netskope

Whitepaper +

Ihre Netzwerksicherheit – vom Heute in die Zukunft

+ So stellen Sie auf cloudnative Netzwerke und Websicherheit um

Inhalts-verzeichnis

EINLEITUNG: DIE HERAUSFORDERUNG MIT VERALTETER NETZWERKSICHERHEIT

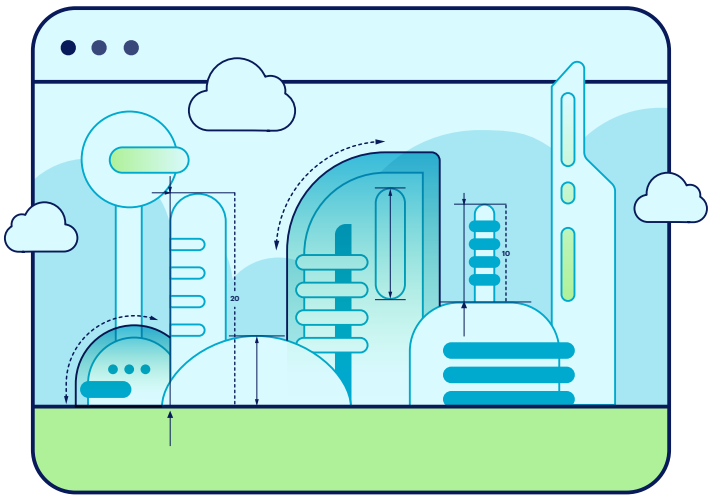
Netzwerkteams und die für Infrastruktur und Betriebsabläufe zuständige I&O-Gruppe sind gemeinsam für die Leistung und Sicherheit des Unternehmensnetzwerks verantwortlich. Ein wichtiger Aspekt dabei ist die Inline-Netzwerksicherheit, also die Überwachung und Abwehr von potenziellem Schad-Traffic in Echtzeit.

Viele Jahre lang drehten sich Diskussionen vor allem um die Vorteile von Firewalls im Vergleich zu Proxy-Gateways. Fachleute wählten zwar je nach der Situation im Unternehmen eine der beiden Alternativen aus. Andere Möglichkeiten hatten sie jedoch keine.

Doch in letzter Zeit wurde diese Auseinandersetzung von den Ereignissen überholt. Millionen von Unternehmen in aller Welt arbeiten jetzt hybrid und mit cloudbasierten Architekturen. Dem zugrunde liegt ein Prozess, der zwar durch die COVID-Pandemie beschleunigt wurde, seine Wurzeln aber in langfristigen technologischen Veränderungen hat.

In diesem Kontext wird klar, dass herkömmliche Netzwerksicherheitssysteme nicht mehr angemessen sind. Herkömmliche Firewalls und Proxy-Gateways tun sich oft schwer mit der Skalierbarkeit, Leistung und Transparenz in Cloud- und Remote-Arbeitsumgebungen. Das führt zu Ineffizienzen und Sicherheitslücken. Ältere Systeme sind im Zeitalter der Hybrid- und Remote-Arbeit einfach nicht mehr zweckdienlich.

Heutzutage benötigen Unternehmen dringend cloudnative Sicherheit, die beispielsweise durch Security Service Edge (SSE)-Lösungen bereitgestellt wird. Diese bieten Skalierbarkeit und Flexibilität und lassen sich mit den Zero-Trust-Prinzipien vereinbaren. Die technologischen Lösungen gibt es, doch die große Herausforderung für die verantwortlichen Teams ist die überlegte Umstellung von den älteren Systemen auf moderne Lösungen wie SSE. Und das, ohne die laufenden Investitionen zu erhöhen oder bei der Migration zu neuen Arbeitsmethoden Sicherheitslücken aufzutun.



CLOUDNATIVE NETZWERKSICHERHEITSLÖSUNGEN IM ÜBERBLICK

Cloudnative Netzwerksicherheitslösungen wie SSE sorgen in Unternehmen mit zunehmend verteilter Belegschaft für Skalierbarkeit, Leistung und Sicherheit.

