netskope

E-Book

6 Zero-Trust-Anwendungsfälle für Netskope One, eine einheitliche SASE-Plattform

6 Zero-Trust-Anwendungsfälle für Netskope One, die einheitliche SASE-Plattform

Einleitung

Viele Netzwerk- und Sicherheitsteams haben heute die Aufgabe, eine hybride Arbeitsumgebung zu unterstützen, in der größtenteils veraltete Abwehrsysteme eingesetzt werden. Sie befinden sich in einer wenig beneidenswerten Lage, denn wenn Ressourcen in rasantem Tempo in die Cloud verlegt werden und Mitarbeiter ins Homeoffice abwandern – wie seit dem Ausbruch der COVID-19-Pandemie im Jahr 2020 zu beobachten war – verlieren die lokalen Perimeter-Sicherheitslösungen und die hardwarezentrierte Netzwerksegmentierung ihre Wirksamkeit.

Ein besserer Ansatz zur Sicherung der Assets eines modernen Unternehmens lautet Zero Trust. Dieser Ansatz basiert auf einer Reihe verschiedener Prinzipien. Beim Zero-Trust-Sicherheitsmodell müssen Benutzer und Geräte für jede neue Sitzung authentifiziert werden und erhalten nur Zugriff auf die Ressourcen, die sie auch benötigen. Dieser Ansatz des Zugriffs mit der minimalen Berechtigung wird durch eine umfassende Sicherheitsüberwachung unterstützt, bei der die Aktivitäten und das Verhalten von Benutzern und Ressourcen sowie von Trends *kontinuierlich* beobachtet und analysiert werden.

Wesentliche Elemente einer Zero-Trust-Strategie

Zero-Trust-Sicherheit ist kein Produkt, das Unternehmen kaufen können, sondern eine wichtige Unternehmensstrategie, die auf die Kontrollen für die heutigen Arbeitsumgebungen zugeschnitten ist. Das Zero-Trust-Sicherheitsmodell wird unter anderem durch die folgenden interoperabel arbeitende Technologien unterstützt:

- ***Benutzer- und Identitätsverwaltung:*** Identitäts- und Zugriffsverwaltung (IAM) oder die Verwaltung von Zugriffsrechten, rollenbasierte Zugriffskontrollen und die Analyse des Benutzerverhaltens (UEBA)
- ***Geräteverwaltung:*** Prüfung der Geräteintegrität und Vertrauensbewertungen
- ***Anwendungs- und Workload-Management:*** Secure Web Gateways (SWGs) und Security Service Edge (SSE)-Lösungen mit CASB-Funktionalität (Cloud Access Security Broker)
- ***Netzwerksicherheitseinrichtungen:*** Firewalls der nächsten Generation (NGFWs), sichere E-Mail-Gateways und SSE-Lösungen mit SWG-, CASB- und ZTNA-Funktionalität (Zero Trust Network Access)

