Kunde Fallstudien aus der Praxis

Entdecken Sie Transformationsgeschichten aus der Praxis, mit Hilfe von Zscaler Zero Trust + KI.

Erfahren Sie, wie Unternehmen mit Zero Trust + KI ihren Sicherheitsstatus verbessern, erstklassige Anwendererfahrungen gewährleisten, Integrationen nach Fusionen und Übernahmen beschleunigen und mehr.

Kundenorientierung zählt bei Zscaler zu unseren Grundwerten. Entsprechend sind wir bestrebt, marktführende Zero-Trust-Innovationen bereitzustellen, die Ihr Unternehmen bei der Realisierung seiner Ziele unterstützen. Mithilfe der Kernfunktionen unserer KI-gestützten Zero Trust Exchange haben wir weltweit über 5.000 Unternehmen dabei geholfen, Kosten und Komplexität zu senken, ihre Netzwerkarchitekturen zu vereinfachen, ihre User zu schützen und neuartige Cyberbedrohungen abzuwehren. In diesem E-Book präsentieren wir Fallstudien einiger der erfolgreichsten Unternehmen der Welt, die ihre Netzwerkarchitektur, ihren Sicherheitsstatus und ihre Betriebsabläufe mit Zscaler transformiert haben.

Zscaler leistet seit über 15 Jahren Pionierarbeit im Bereich Zero Trust und unterstützt Unternehmen aller Größen und Branchen dabei, ihre Zero-Trust-Ziele zu erreichen und zu übertreffen. Die einzige Konstante in der Technologie ist bekanntlich der Wandel. Mit unserer Zero Trust Exchange sind Unternehmen auf alle Herausforderungen der Gegenwart und Zukunft vorbereitet — und können gleichzeitig ihre IT-Infrastruktur kontinuierlich weiterentwickeln und transformieren.

Mike Rich
CRO & President of Global Sales

Inhalt

Kundenreferenzen nach Branchen durchsuchen

AMS

Kundenreferenzen
nach Regionen
durchsuchen

AMN Healthcare setzt zum Schutz von Usern und Daten weltweit auf die Zscaler Zero Trust Exchange

Zscaler sichert die Remote-Arbeit von über 5.000 Usern und schützt Patientendaten vor zunehmenden Cyberbedrohungen im Gesundheitswesen

AMN HEALTHCARE: KURZPORTRÄT

Bereitstellung von Personallösungen im Gesundheitswesen für Kunden zur Verbesserung der Behandlungsergebnisse

- Gesundheitswesen und Pharma
- USA: Dallas (Texas)
- Über 10.000 Kunden an 24 Standorten

1,2 Milliarden
Web-Transaktionen monatlich verarbeitet

7 Mio.
Bedrohungen blockiert in drei Monaten

Stündlich
zur Bereitstellung einer sicheren Edge überall

Herausforderungen

- Eine Legacy-Sicherheitsinfrastruktur war nicht mehr mit dem dynamischen Cloud-First-Betriebsökosystem des Unternehmens kompatibel.
- Herkömmliche VPNs waren der wachsenden Anzahl von Remote-Usern nicht mehr gewachsen, wodurch private Unternehmensressourcen anfälliger für Cyberbedrohungen wurden.
- Eine komplexe Sicherheitsarchitektur aus disparaten Einzellösungen beeinträchtigte die Transparenz und Behebung von Problemen.

Schritte der Transformation

1. **Bereitstellung eines sicheren Direkt-Internetzugangs**, der einer weltweit verteilten Belegschaft flexibles Arbeiten von jedem beliebigen Standort aus ermöglicht
2. **Einführung eines mikrosegmentierten, Zero-Trust-Zugriffs auf private Unternehmensanwendungen** als bessere Alternative zu herkömmlichen VPNs
3. **Optimierte den Monitoring-Stack und nutzte die lückenlose End-to-End-Sichtbarkeit** zur effektiveren Behebung von User-Problemen

Ergebnisse

- **Sichert die aus- und eingehende Konnektivität für über 5.000 User** und verbessert so die Möglichkeiten und Effizienz der globalen Remote-Arbeit
- **Setzt Zero-Trust-Zugriffsrichtlinien für private Unternehmensanwendungen und digitale Produkte durch,** die von mehr als 10.000 Kunden weltweit verwendet werden
- **Vereinfacht die Architektur und senkt die Technologiekosten**, um einen stärkeren Sicherheitsstatus mit weniger Aufwand zu erreichen

Der Ansatz von Zscaler entspricht unserer allgemeinen Zero-Trust-Philosophie und die Zero Trust Exchange war die Realisierung unserer Vision einer Zero-Trust-Architektur bei AMN Healthcare.

Mani Masood
Head of Information Security,
AMN Healthcare

Kundenreferenz anzeigen

ATN International sichert den Betrieb und verbessert die Effizienz mit Zscaler Zero Trust Exchange

Zscaler verbessert die Remote-Arbeitsfunktionen für mehr als 2.500 Mitarbeiter, beseitigt VPN-bezogene User-Probleme und sorgt für mehr Sicherheit bei Integrationen und Onboarding infolge von Fusionen und Übernahmen

ATN INTERNATIONAL: KURZPORTRÄT

Anbieter von Kommunikationsinfrastruktur und -diensten mit Spezialisierung auf entfernte Märkte

Telekommunikation

USA: Beverly (Massachusetts)

750.000 Kunden in aller Welt

100 %

Eliminierung von VPNs und VPN-Hilfetickets

Alle

Mitarbeiter mit Zscaler geschützt

Minute

statt mehrerer Stunden zur Problembehebung User-Probleme

Herausforderungen

- Die On-Premise-Sicherheitsinfrastruktur konnte weder Cloud-First-Betriebsabläufe noch zukünftig angestrebte Fusionen und Übernahmen unterstützen
- Legacy-VPN-Appliances konnten bei einem Anstieg der Remote-Arbeit nur schwer skaliert werden, was zu einer schlechten User Experience und höherem Risiko führte.
- Herkömmliche Sicherheitslösungen boten nicht die Cloud-Integrationen, die für eine proaktive Behebung von User-Problemen unverzichtbar sind.

Schritte der Transformation

1. **Bereitstellung von Direktzugang zum Internet und** Funktionen zur Traffic-Überwachung und Protokollierung, um Richtlinienverstöße zu verhindern.
2. **Umstellung von VPN-Geräten auf Zero Trust und berechtigungsbasierten Zugriff** auf private Unternehmensanwendungen und Ressourcen
3. **Nutzung von KI-gestützten Zscaler-Funktionen und tiefer Microsoft-Integration** zur schnelleren Erkennung und Lösung von User-Problemen

Ergebnisse

- **Verbessert die Remote-Arbeitserfahrung für mehr als 2.500 User** und beseitigt VPN-bezogene User-Probleme — die Anzahl der Servicetickets sinkt um 100 %
- **Beschleunigt IT-Integrationen nach Fusionen und Übernahmen und gewährleistet ein sichereres Onboarding** übernommener Unternehmen mit einer Zero-Trust-Sicherheitsarchitektur
- **Reduziert die zur Erkennung und Lösung von Problemen erforderliche Zeit** auf wenige Minuten dank robuster Berichts- und Überwachungsfunktionen

Infrastruktur- und Sicherheitstools müssen Ihnen zu mehr Betriebseffizienz verhelfen und für mehr Sicherheit sorgen. Zscaler erfüllt beide Anforderungen.

Richard Casselberry
VP, IT Security, Architecture & Compliance, ATN International

Kundenreferenz anzeigen

COX AUTOMOTIVE

Cox Automotive implementiert Zero Trust stufenweise mit der Zscaler Zero Trust Exchange

Zscaler optimiert die Sicherheitsarchitektur, sichert die Konnektivität für User auf fünf Kontinenten und schützt die Daten von Millionen Online-Autokäufern

COX AUTOMOTIVE: KURZPORTRÄT

Weltweit führender Anbieter von Dienstleistungen und Technologien für die Automobilindustrie

- Einzel- und Großhandel
- USA: Atlanta (Georgia)
- 2,3 Milliarden Online-Interaktionen jährlich

>30.000
Mitarbeiter Geschützt

40.000
Unterstützte Kunden aus dem Autohandel

Eine
zentrale Plattform reduziert die Komplexität

Herausforderungen

- Wollten eine Cloud-kompatible Plattform als Grundlage für die Umstellung auf eine ganzheitliche Zero-Trust-Sicherheitsarchitektur
- Herkömmliche Firewall-Appliances hatten Schwierigkeiten, den Internet-traffic einer global verteilten Usergruppe in großem Umfang zu überprüfen
- Legacy-VPNs unterstützten keine identitätsbasierten Zugriffskontrollrichtlinien, wodurch private Unternehmensanwendungen und -daten einem höheren Risiko ausgesetzt waren

Schritte der Transformation

1. **Bereitstellung einer Cloud-nativen, mandantenfähigen Zero-Trust-Plattform**
   speziell für die einfache Integration mit anderen Cloud-Lösungen entwickelt
2. **Bereitstellung sicherer Direktverbindungen zum Internet und zu SaaS-Apps** unter Nutzung der Möglichkeiten zur Inline-Traffic-Überprüfung
3. **VPNs durch Zero-Trust-Zugriff ersetzt,** um mikrosegmentierte Sicherheitsrichtlinien nach dem Prinzip der minimalen Rechtevergabe für private Unternehmensanwendungen durchzusetzen

Ergebnisse

- **Sichert ein Team, das auf fünf Kontinenten arbeitet,**, ermöglicht ortsunabhängige Flexibilität und verbessert die User Experience
- **Schützt kritische private Unternehmensanwendungen und -ressourcen**, einschließlich der Daten von Millionen von Kunden, auf kostengünstige Weise
- **Ersetzt Legacy-Sicherheitslösungen wie Firewalls und VPNs,** um IT-Prozesse zu optimieren und das Onboarding nach Fusionen und Übernahmen zu beschleunigen

Sobald die Agents auf allen Geräten installiert sind, können wir problemlos weitere Zscaler-Funktionen in unsere Architektur integrieren. Sie können dann problemlos aktiviert werden.