Drei Elemente dieser modernen Netzwerkarchitekturen sind besonders wichtig.

Zero Trust Network Access (ZTNA): Setzt die Vorgabe durch, dass niemandem blindes Vertrauen gewährt wird und jeder nur Zugriff mit den geringsten Rechten erhält. Der Zugriff erfolgt nur auf ausgewählte Ressourcen, die die jeweiligen Einzelpersonen oder Personengruppen benötigen – sonst nichts.

Secure Web Gateway (SWG): Bietet granulare Kontroll- und Sicherheitsmechanismen und ermöglicht die Reaktion auf Bedrohungen und Datenrisiken aus der Cloud, denen persönliche Instanzen von verwalteten Anwendungen, Tausende Schatten-IT-Anwendungen und Cloud-Services ausgesetzt sind.

Firewall-as-a-Service (FWaaS): Bietet einheitliche Netzwerksicherheit für alle ausgehenden Ports und Protokolle und ermöglicht sicheren, direkten Internetzugriff über einen Agent (auf verwalteten Geräten) oder über GRE (Generic Routing Encapsulation) und IPSec (Internet Protocol Security) für Büros. Oft sind darin Komponenten wie DNS-Sicherheit und IPS (Intrusion Prevention Systems) integriert, um vom DNS ausgehende Angriffe zu erkennen und abzuwehren oder Bedrohungen in Echtzeit zu identifizieren.

Cloudnative Netzwerksicherheitslösungen sorgen in Unternehmen mit zunehmend verteilter Belegschaft für Skalierbarkeit, Leistung und Sicherheit.

REALE VORTEILE

Vier Gründe, warum moderne Sicherheitsinfrastrukturen geschäftlichen Mehrwert bringen

Durch die Umstellung auf den cloudnativen SSE können Unternehmen ihre Netzwerksicherheit stärken. Es gibt aber noch andere Vorteile. Bei der Modernisierung der Infrastruktur reduzieren SSE-Architekturen tatsächlich die Kosten, optimieren die Effizienz betrieblicher Abläufe und verbessern die Netzwerkleistung und damit auch das Benutzererlebnis. Dank all dieser Vorteile sind Unternehmen für den Erfolg im digitalen Zeitalter besser aufgestellt.

VORTEIL	WIRKUNG
Konsolidierung der Infrastruktur Durch die Konsolidierung der Netzwerksicherheitsinfrastruktur in einem modernen cloudbasierten System können Unternehmen veraltete Systeme und Lösungen außer Betrieb nehmen.	Sie profitieren dann von reduzierten Kosten für physische Server, Netzwerkgeräte und den damit verbundenen Wartungsaufwand. Forrester schätzt, dass der Wechsel von älteren Sicherheitssystemen zu SSE-Lösungen von Netskope in einem typischen Unternehmen über drei Jahre hinweg einen ROI von 109 % generiert. Die Kosten amortisieren sich bereits nach weniger als sechs Monaten, und die Konsolidierung der Infrastruktur allein bringt Einsparungen in Höhe von 5,4 Mio. US-Dollar.*
Vereinfachte Sicherheitsabläufe und Verwaltung Mit optimierten Workflows und automatisierten Prozessen können Teams sich auf strategische Initiativen statt auf alltägliche technische Probleme konzentrieren.	Die Vereinfachung der Prozesse spart Unternehmen Arbeitskosten für die Netzwerk- und weiter gefassten I&O-Teams sowie die gesamte Belegschaft. Schätzungen von Forrester zufolge helfen SSE-Lösungen von Netskope Sicherheitsteams dabei, 35.000 Arbeitsstunden im Wert von 1,5 Mio. US-Dollar einzusparen, die sie stattdessen gewinnbringender einsetzen können. Inzwischen konnten unternehmensweit fast 30.000 Stunden bei der Remote-Arbeit eingespart werden, weil die Benutzer nicht mehr ständig zeitaufwendige VPN-Prozesse befolgen müssen.*
Verbesserte Netzwerkleistung Eine moderne Cloud-Infrastruktur ist schneller und zuverlässiger und bietet geringere Ausfallzeiten, weniger Betriebsunterbrechungen und höhere Erkennungsraten.	Dank moderner und agiler Systeme können Unternehmen laut Forrester mit einer SSE-Lösung von Netskope das Arbeitsaufkommen im Helpdesk um 80 % reduzieren und die mittlere Lösungszeit (Mean Time to Resolve, MTTR) bei auftretenden Problemen um 60 % verkürzen. Die SSE-Lösung von Netskope gewährt mehr Einblicke in die Benutzerumgebung und verbessert dadurch letztlich den Netzwerkschutz und die Data Loss Prevention. Außerdem verringert Netskope die ungeplanten Ausfallzeiten um 15 %.
Stärkere Abwehrmechanismen Cloudnative Lösungen können Cyberbedrohungen effektiver verstehen und blockieren.	Laut Forrester reduzieren die modernen SSE-Lösungen von Netskope das Risiko schwerer Datenschutzverletzungen durch externe Angriffe um 80 %.