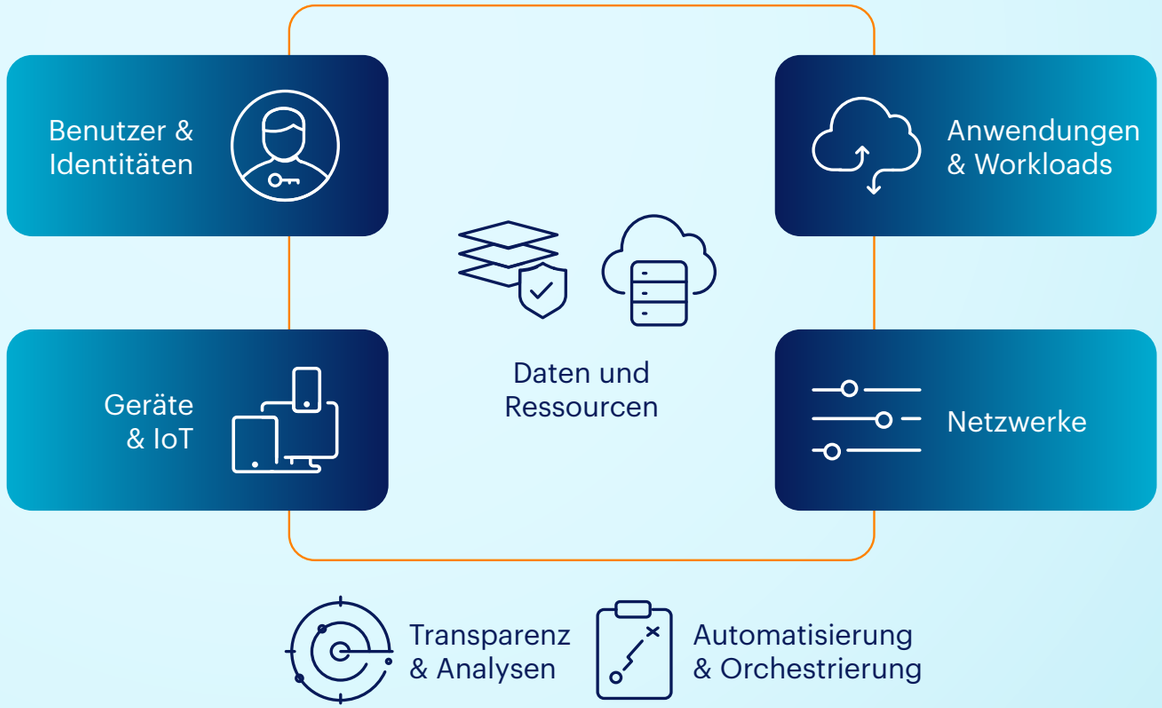


Abbildung 1: Zero-Trust-Sicherheitsmodell

Die ersten – oder nächsten – Schritte mit Zero Trust

Ein effektives Zero-Trust-Sicherheitsmodell bietet ein großartiges Benutzererlebnis, macht Sicherheitsmaßnahmen transparent und sorgt für wenig oder keine Reibungsverluste bei den Workloads in Ihrem Unternehmen. Das bedeutet, dass sich Unternehmen zunächst ihre Mitarbeiter und Prozesse genauer ansehen müssen. Ein Unternehmen, das auf ein Zero-Trust-Modell umstellt, sollte damit beginnen, seine geschäftlichen Anwendungsfälle und Prozesse genau abzubilden.

Was die Technologie angeht, konzentrieren sich viele Unternehmen darauf, den Zugriff von Remote-Mitarbeitern auf Ressourcen in der Cloud und im Rechenzentrum zu sichern. Der bisherige Ansatz, Hardware-Sicherheitsgeräte in den Wohnungen der Mitarbeiter zu platzieren, ist teuer und schwer zu skalieren, während das Backhauling des Datenverkehrs dieser Mitarbeiter zu den Firewalls des Unternehmens zu Engpässen führt. Die einfachere Lösung besteht darin, einen Software-Client auf den Geräten der Mitarbeiter zu installieren, der eine Verbindung zu den Cloud-Edge-Sicherheitsdiensten herstellt – also eine SSE-Cloud-Sicherheitsplattform, die CASB, SWG und ZTNA integriert.

Ein weiterer beliebter Ausgangspunkt für die Umstellung auf die Zero-Trust-Technologie ist die Priorisierung und Sicherung des Datenverkehrs von Geschäftsanwendungen. SaaS-basierte (Software-as-a-Service) Anwendungen, wie Microsoft 365 und Salesforce, erfordern direkte Internetverbindungen für Remote-Mitarbeiter und alle Büros. Die Einführung einer SSE-Lösung ermöglicht die Inspektion des Web-, SaaS- und IaaS-Benutzerdatenverkehrs (Infrastructure-as-a-Service) für alle Benutzer, alle Geräte und alle Standorte und bietet auf diese Weise Transparenz und Kontrolle über das gesamte digitale Ökosystem des Unternehmens.

Ein effektives Zero-Trust-Sicherheitsmodell bietet ein hervorragendes Benutzererlebnis. Das bedeutet, dass ein Unternehmen, das auf ein Zero-Trust-Modell umstellt, damit beginnen sollte, seine geschäftlichen Anwendungsfälle und Prozesse genau abzubilden.

So unterstützt Netskope SSE die Umstellung auf Zero Trust

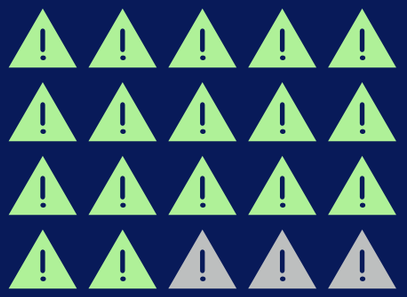
Anstelle der binären Kontrollen der traditionellen Perimeter-Sicherheit, die für Ports, Protokolle, Domains, URLs und Anwendungen nur die beiden Optionen „Erlauben“ oder „Blockieren“ zulassen, bewertet Netskope Intelligent SSE die Transaktionsrisiken bei jeder Sitzung. Die Anwendung hat die Eigenschaft, dass sie keinem Netzwerk, Gerät oder Benutzer von vornherein vertraut.

Das Herzstück der Netskope One-Plattform und der Intelligent SSE-Komponente ist die Zero Trust Engine (ZTE). Die Engine-Technologie, die Netskope Intelligent SSE zugrunde liegt, unterstützt neben Risikoprofilen von Anwendungen und Benutzern auch Prüfungen des Gerätesicherheitsstatus und kann diese Risikoprofilemit den Sicherheitslösungen anderer Anbieter austauschen. Die Zero Trust Engine lässt sich mit führenden IAM-Lösungen für Identitätsdienste und der Multi-Faktor-Authentifizierung (MFA) integrieren und kann je nach Transaktionsrisiko der Sitzung eine Step-up-Authentifizierung anfordern.