Jon Mahes
Sr. Manager, Cybersecurity,
Cox Automotive

Kundenreferenz anzeigen

Kommunalverwaltung des District of Columbia konsolidiert die Sicherheit mit der Zscaler Zero Trust Exchange

Zscaler ersetzt veraltete VPN-Geräte, optimiert die Sicherheitsarchitektur, verbessert das Risikobewusstsein in Echtzeit und schützt 15.000 User

KOMMUNALVERWALTUNG DISTRICT OF COLUMBIA: KURZPORTRÄT

Beaufsichtigt und verwaltet alle kritischen Serviceleistungen für die Bewohner des District of Columbia

- Bund und Regierung
- Washington D.C., USA
- >15,000 Mitarbeiter

15.000
Regierungsmitarbeiter gesichert

ca. 3 Milliarden
verarbeitete Transaktionen pro Monat

Über 200.000
blockierte Sicherheitsbedrohungen pro Monat

Herausforderungen

- Eine Legacy-Sicherheitsinfrastruktur konnte die Remote-Arbeit nicht unterstützen und trug zu betrieblichen Ineffizienzen bei.
- Herkömmliche VPN-Geräte erweiterten das Unternehmensnetzwerk auf die Geräte der Enduser und setzten so vertrauliche Daten dem Risiko einer Kompromittierung aus.
- Legacy-Sicherheitsprodukte schränkten die Transparenz von Bedrohungen ein und erschwerten so die Risikobewertung und -minimierung.

Schritte der Transformation

1. **Bereitstellung sicherer Direktverbindungen zum Internet und zu SaaS-Anwendungen** und Unterstützung flexibler Arbeitskonzepte
2. **Ersetzung von Legacy-VPNs durch mikrosegmentierten Zero-Trust-Zugriff,** um einheitliche Sicherheitsrichtlinien für private Unternehmensressourcen durchzusetzen
3. **Nutzung KI-gestützter Daten und Erkenntnisse, um das Risikobewusstsein zu stärken** und potenzielle Bedrohungen in Echtzeit und im großen Maßstab einzudämmen

Ergebnisse

- **Zero-Trust-Architektur verbessert** Sicherheitsprozesse für ca. 3 Milliarden Transaktionen und blockiert über 200.000 Bedrohungen monatlich
- **Verbessert die User Experience für 15.000 Remote-User** und lässt sich nahtlos in vorhandene Lösungen zur Identitätsverwaltung integrieren
- **Ermöglicht einen ganzheitlichen Fokus auf das Risikomanagement** durch bessere Einblicke in Risikofaktoren und den Sicherheitsstatus

Die Partnerschaft mit Zscaler war für uns von unschätzbarem Wert. Wir haben die Plattform in Rekordgeschwindigkeit bereitgestellt, das Onboarding für die User effektiver gestaltet und die User Experience verbessert.

Suneel Cherukuri
CISO, Kommunalverwaltung des District of Columbia

Kundenreferenz anzeigen

DMI implementiert BYOD in großem Maßstab, verbessert den Datenschutz und erzielt erhebliche Kosteneinsparungen

Zscaler bietet Zero-Trust-Konnektivität für die gesamte Belegschaft und ermöglicht Mitarbeitern, sicher an Geräten ihrer Wahl zu arbeiten

DMI: KURZPORTRÄT

DMI ist ein weltweit führender Anbieter digitaler Dienste, der an der Schnittstelle zwischen öffentlichem und privatem Sektor arbeitet.

Hightech

USA: McLean (Virginia)

>2.100 Mitarbeiter in 80 Ländern

>700.000 USD
jährliche Einsparungen

>2
Wochen für die Bereitstellung

3 %
schnellere SLA-Auflösung nach der Bereitstellung

Herausforderungen

- Die Installation neuer Hardware in einer Legacy-Umgebung führte zu Ausfallzeiten und erforderte regelmäßige Updates
- Die Anforderung, von DMI-Geräten aus zu arbeiten, verringerte die Produktivität der Mitarbeiter und wirkte sich negativ auf die globale CO2-Bilanz des Unternehmens aus

Schritte der Transformation

1. **Gesicherter Internetzugang und echte Zero-Trust-Konnektivität** für Mitarbeiter, Auftragnehmer und Dritte ohne zeitaufwendige, manuelle Geräteeinrichtung
2. **Einführung der BYOD-Initiative (Bring-your-own-device), die durch Browser-Isolierung unterstützt wird und** Mitarbeitern ermöglicht, an Geräten ihrer Wahl zu arbeiten.

Ergebnisse

- **Umstellung auf Zero Trust innerhalb von 2 Wochen** ohne Auswirkungen auf die User und ohne Ausfallzeiten
- **Einsparungen in Höhe von 700.000 jährlich,** effektiveres Onboarding und Offboarding und schnellere Einrichtung neuer Standorte und Geräte

Mit dem BYOD-Projekt konnten wir Einsparungen erzielen, da wir keine Laptops für Personen anschaffen mussten, die sie nicht benötigten. Insgesamt beliefen sich die Ersparnisse auf über 700.000 USD. Das ist eine beachtliche Summe!

Mauricio Mendoza
Vice President, Global IT and Security, DMI

Kundenreferenz anzeigen

Eaton sichert globale Betriebsabläufe mit KI-gestützter Segmentierung

Zscaler unterstützt global aufgestellten Fertigungskonzern bei der Migration in die Cloud mit erweitertem Bedrohungsschutz, Reduzierung des Sicherheitsrisikos und erhöhter Transparenz durch Partnerintegrationen

EATON: KURZPORTRÄT

Weltweit tätiger Hersteller von Elektrogeräten für die Luft- und Raumfahrt und andere Branchen

Fertigung

USA: Cleveland (Ohio)

>90.000 Mitarbeiter und User in 170 Ländern weltweit

4 Mio.

Bedrohungen blockiert in einem Monat

90.000

Mitarbeiter weltweit greifen über Zero Trust auf Internet und private Unternehmensanwendungen zu

Mehrere

strategische Geschäftspartner werden nahtlos integriert

Herausforderungen

- Legacy-VPNs und Firewalls behinderten das Wachstum und waren während der Pandemie und darüber hinaus nicht in der Lage, eine Belegschaft von über 30.000 Fabrikmitarbeiter zu unterstützen
- Die herkömmliche perimeterbasierte Sicherheitsarchitektur war mit der Cloud-First-Strategie und den Segmentierungsanforderungen des Unternehmens nicht kompatibel.
- Mangelnde Transparenz beschränkte die Erkennung von Bedrohungen und verzögerte ihre Behebung.

Schritte der Transformation

1. **Umstellung von Sicherheits-** und Zugriffstools auf Zero-Trust-Konnektivität zum Internet und zu privaten Unternehmensanwendungen
2. **Nutzung von KI-Innovationen** zur Erkennung und Bekämpfung KI-basierter Bedrohungen sowie zur Segmentierung von Produktionsstandorten
3. **Verbessertes Angriffsbewusstsein** durch präventive und vorausschauende Erkennung und Reaktion auf Sicherheitsverletzungen

Ergebnisse

- **Sichere, zuverlässige, regulierte** User Experience für Mitarbeiter und externe User
- **Nutzt die Leistungsfähigkeit der KI zur Bedrohungserkennung**, zur Verhinderung von Datenverlusten, zur Behebung von Problemen, zur Transparenz bei der ChatGPT-Nutzung und zur Anwendungssegmentierung
- **Stärkt die Zugriffskontrolle** durch Zero-Trust-Segmentierung und Integration mit EDR-, CDR- und NDR-Tools

Zscaler ist userfreundlich und alle Funktionen sind in einen Endgeräte-Agent integriert. Wir konnten Zscaler schnell und mit geringfügigem Ressourcenaufwand unsererseits in unserer globalen Umgebung implementieren.

Jason Koler
CISO, Eaton Corporation

Kundenreferenz anzeigen

Garantueed Rate blockiert Millionen von Bedrohungen und verkürzt die Integration nach Fusionen und Übernahmen von Monaten auf wenige Tage

Zscaler ersetzt Sicherheitshardware durch überlegene Ausfallsicherheit, ständig aktive Sicherheit und eine minimierte Angriffsfläche

GUARANTEED RATE: KURZPORTRÄT

Zweitgrößter Anbieter von Hypothekendarlehen in den USA mit über 500 Filialen in 50 Bundesstaaten

Finanzdienstleistungen und Versicherungen

USA: Chicago (Illinois)

über 6.000 Mitarbeiter

97 %
des verschlüsselten Traffics untersucht

2,5 Mio.
blockierte Bedrohungen in 3 Monaten

2–3 x
schnellerer Zugriff auf Applikationen

Herausforderungen

- Der Einsatz von VPNs zur Verbindung mit Hunderten von privaten Unternehmensanwendungen On-Premise und in AWS vergrößerte die Angriffsfläche.
- Durch Backhauling des Datenverkehrs von über 500 Filialen zum Rechenzentrum wurden Leistung und Produktivität beeinträchtigt.
- Legacy-Firewalls konnten keine Zero-Day-Bedrohungen erkennen, die über das Internet ins Netzwerk eindringen und sich lateral ausbreiten.

