5 wichtige Überlegungen bei der Auswahl einer Zero Trust Network Access-Lösung

netskope

5 wichtige Überlegungen bei der Auswahl einer Zero Trust Network Access-Lösung

Unternehmen setzen zunehmend auf Security Service Edge (SSE), um die Vorteile einer SASE-Architektur sicher nutzen zu können. Ein wichtiger Bestandteil von SSE ist eine Zero Trust Network Access (ZTNA)-Lösung, die anwendungsspezifische Konnektivität für Benutzer überall an jedem Ort ermöglicht. Security Service Edge unterstützt die Zusammenführung von Sicherheitsfunktionen, senkt die Gesamtbetriebskosten und verbessert langfristig die betriebliche Effizienz, was zu einer besseren Sicherheit insgesamt führt.

Unternehmen setzen zunehmend auf Security Service Edge (SSE), um die Sicherheitstransformation in der neuen Ära von Cloud- und hybrider Arbeit zu ermöglichen.

netskope

Die Plattform ist wichtig

Ob Sie ZTNA für ein Remote-/Hybrid-Arbeitsprojekt, für ein Erstprojekt auf dem Weg zu einer größeren Implementierung von Zero-Trust-Sicherheit oder im Rahmen einer vollständig definierten Vision für SSE und SASE auswählen und implementieren: Am besten ist es, mit einem Anbieter zusammenzuarbeiten, der über eine vollständige SSE-Plattform verfügt – ein einziger Agent, eine einzige Konsole und eine einzige Richtlinien-Engine mit Unterstützung für eine Multi-Cloud-Umgebung.

Gartner schätzt, dass „bis 2025 70% der Unternehmen, die einen agentenbasierten Zero Trust Network Access (ZTNA) implementieren, sich für einen Security Service Edge (SSE)-Anbieter für ZTNA entscheiden werden, anstatt für ein eigenständiges Angebot, im Gegensatz zu nur 20% im Jahr 2021.“*

Ob Sie ZTNA auswählen und implementieren oder

*Gartner, „Magic Quadrant for Security Service Edge“, John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, 15. Februar 2022

02

Hybrides Arbeiten überall ermöglichen

Um hybrides Arbeiten von überall aus zu ermöglichen, ist es wichtig, einen Anbieter mit einer Präsenz zu wählen, die Ihren globalen Expansionsplänen und der Agilität Ihres Unternehmens gerecht wird. Stellen Sie sicher, dass Sie mit einem ZTNA-Anbieter zusammenarbeiten, der über Rechenzentren an allen wichtigen geografischen Standorten verfügt, von denen aus sich Ihre Mitarbeiter möglicherweise verbinden. Bei der Auswahl Ihres Anbieters sollten Sie sich aber nicht nur nach der Anzahl der Rechenzentren richten. Wählen Sie stattdessen einen Anbieter, der in jeder Region den gesamten Sicherheits-Stack zur Verfügung stellt – mit kompletter Rechenleistung am Edge in der Nähe Ihrer Benutzer – mit On-Ramps mit niedriger Latenz in Kombination mit umfangreichem Peering für die beste Benutzer- und Anwendungserfahrung.

Einfach festzulegende Richtlinien

Zusätzlich zu einem einzigen Agenten sollte nur noch ein einziger Schritt erforderlich sein, um Identitäts- und Zugriffsrichtlinien über eine zentrale Konsole zu konfigurieren. Sie profitieren davon, dass Sie zur Unterstützung von Fusionen und Übernahmen sowie von anderen zeitkritischen Aktivitäten innerhalb von nur wenigen Tagen den Zugriff auf Cloud- und private Anwendungen ermöglichen können.

Geben Sie sich nicht mit einem Anwendungs-VPN und komplexen Firewall-Regeln zufrieden, die sich als echter ZTNA ausgeben.

Daten überall schützen

Ihre ZTNA-Lösung sollte die Datennutzung, Aktivitäten und anomales Verhalten (UEBA - User & Entity Behaviour Analytics) erkennen, fortschrittliche DLP-Regeln und -Richtlinien durchsetzen und adaptive Zugriffsrichtlinien auf der Grundlage von Benutzerrisiken anwenden.

ZTNA verbindet Benutzer auf sichere Weise mit privaten Anwendungen und Ressourcen. Diese Ressourcen sind oft die Kronjuwelen des Unternehmens – vom Code bis hin zu anderen Formen von geschützten Daten wie Geschäftsgeheimnissen. Wählen Sie eine Lösung, die mehrere Optionen bietet, um Ihrem Unternehmen den Schutz der Informationen zu ermöglichen. Eine moderne ZTNA-Lösung sollte zum Beispiel die Möglichkeit bieten, den Datenverkehr zu überprüfen und DLP zum Schutz der Daten anzuwenden. Einige Unternehmen bevorzugen jedoch UEBA und Benutzer-Risikobewertungen, um ohne die Entschlüsselung des Datenverkehrs Echtzeit-Kontext zu erhalten und das Insiderrisiko zu minimieren.

05

Effektive Integration von Drittanbietern

Mit den richtigen Integrationen und dem richtigen Datenaustausch in Umgebungen mit mehreren Anbietern entfaltet ZTNA sein volles Potenzial. Der beste Datenaustausch bietet Vertrauensbewertungen für Benutzer und Geräte, die in der gesamten Umgebung normalisiert sind und adaptive Zugriffskontrollen, Benutzergruppeneinstellungen und automatisches Ticketing für Untersuchungen auslösen können.

Fazit

Denken Sie daran: Zero Trust bedeutet nicht, dass Sie niemandem vertrauen, denn Geschäfte sind nur möglich, wenn Sie den Zugang (das Vertrauen) erweitern. Der Schlüssel zur optimalen Nutzung der Zero-Trust-Prinzipien in Ihrem Unternehmen, ob speziell mit ZTNA oder auf andere Weise, ist der Einsatz von Technologie, um bessere, kontextbezogene Entscheidungen über das Vertrauen und den Zugriff für einen bestimmten Benutzer zu treffen und die Risiken kontinuierlich zu überwachen und zu minimieren.

Dieser Kontext basiert auf einer Reihe von Faktoren wie Benutzerrolle und -identität, Geräteidentität, Sicherheitsstatus, Anwendungstyp, -risiko und -instanz sowie der Sensibilität der Daten. Kontextbezogene Entscheidungen führen zu robusten Zugriffsrichtlinien, die risikooptimiert sind, einheitlich in der Cloud, im Web und in privaten Anwendungen angewandt werden können und dabei gleichzeitig geschäftliche Agilität und Benutzerproduktivität ermöglichen.

Für mehr Informationen

Netskope, ein weltweit führendes Unternehmen im Bereich Cybersicherheit, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen bei der Anwendung von Zero Trust-Prinzipien zum Schutz von Daten zu unterstützen. Die Netskope Intelligent Security Service Edge (SSE)-Plattform ist schnell und leicht zu bedienen; sie schützt Menschen und sichert Geräte sowie Daten überall.

Besuchen Sie netskope.com und erfahren Sie, wie Netskope Kunden dabei unterstützt, auf Ihrem Weg zur vollständigen SASE-Implementierung auf alles vorbereitet zu sein.