Außerdem nutzt die umfassende Sicherheitsüberwachung innerhalb von Netskope Intelligent SSE Geschäftsanalysen und Datenvisualisierungen, um die Verfeinerung der Zero-Trust-Richtlinien eines Unternehmens nach dem Prinzip des Zugriffs mit der minimalen Berechtigung zu unterstützen. In Dashboards und Diagrammen werden auffällige Benutzerrisiken, Datenverschiebungen zwischen Anwendungsinstanzen, Anwendungsrisikoprofile und Trends sowie verdächtiges Verhalten von Benutzern aufgezeigt. Der gleiche umfangreiche Kontext, der adaptive Zugriffskontrollen nach dem Prinzip der minimalen Berechtigung ermöglicht, ist über einen Zeitraum von 3, 6 oder 13 Monaten verfügbar.

Netskope Intelligent SSE und die Zero Trust Engine bieten erhebliche Vorteile für jedes Unternehmen mit Workloads in der Cloud. Es folgen Beschreibungen der sechs wichtigsten Anwendungsfälle, die den Nutzen und die Vorteile der Anwendungen aufzeigen.

Netskope Intelligent SSE trifft Zugriffsentscheidungen mithilfe von adaptiven Kontrollen, die auf einem umfangreichen Kontext und Benutzereingaben basieren und durch mehr als 100 einzigartige detaillierte Aktivitäten für Tausende von Anwendungen erweitert werden. Wenn Netskope Intelligent SSE beispielsweise über ein Dutzend Aktivitätskontrollen für eine bestimmte Anwendung verfügt und Risiken auf der Grundlage des Benutzer- und Sitzungskontexts erkennt, kann es das Verhalten des Benutzers innerhalb der Anwendung entsprechend einschränken, anstatt einfach den Zugriff auf die Software ganz zu sperren.



85 %

Risikominderung durch die Nutzung von Security Service Edge bei gleichzeitiger Steigerung der Unternehmensagilität

Quelle: Enterprise Strategy Group

Zero-Trust-Anwendungsfall 1

Die SaaS-Transparenz erhöhen

Untersuchungen von Netskope haben ergeben, dass die Mitarbeiter eines durchschnittlichen mittelgroßen Unternehmens mehr als 800 Anwendungen nutzen, während Mitarbeiter von größeren Unternehmen 2.400 oder mehr Anwendungen nutzen können. Viele davon sind cloudbasierte SaaS-Anwendungen , von denen 97 % werden von Geschäftseinheiten oder einzelnen Benutzern ohne die Aufsicht des IT-Teams eingeführt werden.

Die Vorstellung, dass Mitarbeiter Unternehmensdaten in nicht vom Unternehmen verwaltete SaaS-Anwendungen verschieben, ist beunruhigend. Aus diesem Grund bietet Netskope Intelligent SSE eine CASB-Inline-Inspektion für Tausende von Anwendungen. Genauso wie Firewalls Pakete über Ports und Protokolle hinweg analysieren, decodieren SSE-Lösungen mit CASB-Funktionen Anwendungen inline, um den Kontext und Inhalt jedes Vorgangs nachzuvollziehen. Dies ermöglicht adaptive Zugriffskontrollrichtlinien, die auf den Zero-Trust-Prinzipien beruhen.

Über den Cloud Confidence Index referenziert Netskope Intelligent SSE auch die Risikoprofile von mehr als 75.000 Anwendungen heran, um eine Risikobewertung für alle im Unternehmen genutzten Cloud-Anwendungen zu erstellen.

Dank dieser Funktionen können Sicherheitsteams die Nutzung der Cloud-Anwendungen durch die Mitarbeiter viel besser verstehen. Dabei ist es vollkommen unerheblich, ob die Anwendungen vom Unternehmen oder privat bezogen und ob sie verwaltet oder nicht verwaltet sind. Das Sicherheitsteam kann riskantes Verhalten von Mitarbeitern in der Cloud besser verstehen und die Gefährdung der Unternehmensressourcen durch risikoreiche SaaS-Lösungen begrenzen.

97 % der in Unternehmen genutzten Anwendungen werden nicht von der IT verwaltet, sondern eigenständig von Geschäftseinheiten oder Endbenutzern eingeführt.

800 Anwendungen werden in einem durchschnittlichen mittelgroßen Unternehmen genutzt

mehr als 2.400 Anwendungen werden in größeren Unternehmen genutzt

Zero-Trust-Anwendungsfall 2

Die Cloud-Collaboration schützen

In Unternehmen, die verstärkt auf Remote-Arbeit angewiesen sind, sind Cloud-Collaboration-Plattformen geschäftskritisch. Mitarbeiter nutzen sie, um Informationen auszutauschen, sich mit Kunden und Lieferanten zu treffen und all das zu besprechen, was früher in Konferenzräumen und in der Kaffeeküche Thema war.