Schritte der Transformation

1. **Sicherung des Internet- und SaaS-Zugriffs aus der Cloud**— kein Backhauling mehr von über 500 Filialen
2. **Umstellung von VPN** auf schnellen, zuverlässigen Zugriff auf über 500 private Unternehmensanwendungen im Rechenzentrum und in der Cloud
3. **Optimierte User Experience** durch schnellere und effizientere Erkennung und Lösung von Performance-Problemen

Ergebnisse

- **Minimale Angriffsfläche** durch Direktzugriff nach dem Prinzip der minimalen Rechtevergabe bei gleichzeitiger Verbesserung von Erkennung und Reaktion
- **Reduziert das Risiko von Kompromissen** durch Inline-TLS/SSL-Überwachung und KI-gestützten Schutz vor komplexen Bedrohungen
- **Verhindert laterale Bewegungen** mithilfe von Deception-Technologie, um Angreifer von sensiblen Ressourcen wegzulocken und Bedrohungen in Echtzeit einzudämmen

Mit Risk360 gewinnen wir lückenlosen Einblick in die Cyberrisiken. Dank dieser Transparenz können wir effizienter Prioritäten setzen, um die dringendsten Cyberrisiken angehen und reduzieren.

Darin Hurd
CISO, Guaranteed Rate

Kundenreferenz anzeigen

MGM Resorts International setzt verstärkt auf Cloud-native Zero-Trust-Architektur

Zscaler bietet unübertroffene Time-to-Value mit Zero-Trust-Segmentierung, Schutz vor Datenverlusten und gründlichen, aussagekräftigen Einblicken in das gesamte Unternehmen.

MGM RESORTS INTERNATIONAL: KURZPORTRÄT

Führender Anbieter im Gaming-, Unterhaltungs- und Gastgewerbe mit 31 Urlaubszielen weltweit

- Unterhaltung und Gastgewerbe
- USA: Las Vegas (Nevada)
- 70.000 Mitarbeiter weltweit

Tag 1
sofortiger Nutzen von der Plattform

>275.000
blockierte Bedrohungen pro Monat

50 %
effizientere Gerätenutzung für Mitarbeiter

Herausforderungen

- Perimeterbasierte Sicherheit erhöhte das Risiko von lateralen Bewegungen, indem sie den Usern einen breiten Netzwerkzugriff gewährte
- Herkömmliche VPN-Gateways verursachten Traffic-Engpässe und beeinträchtigten die User Experience
- Legacy-Sicherheitstools boten nur eingeschränkten Einblick in die Browseraktivitäten der User.

Schritte der Transformation

1. **Umstellung von VPNs auf Zero-Trust-Segmentierung** für die gesamte Belegschaft
2. **Schnelle Bereitstellung** von privaten Zugriffslösungen, Digital Experience Monitoring und Data Protection
3. **Implementierung von Deception-Technologie** zum Schutz vor Kompromittierung durch aktive Angreifer

Ergebnisse

- **Verbesserte Mitarbeitererfahrung** durch schnellere Performance und Konnektivität in der gesamten Umgebung
- **Schutz vor neuartigen Bedrohungen** durch umfassende DLP, private Zugriffslösungen und Zero-Trust-Segmentierung
- **Stärkung des Sicherheitsstatus des Unternehmens** und Beschleunigung des Betriebs mit einem Cloud-First-Ansatz

Wir haben in Rekordzeit eine Zero-Trust-Segmentierung in unserer Belegschaft erreicht und die tägliche Wartung der Lösung mit Data Loss Protection und Einblicken in unsere Anwendungen sichergestellt. Aus unserer Sicht verlief alles zügig und problemlos.

Stephen Harrison
CISO, MGM Resorts International

Kundenreferenz anzeigen

Mercury Financial verbessert Sicherheit und Effizienz mit der Zscaler Zero Trust Exchange

Zscaler stellt nahtlose Integrationen und KI-Funktionen bereit, um sichereres Arbeiten von jedem Standort aus zu unterstützen und vertrauliche Finanzdaten vor Bedrohungen zu schützen.

MERCURY FINANCIAL: KURZPORTRÄT

Ein Finanzdienstleistungsunternehmen, das Kunden beim Aufbau und der Verwaltung von Guthaben unterstützt

- Finanzdienstleistungen und Versicherungen
- USA: Austin (Texas)
- Über 500 Mitarbeiter

100 %
nahtlose User Experience für Remote-Mitarbeiter

76 %
weniger IT-Supporttickets

Null
Ausfallzeit aufgrund von Malware

Herausforderungen

- Herkömmliche Sicherheitslösungen ermöglichten keine vollständige Inline-Überprüfung des Datenverkehrs und behinderten so die Erkennung und Abwehr von Bedrohungen.
- Legacy-VPNs waren nicht mit den Cloud-First-Anforderungen einer verteilten Belegschaft kompatibel, was zu einer schlechten User Experience führte.
- Eingeschränkte Daten zu Useraktivitäten und zum Gerätestatus erschwerten die Diagnose und Lösung von Problemen für eine Remote-Belegschaft.

Schritte der Transformation

1. **Sichere Direktverbindungen zum Internet** durch Einsatz KI-gestützter Funktionen zur Verhinderung von Datenkompromittierung
2. **Umstellung von VPNs auf mikrosegmentierten Zero-Trust-Zugriff** für private Unternehmensanwendungen, um sicherzustellen, dass Remote-Verbindungen kontrolliert und sicher sind
3. **Nutzung wichtiger Integrationen und aussagekräftiger Usereinblicke** zur Reduzierung des Verwaltungsaufwands ohne Erhöhung des Risikos

Ergebnisse

- **Reduzierte Angriffsfläche**— keine Ausfallzeiten durch Malware oder Ransomware seit der Bereitstellung von Zscaler
- **Einschränkung der lateralen Bewegungsfreiheit und geringeres Schadenspotenzial,** wenn eine Bedrohung in den Sicherheits-Stack eindringt, wodurch eine schnellere Behebung gewährleistet wird
- **Integrationen mit AWS, Crowdstrike und Okta optimieren die Sicherheitsinfrastruktur** und verbessern die aufsichtsrechtliche Compliance

Wir betrachten Zscaler als führenden Anbieter auf diesem Gebiet, da das Unternehmen sämtliche Facetten von Zero Trust abdeckt. Sonst müssten wir Lösungen mehrerer Anbieter einsetzen, um die gleiche Funktionalität wie bei Zscaler zu erhalten.

Arjun Thusu
Chief Information Officer,
Mercury Financial

Kundenreferenz anzeigen

Molson Coors gewährleistet mit der Zscaler Zero Trust Exchange eine erstklassige User Experience

Zscaler macht VPN-Geräte überflüssig, sichert die Konnektivität einer globalen Belegschaft und liefert Einblicke, die zur schnelleren Problembehebung beitragen

MOLSON COORS: KURZPORTRÄT

Die drittgrößte Brauerei der Welt und ein globaler Innovator in der Getränkeindustrie

- Lebensmittel, Getränke und Tabakwaren
- USA: Chicago (Illinois)
- >17.000 Mitarbeiter
  >42 Brauereien

17.000
geschützte User mit Zero Trust

96 %
schnellere Lösung von User-Problemen

Millionen
täglich blockierter Bedrohungen

Herausforderungen

- Firewall-Geräte konnten nicht mit der Nachfrage nach Remote-Internetzugang skaliert werden und hatten Probleme, den Datenverkehr inline zu überprüfen.
- Mangelnde Transparenz hinsichtlich Useraktivitäten und Gerätestatus erschwerte die Erkennung und Behebung von Performance-Problemen.
- Eine Legacy-Sicherheitsarchitektur, die auf VPN-Geräten basiert, führte zu einer flachen Netzwerkumgebung und einer größeren Angriffsfläche.

Schritte der Transformation

1. **Bereitstellung von Direktzugriff aus Internet mit ATD-Funktionen** zum Schutz von Remote- und Drittusern
2. **Lückenlose Transparenz über alle User und Geräte,** um das Sicherheitsmanagement zu vereinfachen und User-Probleme schneller zu lösen
3. **Umstellung von herkömmlichen VPNs auf Zero-Trust-Zugriff für private Unternehmensanwendungen** zum Schutz von Ressourcen und zur Verbesserung der User Experience

Ergebnisse

- **Erstklassige User Experience für Mitarbeiter** von 42 Brauereien weltweit sowie für externe Partner
- **Schnellere Lösung von User-Problemen** durch Ermittlung der Grundursachen und die Automatisierung der Schadensbehebung in Minuten statt in Stunden.
- **Blockierung komplexer Bedrohungen** und lateraler Bewegungen, um private Unternehmensanwendungen und vertrauliche Unternehmensdaten zuverlässiger zu schützen

Die Anzahl der Bedrohungen, die allein von Zscaler blockiert wurden, liegt je nach Tag immer im Hunderttausende- oder Millionenbereich. Die Lösung von Zscaler ist sehr userfreundlich. Man kann sofort mit dem Training beginnen. Es gibt keine Einschränkungen.

Jeremy Bauer
Sr. Director Information Security (CISO),
Molson Coors Beverage Company

Kundenreferenz anzeigen

New Yorker Bildungsdezernat migriert von VPN zu Zero Trust

Zscaler sichert den Zugriff auf Internet und interne Anwendungen für über 1 Million User und über 2 Millionen Geräte

BILDUNGSDEZERNAT DER STADT NEW YORK: KURZPORTRÄT

Das Bildungsdezernat der Stadt New York ist das größte Schulsystem der USA und eines der größten der Welt. Es betreut über 1 Million Schüler vom Kindergarten bis zur 12. Klasse mit einem Personal von mehr als 150.000 Lehrern und Administratoren in allen fünf Bezirken von New York.

Bildung

USA:
New York City

>1 Mio. User und
>2 Mio. Geräte

>2 Millionen

Geräte von Schülern und Mitarbeitern gesichert

15 %

Rückgang der Angriffe

40 %

mehr Bedrohungen blockiert

Herausforderungen

- Die bestehende Infrastruktur war nicht skalierbar, um sichere und konsistente Erfahrungen für mehr als 1 Million User zu gewährleisten.
- Der herkömmliche VPN- und Firewall-Ansatz war bei der Blockierung fortgeschrittener Cyberbedrohungen unwirksam.
- Aufgrund der mangelnden Einblicke in Endgeräte war es schwierig, die Geräte zum Remote-Lernen zu verwalten und zu überwachen.

