Sophos ZTNA

Zero Trust Network Access

Sophos ZTNA verbindet jeden Mitarbeiter an jedem beliebigen Standort mit jeder beliebigen Anwendung. Dabei bietet es neben einer besseren Segmentierung mehr Sicherheit und Transparenz als herkömmliches Remote Access VPN. Sophos ZTNA ist eine Einzellösung, kann aber auch als integrierte Synchronized-Security-Lösung zusammen mit der Sophos Firewall und Intercept X verwendet werden.

So gewähren Sie Vertrauen im Zeitalter von 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.

Remote-Mitarbeiter optimal unterstützen

ZTNA ermöglicht Ihren Remote-Mitarbeitern, sicher und von jedem Standort aus auf genau die Daten und Anwendungen zuzugreifen, die sie benötigen. Gleichzeitig wird die Bereitstellung, Registrierung und Verwaltung wesentlich einfacher als bei herkömmlichem VPN.

Ihre Anwendungen mikrosegmentieren

Sophos ZTNA bietet die ultimative Mikrosegmentierung, sodass Sie überall einen sicheren Anwendungszugriff bereitstellen können – egal, ob Ihre Anwendungen vor Ort, in einem Rechenzentrum oder in Ihrer Public Cloud-Infrastruktur gehostet werden. Außerdem erhalten Sie in Echtzeit Einblick in Anwendungsaktivitäten (Status, Security Posture und Nutzung).

Ransomware und Bedrohungen stoppen

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 lediglich auf bestimmte Anwendungen expliziten richtlinienbasierten Zugriff. Dadurch werden die größten VPN-Schwachstellen, wie implizites Vertrauen und weitreichender Netzwerkzugriff, eliminiert.

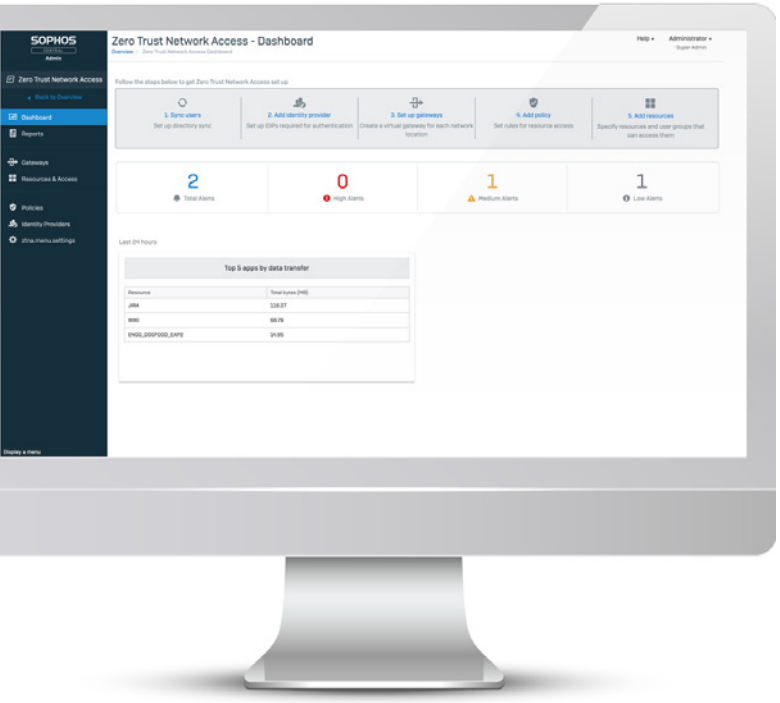
Schnelle Bereitstellung, Anpassung und Skalierung

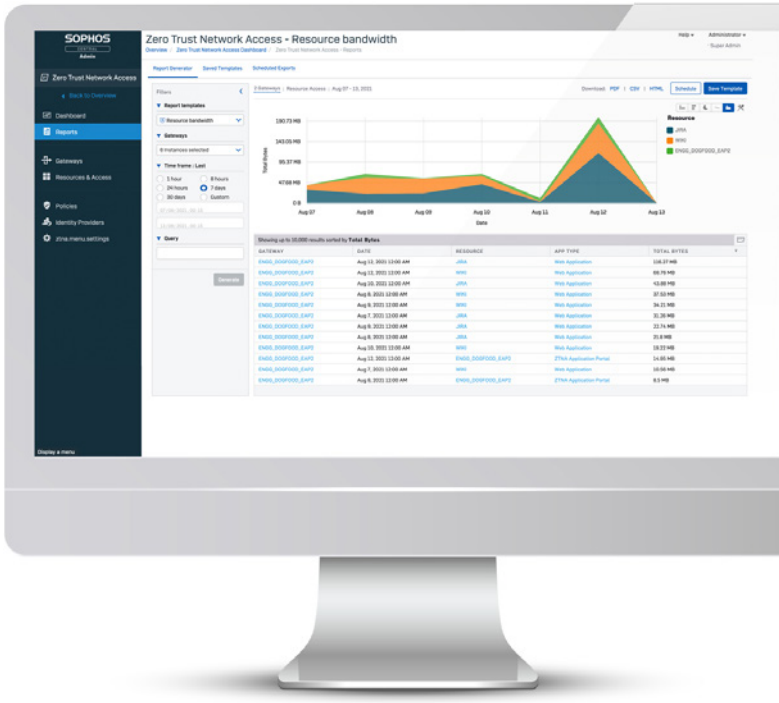
Sophos ZTNA wurde für moderne Netzwerke entwickelt, die sich dynamisch verändern, schnell wachsen und mit enormer Geschwindigkeit in die Cloud verlagert werden. Sophos ZTNA ist eine schlanke, saubere Lösung, mit der Sie schnell und einfach neue Anwendungen sicher implementieren, Geräte und Benutzer an-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