Cloud-Collaboration-Lösungen stellen ein besonderes Sicherheitsrisiko dar, weil sie zwar häufig und für zahlreiche Geschäftsaktivitäten genutzt, aber in der Regel nicht von der IT-Abteilung des Unternehmens verwaltet werden. Das Sicherheitspersonal muss kontrollieren können, wie die Mitarbeiter diese Lösungen nutzen und welche Informationen über sie ausgetauscht werden.

Die adaptiven Zugriffskontrollen in Netskope Intelligent SSE sind eine hervorragende Lösung für diese Herausforderung. Die Netskope-Plattform enthält Aktivitätskontrollen für gängige Cloud-Collaboration-Lösungen.

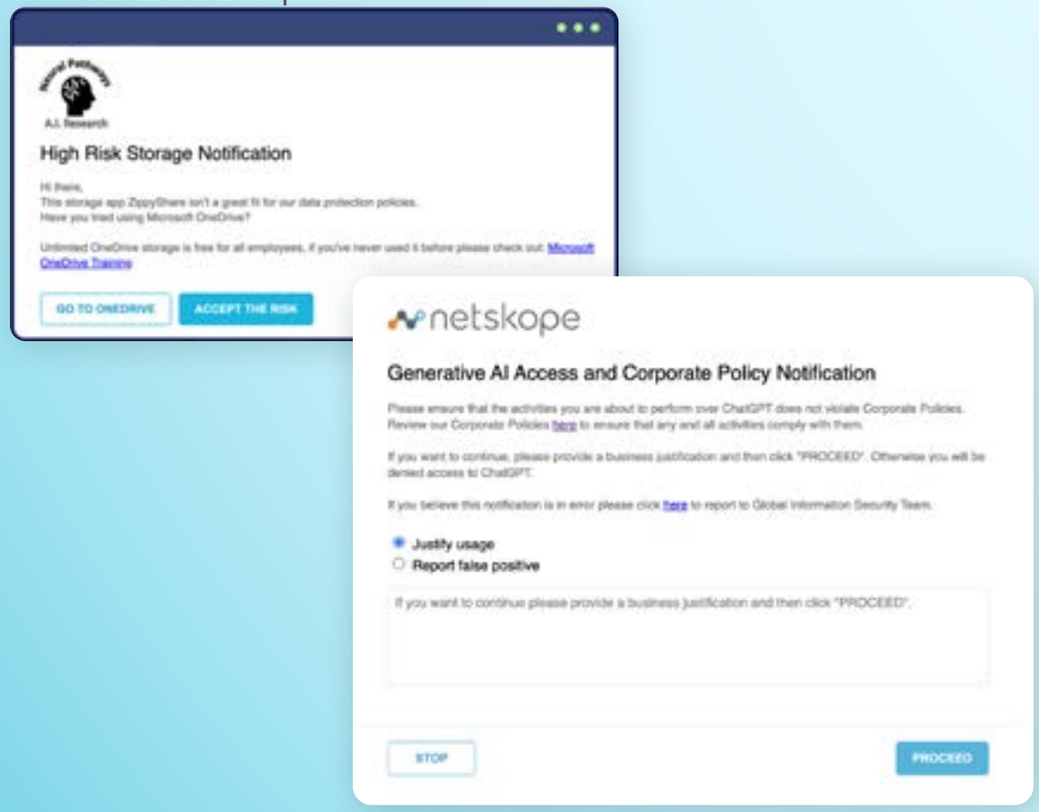
Für Slack sind in Netskope Intelligent SSE zum Beispiel 15 Aktivitätskontrollen beschrieben, für Zoom 10. Das bedeutet, dass Sicherheitsteams Netskope Intelligent SSE verwenden können, um das Verhalten von Benutzern im Zusammenhang mit diesen Aktivitäten einzuschränken, ohne den Benutzern den Zugang zu Slack oder Zoom komplett zu verwehren. So können Benutzer zwar beliebig oft Zoom-Meetings erstellen und an ihnen teilnehmen, aber der Austausch von Bildern und Daten ist begrenzt, eingeschränkt oder wird anderweitig kontrolliert.