* Ausgegangen wird von einem Mischunternehmen mit einem Wert von mehreren Milliarden Dollar und 60.000 Mitarbeitern (Vollzeitäquivalent) weltweit, von denen die Hälfte Zugriff auf private Unternehmensanwendungen benötigt.

So unterstützen cloudnative Lösungen moderne Arbeitsgewohnheiten

Wenn sich das Verhalten ändert, muss auch Sicherheit neu gedacht werden.

In den Jahren vor der COVID-Pandemie waren im Durchschnitt weniger als 20 % der Beschäftigten eines Unternehmens remote tätig. Heute arbeiten in vielen Unternehmen zwischen 50 % und 100 % der Mitarbeiter an bestimmten Wochentagen nicht am Unternehmensstandort, denn Hybridarbeit ist inzwischen weitverbreitet.

Dadurch haben sich der Remote-, Web- und SaaS-Zugriff (und die damit verbundenen Sicherheitsfunktionen) grundlegend geändert. Unternehmen stützen sich zunehmend auf in der Cloud gehostete SWG- (Secure Web Gateway) und FWaaS-Komponenten (Firewall-as-a-Service), die auf SSE-Plattformen (Security Service Edge) bereitgestellt werden. Zwar sind Edge-Firewalls weiterhin nötig, um den externen Zugriff auf Daten (in Rechenzentren und in der Public Cloud, wo sich die Daten befinden) zu verwalten, doch in Zweigstellen (Ladengeschäfte, Filialen oder Regionalbüros) werden sie nicht mehr benötigt.

Zero Trust Network Access (ZTNA) ersetzt VPNs auch als Standardmethode zur Gewährung von sicherem Remote-Zugriff auf öffentlich zugängliche, anfällige Services und die anschließende Genehmigung lateraler Bewegungen. Das sicherere Inside-Out-Verbindungsmodell des ZTNA gewährt Benutzern ausschließlich direkten Zugriff auf die gewünschten Anwendungen oder Ressourcen, was die Reichweite böswilliger Akteure einschränkt.

Inhalte und Kontext sind jetzt für adaptive Zugriffskontrolle in Echtzeit entscheidend

Moderne Netzwerke, die auf ZTNA-Grundsätzen basieren, können bei der Analyse von Inhalten den Kontext besser berücksichtigen und in Echtzeit Sicherheitsentscheidungen treffen als ältere. Diese anpassungsfähigeren, intelligenten Netzwerke eignen sich gut für die neue Generation an Lösungen für geschäftliche Agilität, Remote-Arbeit und den Cloud-Zugriff.

Die Inline-Überprüfung von SaaS- (Software-as-a-Service) und IaaS-Inhalten (Infrastructure-as-a-Service) und -Kontext in Echtzeit wird zukünftiger Bestandteil von SSE-Lösungen für die Zugriffskontrolle sein. In einer früheren technologischen Ära haben Firewalls die Überprüfung des Netzwerk-Traffics perfektioniert. SWGs haben später dasselbe für Web-Traffic geleistet. Jetzt bringen SSE-Produkte durch Inhalt- und Kontextprüfungen mit Inline-CASB (Cloud Access Security Broker) beides zusammen.