Schritte der Transformation

1. **Sicherung des Zugriffs auf Internet und SaaS** mit einer Zero-Trust-Proxy-Architektur, die den gesamten TLS/SSL-Traffic auch bei hohen Datenvolumen lückenlos überprüft
2. **Umstellung von VPN auf Zero Trust Network Access (ZTNA)** für schnelle, nahtlose User-Verbindungen
3. **Verbesserte Transparenz** über alle Netzwerke und Geräte durch lückenloses Digital Experience Monitoring

Ergebnisse

- **Schneller, zuverlässiger und sicherer Zugriff** auf Lernanwendungen für Schüler und Mitarbeiter unabhängig von Standort und Gerät
- **Inhaltsbasierte Filterung des Traffics** über die einfache URL-Blockierung hinaus, um die CIPA-Konformität auf Lerngeräten zu unterstützen
- **Verbesserte Netzwerkleistung** durch Erkennung und Behebung von Netzwerk- und DNS-Problemen in der Umgebung

Ich halte Zscaler für einen ausgezeichneten Partner, der uns bei der sinnvollen Implementierung von KI unterstützt und uns dabei hilft, schneller auf Vorfälle zu reagieren und die berüchtigte Nadel im Heuhaufen zu finden.

Demond Waters
CISO, Bildungsdezernat der Stadt New York

Kundenreferenz anzeigen

Southwest Gas nutzt die Zscaler Zero Trust Exchange zur Optimierung sicherer Anwendererfahrungen

Zscaler stellt eine effektivere Alternative zu herkömmlichen Sicherheitslösungen bereit, die schnellere und zuverlässigere Verbindungen für 2.300 Hybrid-Mitarbeiter und 50 Außenstellen gewährleistet

SOUTHWEST GAS: KURZPORTRÄT

Erdgasversorgungsbetrieb in Arizona, Nevada und Kalifornien

- Energie, Öl, Gas und Bergbau
- USA: Las Vegas (Nevada)
- 2 Millionen Kunden

4–6

Wochen zur Bereitstellung einer ganzheitlichen von Zero Trust

95 %

der Anwendungsfälle erfüllt

Eine

Single-Vendor-Plattform

Herausforderungen

- Eine herkömmliche Sicherheitsinfrastruktur ließ sich nicht skalieren, um die Cloud-Transformation oder die Umstellung auf hybrides Arbeiten zu unterstützen.
- Die Bereitstellung einer schnellen und zuverlässigen Internetverbindung für Außenstellen und Remote-Mitarbeiter in ländlichen Gebieten stellte eine Herausforderung dar.
- Legacy-VPNs unterstützten keine identitätsbasierten Zugriffsrichtlinien, wodurch private Unternehmensanwendungen und -daten anfälliger für Bedrohungen waren.

Schritte der Transformation

1. **Bereitstellung einer mandantenfähigen Zero-Trust-Plattform**, Rationalisierung des Sicherheits-Stacks und Optimierung von Remote-Arbeitsumgebungen
2. **Bereitstellung von Direktzugriff auf das Internet und SaaS-Apps** mit durchgängigem Schutz vor Bedrohungen, unabhängig vom Standort
3. **Umstellung von VPNs auf Zero-Trust-Zugriff für private Unternehmens-anwendungen,** um die Angriffsfläche zu verkleinern und Datenverluste auszuschließen

Ergebnisse

- **Sicherer standortunabhängiger Zugriff für 2.300 Hybrid-Mitarbeiter** und Schutz für User und Daten in 50 Außenstellen
- **Durchsetzung mikrosegmentierter Zugriffskontrollrichtlinien nach dem Prinzip der minimalen Rechtevergabe** für private Unternehmensanwen-dungen zum Schutz kritischer Daten
- **Beschleunigte Einführung von Zero Trust**, Vereinfachung des Sicherheitsmanagements und weniger technische Supportanfragen

Nachdem wir einen Proof of Value (PoV) durchgeführt hatten, entschieden wir uns für Zscaler aufgrund der zukunftsfähigen Architektur, die es uns ermöglichte, unseren Sicherheits-Stack in die Cloud zu verlagern und eine Remote-Belegschaft zu optimieren.

David Petroski
Senior Infrastructure Architect,
Southwest Gas

Kundenreferenz anzeigen

United Airlines erkennt und blockiert neuartige Bedrohungen mit der Zscaler Zero Trust Exchange

Zscaler eliminiert 40 % mehr Bedrohungen als frühere Legacy-Lösungen, schützt 80.000 User weltweit und sorgt für sicherere Reisen für 143 Millionen Passagiere

UNITED AIRLINES: KURZPORTRÄT

US-amerikanisches Luftfahrtunternehmen und drittgrößte Fluggesellschaft der Welt mit Standorten in 48 Ländern

- Transportdienstleistungen
- USA: Chicago (Illinois)
- >80.000 Mitarbeiter an über 350 Standorten

6
Monate bis zur Zero-Trust-Transformation

1 PB
des TLS-Traffics untersucht

>3 Mio. USD
Kosteneinsparungen gegenüber Legacy-Lösungen

Herausforderungen

- Eine traditionelle, perimeterbasierte Architektur, die auf Rechenzentren angewiesen ist, kann die beschleunigte digitale Transformation nicht unterstützen.
- Legacy-Firewalls und VPNs waren nicht flexibel genug, um mit der zunehmenden Zahl von Remote-Arbeitern Schritt zu halten, was User und Daten gefährdete.
- Frühere Sicherheitsprodukte verfügten nicht über erweiterte Funktionen zur Bedrohungserkennung, wodurch eine größere Angriffsfläche entstand.

Schritte der Transformation

1. **Sichere Direktverbindungen zum Internet und zu SaaS-Apps,** um standort-übergreifend einen einheitlichen Schutz für User zu gewährleisten
2. **Umstellung von VPNs auf Zero-Trust-Zugriffsrichtlinien nach dem Prinzip der minimalen Rechtevergabe,** um private Unternehmensanwendungen und Daten vor Kompromittierung zu schützen
3. **Nutzung von Cloud-Integrationen und Digital Experience Monitoring** zur Verbesserung der Echtzeittransparenz bei Bedrohungen

Ergebnisse

- **Ermöglicht 80.000 Mitarbeitern, von jedem beliebigen Standort aus sicher zu arbeiten,** und sichert den Remote-Zugriff auf über 2.000 kritische private Unternehmensanwendungen
- **Reduziert die Komplexität und Kosten der Architektur**— keine Firewalls an Flughäfen erforderlich und Verzicht auf sechs Einzelprodukte
- **Vereinheitlichtes Sicherheitsökosystem mit dynamischer Richtliniendurch-setzung,** um 40 % mehr Bedrohungen zu blockieren und den Sicherheits-status zu verbessern.

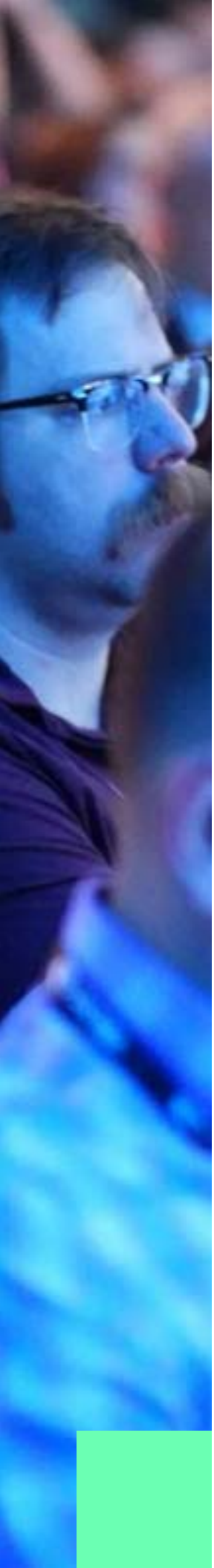
Zscaler gibt uns die Gewissheit, dass der Datenverkehr für unsere Mitarbeiter, Kunden und Partner unabhängig vom zugrunde liegenden Netzwerk sicher ist.

Deneen DeFiore
Vice President & Chief Information Security Officer, United Airlines

Kundenreferenz anzeigen

EMEA

Kundenreferenzen
nach Regionen
durchsuchen



Raiffeisen Bank International

Raiffeisen Bank International transformiert die Sicherheit mit der Zscaler Zero Trust Exchange

Zscaler ersetzt Legacy-Appliances, um umfassenden Schutz vor Bedrohungen zu gewährleisten, flexible Arbeitskonzepte zu ermöglichen und die Sicherheitskosten zu senken.

RAIFFEISEN BANK: KURZPORTRÄT

Eine der führenden Firmenkunden- und Investmentbanken Österreichs

Finanzdienstleistungen und Versicherungen

Wien, Österreich

Millionen von Kunden in 12 Märkten

44.000

Mitarbeiter durch Zero Trust geschützt

18,6 Mio.

Kunden profitieren von sicherem Banking

Eine

Plattform gewährleistet Komplettschutz mit Zero Trust

Herausforderungen

- Eine herkömmliche Sicherheitsinfrastruktur war nicht mit einem Cloud-First-Ansatz kompatibel, was User und Workloads gefährdete.
- Veraltete Sicherheits-Appliances unterstützten nicht die Flexibilität, von überall aus arbeiten zu können, was zu Latenz und schlechter Leistung führte.
- VPNs ermöglichten keinen identitätsbasierten Zugriff für private Unternehmensanwendungen, was zu inkonsistenten Richtlinien und einer größeren Angriffsfläche führte

Schritte der Transformation

1. **Bereitstellung einer umfassenden Zero-Trust-Plattform**, die private und öffentliche Service-Edges nutzt, um User an sämtlichen Standorten zu schützen
2. **Sichere Direktverbindungen zum Internet ohne Backhauling,** um eine einheitliche User Experience für eine hybride Belegschaft zu gewährleisten
3. **Umstellung von VPN-Appliances auf Zero-Trust-Zugriff für private Unternehmensanwendungen** und optimierte identitätsbasierte Zugriffsrichtlinien

Ergebnisse

- **Sicherung der aus- und eingehenden Verbindungen einer hybriden Belegschaft** mit konsistentem Schutz an sämtlichen Standorten
- **Geringere Latenz und bessere Performance von SaaS und privaten Anwendungen,** um die User Experience in der Unternehmenszentrale und an Remote-Standorten zu verbessern
- **Optimiert die Sicherheitsarchitektur und bietet umfassenden Schutz vor Bedrohungen** bei gleichzeitiger Reduzierung der Sicherheitsausgaben

Die Partnerschaft mit Zscaler brachte uns durch die Durchsetzung von Zero-Trust-Prinzipien mehr Sicherheit, geringere Kosten und bessere Anwendererfahrungen.