Sicherheitsteams galten früher als strikte Neinsager. Da sie mit Netskope Intelligent SSE jetzt aber die Fähigkeit haben, die Handlungen einzelner Mitarbeiter innerhalb einer nicht verwalteten Anwendung zu kontrollieren, können sie sich stattdessen fragen: „Wie können wir diese Funktionen verfügbar machen – und zwar sicher?“

Zero-Trust-Anwendungsfall 3

Aktives Benutzer-Coaching

Wenn Benutzer versuchen, eine riskoreiche Aktion durchzuführen, kann Netskope Intelligent SSE diese entweder direkt blockieren oder eine Warnung herausgeben. Versucht ein Benutzer beispielsweise, eine risikoreiche Anwendung zu öffnen oder sensible Daten an eine private Instanz einer vom Unternehmen genehmigten Anwendung zu übertragen, kann Netskope Intelligent SSE den Benutzer in Echtzeit anweisen, eine sicherere Option zu wählen. Zum Beispiel:



Alternativ kann Netskope Intelligent SSE den Benutzer auffordern, die risikoreichere Wahl zu begründen. Oder die Anwendung kann so eingestellt werden, dass der Benutzer bei jedem von ihm gestarteten risikoreichen Vorgang gewarnt wird und die Möglichkeit erhält, ihn abzubrechen. Nach dem Hinweis, dass die beabsichtigte Datenaktivität riskant ist, brechen mehr als 95 % der Benutzer den Vorgang ab. Bei den restlichen 5 % kann das Sicherheitsteam die Begründungen sammeln und diese ggf. zur detaillierten Ausarbeitung der Sicherheitsrichtlinien für die entsprechenden Anwendungsfälle verwenden.

Netskope Intelligent SSE berücksichtigt einen umfangreichen Kontext und führt Transaktionsrisikobewertungen durch. Dadurch werden Benutzer dabei unterstützt, die richtigen Entscheidungen zu treffen. Netskope Intelligent SSE informiert die Benutzer, anstatt sie daran zu hindern, auf die von ihnen benötigten Anwendungen zuzugreifen. Dieser behutsamere Ansatz hilft dabei, Mitarbeiter zu verantwortungsvollen digitalen Bürgern zu erziehen, die alles daran setzen, die Sicherheitsrichtlinien des Unternehmens einzuhalten.

„Menschen sind nicht das schwächste Glied in unserer Sicherheitsstruktur, sie sind unsere letzte Verteidigungslinie. Es ist also wichtig, dass wir diese Tatsache anerkennen und Mitarbeiter schulen.“

— Dane Blackmore, Netskope

Zero-Trust-Anwendungsfall 4

Sicherer Zugriff auf interne Anwendungen

Obwohl Unternehmensdaten zunehmend in SaaS-Anwendungen verlagert werden, arbeiten viele Unternehmen weiterhin mit intern entwickelten Anwendungen. Auch diese sollten möglichst mit Zero-Trust-Sicherheit geschützt werden, sodass die Benutzer über die ZTNA-Software des Unternehmens auf sie zugreifen. Dieser Ansatz stellt sicher, dass die Benutzer nur auf das zugreifen, was sie benötigen, und sich nicht unnötigerweise lateral durch das Unternehmensnetzwerk bewegen.

Ein weiterer Vorteil des ZTNA-Ansatzes bei der Anwendungsentwicklung ist, dass Sicherheitsteams in die Entwicklungs- und Betriebsprozesse (DevOps) eingebunden werden können. Allzu oft ignorieren Softwareentwicklungsteams das Thema Sicherheit, bis es zu spät ist, und erwarten dann, dass das Sicherheitsteam der Anwendung im Nachhinein Kontrollmechanismen hinzufügt. Stattdessen sollten die Sicherheitsteams von Anfang bis Ende in DevOps einbezogen werden.

Das Zero-Trust-Sicherheitsmodell macht es möglich. Der Zero-Trust-Ansatz macht die Sicherheit zu einem „Business Enabler“ und ermutigt die Entwicklungsteams dazu, das Sicherheitspersonal früher in den Entwicklungsprozess einzubinden und Sicherheitsprüfungen gleich im Rahmen der Entwicklung durchzuführen. In einigen Fällen führt diese engere Zusammenarbeit zwischen Teams zu einer integrierten DevSecOps-Gruppe.

Eine solche Partnerschaft zwischen den verschiedenen Teams im Unternehmen bildet eine Grundlage für den Erfolg des gesamten Unternehmens. Durch die Kooperation können Schwachstellen in intern entwickelter Software reduziert, Probleme in der Software-Lieferkette beseitigt, und Sicherheitsmängel in Webanwendungen minimiert werden.

