AWS und Zscaler – eine einheitliche Lösung für hohe, skalierbare Cloud-Sicherheit

aws

zscaler™

Inhaltsverzeichnis

Die Cloud-Herausforderung – schnell und sicher expandieren

VPNs und andere perimeterbasierte Sicherheitspraktiken können mit den modernen Herausforderungen der Cloud nicht länger Schritt halten. Aber welche Alternativen gibt es?

Im Jahr 2020 haben mehr als die Hälfte aller Unternehmen ihre Workloads in die Cloud verlagert, wobei 76 % von ihnen Amazon Web Services (AWS) wählten. Die Vorteile des Wechsels in die Cloud liegen auf der Hand – von Kosteneinsparungen bis hin zu flexibler Skalierbarkeit. Unternehmen, die ihren Betrieb in die Cloud verlagern, sehen sich mit zwei neuen Herausforderungen konfrontiert: dem Zugriffsmanagement und der Verwaltung von Betriebsabläufen im Zuge der zunehmenden Verlagerung zu dezentralen und hybriden Arbeitsstrukturen sowie der immer raffinierteren Bedrohung durch Malware und Ransomware.

Früher erforderte die Implementierung einer sicheren Umgebung ein netzwerkzentriertes VPN. Dabei ging die Kontrolle jedoch zulasten der Geschwindigkeit, Benutzerfreundlichkeit und Flexibilität. Da Unternehmen heutzutage zunehmend ihre Aktivitäten in die Cloud verlagern und der IT-Betrieb immer umfangreicher wird, sind die Nachteile der Verwendung eines VPN mittlerweile größer als die Vorteile.

Ein VPN ist nicht dafür ausgelegt, einen inhärent sicheren Internetzugang zu bieten. Darüber hinaus muss die Belegschaft selbst für eine stabile Internetverbindung und den aktuellen Anforderungen entsprechende Sicherheitsmaßnahmen sorgen. Unternehmen, die auf die Cloud umsteigen, beschäftigen User, die von unterschiedlichen Standorten aus arbeiten. Dadurch steigt die Zahl der eingehenden Verbindungen und damit auch die Wahrscheinlichkeit für DDoS-Angriffe. Dies wiederum erhöht die Komplexität der Zugriffssegmentierung und reduziert die Transparenz über die Vorgänge im Netzwerk. Letztlich beeinträchtigen diese Probleme die Skalierbarkeit, führen zu höheren Kosten, schränken die Produktivität ein und beeinträchtigen die Anwendererfahrung. In einigen Fällen hat dies auch Auswirkungen auf den Enduser – den Kunden.

Diese Hürden sind der Grund für die gute Zusammenarbeit von AWS und Zscaler, einer führenden Zero Trust Exchange, die die Netzwerk- und Sicherheitsbranche revolutioniert. Als Advanced Technology Partner von AWS bietet Zscaler Security-as-a-Service auf der Grundlage eines Zero-Trust-Modells. So können Unternehmen nicht nur jetzt, sondern auch in Zukunft eine echte Cloud-Transformation erzielen – und zwar sicher und einfach.

Die moderne, umfassende, Cloud-First-Lösung von Zscaler

Eine konfigurierbare Produktsuite für vereinfachten Zugriff und erhöhte Sicherheit, die mit Blick auf die Multicloud-Komplexität entwickelt wurde

Ganz gleich, ob ein Unternehmen Workloads in die Cloud verlagern oder sich einfach nur von einem VPN lösen möchte, das Fazit ist eindeutig: Die Kombination von Zscaler und AWS bietet erstklassige Sicherheit und eine hervorragende Anwendererfahrung mithilfe modernster Technologie und eines Zero-Trust-Modells.