Die adaptive Zugriffskontrolle, die sich nach dem Anwendungsrisiko, dem Risikoverhalten, dem Gerätestatus, den Aktivitäten, der Vertraulichkeit von Daten oder anderen Variablen richtet, wird zur Überprüfung von Inhalten und Kontext auf jede geschäftliche Transaktion angewendet.

Wenn ein Benutzer 100 Dateien mit vertraulichen Unternehmensdaten löschen möchte, kann die adaptive Zugriffskontrolle eine Step-up-Authentifizierung oder eine Begründung vom Benutzer verlangen. Wenn ein anderer Benutzer auf eine nicht verwaltete riskante Cloud-Speicher-Anwendung zugreifen möchte, um Dateien zu verschieben, kann die adaptive Zugriffskontrolle ihn warnen und ihm vom Unternehmen genehmigte Cloud-Speicheroptionen zur Verfügung stellen.

Dieses „Echtzeit-Coaching“ ähnelt in vielerlei Hinsicht der Satellitennavigation (GPS) beim Autofahren. Die Benutzer werden vor potenziellen Fehlentscheidungen gewarnt und auf sicherere Alternativen hingewiesen. Von diesen Orientierungshilfen profitieren Benutzer in modernen Unternehmen bei der Navigation in ihren Netzwerken.

Ein Framework für eine stufenweise SSE-Implementierung

Der Wechsel von herkömmlichen Netzwerksicherheitssystemen zu modernen SSE-Lösungen muss nicht auf einen Schlag erfolgen. Das sollte er auch nicht. Ein stufenweiser Ansatz, bei dem allmählich umgestellt und auf erfolgreiche Implementierungen aufgebaut wird, liefert bessere Ergebnisse, ohne Leistungseinbußen zu riskieren, und nutzt getätigte Investitionen optimal aus.

WICHTIGE SCHRITTE	BEST PRACTICE
Anfängliche Evaluierung und Planung Zunächst prüfen Sie die Sicherheitslage und ermitteln, welche Sicherheitslücken SSE schließen kann. Evaluieren Sie Ihre Netzwerkarchitektur, die vorhandenen Sicherheitslösungen und die konkreten geschäftlichen Anforderungen, um herauszufinden, welche SSE-Lösung am besten für Sie ist.	Entwickeln Sie eine klare Strategie für die SSE-Bereitstellung. Unter anderem sollten Sie die Ziele, die erwarteten Ergebnisse und die Leistungskennzahlen festlegen.
Auswahl des richtigen SSE-Anbieters Evaluieren Sie die Eignung der verschiedenen SSE-Anbieter für Ihre konkreten Anforderungen und Anwendungsfälle. Berücksichtigen Sie Faktoren wie den Umfang der Sicherheitsservices, die zugrundeliegende Architektur, Integrationsmöglichkeiten in bestehende Systeme, Kundensupport und das Preis-Leistungs-Verhältnis.	Führen Sie in Ihrer Umgebung einen Pilotversuch mit den Anbietern in der engeren Auswahl durch, um ihre Eignung für Ihre konkreten Sicherheitsvorgaben, Traffic-Muster und Sichtbarkeitsanforderungen zu prüfen.
Stufenweise Bereitstellung Konfigurieren Sie die SSE-Lösung mithilfe des gewählten Anbieters so, dass sie Ihren individuellen Sicherheitsrichtlinien und Compliance-Anforderungen entspricht. Bei dieser Anpassung können Sie zum Beispiel Sicherheitsregeln einrichten, DLP-Einstellungen (Data Loss Prevention) konfigurieren und Zugriffskontrollen festlegen.	Integrieren Sie die SSE-Lösung mit der vorhandenen IT-Infrastruktur, etwa mit den Identitätsmanagementsystemen, der Netzwerkinfrastruktur und anderen Sicherheitstools. Die ordnungsgemäße Integration ist entscheidend, dass der Betrieb reibungslos läuft und Sie die SSE-Lösung optimal nutzen können. Evaluieren Sie Anbieter daher anhand ihres Partnerökosystems und der Integrationen.
Schwerpunkt Benutzererlebnis Führen Sie vor jeder Bereitstellungsphase umfangreiche Schulungen durch. Geben Sie Veränderungen rechtzeitig bekannt und holen Sie Feedback von den Benutzern ein, um Schwierigkeiten schnell entgegenzuwirken.	Verfolgen Sie mithilfe von Analysen die Effektivität der Sicherheitsmaßnahmen und die Akzeptanz bei den Benutzern. Richten Sie Prüfpfade ein, um die Sicherheitsverbesserungen im Zeitverlauf nachzuweisen.