Peter Gerdenitsch
Group CISO, Raiffeisen Bank International

Kundenreferenz anzeigen

Magdeburger Stadtverwaltung sichert ihre digitale Transformation mit der Zscaler Zero Trust Exchange

Die deutsche Landeshauptstadt ersetzt VPN-Appliances, unterstützt die hybride Belegschaft und legt mit Zscaler den Grundstein für die weitere digitale Entwicklung

LANDESHAUPTSTADT MAGDEBURG: KURZPORTRÄT

Erbringt Verwaltungsdienstleistungen für die Bürger der sachsen-anhaltischen Landeshauptstadt

Bund und Regierung

Magdeburg, Deutschland

2,500 Mitarbeiter

2.500
Hybrid-Mitarbeiter gesichert

230.000
Stadtbewohner unterstützt

Eine
Lösung aus einer Hand zur Vereinfachung der Sicherheit

Herausforderungen

- Die bisherige hardwarebasierte Sicherheitsarchitektur war nicht flexibel genug, um die Ziele der digitalen Transformation zu unterstützen.
- Herkömmliche Proxy- und Firewall-Lösungen waren nicht skalierbar genug, um die Internetkonnektivität einer zunehmend hybriden Belegschaft zu sichern.
- VPNs ermöglichten keine granulare Zugriffskontrolle, was interne Anwendungen einem größeren Risiko aussetzte und die Möglichkeiten der Remote-Arbeit einschränkte.

Schritte der Transformation

1. **Bereitstellung einer Cloud-nativen Zero-Trust-Plattform** zur Modernisierung der Sicherheitsarchitektur und Ermöglichung einer weiteren digitalen Transformation
2. **Einführung sicherer Direktverbindungen zum Internet** unter Nutzung der integrierten Traffic-Überprüfungsfunktionen zur Abwehr von Bedrohungen
3. **Sicherer Zugriff auf private Unternehmensanwendungen mit identitätsbasierten Zero-Trust-Kontrollen**, die einen konsistenten Schutz kritischer Daten gewährleisten

Ergebnisse

- **Verbesserte User Experience für eine hybride Belegschaft** und sicheres Remote-Arbeiten für bis zu 1.500 User monatlich
- **Reduziert Sicherheitskosten und Verwaltungskomplexität** mit einer Architektur, die veraltete Einzelprodukte überflüssig macht
- **Beschleunigt zukünftige Digitalisierungsprojekte** mit einer umfassenden und skalierbaren Zero-Trust-Sicherheitsarchitektur

„Wir wollten einen Leuchtturm-Charakter für andere Kommunen haben und diese ermutigen, gute Lösungen aus der Wirtschaft zu evaluieren und einzuführen, so wie wir es mit cloudbasierter Sicherheit getan haben."

Dr. Tim Hoppe
Amt für Statistik, Wahlen und Digitalisierung der Landeshauptstadt Magdeburg

Kundenreferenz anzeigen

Cisalfa Sport stärkt den Sicherheitsstatus durch beschleunigte Einführung von Zscaler in weniger als drei Monaten

Die Zero-Trust-Plattform reduziert die Angriffsfläche und gewährleistet nahtlose Anwendererfahrungen für Mitarbeiter und externe User.

CISALFA SPORT: KURZPORTRÄT

Italiens führender Omnichannel-Sporthändler

Einzel- und Großhandel

Italien: Curno

>3.600 Mitarbeiter

2,5

Monate für die unternehmensweite Zscaler-Bereitstellung

>130

Drittpartner und Auftragnehmer profitieren von sicherem Zugriff auf private Unternehmensanwendungen und On-Premise-Infrastruktur

70 %

der User erhalten Zugriff innerhalb von 2 Wochen nach Bereitstellung

Herausforderungen

- VPN ermöglichte allen Mitarbeitern und Dritten unsegmentierten Zugriff auf das gesamte Unternehmensnetzwerk, was das Risiko und Schadenspotenzial potenzieller Angriffe erhöhte.
- Zwei Legacy-VPN-Lösungen wiesen widersprüchliche Richtlinien und Konfigurationen auf, was zu inkonsistenten Sicherheits- und Sicherheitsmanagementproblemen führte
- Der Zugriff auf Apps über VPN führte zu Performance-Verzögerungen und einer hohen Anzahl an Helpdesk-Tickets von internen und externen Usern.

Schritte der Transformation

1. **Reduzierung der Angriffsfläche** durch Umstellung von anfälligen VPNs auf Direktzugriff auf private Unternehmensanwendungen
2. **Verhinderung der lateralen Ausbreitung von Bedrohungen** durch Durchsetzung von Zugriffsrichtlinien nach dem Prinzip der minimalen Rechtevergabe für alle User
3. **Verbesserte User Experience** durch verbesserte App-Leistung und Zuverlässigkeit — keine Unterbrechungen oder mehrfachen VPN-Anmeldungen mehr, um auf Ressourcen zuzugreifen

Ergebnisse

- **Verbessert den allgemeinen Sicherheitsstatus** durch Direktzugriff für alle User und konsequente Richtliniendurchsetzung
- **Nahtloser, transparenter, clientlosen Zugriff** auf private Unternehmensanwendungen und -daten für Geschäftspartner und Auftragnehmer
- **Reduziert die Anzahl latenzbedingter Helpdesk-Tickets** durch blitzschnelle Konnektivität über den nächstgelegenen Präsenzpunkt

Die Zscaler Zero Trust Exchange … erfüllt sämtliche Anforderungen: schnelleren und sichereren Zugriff auf Anwendungen ohne VPN, Risikominderung in der gesamten Umgebung und einen eindeutigen Pfad zur Zero-Trust-Erweiterung.

Fabio Freti
IT Operations & Infrastructure Manager, Cisalfa Sport

Kundenreferenz anzeigen

Hydro verbessert den Sicherheitsstatus und die Nachhaltigkeit mit der Zscaler Zero Trust Exchange

Zscaler reduziert Angriffsfläche und verbessert die O2-Bilanz bei Anbieter erneuerbarer Energien, der zu 100 % auf die Cloud umstellen möchte

HYDRO: KURZPORTRÄT

Eines der weltweit größten Unternehmen für erneuerbare Energien mit Präsenz in 40 Ländern

Fertigung

Norwegen: Oslo

31.000 Mitarbeiter

33.000
Mitarbeiter mit Zero Trust geschützt

Eine
Anbieteransatz zur Reduzierung von Kosten und Komplexität

100 %
Cloud Operations Ziel

Herausforderungen

- Die herkömmliche Sicherheitsinfrastruktur und -hardware war energieintensiv und entsprach nicht den Nachhaltigkeitszielen des Unternehmens.
- Ein MPLS-Netzwerk mit geringer Bandbreite konnte nicht skaliert werden, um einen Anstieg des Cloud-Traffics zu bewältigen, was zu Performance-Abfällen führte.
- Herkömmliche VPNs mit rigiden Zugriffsrichtlinien gefährden das Netzwerk und können zu kostspieligen Ransomware-Angriffen führen.

Schritte der Transformation

1. **Bereitstellung einer sicheren Direktverbindung zum Internet**, wodurch das Backhauling des Traffics entfällt und die Zuverlässigkeit verbessert wird
2. **Umstellung von Legacy-VPNs auf richtlinienbasierten Zero-Trust-Zugriff** für private Unternehmensanwendungen zum Schutz von Daten vor Cyberangriffen
3. **Implementierung einer speziell für den Cloud-Traffic entwickelten Experience-Monitoring-Lösung** zur schnelleren Lösung von User-Problemen

Ergebnisse

- **Eliminiert die Abhängigkeit von veralteten Einzelprodukten** und verbessert die CO2-Bilanz mit einer Cloud-nativen, mandantenfähigen Sicherheitsplattform
- **Verbessert die Leistung von SaaS-Anwendungen** und die User Experience für 33.000 Mitarbeiter an 140 Standorten
- **Reduziert Kosten und Verwaltungskomplexität und verbessert gleichzeitig den Sicherheitsstatus** durch die Verwendung einer Single-Vendor-Lösung für Zero Trust

Seit wir auf Zscaler Private Access umgestiegen sind, müssen User nicht mehr mit dem Netzwerk verbunden werden, um auf private Unternehmensanwendungen zuzugreifen. Im Zuge der weiteren Umsetzung unseres Modernisierungskonzepts wollen wir VPN durch eine zukunftsfähige Alternative ersetzen.

Armin Auth
Head of I&T Strategic Programs

Kundenreferenz anzeigen

Capitec beschleunigt die digitale Transformation und schützt Finanzdaten mit Zscaler

Südafrikas größte Bank führt in drei Monaten Zero-Trust-Sicherheit ein, schützt 17.000 User und blockiert 745.000 Bedrohungen mit der Zero Trust Exchange

CAPITEC: KURZPORTRÄT

Größte Bank in Südafrika, betreut 21 Millionen Kunden und ist Nr. 1 für Kundenzufriedenheit

Finanzdienstleistungen und Versicherungen

Kapstadt (Südafrika)

15.450 Mitarbeiter in 860 Filialen

3

Sekunden, um private Unternehmensanwendungen zu AWS zu migrieren

125 Millionen

Richtlinienverstöße in einem Jahr verhindert

3

Monate für die Umsetzung von Zero Trust

Herausforderungen

- Eine perimeterbasierte Sicherheitsarchitektur konnte wertvolle Finanzdaten nicht wirksam vor Kompromittierung und Verlust schützen.
- Legacy-Sicherheitsanwendungen wie Firewalls und VPNs waren komplex zu verwalten und die User-Produktivität litt darunter.
- Die eingeschränkte Transparenz hinsichtlich der User Experience verhinderte einen proaktiven Ansatz zur Erkennung und Lösung von Problemen.

