale Bedingungen für Remote-Mitarbeiter

ZTNA ermöglicht Ihren Remote-Mitarbeitern, von überall aus sicher auf die Daten und Anwendungen zuzugreifen, die sie benötigen. Außerdem sind Bereitstellung, Registrierung und Verwaltung wesentlich einfacher als bei traditionellem VPN.

Sicherer Zugriff auf Ihre Anwendungen

Dank der Mikrosegmentierung in Sophos ZTNA können Sie einen sicheren Zugriff auf Ihre Anwendungen ermöglichen – egal, ob Ihre Anwendungen lokal, in einem Rechenzentrum oder in Ihrer Public Cloud-Infrastruktur gehostet werden. Außerdem erhalten Sie in Echtzeit Einblick in Anwendungsaktivitäten (Status, Security Posture und Nutzung). Durch die Beschränkung von IP-Adressen können Sie auch den Zugriff auf viele SaaS-Anwendungen steuern und nur Verbindungen von Ihren ZTNA-Gateways erlauben.

Abwehr von Ransomware und anderen Bedrohungen

Die Gefahr, dass Ransomware und andere Bedrohungen ein kompromittiertes Endgerät infizieren und sich von dort aus im gesamten Netzwerk verbreiten, besteht bei ZTNA nicht mehr. Denn Benutzer und Geräte haben nur auf bestimmte Anwendungen expliziten richtlinienbasierten Zugriff. Dadurch werden die größten VPN-Schwachstellen, wie implizites Vertrauen und weitreichender Netzwerkzugriff, eliminiert.

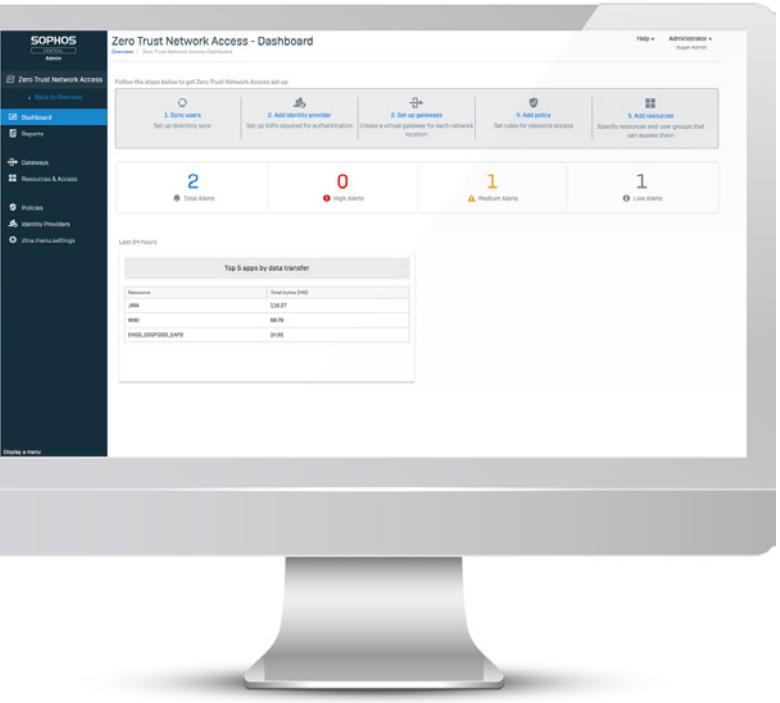
Schnelle Bereitstellung, Anpassung und Skalierung