Die Grundlagen für langfristigen Erfolg

Warum Zero-Trust-Modelle wichtig sind

Da der bisherige Netzwerkperimeter mit dem Aufkommen der Remote-Arbeit und Cloud-Services überholt ist, spielt der Zero-Trust-Ansatz heute eine wichtige Rolle für die effektive Netzwerksicherheit. Mit Zero-Trust-Prinzipien sollen der implizite Zugriff entfernt, der Zugriff mit den geringsten Berechtigungen verfeinert und eine kontinuierliche Überwachung ermöglicht werden. Auf diese Weise können die zunehmenden raffinierten Cyberbedrohungen bekämpft und die Transparenz und Kontrolle für Sicherheitsteams verbessert werden.

Ein durchschnittliches Unternehmen hat 2024 mehr als dreimal so viele GenAI-Apps wie im Vorjahr genutzt – und hatte beinahe dreimal so viele Benutzer, die diese Apps aktiv eingesetzt haben.

Der Zero-Trust-Ansatz wird aber oft missverstanden. Viele Erklärungen beschränken sich auf den sicheren Zugriff und berücksichtigen nicht, dass Daten auch durch all die anderen Zero-Trust-Komponenten (Benutzer, Anwendungen, Geräte und Netzwerke) fließen.

SSE-Lösungen kombinieren CASB- und SWG-Funktionen zu einem zentralen Inline-Proxy mit FWaaS und ZTNA, um die bisherigen Rollen von NGFWs und VPNs neu zu definieren und das Zero-Trust-Modell zu unterstützen. Dadurch wird Ihre Infrastruktur widerstandsfähiger und sicherer. Wichtig ist, dass SSE über die nötige Skalierbarkeit und Leistung für alle Benutzer, Geräte oder Standorte verfügt, um ein großartiges Benutzererlebnis bereitzustellen – ganz ohne Kompromisse hinsichtlich Leistung und Sicherheit.

Die Weitergabe von urheberrechtlich geschütztem Quellcode an GenAI-Apps ist für 46 % aller Verstöße gegen Datenrichtlinien verantwortlich.

Mit einem Zero-Trust-Framework und einer modernen SSE-Lösung haben Unternehmen eine solide Grundlage für nachhaltige Sicherheit, die mit dem Unternehmen mitwächst und sich wandelt, dabei aber einheitliche Sicherheitsmechanismen für alle Umgebungen und Anwendungsfälle aufrechterhält.

Die Wirkung der KI

Künstliche Intelligenz (KI) und maschinelles Lernen (ML) werden schon seit Jahren im Hintergrund eingesetzt, etwa für Bedrohungsabwehr-Engines, zur Datenklassifizierung, für dynamisches URL Rating und zur Planung von IT-Abläufen. Heute werden KI- und ML-basierte Sicherheitseinrichtungen inline eingesetzt, um unbekannte Zero-Day-Bedrohungen und vertrauliche Daten in Dokumenten und Bildern in Echtzeit zu erkennen.

35 % aller derartigen Verstöße gehen auf Daten zurück, die Branchenvorschriften oder Compliance-Anforderungen unterliegen, bei 15 % sind es geistige Eigentumsrechte.

