

Sophos ZTNA Qualification Guide

Zero Trust Network Access: Der sichere Nachfolger von Remote Access VPN

Wer trifft die Kaufentscheidung?

Welche ZTNA-Lösung gekauft wird, entscheidet oft der Desktop-IT-Administrator. Denn er ist dafür verantwortlich, dass seine Remote-Mitarbeiter über die Tools verfügen, die sie für ihre Arbeit benötigen. Es können auch Netzwerk-Verantwortliche involviert sein, bei denen ein Wegfall von Remote-Access-VPN vermutlich auf positive Resonanz stoßen wird.

Gesprächseinstieg, Skript zur Kundengewinnung, Elevator Pitch:

Haben Sie Remote-Mitarbeiter oder Interesse an der Implementierung von Zero Trust? Wie ermöglichen Sie Ihren Mitarbeitern flexibles, standortunabhängiges Arbeiten ohne Risiken für Ihre Netzwerkanwendungen?

- Viele Unternehmen müssen heutzutage Mitarbeiter an verschiedensten Orten unterstützen und stoßen beim Einsatz von Remote-Access-VPN für den sicheren Anwendungszugriff zunehmend an ihre Grenzen.
- Ab sofort gibt es eine bessere Methode für den Remote-Zugriff – ZTNA. Zero Trust Network Access ist viel einfacher, skalierbarer und transparenter für die Anwender. ZTNA hat keine Performance-Probleme, funktioniert überall und bietet besseren Schutz vor Ransomware und sonstigen Bedrohungen.
- Außerdem wird Sophos ZTNA gemeinsam mit Sophos Intercept X in einem einzigen Agenten bereitgestellt. Sie erhalten damit den besten Endpoint-Schutz und ZTNA von einem Anbieter, in einem einzigen Agenten und komplett verwaltet über eine einzige Konsole. Diese einzigartige Lösung finden Sie nur bei Sophos.

Warum ZTNA?

Gezielte Zugriffskontrolle

VPN bietet weitreichenden Netzwerkzugriff, wohingegen ZTNA gezielt nur Zugriff auf bestimmte Anwendungen ermöglicht. Diese Mikrosegmentierung reduziert das Risiko und die Möglichkeit, dass Bedrohungen sich lateral bewegen.

Mehr Sicherheit

ZTNA eliminiert alte anfällige VPN-Clients, berücksichtigt den Integritätsstatus der Geräte in Richtlinien und stoppt laterale Bewegungen.

Überall einsetzbar

ZTNA ist in jedem Netzwerk einsetzbar (zu Hause, im Hotel, am Flughafen) und ist insbesondere für Unternehmensnetzwerke geeignet, die häufig mit VPN-Problemen zu kämpfen haben.

Transparent

ZTNA ist für die Anwender viel transparenter – es funktioniert einfach – im Hintergrund.

Umfassender Einblick

Mit VPN erhalten Administratoren keine Einsicht in Benutzeraktivitäten, ZTNA hingegen bietet detaillierten Einblick in die Anwendungsnutzung.

Leichtere Verwaltung

Cloud-verwaltetes ZTNA ist wesentlich skalierbarer und lässt sich einfacher hinzufügen und außer Betrieb nehmen als ein Firewall-verwaltetes VPN.

Warum Sophos ZTNA?

Sophos ZTNA ist eine „Single Agent, Single Console, Single Vendor“-Lösung. Im Klartext bedeutet das: Sophos ZTNA bietet eine einfachere Bereitstellung, weniger Footprint auf dem Gerät, eine leichtere Verwaltung und Integration mit anderen Sophos-Produkten für Synchronized Security™, eine einfache Lizenzierung und niedrigere Gesamtkosten.

Qualification Guide

Ihr Interessent ist ein potenzieller Kandidat für Sophos ZTNA, wenn er die folgenden Fragen mit „Ja“ beantwortet:

Hat/nutzt der Interessent ...	Ja ...
... Remote-Mitarbeiter oder Interesse an Zero Trust?	ZTNA eignet sich optimal für Remote-Mitarbeiter und den Aufbau eines Zero-Trust-Netzwerks.
... selbst gehostete Anwendungen?	ZTNA ermöglicht einen sicheren Zugriff auf diese Anwendungen. Zudem kann ZTNA auch den Zugriff auf SaaS-Anwendungen steuern, die eine IP-Adressen-Zugriffskontrolle unterstützen.
... lokal oder in AWS gehostete Anwendungen?	Sophos ZTNA sorgt für sicheren Zugriff auf diese Anwendungen (weitere Public-Cloud-Plattformen folgen in Kürze).
... Active Directory (lokal oder in Azure) oder Okta?	Sophos ZTNA kann mit den Identity-Anbietern Azure und Okta genutzt werden (weitere Anbieter werden in Kürze unterstützt).
... VMware oder Hyper-V vor Ort?	Sophos ZTNA-Gateways laufen auf VMware ESXi und Hyper-V (weitere Plattformen folgen in Kürze).
... Windows oder macOS auf den Endgeräten der Anwender?	Sophos ZTNA bietet derzeit sicheren Thick-Client-Zugriff für Windows und macOS oder clientlosen Zugriff für Web-Anwendungen auf jeder Plattform bieten, einschließlich Mobilgeräten.
... Intercept X oder besteht Interesse an Intercept X?	Sophos ZTNA ist optimal auf den gemeinsamen Einsatz mit Intercept X abgestimmt und wird in Sophos Central verwaltet. Allerdings ist auch die Nutzung mit anderen Endpoint-Produkten möglich.

Umgang mit Einwänden:

Ich bin mit meiner Remote-Access-VPN-Lösung sehr zufrieden

- Wenn Sie nur wenige Benutzer haben, mag das der Fall sein. Sollten jedoch weitere Benutzer hinzukommen, sind Probleme praktisch vorprogrammiert.
- Wenn Ransomware Ihnen Sorgen bereitet, bietet der Wechsel von VPN zu ZTNA weit besseren Schutz vor Angreifern, die versuchen, sich durch die Ausnutzung von VPN Zugriff auf Ihr Netzwerk zu verschaffen.

VPN-Zugriff ist günstig oder kostenlos

- Dies trifft häufig zu. Jedoch verursacht VPN versteckte Kosten, z. B. in Form eines hohen Zeit- und Verwaltungsaufwands. Wie bei den meisten Dingen im Leben gilt also auch hier, dass man nichts geschenkt bekommt – und ganz sicherlich keinen Schutz.

Wir benötigen Unterstützung für Plattform X

- Möglicherweise benötigen Sie eine Plattform für Clients, Gateways oder Identitätsanbieter, die wir derzeit nicht unterstützen. Wenn das der Fall ist, haben wir die Unterstützung dieser Plattform wahrscheinlich schon auf unserer Roadmap und sollten in Kontakt bleiben. Beispielsweise unterstützen wir mittlerweile schon Mac-Clients und Hyper-V-Gateways.

Ich nutze bereits eine ZTNA-Lösung von Anbieter A

- Dann gibt es keinen Grund für einen Wechsel – es sei denn, der Interessent zieht Sophos Intercept X für seine Endpoints in Betracht. In diesem Fall bietet der Wechsel zu unserer ZTNA-Lösung zahlreiche zusätzliche Vorteile: einen Agenten, eine Konsole, einen Anbieter, einfachere Lizenzierung und besseren integrierten Schutz mit Synchronized Security™.

Weitere Informationen unter
sophos.de/ztna

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

© Copyright 2023. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

23-01-30 DE [PC]

SOPHOS