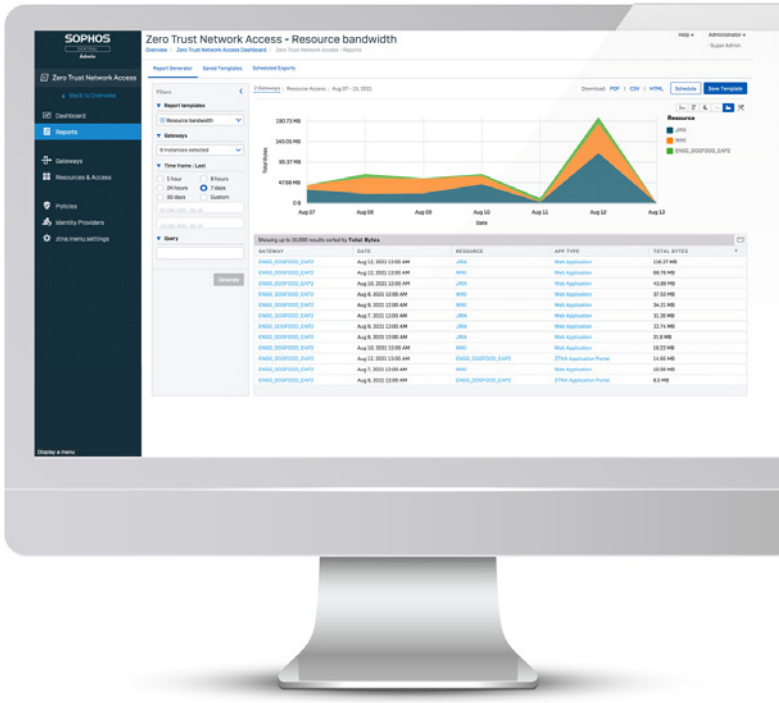
Sophos ZTNA wurde für moderne Netzwerke entwickelt, die sich dynamisch verändern, schnell wachsen und mit enormer Geschwindigkeit in die Cloud verlagert werden. Sophos ZTNA ist eine schlanke, saubere Lösung, mit der Sie schnell und einfach neue Anwendungen sicher implementieren, Geräte und Benutzer an- und abmelden und Informationen über Anwendungsstatus und -nutzung erhalten.

Vorteile auf einen Blick

- Deutlich mehr Sicherheit als mit Remote Access VPN
- Nutzerfreundlich und transparent für Anwender
- Praktische Lösung mit nur einem Agenten und einer Konsole
- Mikrosegmentierung und Schutz Ihrer Netzwerkanwendungen
- Funktioniert überall – innerhalb und außerhalb des Netzwerks
- Einfache Bereitstellung und Verwaltung in der Cloud
- Genaue Übersicht und Einblicke in Ihre Anwendungen
- Integriert den Gerätestatus in Zugriffsrichtlinien
- Einfache jährliche Subscription-Lizenzierung pro Benutzer

SOPHOS





Bereitstellung und Verwaltung in der Cloud

Sophos ZTNA basiert auf dem Zero-Trust-Prinzip und sorgt für einfachen, integrierten und sicheren Netzwerkzugriff. Unsere ZTNA-Lösung wird in der Cloud bereitgestellt und verwaltet und ist in Sophos Central integriert – unsere Cloud-Security-Plattform, der weltweit die meisten Kunden vertrauen.

In Sophos Central verwalten Sie nicht nur ZTNA, sondern auch Ihre Sophos Firewalls, Endpoints, Mobilgeräte, Cloud-Security, Ihren Server- und E-Mail-Schutz und vieles mehr. Sie können sich jederzeit und von jedem Gerät aus anmelden und Ihre IT-Sicherheit verwalten.

Ein Agent, eine Konsole, ein Anbieter

Sophos ZTNA lässt sich perfekt in das umfassende Sophos-Cybersecurity-Ökosystem integrieren, um Ihren Arbeitsalltag deutlich zu erleichtern. Sie erhalten eine Single-Agent-Lösung für ZTNA und Ihre Next-Gen Endpoint Protection. Zudem bietet Ihnen Sophos Central eine zentrale Management-Konsole, in der alle Informationen von Ihren IT-Security-Produkten zusammenlaufen. So haben Sie Ihre gesamte IT-Sicherheit stets im Blick.

Unsere Kunden bestätigen uns: Eine integrierte Cybersecurity-Lösung von Sophos spart enorm viel Zeit und verdoppelt die Leistung der IT-Abteilung.

Nahtlos integriert: ZTNA und Next-Gen Endpoint Protection

Sophos ZTNA ist die einzige Lösung für Zero Trust Network Access, die nahtlos mit einem Next-Gen-Endpoint-Produkt verknüpft ist – Sophos Intercept X. Dies bietet deutliche Vorteile für die Sicherheit, Bereitstellung und Verwaltung.