Zero-Trust-Anwendungsfall 5

Nicht genehmigte Datenverschiebungen

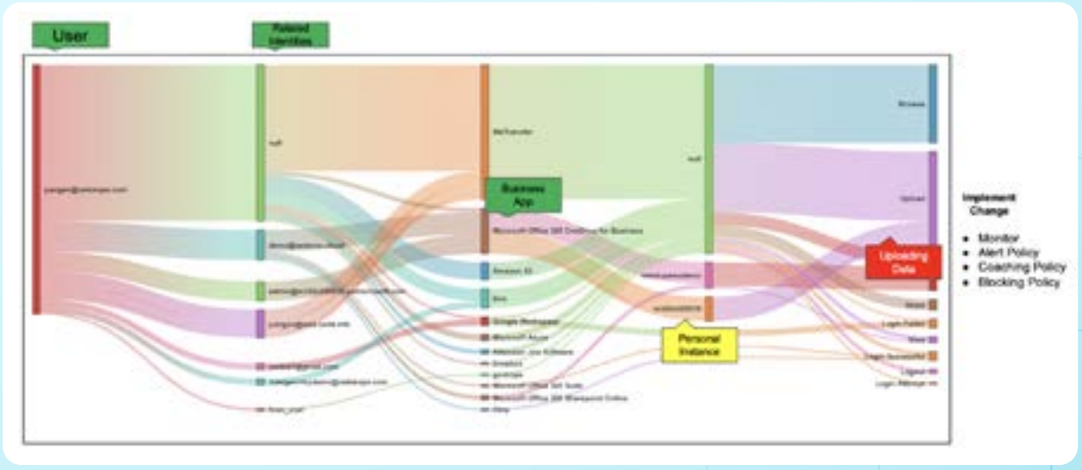
Datensicherheit war schon immer ein wesentlicher Bestandteil des Risikomanagements von Unternehmen. Heutzutage können die Netzwerkgrenzen eines Unternehmens jedoch nicht verhindern, dass Daten nach außen gelangen, sodass traditionelle Ansätze zur Gewährleistung der Datensicherheit ins Leere laufen.

Im Gegensatz dazu hilft Netskope Intelligent SSE Sicherheitsexperten dabei, nachzuvollziehen, wie ihr Unternehmen Daten über SaaS-, IaaS- und intern entwickelte Anwendungen sammelt, überträgt, speichert und weitergibt. Sie können Fragen beantworten wie etwa: Wohin fließen unsere Daten und in welche Anwendungen? Welche Risikoprofile haben Benutzer, die versuchen, Daten zu verschieben? Welche Geräte verwenden sie und in welchen Netzwerken? Wenn ein Mitarbeiter aus dem Unternehmen ausscheidet, kann das Sicherheitsteam die Datenverschiebungen und die Anwendungsnutzung dieser Person in den letzten Monaten bewerten. Und nach einer Aktualisierung von SaaS-Anwendungen kann das Sicherheitsteam feststellen, ob diese Änderungen zu neuen Datenpfaden oder Vorgängen geführt haben.

Netskope Intelligent SSE bietet Instanzerkennung für mehr als 450 Anwendungen, sodass das Sicherheitsteam erkennen kann, ob sich die Daten in der Unternehmensinstanz einer Anwendung oder in einer privaten Instanz derselben Anwendung befinden.

Dadurch erhält Netskope Intelligent SSE Einblick in alle Versuche von Benutzern, Daten zu exfiltrieren. Während herkömmliche Kontrollsysteme es Benutzern beispielsweise erlauben, sensible Daten aus dem Google Workspace des Unternehmens in ihre eigenen privaten Workspace-Umgebungen zu verschieben, erkennt Netskope Intelligent SSE den Unterschied und kann Echtzeit-Coaching anbieten oder einfach die Exfiltration verhindern.

Bei Anwendungen, die keine Instanzerkennung unterstützen, kann die Identitätszuordnung in Netskope Intelligent SSE dienstliche und private Anmeldungen zuordnen, um zu unterscheiden, in welchem Anwendungs-Tenant ein Benutzer gerade arbeitet.



Netskope Advanced Analytics macht die unerkannte Datenexfiltration auf privaten Speicher sichtbar