Die anwendungszentrierten Sicherheitsservices von Zscaler wurden von Grund auf in der Cloud entwickelt und ersetzen die traditionellen ein- und ausgehenden Gateways durch einen moderneren Ansatz, was sich insbesondere für Unternehmen, die AWS nutzen, anbietet. Drei Kern-Services unterstützen AWS-Kunden dabei, das Beste aus ihrem Cloud-Betrieb herauszuholen:

Dank **Zscaler Private Access** (ZPA) werden VPNs überflüssig, da User mit Anwendungen anstatt mit Netzwerken verbunden werden. So werden Applikationen aus dem Internet entfernt, was durch einfachere Verwaltung der Tools und Vorgänge hinter den Kulissen, mit denen User nicht interagieren, zu einer sichereren Umgebung und einer geringeren Backend-Komplexität führt.

Zscaler Internet Access (ZIA) ist ein in der Cloud bereitgestellter, vollständiger Security-Stack, mit dem die Kosten und die Komplexität herkömmlicher Secure-Web-Gateway-Ansätze reduziert werden.

Zscaler Digital Experience Monitoring (ZDX) ist eine mandantenfähige Cloud-basierte Monitoring-Plattform, die digitale Anwendererfahrungen für jeden einzelnen User innerhalb einer Organisation prüft, bewertet und misst.

Gemeinsam unterstützen Zscaler und AWS Organisationen dabei, Unternehmen optimal für die Zukunft aufzustellen. Erreicht wird dies durch:

- einen ununterbrochenen Zugriff zur Verbesserung der Anwendererfahrung;
- effizienteres Routing für geringere Latenz und eine kürzere Zeit zur Produktion;
- einen stärkeren, umfassenderen Sicherheitsstatus zur Beseitigung von Bedrohungen;
- eine schnellere Migration von Applikationen für minimale Ausfallzeiten;
- eine erhöhte Geschäftsagilität zur Steigerung des Wettbewerbsvorteils;
- geringere Kosten und damit die Freisetzung finanzieller Mittel, die anderweitig im Unternehmen besser eingesetzt werden können.

Diese Tools können zwar jedem Unternehmen dabei helfen, zukunftsfähig zu werden, aber sie erweisen sich als besonders wertvoll, wenn es um kritische Anwendungsfälle geht. Mit Zscaler lassen sich beispielsweise viele der technischen Probleme beseitigen, mit denen sich IT-Teams bei Fusionen und Übernahmen konfrontiert sehen. Durch eine deutlich geringere Komplexität des Integrationsprozesses sowie die Einhaltung von Best Practices im Bereich Sicherheit hat Zscaler Unternehmen dabei geholfen, technische Einrichtungsprozesse von Monaten auf Wochen zu verkürzen. Die fusionierten Unternehmen können ihre Mitarbeiter direkt mit den Anwendungen verbinden, ohne dass es zu Problemen oder Verzögerungen bei der Erstellung oder Verlegung von Netzwerken kommt.

Zscaler im Überblick

Jeden Tag leistet Zscaler Folgendes:

Blockierung von
7 Mrd.
Bedrohungen

Verarbeitung von
mehr als 200 Mrd.
Anfragen

Bereitstellung von
mehr als 200.000
individuellen Sicherheitsupdates

ZPA – eine nahtlose Cloud-First-Lösung für Zero-Trust-Zugriff auf private Apps

Umständliche VPNs durch reibungslosen Zugriff auf Anwendungen ersetzen, mit dem private Apps nicht ins Internet gelangen und so für externe Bedrohungsakteure unsichtbar bleiben

Die einst als beste Option für Private Access geltenden VPNs sind in der Cloud-basierten Welt von heute zunehmend umständlich und anfällig: User werden in ein Netzwerk geroutet, um anschließend wieder hinausgeleitet zu werden. App-Verbindungen für Remote-Mitarbeiter durchlaufen weltweit unterschiedliche Touchpoints – von Firewalls bis hin zu Load Balancern – und umfassen somit sogar noch mehr Schritte. Darüber hinaus setzt ein VPN voraus, dass der User weiß, welches Profil zu verwenden ist und welche Ressourcen den Zugriff und somit eine Verbindung zum Netzwerk ermöglichen. All dies führt zu einer suboptimalen Anwendererfahrung, insbesondere für technisch weniger versierte Mitarbeiter.