- End-to-End-Schutz: Sorgen Sie für einen sicheren Zugriff auf Ihre Anwendungen und schützen Sie Ihre Endpoints und Netzwerke vor Sicherheitspannen und Bedrohungen wie Ransomware – mit marktweit leistungsstärkstem Machine Learning und führender Next-Gen-Endpoint-Technologie.
- Synchronized Security: Durch die Integration von ZTNA und Endpoint Protection werden kontinuierlich Status- und Integritätsdaten ausgetauscht. So lassen sich kompromittierte Systeme automatisch isolieren, damit Bedrohungen sich nicht weiter verbreiten und keine Daten abgeschöpft werden können.
- Ein Agent, eine Konsole, ein Anbieter.

Diese perfekte Kombination finden Sie nur bei Sophos.

Bereitstellung mit einem Agenten

Sophos ZTNA ist direkt mit der Sophos Next-Gen Endpoint Protection Intercept X integriert. Dadurch lassen sich beide gemeinsam in einem einzigen Client bereitstellen.

Somit erhalten Sie einzigartigen Endpoint- und Ransomware-Schutz, plus maximale Anwendungs-Sicherheit und Segmentierung – alles bereitgestellt in einem einzigen Client.

Ein clientloser Zugriff für browserbasierte Anwendungen ist ebenfalls möglich.

Skalierbare Anwendungs-Gateways

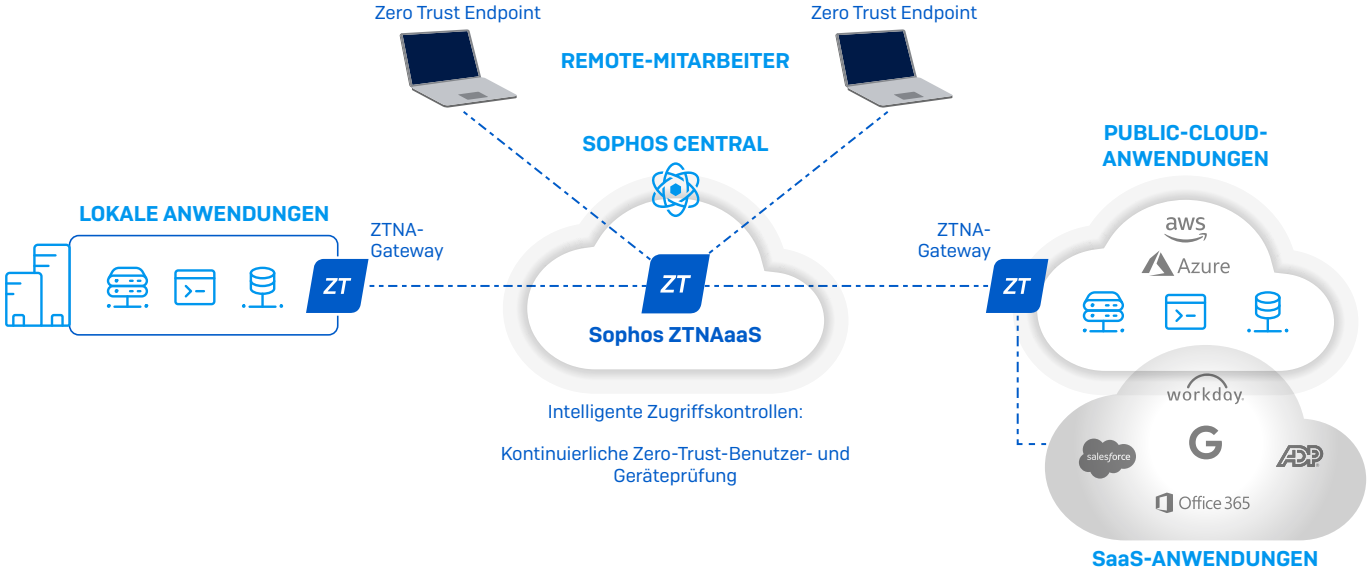
Sophos ZTNA-Gateways sind als virtuelle Appliance erhältlich und lassen sich schnell und einfach dort bereitstellen, wo sie benötigt werden. So können Sie ganz einfach Hochverfügbarkeits-Gateways bereitstellen und sie skalieren, wenn Ihr Unternehmen wächst.