Der KI-Boom an sich ermöglicht sowohl guten als auch böswilligen Akteuren die schnelle Entwicklung von neuem Code, die Erstellung von Inhalten und schnelles Lernen. Er ist daher sowohl ein Fluch als auch ein Segen, weil vertrauliche Daten offengelegt werden können. Quellcode ist unter anderem die beliebteste Art von Inhalt, der in KI-Anwendungen wie ChatGPT eingegeben wird.

Veraltete Sicherheitseinrichtungen sind nicht in der Lage, unternehmenseigene KI-Instanzen zuzulassen oder öffentliche und private Instanzen von Benutzern zu kontrollieren. Sie können auch keine Inhalte wie Quellcode identifizieren, mit denen KI-Anwendungen trainiert wurden.

KI/ML-basierte Inline-Sicherheitseinrichtungen erkennen dagegen mittlerweile schädliche ausführbare Dateien und Phishing-Angriffe und klassifizieren Dutzende Dokumente und Bilder sowie Quellcode. Da KI-Anwendungen und -Anwendungsfälle in Unternehmen jeder Art schnell Verbreitung finden, muss jede zukunftsgerichtete Strategie für Netzwerksicherheit solchen Risiken gewachsen sein.

FAZIT: SICHERHEIT MUSS SICH WEITERENTWICKELN

Die Technologien in Unternehmen und Verhaltensweisen von Menschen ändern sich ständig. Wir haben das in den vergangenen Jahren am eigenen Leib erlebt: Der Wechsel in die Cloud, die Explosion der Remote- und Hybridarbeit und das Aufkommen der KI haben unseren Alltag transformiert.

Netzwerk- und I&O-Fachleute haben jetzt die wichtige Aufgabe, die Architekturen im Einklang mit den Änderungen in ihrem Umfeld zu modernisieren. Dieser Prozess hat zwei Seiten.

Zunächst einmal müssen die Teams ihre älteren Systeme genau analysieren. Es gibt einen anhaltenden Trend hin zu Inline-Prüfungen von SaaS und IaaS, zusätzlichem Inline-Schutz durch KI/ML und adaptivem Zugriff mit Echtzeit-Coaching für die Benutzer.
In diesem Kontext kann sich die Erneuerung von NGFW-, SWG- und VPN- als kostspielig erweisen.

Unternehmen sollten zudem eine Migration zu modernen SSE-Lösungen planen. Wenn diese in verschiedenen Stufen erfolgt, ist sie besser kontrollierbar und effektiver. Das verhindert, dass die bestehenden Systeme von heute auf morgen abgeschaltet werden. Die Netzwerkteams können dann Vertrauen in die neuen Arbeitsmethoden aufbauen.

In dieser dynamischen IT-Umgebung wird der Erfolg eines Unternehmens maßgeblich davon abhängen, wie schnell es sich an diese Veränderungen anpasst und sie sich zunutze macht. Netzwerk- und I&O-Teams mag der Wechsel zunächst kompliziert erscheinen. Er lässt sich aber vereinfachen und verspricht letztlich beträchtliche Leistungsverbesserungen, Produktivitätssteigerungen und Kosteneinsparungen.

Sie möchten mehr erfahren?

Demo anfordern

Netskope ist ein führender Anbieter von modernen Sicherheits- und Networking-Lösungen und gibt Sicherheit- und Netzwerkteams, was sie brauchen: optimierten Zugriff und kontextbasierte, ortsunabhängige Sicherheit in Echtzeit für Menschen, Geräte und Daten. Tausende Kunden (darunter mehr als 30 Unternehmen der Fortune 100) vertrauen der Netskope One-Plattform, ihrer Zero Trust Engine und ihrem leistungsstarken NewEdge-Netzwerk, wenn es um die Verringerung von Risiken geht. Sie erhalten vollen Einblick in die Aktivitäten sämtlicher Cloud-, KI-, SaaS-, Web- und privaten Anwendungen und können ihre Sicherheitslage und Leistung ohne Kompromisse verbessern.