Satellitenbüros in der Umlaufbahn halten

ZPA gewährleistet einen sicheren Fernzugriff auf Applikationen ohne VPN und Netzwerkzugang und ohne sich dabei auf IP-zentrierte physische oder virtuelle Appliances zu stützen. Der autorisierte User-Zugriff wird vor, während und nach der Migration von Anwendungen zu AWS verwaltet. Dabei wird ein wesentlich effizienterer und sicherer Pfad verwendet: eine SDP-Lösung (Software Defined Perimeter) basierend auf Zero Trust, die eine von einem AWS App Connector in der globalen Security Cloud von Zscaler hergestellte ausgehende Verbindung nutzt – eine Lösung, die auch ergänzend zu AWS Native Security Groups und AWS Direct Connect eingesetzt werden kann. Unabhängig davon, von wo aus ein User versucht, sich mit internen Anwendungen zu verbinden, sorgt ZPA für eine schnellere Migration von Applikationen, geringere Kosten und ein reduziertes Bedrohungsrisiko – selbst für Unternehmen, die noch auf ein privates Rechenzentrum angewiesen sind. So werden Skalierbarkeit und Agilität perfekt miteinander vereint.

ZPA Northstar: Wie GROWMARK die Lebensmittelproduktion am Laufen hält

Das nordamerikanische Landwirtschaftsunternehmen GROWMARK bietet unterschiedliche Materialien und Services zur Unterstützung des Pflanzenwachstums an. Das Unternehmen beschäftigt Mitarbeiter an mehr als 500 ländlichen Standorten und ist mit den Herausforderungen unzuverlässiger Internetverbindungen bestens vertraut. Angesichts der COVID-19-Pandemie sowie der daraus resultierenden Lieferkettenprobleme war es für das Unternehmen noch wichtiger als sonst, für reibungslose Abläufe zu sorgen.
Im Zuge der Modernisierungsbemühungen von GROWMARK verlagerte das Unternehmen Hunderte von Anwendungen zu AWS. Gleichzeitig wurden einige Applikationen vor Ort gehostet, weshalb eine Lösung benötigt wurde, die sich mit der hybriden Struktur vereinbaren ließ. Nachdem sich GROWMARK für ZPA entschieden hatte, konnte das Unternehmen seinen Mitarbeitern eine zuverlässigere Verbindung zur Verfügung stellen und gleichzeitig öffentliche Schnittstellen aus der privaten Umgebung entfernen, was letztlich zu einer Reduzierung der Angriffsfläche führte.
Zum Höhepunkt der Pandemie konnten 98 % der GROWMARK-Mitarbeiter nahezu ohne Probleme eine Verbindung zu ZPA herstellen.

ZIA – ein zuverlässiger Cloud-Security-Stack als Service

Geringeres Risiko und niedrigere Netzwerkkosten durch den Wechsel von veralteter Perimeter-Sicherheit zu Zero-Trust-Schutz von Cloud-Umgebungen

Unternehmen, die Rechenzentren und perimeterbasierte Sicherheitsmodelle nutzen, erkennen, dass der Wechsel in die Cloud mit einem Übergang zu Secure-Web-Gateway-Ansätzen verbunden ist.

Der Wechsel von einem Rechenzentrum in die Cloud geht mit einer Verlagerung der betreffenden Anwendungen einher: Die zentralisierten Gateways, die zuvor für einen vereinfachten Zugriff und geringere Kosten sorgten, bieten angesichts der neuen Sicherheitsrisiken, die durch den direkt in die Cloud fließenden User-Traffic entstehen, keinen ausreichenden Schutz mehr. Dadurch wird das veraltete perimeterbasierte Sicherheitsframework zum Risiko. Hinzu kommt die Belastung durch neue Sicherheitsappliances, die das ohnehin schon überlastete Gateway noch zusätzlich strapazieren. Dies führt dazu, dass IT-Abteilungen kaum Schritt halten können.