Synchronized Device Health

Sophos ZTNA schöpft die Vorteile von Sophos Synchronized Security voll aus und nutzt den Security Heartbeat™ zwischen Sophos Intercept X Endpoints, Sophos Central und ZTNA, um den Gerätestatus zu bewerten sowie aktive Bedrohungen und Anzeichen von Kompromittierungen zu erkennen. Auf diese Weise kann der Zugriff durch kompromittierte und nicht richtlinienkonforme Geräte sowohl im Netzwerk als auch außerhalb des Netzwerks umgehend beschränkt werden.

Integrierte Identität

Identität ist die Grundlage bei Zero Trust. Sophos ZTNA überprüft kontinuierlich die Benutzeridentität und unterstützt die gängigsten IDP-Lösungen, darunter Microsoft Azure und Okta. Sie können Ihre bevorzugte MFA-Lösung (Multi-Faktor-Authentifizierung) gemeinsam mit diesen IDPs nutzen, um sich vor Diebstahl von Zugangsdaten oder kompromittierten Geräten zu schützen.



Sophos Zero Trust Endpoint

Kann agentenlos oder mit unserem kompakten Sophos ZTNA-Agenten ausgeführt werden, der sich in Sophos Intercept X integrieren lässt und mit Synchronized Security eine einzigartig starke Zero-Trust-Endpoint-Lösung bietet. Sophos ZTNA lässt sich auf Wunsch auch mit bereits vorhandenen Endpoint-Protection-Produkten nutzen.

Sophos Central

Mit Sophos Central wird ZTNA as a Service ganz einfach: mit schneller Bereitstellung, detaillierten Richtlinienkontrollen sowie maximaler Transparenz und aufschlussreichen Reports aus der Cloud. Funktioniert mit gängigen Identitätsanbietern und ermöglicht intelligente Zugriffskontrollen für Ihre Anwendungen durch kontinuierliche Benutzer- und Geräteprüfung.

Sophos ZTNA-Gateway

Ist erhältlich als virtuelle Appliance auf Hyper-V, VMware und Amazon Web Services. Die Bereitstellung geht schnell und einfach. Das Gateway macht Ihre Anwendungen für das öffentliche Internet unsichtbar und stellt eine sichere Verbindung für verifizierte Benutzer und ihre validierten Geräte zu den Anwendungen bereit, die sie für ihre Arbeit benötigen.

Sophos ZTNA – Funktionsübersicht

- Sicherer Zugriff: für Geschäftsanwendungen, die vor Ort oder in Ihrer Public-Cloud-Infrastruktur gehostet werden
- Anwendungen: alle browserbasierten Web-Anwendungen im clientlosen Modus; Thick-Anwendungen (z. B. SSH, VNC, RDP und andere) über den ZTNA-Client
- Zugriffsrichtlinien: auf Basis von Benutzergruppen und Integritätsstatus (Synchronized Security)
- Reporting, Monitoring, Protokollierung und Auditing von Anwendungsstatus, Zugriff und Nutzung über Sophos Central
- Benutzerportal für Anwender zum Zugriff auf Anwendungen mit Lesezeichen

Technische Spezifikationen

Unterstützte Plattformen	Aktuell	In Planung
Identitätsanbieter	Microsoft Azure und Okta	Zusätzliche IDPs nach Bedarf
ZTNA-Gateway-Plattformen	VMware ESXi 6.5+, Hyper-V 2016+ 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

Gateway-Spezifikationen	
Empfohlene VM	2 Core/4 GB
Multi-Knoten-Clustering	Bis zu 9 Knoten mit Load Balancing für Performance, Kapazität und Business Continuity
Knoten-Kapazität und -Skalierung	10.000 Agent-Verbindungen für einen einzelnen Knoten, bis zu 90.000 Agent-Verbindungen in einem Cluster (max. 9 Knoten)

Informationen zum Kauf

Sophos ZTNA wird pro Benutzer auf Basis einer jährlichen Subscription lizenziert. Im Rahmen dieser Lizenzierung können Sie so viele Gateways bereitstellen, wie Sie benötigen.

Weitere Informationen unter:
sophos.de/ztna

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

23-01-10 DS-DE (DD)

SOPHOS