Schritte der Transformation

1. **Sichere Direktverbindungen zum Internet und zu SaaS-Apps** durch Traffic-Monitoring zur Verhinderung von Datenmissbrauch
2. **Umstellung von VPN-Appliances auf Zero-Trust-Zugriff** für private Unternehmensanwendungen und vertrauliche Finanzdaten
3. **Nutzung erweiterter Funktionen zum Digital Experience Monitoring und umsetzbarer Erkenntnisse** zur Lösung langjähriger Probleme mit der User Experience

Ergebnisse

- **Sicherer Zugriff auf das Internet und Cloud-Anwendungen für 17.000 User** und Verhinderung von 125 Millionen Richtlinienverstößen pro Jahr
- **Schutz einer Private-Banking-Anwendung, auf die mehr als 11 Millionen Kunden zugreifen**, mit richtlinienbasiertem Zero-Trust-Zugriff
- **Ermöglicht eine schnellere digitale Transformation**— die Migration von Apps zu AWS dauert nur Sekunden, ohne Ausfallzeiten und ohne Sicherheitsmängel

Wir haben die Zero Trust Exchange in unsere Umgebung integriert und unsere Zero Trust-Sicherheitssoftware-Agents innerhalb von drei Monaten für alle unsere User bereitgestellt.

Andrew Baker
CTO, Capitec

Kundenreferenz anzeigen

Noatum implementiert eine Reihe von Zscaler-Technologien zur Unterstützung einer Vielzahl von Anwendungsfällen

Sicherer Zugriff auf Internet, SaaS und private Unternehmensanwendungen, verbesserter Erkennung von Cyberbedrohungen und optimierter User Experience

NOATUM: KURZPORTRÄT

Noatum ist eine führende multinationale Gruppe im Bereich Transport- und Logistikdienstleistungen

- Transportdienstleistungen
- Spanien: Barcelona
- Mehr als 4,300 Mitarbeiter

Tag 1
Sofortiger Mehrwert durch die Plattform

Keine
Abhängigkeit von VPNs und Firewalls

360
Grad der Risikoquantifizierung

Herausforderungen

- Mit herkömmlichen VPNs ist das Unternehmen Cyberangriffen zu stark ausgesetzt, wenn User auf das Internet zugreifen.
- Veraltete Sicherheitsmaßnahmen wie Firewalls ermöglichten keine Überprüfung des verschlüsselten Traffics.
- Perimeterbasierte Architekturen führten zu unnötigen Verzögerungen beim Onboarding nach Fusionen und Übernahmen.

Schritte der Transformation

1. **Umstellung von VPNs** auf eine Cloud-Plattform ermöglicht sicheren Zugriff auf das Internet und private Unternehmensanwendungen
2. **Implementierung von ZDX zur Konfiguration eines einzigartigen, cloudbasierten Experience Monitoring Hub**
3. **Ganzheitliche Bewertung von Geschäftsrisiken** mit Zscaler Risk360

Ergebnisse

- **Sicherer, nahtloser Userzugriff zur Unterstützung dezentraler Arbeitskonzepte**
- **Minimiert Uservorfälle** und verbessert die Ursachenanalyse, wodurch Wissen und Agilität gewonnen werden
- **Verbessert die Risikobewertung** sowie die Bedrohungsabwehr durch Verbergen von Systemen und Anwendungen vor dem Internet

Das herkömmliche VPN war das Problem, unsere Präsenz bei Internetdiensten und das Risiko ständiger Angriffe — das war für uns der eigentliche Auslöser, nach einer Lösung wie Zscaler zu suchen.

Josep Pou
CISO, Noatum

Kundenreferenz anzeigen

Sanitas bietet sichere, nahtlose Konnektivität mit Zscaler Internet Access

Implementierung von Schutzmaßnahmen für Internet, SaaS und private Unternehmensanwendungen für über 12.000 User

SANITAS: KURZPORTRÄT

Großes, wachstumsstarkes Krankenversicherungsunternehmen

Gesundheitswesen und Pharma

Madrid, Spanien

>11.700 Mitarbeiter in Spanien, Europa und LATEINAMERIKA

2,5

Monate für die Bereitstellung an alle User

12.000–15.000

User werden durch unsere Plattform geschützt

Keine

Verbindungen zu einem Rechenzentrum herstellen

Herausforderungen

- Separate Geschäftseinheiten implementierten separate Sicherheitsmaß-nahmen ohne ein cloudbasiertes Modell.
- VPNs führten zu einem langwierigen Prozess der Userauthentifizierung mit unzureichender Sicherheit.
- Partner-Standorte konnten keine Verbindung zu Rechenzentren herstellen und nicht auf Anwendungen zugreifen.

Schritte der Transformation

1. Implementierung von homogener cloudbasierter Zero-Trust-Lösung, um skalierbare Sicherheit für das gesamte Unternehmen zu gewährleisten
2. Umstellung von VPNs auf ein Zero-Trust-Modell, um die Konnektivität für alle User unabhängig vom Standort zu verbessern
3. Sicherer und nahtloser Anwendungszugriff für alle User, einschließlich externe Geschäftspartner

Ergebnisse

- Sichert 12.000—15.000 User in 2 1/2 Monaten mit Zscaler Internet Access
- Ermöglicht standortsunabhängiges Arbeiten und sorgt für flexibles, agiles Arbeiten mit einer büroähnlichen User Experience
- Gewährleistet sicheren Zugriff auf Workloads und Anwendungen

Heute können Mitarbeiter im Homeoffice genauso arbeiten wie im Büro — und zwar auf transparente, flexible, äußerst agile Weise und ohne die Barrieren, die wir früher bei anderen Lösungen hatten.

Antonio Cerezo
Head of Cybersecurity, Europe & LATAM

Kundenreferenz anzeigen

Colt Technology Services verbessert Sicherheit und User Experience mit Zero Trust Exchange

Durch die Partnerschaft mit Zscaler zur Bereitstellung einer Zero-Trust-Architektur in drei Monaten kann das Unternehmen die eigenen Kunden bei der Sicherheitstransformation unterstützen

COLT TECHNOLOGY SERVICES: KURZPORTRÄT

Stellt Netzwerk-, Sprach- und Rechenzentrumsleistungen für mehr als 25.000 Unternehmen weltweit bereit

Telekommunikation

London, Großbritannien

Mehr als 5.000 Mitarbeiter an 60 Standorten weltweit

5.000

Hybrid-Mitarbeiter geschützt

83 %

schnellere Bereitstellung als Legacy-Lösungen

100 Mio.

vierteljährlich verhinderte Richtlinienverstöße

Herausforderungen

- Die beschleunigte Cloud-Migration zur Unterstützung einer hybriden Arbeitsumgebung vergrößerte die Angriffsfläche und das Risiko einer Kompromittierung.
- Eine veraltete Proxy-Lösung konnte die Inline-Prüfung des verschlüsselten Traffics nicht bewältigen, was zu Transparenzlücken bei der Erkennung von Malware führte.
- VPN-Appliances ermöglichten keine dynamischen Zugriffsrichtlinien für private Unternehmensanwendungen, was die Unterstützung der Remote-Arbeit erschwerte.

Schritte der Transformation

1. **Bereitstellung einer Cloud-nativen Zero-Trust-Sicherheitsarchitektur** zur Unterstützung von Cloud-First-Geschäftsabläufen und Hybridarbeit
2. **Sicherer Direktzugriff aufs Internet**, Überprüfung des gesamten verschlüsselten Traffics, um Bedrohungen und Datenverluste zu verhindern
3. **Umstellung von VPN-Appliances auf Zero-Trust-Zugriff für private Unternehmensanwendungen** zur Unterstützung sicherer Remote-Arbeit

Ergebnisse

- **Herausragende User Experience für mehr als 5.000 Hybrid-Mitarbeiter** bei gleichzeitiger Sicherung des aus- und eingehenden Traffics
- **Überprüft den Internettraffic auch bei hohen Datenvolumen**, verarbeitet 6,7 Milliarden Transaktionen und blockiert vierteljährlich 476.000 Sicherheitsbedrohungen
- **Unterstützt die mikrosegmentierten, richtlinienbasierten Richtlinien für den Zugriff auf private Unternehmensanwendungen,** die mit herkömmlichen VPNs nicht möglich sind

Mit Unterstützung von Zscaler können wir sowohl die User Experience als auch die Sicherheit verbessern Die Cloud-native Zscaler-Plattform schützt unsere Mitarbeiter unabhängig vom jeweiligen Standort und Gerät.

Ash Surti
Chief Digital und Information Officer, Colt Technology Services

Kundenreferenz anzeigen

Primetals Technologies unterstützt sichere Hybridarbeit mit der Zscaler Zero Trust Exchange

Weltweit führender Anbieter in der Metallproduktion verabschiedet sich von Rechenzentren und konsolidiert den Sicherheits-Stack, um die digitale Transformation mit Zscaler zu beschleunigen

PRIMETALS TECHNOLOGIES: KURZPORTRÄT

Weltweit führender Anbieter von metallurgischen Anlagenlösungen, spezialisiert auf die Stahlproduktion

Hightech

London, Großbritannien

7,500+ Mitarbeiter

7.500
User mit Zero Trust geschützt

Bis zu 35 %
Senkung der Infrastrukturkosten

4.53/5
Mitarbeiterzufriedenheitsbewertung

Herausforderungen

- Ein herkömmlicher, auf Rechenzentren basierender Sicherheits-Stack ließ sich nicht ausreichend skalieren, um die Cloud-First-Digitaltransformation zu unterstützen.
- Legacy-Sicherheits-Appliances wie Firewalls und VPNs gewährleisteten nicht die erforderliche Flexibilität, um die Neugestaltung eines SD-WAN-Netzwerks zu unterstützen.
- Veraltete VPN-Appliances konnten die Remote-Konnektivität für eine global verteilte hybride Belegschaft nicht effektiv sichern.