Kein Spielraum für Fehler im Weltraum

Zscaler und AWS setzen auf Zero Trust, sodass Unternehmen auch in neuen Umgebungen stets gut geschützt sind. So sind sie dank Zero Trust ihrer Zeit voraus: Laut Forrester entwickelt sich Zero Trust immer mehr zur bevorzugten Sicherheitsarchitektur.

Mit ZIA können Unternehmen eine sicherere Verbindung zu SaaS-Lösungen (Software-as-a-Service) gewährleisten. Sämtliche Internetaktivitäten der User eines Unternehmens sind einsehbar und gleichzeitig wird ein einfacher und sicherer Remotezugriff auf interne Apps auf AWS ermöglicht.

Dank der Struktur und der Services von Zscaler werden Angriffsflächen reduziert, die Zugriffskontrolle verbessert und der Datenschutz gestärkt, sodass granulare Richtlinien in großem Maßstab durchgesetzt werden können.

ZIA Northstar: Einführung von ZIA bei MAN Energy Systems

Der deutsche Anbieter von Fertigungs- und Transportdienstleistungen MAN Energy Systems bietet wichtige Produkte und Services an, darunter Dieselmotoren und Turbomaschinen, mit denen die globale Wirtschaft am Laufen gehalten wird. Um dauerhaft wettbewerbsfähig zu bleiben, verlagerte das Unternehmen seine Workloads zu AWS. Die wachsenden, weltweit verteilten Teams von MAN benötigten jedoch zunehmend mobilen Zugriff auf Anwendungen und benutzerdefinierte Geschäftstools. Dadurch entstand ein erhöhtes Sicherheitsrisiko und der zeitaufwendige und komplizierte Authentifizierungs- und Zugriffsprozess für die zahlreichen Applikationen auf individueller Ebene sorgte für Frustration unter den Mitarbeitern. Das Führungsteam wandte sich vom VPN ab und entschied sich für ZIA, sodass nur vertrauenswürdige User auf vertrauenswürdige Anwendungen zugreifen können. So kann die mobile Belegschaft jederzeit und von jedem Standort aus sicher mit den SaaS-Anwendungen von MAN verbunden werden.

ZDX – schnelle, nahtlose Anwendererfahrungen für Enduser

Tiefe, verwertbare Einblicke in die Benutzererfahrung anhand einer einheitlichen Sicht auf die Performancemetrik von Applikationen, Endgeräten und CloudPath.

In puncto Anwendererfahrung sind Verbraucher heutzutage einen extrem hohen Standard gewöhnt – selbst ein vorübergehender Social-Media-Ausfall sorgt mittlerweile für Schlagzeilen. Unternehmen waren zwar im Begriff, Probleme hinsichtlich der Anwendererfahrung mithilfe der internen Technologie vor Ort zu bewältigen, doch angesichts der durch schlechte Internetverbindungen und unterschiedliche (und teils veraltete) persönliche Mobilgeräte verursachten Probleme von Remote- und Hybrid-Teams kam es verstärkt zu Engpässen. Führt dies zu Unterbrechungen und ständigen Neuverbindungen, sammeln sich Support-Tickets an und Arbeit bleibt liegen. Dadurch gerät die IT-Abteilung unter Druck: Die Ursache (und Lösung) der spezifischen Probleme muss schnellstmöglich gefunden werden.