Zero-Trust-Anwendungsfall 6

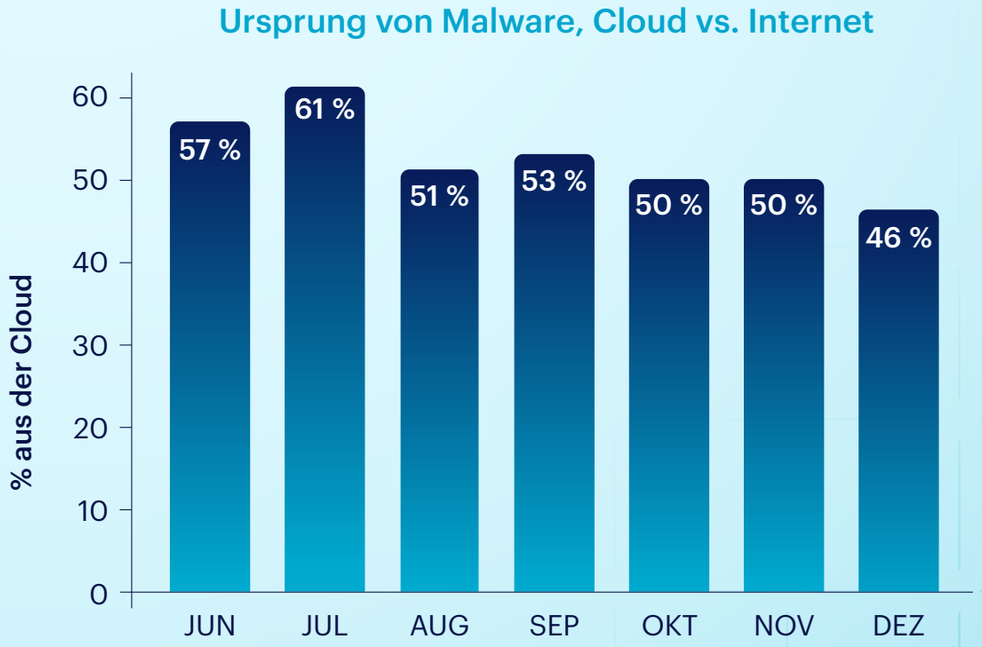
Cloud-Fehlkonfigurationen

Die überwiegende Mehrheit der Sicherheitsverletzungen in der Cloud ist auf Konfigurationsfehler zurückzuführen. Die korrekte Implementierung von CSPM- (Cloud Security Posture Management) und SSPM-Lösungen (SaaS Security Posture Management) ist der beste Weg für ein Unternehmen, um sicherzustellen, dass seine Mitarbeiter die Cloud sicher nutzen.

Diese Systeme ermöglichen es Unternehmen, den Sicherheitsstatus der Workloads zu verstehen, die sie in einer Public-IaaS-Cloud bzw. in SaaS-Anwendungen bereitgestellt haben. Sie bewerten die Konfigurationen, die Konformität und den allgemeinen Sicherheitsstatus der Cloud-Plattformen oder -Anwendungen eines Unternehmens und vergleichen diese Ergebnisse dann mit den Empfehlungen für Sicherheitskontrollen von externen Experten wie dem National Institute of Standards and Technology (NIST) und der Cloud Security Alliance (CSA). Da CSPM- und SSPM-Systeme Cloud-Konfigurationen mithilfe von APIs untersuchen, sind keine Produktionsunterbrechungen oder langwierigen Integrationsprozesse erforderlich.

Netskope Intelligent SSE enthält Hunderte von sofort einsatzbereiten Regeln für beliebte SaaS-Anwendungen, darunter Salesforce, Microsoft Exchange und SharePoint, sowie für IaaS-Plattformen wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform. Bei all diesen Lösungen kann Netskope Intelligent SSE die Sicherheitskonfigurationen kontinuierlich überprüfen und bei auftretenden Problemen Schritte zu deren Behebung aufzeigen. So wird die Wahrscheinlichkeit verringert, dass eine Fehlkonfiguration in einem Cloud-System eine ernsthafte Sicherheitskrise im Unternehmen auslöst.

46 % **der Malware-Downloads stammen von beliebten Cloud-Apps.***



** Quelle: Cloud- und Bedrohungsbericht 2024 von Netskope*

Die treibende Kraft hinter den Kulissen: die Zero Trust Engine von Netskope

Wie in der Einleitung erwähnt, werden die beschriebenen Sicherheitsoptionen alle durch die Netskope Zero Trust Engine ermöglicht, die das Herzstück von Netskope Intelligent SSE bildet. Die Zero Trust Engine ist die Technologie, die die unzähligen Variablen von Geschäftsvorgängen in Echtzeit bewertet, Benutzer in Echtzeit coacht, Begründungen sammelt und Ereignisse mit umfangreichen Details zum Zweck einer kontinuierlichen Überwachung protokolliert. Abbildung 2 zeigt, wie die Zero Trust Engine die sechs beschriebenen Anwendungsfälle unterstützt.