Schritte der Transformation

1. **Implementierung einer SD-WAN-kompatiblen Direktverbindung zum Internet** zur Optimierung der Infrastruktur und Verbesserung der Performance
2. **Umstellung von VPNs auf Zero-Trust-Zugriff für private Unternehmens-anwendungen,** um Usern weltweit sicheres Arbeiten von jedem beliebigen Standort aus zu ermöglichen
3. **Nutzung erweiterter Funktionen zur Überwachung der User Experience**, um sicherzustellen, dass die Tools für die Mitarbeiterzusammenarbeit optimal funktionieren

Ergebnisse

- **Vereinfacht den Sicherheits-Stack**, reduziert die Abhängigkeit von Rechenzentren und senkt die Gesamtkosten der Infrastruktur
- **Sichert nahtlose aus- und eingehende Konnektivität** für eine hybride Usergruppe (darunter 25 % komplett in Remote-Arbeit
- **Reduziert die Anzahl der Helpdesk-Tickets und löst Probleme schneller**, verbessert die User Experience und verringert den Verwaltungsaufwand.

Im Zuge der Transformation in die Cloud war es notwendig, dass auch der Security-Stack, der bisher zentral in den Rechenzentren vorgehalten wurde, modernisiert wird. Mit der Zscaler Zero Trust Exchange sind wir unserer Vision einen großen Schritt näher gekommen.

Ralph Deleja-Hotko
Head of Backend & Cloud Solutions
bei Primetals Technologies

Kundenreferenz anzeigen

Unilever verbessert globale Sicherheit und erreicht mit Zero Trust Zugriff auf Apps mit minimaler Rechtevergabe

Dank Zscaler kann Unilever VPNs eliminieren, Usern eine sichere Direktverbindung zu Apps und dem Internet bieten und Betriebsabläufe in 190 Ländern optimieren

UNILEVER: KURZPORTRÄT

Globaler Konsumgüterkonzern mit Produkten, die täglich von 3,4 Milliarden Menschen genutzt werden

Fertigung

London, Großbritannien

Vertrieb in 190 Ländern

>3 Milliarden

wöchentlich gesicherte Transaktionen

99,9 %

Verfügbarkeit bei der Verarbeitung von 220 TB Daten in zwei Monaten

>1.500

Anwendungen, die mit Zero-Trust-Zugriff mit minimaler Rechtevergabe verwaltet werden

Herausforderungen

- Legacy-VPNs hatten eine begrenzte Flexibilität und unzureichende Skalierbarkeit für die globale Cloud-Strategie von Unilever.
- Traditionelles Sicherheitsmodell erhöht das Risiko aufgrund unzureichender Zugriffskontrolle und Transparenz.
- Die steigende Nachfrage nach Remotezugriff belastete die VPN-Infrastruktur und beeinträchtigte die User Experience.

Schritte der Transformation

1. **Sicherer User-Zugriff auf Internet und SaaS** mit lückenloser Überprüfung des TLS/SSL-Traffics und Advanced Threat Protection
2. **Umstellung von VPN** auf Zero-Trust-Zugriff auf private Unternehmensanwendungen
3. **Verbesserte User Experience** durch Digital Experience Monitoring, um Performance-Probleme schnell zu erkennen und zu beheben

Ergebnisse

- **Reduziert das Risiko** durch sicheren Direktzugriff auf Anwendungen und ohne die Einschränkungen und Schwachstellen eines VPN
- **Verbessert die Betriebseffizienz** durch die Verarbeitung hoher Datenvolumen mit 99,99 % Verfügbarkeit
- **Unterstützt die globale Cloud-Strategie** durch Bereitstellung eines sicheren Remotezugriffs in 190 Ländern und erhält so die Flexibilität der Belegschaft von Unilever

Der Zero-Trust-Ansatz von Zscaler hat die Sicherheit bei Unilever verändert. Durch die Beseitigung von VPN-Engpässen können unsere Mitarbeiter weltweit sicher auf Anwendungen zugreifen und so Leistung, Flexibilität und Ausfallsicherheit verbessern.

Richard Mardling
Access and Connectivity Director, Unilever

Kundenreferenz anzeigen

APJ

Kundenreferenzen nach Regionen durchsuchen

John Holland senkt Netzwerkkosten um 50 % mit Zscaler Zero Trust Exchange

Zscaler erleichtert den Übergang zu SD-WAN und ermöglicht den Verzicht auf Hunderte von Firewalls, was die Betriebseffizienz und den Sicherheitsstatus verbessert

JOHN HOLLAND: KURZPORTRÄT

Integriertes Infrastruktur-, Bau-, Schienen- und multimodales Transportunternehmen

Bauwesen

Australien: Melbourne (Victoria)

Über 5.000 Mitarbeiter an über 120 Standorten

1 Woche

für die unternehmensweite Implementierung von Zero Trust

6.000

Mitarbeiter und Auftragnehmer geschützt

122.000

Bedrohungen in drei Monaten blockiert

Herausforderungen

- Eine herkömmliche Perimeter-Sicherheitsarchitektur war nicht skalierbar, um zunehmend Cloud-First-Geschäftsabläufe zu unterstützen.
- Ein veraltetes MPLS-Netzwerk war in erheblichem Maße auf Backhauling des Traffics angewiesen, was die Geschwindigkeit der IT-Services verlangsamte und die Kosten erhöhte.
- Legacy-Firewall-Appliances boten nicht die Flexibilität, verschlüsselten Traffic inline zu prüfen, was die Anfälligkeit für Bedrohungen erhöhte.

Schritte der Transformation

1. **Bereitstellung einer Cloud-nativen, umfassenden Zero-Trust-Sicherheitsplattform** zur Gewährleistung einer agileren und besser skalierbaren IT-Umgebung
2. **Umstellung von Firewall-Appliances und kostspieligen MPLS-Netzwerken** durch sicheren Direktzugriff auf das Internet und SaaS-Apps
3. **Nutzung erweiterter Funktionen zur Bedrohungserkennung, um das Sicherheitsökosystem zu optimieren** und das Risiko einer Datenkompromittierung zu eliminieren

Ergebnisse

- **Migriert 100 % der User innerhalb einer Woche zu Zero Trust** und ermöglicht eine schnellere Bereitstellung des Netzwerkzugriffs an über 120 Projektstandorten.
- **Macht Hunderte von veralteten Firewall-Geräten mit Zero-Trust-Konnektivität** überflüssig und senkt die Netzwerkkosten um 50 %
- **Sichert die Konnektivität der User**, verarbeitet 400 TB Daten und verhindert vierteljährlich 98 Millionen Richtlinienverstöße

Zscaler stellt eine Sicherheitslösung bereit, die unsere Prozesse vereinfacht und uns durch diese Vereinfachung deutlich effektiver schützt.

Kier Morrison
General Manager, IT Technology Operations, John Holland

Kundenreferenz anzeigen

Probe CX stellt zum Schutz von 7.600 Mitarbeitern und kritischen Apps schrittweise von VPNs auf die Zero Trust Exchange

Zscaler rationalisiert den Sicherheits-Stack, vereinfacht die Richtlinienverwaltung und reduziert die Technologieausgaben ohne Abstriche an der Sicherheit

PROBE CX: KURZPORTRÄT

Einer der größten Anbieter für externe Kundendienst- und Geschäftsprozesse in Australien

Services

Australien: Melbourne (Victoria)

19.000 Mitarbeiter, 32 Standorte

100 %

VPNs überflüssig gemacht

8,1 Mrd.

In einem Quartal abgewickelte Transaktionen

3,1 Mio.

blockierte Bedrohungen in drei Monaten

Herausforderungen

- Eine traditionelle Sicherheitsarchitektur konnte mit der schnell wachsenden Belegschaft und dem zunehmenden Übergang zu einem Cloud-First-Ansatz nicht skaliert werden.
- Legacy-VPNs ermöglichten keine mikrosegmentierten Zugriffskontrollrichtlinien, wodurch private Unternehmensanwendungen einem höheren Risiko ausgesetzt waren.
- Die eingeschränkte Transparenz hinsichtlich User Experience und Anwendungsleistung erschwerte die Problembehebung und erhöhte den Zeitaufwand.

Schritte der Transformation

1. **Direktverbindungen zum Internet und zu SaaS-Anwendungen**, mit Inline-Überprüfung des Traffics ohne Backhauling
2. **Umstellung von VPNs auf Zero-Trust-Zugriff für private Unternehmensanwendungen,** um geistiges Eigentum und kritische Daten besser zu schützen
3. **Erweitertes Digital Experience Monitoring,** um Probleme schneller zu lösen und nahtlose Remote-Arbeit zu ermöglichen

Ergebnisse

- **Flexibler Remotezugriff auf Zero-Trust-Basis** für 7.600 User in fünf Ländern
- **Verarbeitet etwa 285 TB Datenverkehr pro Quartal**, setzt einheitliche Sicherheitsrichtlinien durch und minimiert die Angriffsfläche
- **Vereinfacht das Sicherheitsmanagement mit einer mandantenfähigen Plattform**, die Zero-Trust-Sicherheit bei geringeren Gesamtbetriebskosten bietet

Zu den wichtigsten Vorteilen, die wir durch die Implementierung dieser Technologie erzielt haben, gehört der komplette Verzicht auf VPNs in unserer Umgebung.