Problemloser Flug: Reibungslose Anwendererfahrungen für alle Enduser

ZDX ist eine mandantenfähige, Cloud-basierte Monitoring-Plattform zur Prüfung, Bewertung und Messung der digitalen Anwendererfahrungen jeglicher User innerhalb einer Organisation – unabhängig davon, wo sie sich befinden. ZDX ermittelt in Echtzeit, wodurch ein Problem verursacht wird (z. B. durch die Internetverbindung oder den Internetdienstanbieter) und setzt daraufhin seine Remote-Fehlerbehebungsfunktionen ein. Analysen messen die Performance über einen bestimmten Zeitraum nach Standort, User und Abteilung, um Trends zu erkennen und Verbesserungen zu ermöglichen. Das Ergebnis? Eine echte SASE-Architektur (Secure Access Server Edge), die für eine bessere Anwendererfahrung und weitaus weniger IT-Tickets sorgt.

ZDX Northstar: Wie Liberty Mutual das Mitarbeitererlebnis verbesserte

Im Jahr 2020 konnte Liberty Mutual Insurance zum Leidwesen vieler zwar für seine Rechenzentren und die ISP-Bandbreite eine Gewährleistung geben, nicht aber für die Internetverbindung der Mitarbeiter, die von zu Hause aus arbeiteten. Für einen Proof of Concept konzentrierte sich das Sicherheitsteam von Liberty zunächst auf 100 User und führte ZDX als ersten Anwendungsfall für User mit Langzeitproblemen ein. So wurden Probleme an das Level-2-Helpdesk-Team weitergegeben, das die Probleme der User mit Heimnetzwerken mühelos lösen konnte. Inzwischen wurde ZDX im gesamten Unternehmen integriert, um unter anderem Latenzprobleme von Serviceanbietern, Probleme mit WLAN-Routern, Speicherlecks auf Desktop-Computern sowie ISP-Probleme im Zusammenhang mit der Seitenladezeit zu ermitteln und zu beheben.

Eine gemeinsame Lösung mit einfacher Bereitstellung, die schnell einsatzbereit ist

Mit einem auf Geschwindigkeit ausgelegten Bereitstellungsprozess sowie dem Zscaler Client Connector für Zugriffsmanagement sind Teams in nur wenigen Minuten einsatzbereit.

Einfache Umsetzung mit Zscaler und AWS: Der Wechsel zu einer neuen Plattform und IT-Infrastruktur kann komplex und zeitaufwendig sein. Deshalb ist der Einführungsprozess von Zscaler auf Schnelligkeit und Einfachheit ausgelegt. So werden jederzeit ein sicherer Cloud-basierter Betrieb und reibungslose Übergänge für die betreffenden Mitarbeiter gewährleistet.

Wenngleich ZPA, ZIA und ZDX auch einzeln eingesetzt werden können, empfiehlt es sich, sie für ein optimales Framework zu kombinieren. Das Herzstück ihrer Prozesse bildet der Zscaler Client Connector (ZCC).

ZPA verwendet den Client Connector, um User mithilfe eines Zero-Trust-Ansatzes mit privaten Applikationen zu verbinden, wobei für rein webbasierte private Anwendungen auch ein Browser-Zugriff möglich ist.

ZIA nutzt den Client Connector, um User außerhalb des Unternehmensnetzwerks zu schützen. Der Internet-Traffic wird hierbei durch den Service von Zscaler geleitet, um eine granulare Sicherheitsrichtlinie durchzusetzen.

ZDX verwendet den Client Connector für synthetische Tests gewünschter SaaS-Applikation (Software-as-a-Service) oder internetbasierter Services wie z. B. Salesforce oder Zoom.