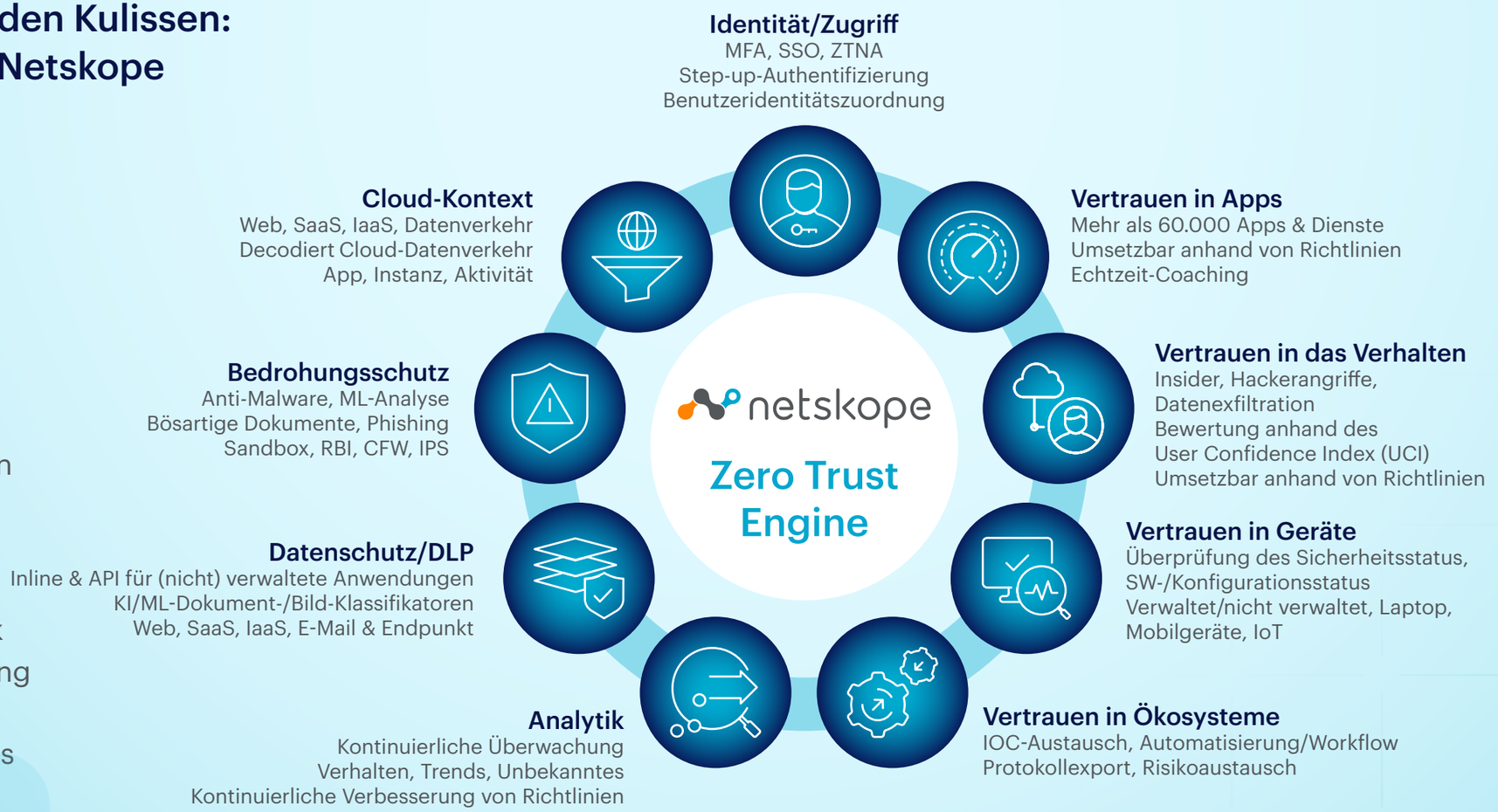


Abbildung 2: Die Netskope Zero Trust Engine bietet risikobasierten Kontext zur Unterstützung von Zero-Trust-Richtlinien

Die enge Integration aller kritischen Zero-Trust-Technologien in die Netskope Zero Trust Engine macht diese zu einer starken Antriebskraft bei der unternehmensweiten Einführung eines Zero-Trust-Sicherheitsmodells. Umfragen mit Hunderten von Netskope-Kunden haben drei entscheidende Ergebnisse im Anschluss an die Einführung einer SSE-Lösung aufgezeigt:

85 % Verringerung des Sicherheitsrisikos durch den Schutz kritischer Ressourcen, Stabilität, Ausfallsicherheit und die Erziehung der Benutzer zu verantwortungsvolleren digitalen Bürgern

51 % Senkung der Gesamtbetriebskosten durch die Außerbetriebnahme von Geräten, die Entlastung von Mitarbeitern, die Reduzierung dedizierter Netzwerkverbindungen und die Optimierung der Cloud-Ausgaben

19 % Verbesserung der Unternehmensagilität, da die Einführung von Zero-Trust-Prinzipien die Verteidigungslinie näher an den Benutzer heranrückt, die Markteinführung beschleunigt und datenbasierte Entscheidungen ermöglicht

Weitere Informationen finden Sie unter: https://www.netskope.com/de/resources/analyst-reports/2023-gartner-magic-quadrant-for-security-service-edge.

Über Netskope

Netskope ist ein führender Anbieter der Lösung Secure Access Service Edge, die Cloud-, Daten- und Netzwerksicherheit neu definiert und Unternehmen bei der Anwendung von Zero-Trust-Prinzipien unterstützt. Die intelligente Security Service Edge (SSE)-Plattform von Netskope ist schnell und einfach zu bedienen; sie schützt Menschen und sichert Geräte und Daten überall – ganz gleich, wo sie sich befinden. Netskope hilft Unternehmen, Risiken zu reduzieren, die Effektivität zu steigern und einen ganzheitlichen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten.

Tausende Kunden, darunter mehr als 25 der Fortune 100-Unternehmen, vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk, um Bedrohungen zu minimieren und auf technologische, organisatorische, netzwerkbezogene und regulatorische Veränderungen reagieren zu können.

netskope