Highlights

- Zero Trust: „Nichts und niemandem vertrauen, alles überprüfen"
- Integriert in Sophos Intercept X
- Lösung mit nur einem Agenten und einer Konsole
- Die bessere Alternative zu Remote Access VPN
- Mikrosegmentierung und Schutz Ihrer Netzwerkanwendungen
- Funktioniert überall, im Netzwerk oder außerhalb
- Bereitstellung und Verwaltung in der Cloud
- Transparent für Enduser
- Genaue Übersicht und Einblicke in Ihre Anwendungen
- Integriert den Gerätestatus in Zugriffsrichtlinien
- Einfache jährliche Subscription-Lizenzierung pro Benutzer mit kostenlosen Gateways

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-Sicherheittools 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 ZTNA-Lösung, die direkt in ein Next-Gen-Endpoint-Produkt – Sophos Intercept X – integriert ist. 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

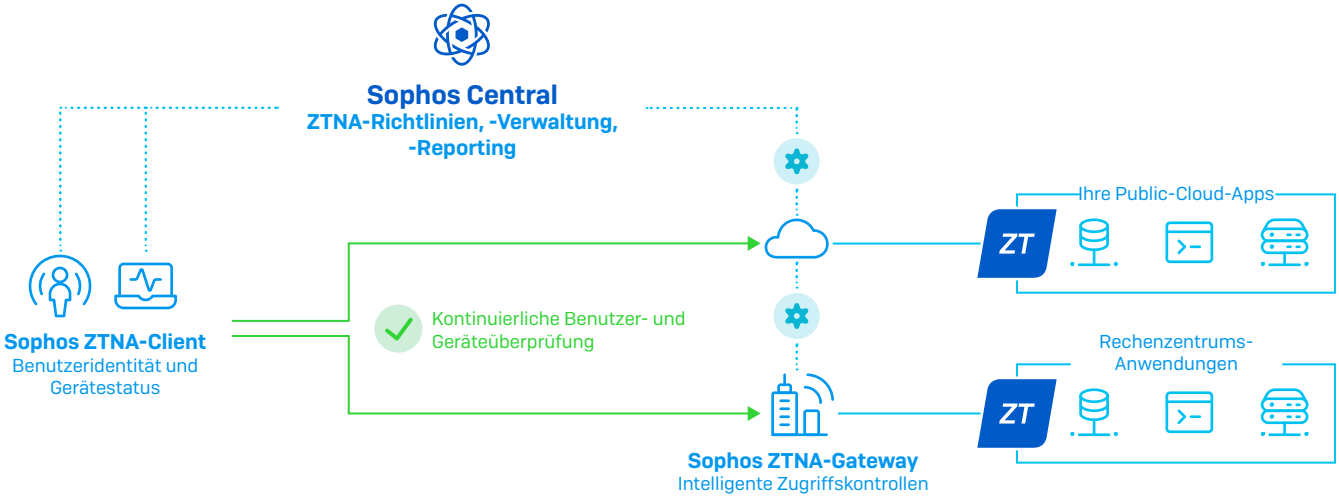
Sophos ZTNA-Gateways sind kostenlos als virtuelle Appliances erhältlich und lassen sich einfach dort bereitstellen, wo Sie sie benötigen. Als Hochverfügbarkeits-Gateways können Sie diese an die wechselnden Anforderungen Ihres Unternehmens anpassen.

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. Außerdem können Sie auch Ihre bevorzugte MFA-Lösung (mehrstufige Authentifizierung) in diese IDPs integrieren, um sich vor Diebstahl von Zugangsdaten oder kompromittierten Geräten zu schützen.



Komponenten von Sophos ZTNA:

Sophos Central: Die Verwaltung in der Cloud sorgt für eine einfache Bereitstellung, detaillierte Richtlinienkontrollen sowie Transparenz und aufschlussreiche Reports. Dank Integration in Intercept X kann ZTNA auch den Synchronized Security Heartbeat™ nutzen.

Sophos ZTNA-Client: Bietet dank gemeinsamer One-Click-Bereitstellung mit Intercept X transparenten und reibungslosen Remote-Zugriff auf Anwendungen auf der Basis von Benutzeridentität und Gerätestatus.

Sophos ZTNA-Gateway: Ist als virtuelle Appliance auf VMware und AWS zum Schutz von Netzwerk-Anwendungen verfügbar und lässt sich einfach und kostenlos bereitstellen. Geschützte Anwendungen können sich vor Ort, in Ihrem Rechenzentrum oder in Ihrer AWS Public Cloud-Infrastruktur befinden.

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 Enduser 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+ und AWS	Azure, Hyper-V, Nutanix und GCP
ZTNA-Client-Plattformen	Windows 10, Version 1803 oder höher	macOS, iOS, 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	1000 Clients für einen einzelnen Knoten, bis zu 3500 Clients in einem Cluster

Informationen zum Kauf

Sophos ZTNA wird pro Benutzer auf Basis einer jährlichen Subscription lizenziert. Eine beliebige Anzahl von Sophos ZTNA-Gateways kann kostenlos bereitgestellt werden.

Weitere Informationen 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

21-11-10 DS-DE (DD)

SOPHOS