Der Abschied von VPNs

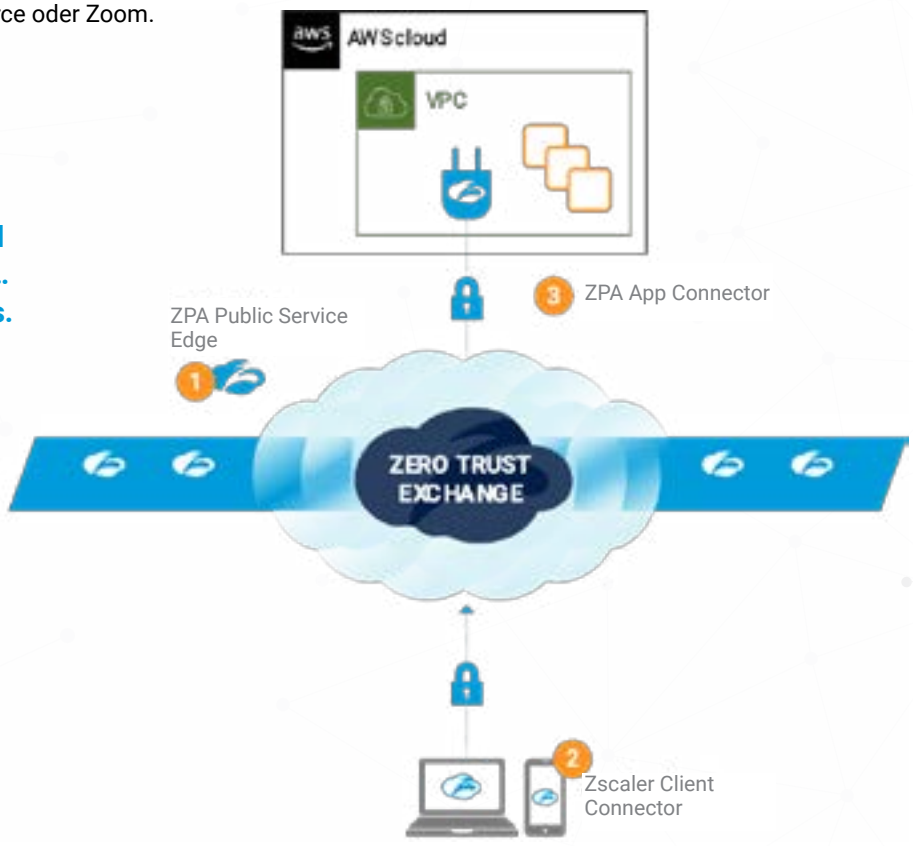
Dank der schnellen und problemlosen Installation von Zscaler können sich unsere Kunden endgültig von ihren VPNs abwenden.

1. Die IT-Abteilung installiert die Anwendungskonnektoren in AWS, wo sich die Applikationen befinden, sodass Zscaler die Anwendungen erreichen kann, auf die User zugreifen müssen.
2. Im ZPA-Portal werden Applikationen und Konnektoren definiert und den Servergruppen zugewiesen.
3. Einmal installiert, erfüllt der Client Connector gleich mehrere Zwecke: Er ermittelt, wohin Anfragen gerichtet sind, wohin sie gehen sollen und wo User verbunden werden.

Weitere Informationen über die Konfiguration für den Client Connector

Zscaler-Kunden wenden sich schnell und ohne Risiko von ihren VPNs ab … und zwar endgültig. So funktioniert's.

1. **ZPA Public Service Edge** hostet die Richtlinien-Engine und vermittelt Verbindungen
2. **Der Endgeräte-Agent Zscaler Client Connector** leitet den Traffic an die Zscaler Cloud weiter
3. **ZPA App Connector** stellt die Verbindung zu privaten Apps her und erkennt neue Applikationen



Bereit für die Transformation der Cloud-Sicherheit?

Unendliche Weiten: Zscaler und AWS haben den User-Zugriff revolutioniert. Jetzt nicht den Sprung in die Zukunft verpassen: Zscaler-Lösungen gibt es im AWS Marketplace.

Mit nur wenigen Klicks lässt sich ein Bericht von Zscaler erstellen, der eine detaillierte Bewertung des Cloud-Sicherheitsstatus liefert und zeigt, wo die Sicherheitsrisiken von Unternehmen im Internet liegen. Analyse der Internet-Bedrohungslage starten.