Rohan Khanna
Chief Technology Officer, Probe CX

Kundenreferenz anzeigen

Persistent

Persistent erhöht die Sicherheit und spart Kosten in Höhe von 2 Mio. USD im Jahresvergleich

Zero Trust schützt vertrauliche Kunden- und IP-Daten, ermöglicht Innovation, reduziert Komplexität und unterstützt ESG-Ziele

PERSISTENT: KURZPORTRÄT

Globaler Partner für digitales Engineering und Unternehmensmodernisierung, der Unternehmen bei der Realisierung von Innovationen unterstützt

Hightech

Pune, Indien

23.000 Mitarbeiter in 21 Ländern

85 %

Verbesserung des Sicherheitsstatus durch Verzicht auf VPN

>80

Angriffe mit hohem Schweregrad wurden in 90 Tagen durch Deception abgefangen

4 x

schnellerer Zugriff auf private Unterneh-mensanwendungen als mit VPN

Herausforderungen

- Gewährleistet schnelle Konnektivität und mehr Produktivität für Remote-Mitarbeiter in 21 Ländern
- Schutz geistigen Eigentums und vertraulicher Kundendaten in der gesamten Cloud-Umgebung
- Vereinfachung einer komplexen Infrastruktur
- Reduzierung der Hardware- und Betriebskosten in der gesamten Umgebung
- Suche nach einem langfristigen Zero-Trust-Partner mit einer skalierbaren Lösung, die eine schnelle Expansion ermöglicht
- Minimierung der Umweltbelastung durch Verbesserung der CO2-Bilanz

Schritte der Transformation

1. **Verbesserter Sicherheitsstatus** durch sichere Direktverbindungen zum Internet, zu SaaS und privaten Unternehmensanwendungen
2. **Weniger Latenz, geringere Kosten und verbesserte User Experience** durch die Beseitigung unzuverlässiger, unsicherer VPNs und Firewalls
3. **Schutz von wertvollem geistigen Eigentum und Kundendaten durch fortschrittliche Data** Loss Prevention und Deception-Technologie

Ergebnisse

- **Verbessert und beschleunigt den Remotezugriff** um das Vierfache für 23.000 weltweit verteilte Mitarbeiter
- **Reduziert die Komplexität** und verbessert die Wirksamkeit und Effizienz der Sicherheitsinfrastruktur
- **Beschleunigte Erkennung und Reaktion** durch Integration mit CrowdStrike, Microsoft Entra ID und Securonix
- **Erweitert das Angebotsportfolio des Unternehmens** für die eigenen Kunden

Zscaler DLP gibt dem Sicherheitsteam einen detaillierten Einblick in die Schattennutzung von generativen KI-Anwendungen, einschließlich Prompts, und erzwingt DLP-Blockierung und Anwendungsisolierung in Echtzeit.

Debashis Singh
Chief Information Officer, Persistent

Kundenreferenz anzeigen

社会医療法人財団董仙会
恵寿総合病院
Keiju Medical Center

Keiju transformiert die digitale Patientenversorgung mit der Zscaler Zero Trust Exchange

Zscaler bietet eine Lösung für den sicheren mobilen Zugriff auf EMR-Daten, ermöglicht Ärzten die ortsunabhängige Zusammenarbeit und verbessert die User Experience für Patienten

MEDIZIN. ZENTRUM KEIJU: KURZPORTRÄT

Einziges Krankenhaus zur medizinischen Unterstützung in der Region Noto, anerkannt als digitaler Marktführer

Gesundheitswesen und Pharma

Japan: Nanao (Präfektur Ishikawa)

Über 800 Mitarbeiter für über 400 Betten

800
medizinisches Personal geschützt

Hunderte
von Mobilgeräten sicher verbunden

Eine
Plattform für Zero-Trust-Sicherheit

Herausforderungen

- Eine Perimeter-Sicherheitsarchitektur konnte sich nicht an den steigenden Bedarf an digitaler Patientenversorgung und Telemedizin anpassen.
- Herkömmliche Firewalls konnten keine Remote-Internetverbindung sichern, sodass die Anwerbung von Ärzten auf einen kleinen lokalen Bereich beschränkt war.
- Herkömmliche VPNs setzen private Unternehmensanwendungen und Ressourcen, einschließlich vertraulicher Patientendaten, einem höheren Risiko einer Kompromittierung aus.

Schritte der Transformation

1. **Implementierung einer Cloud-nativen Zero-Trust-Sicherheits-architektur** zur Unterstützung alternativer Möglichkeiten der digitalen Patientenversorgung
2. **Einführung einer sicheren Direktverbindung zum Internet**, die es dem medizinischen Personal ermöglicht, flexibel und sicher von jedem Standort aus zu arbeiten
3. **Umstellung von VPN-Appliances auf Zero-Trust-Zugriff** für private Unternehmensanwendungen zum Schutz des Remotezugriffs auf EMR-Daten

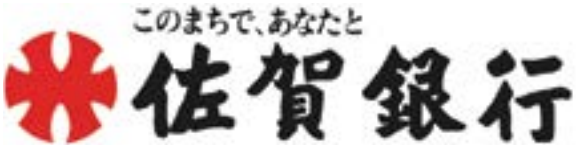
Ergebnisse

- **Ermöglicht dem medizinischen Personal die Flexibilität, von jedem beliebigen Standort aus zu arbeiten,** und erweitert die Möglichkeiten für die Anwerbung qualifizierter Ärzte
- **Schützt vertrauliche Patientendaten vor Bedrohungen** beim Remotezugriff — über 500 Mobilgeräte stellen sichere Verbindungen zu EMR-Daten her
- **Macht herkömmliche Sicherheitsgeräte überflüssig** und verbessert die Betriebseffizienz, was zu einer besseren Patientenversorgung führt

Damit die Mitarbeiter auch mit begrenzten Ressourcen effizient arbeiten können, ist eine digitale Transformation unabdingbar. Viele Ärzte wohnen weiter entfernt … deshalb brauchten wir eine sichere und userfreundliche Umgebung für den Fernzugriff.

Masahiro Kamino
Vorsitzender des Verwaltungsrats,
Medizinisches Zentrum Keiju

Kundenreferenz anzeigen



Die Bank of Saga unterstützt die digitale Transformation mit der Zscaler Zero Trust Exchange

Zscaler rationalisiert die Infrastruktur, reduziert die Abhängigkeit von Legacy-Lösungen und stärkt den Sicherheitsstatus bei der Migration des Bankbetriebs in die Cloud

THE BANK OF SAGA: KURZPORTRÄT

Gemeinschaftsorientierter Finanzdienstleister arbeitet an der Verbesserung des Kundenkomforts

- Finanzdienstleistungen und Versicherungen
- Japan: Saga (Präfektur Saga)
- >1.200 Mitarbeiter

ca. 33 %
geringere Kommunikationskosten

1.800
geschützte User mit Zero Trust

Ein
Single Sign-On steigert die Produktivität

Herausforderungen

- Eine herkömmliche perimeterbasierte Sicherheitsarchitektur könnte die fortlaufenden Cloud-Migrationsmaßnahmen der Bank nicht unterstützen.
- Älteren Sicherheits-Appliances fehlte die nötige Flexibilität, um der steigenden Nachfrage nach direkten und zuverlässigen Internetverbindungen gerecht zu werden.
- VPNs verursachten hohe Wartungskosten und vergrößerten die Angriffsfläche, wodurch private Unternehmensanwendungen und -daten anfällig für Bedrohungen waren.

Schritte der Transformation

1. **Bereitstellung einer Cloud-nativen, umfassenden Zero-Trust-Plattform** zur unternehmensweiten Durchsetzung einheitlicher Sicherheitsrichtlinien
2. **Umstellung auf direkte Internetverbindungen** und Inline-Trafficprüfung zur Sicherung des Zugriffs auf öffentliche SaaS-Apps
3. **Umstellung von VPNs auf Zero-Trust-Zugriff für private Unternehmens-anwendungen** und granulare Konfigurationsoptionen zum Schutz kritischer Daten

Ergebnisse

- **Sichere aus- und eingehende Verbindungen der Mitarbeiter** mit einheitlichen Zugriffsrichtlinien unabhängig vom Standort
- **Schützt Private-Banking-Anwendungen und kritische Daten vor Kompromittierung**und sichert und verbessert so das Kundenerlebnis
- **Optimiert den Sicherheits-Stack und ersetzt Legacy-Appliances**, vereinfacht die Richtlinienverwaltung und senkt die Kosten

Für die digitale Transformation ist eine Verlagerung in die Cloud notwendig. ... Mit herkömmlicher perimeterbasierter Sicherheit kann das Potenzial von SaaS- und Webdiensten jedoch nicht vollständig erschlossen werden. Die Umstellung auf Zero-Trust-Sicherheit war unerlässlich.

Mr. Hiroaki Hayashida
Stellvertretender Direktor, Systems Planning and Development Group, Systems Department, Business Management Headquarters, The Bank of Saga

Kundenreferenz anzeigen

Cebu Pacific Air vertraut zum Schutz der hybriden Belegschaft auf die Zscaler Zero Trust Exchange

Zscaler verbessert das Remote-Arbeitserlebnis für 3.900 Mitarbeiter und schützt kritische Geschäftsabläufe an sieben strategischen Standorten in Asien

CEBU PACIFIC AIR: KURZPORTRÄT

Führende Fluggesellschaft auf den Philippinen mit Flügen zu mehr als 60 Zielen

- Transportdienstleistungen
- Philippinen: Metro Manila
- 3.900 Mitarbeiter an sieben strategischen Standorten

234 Millionen

vierteljährlich verhinderte Richtlinienverstöße

90 %

Steigerung der Userzufriedenheit

2

Wochen zur Bereitstellung von Remote-Anwendungszugriff mit Zero Trust

Herausforderungen

- Eine veraltete Sicherheitsinfrastruktur verlangsamte die digitale Transformation und erhöhte das Risiko von Kompromittierungen und Bedrohungen.
- Herkömmliche Sicherheits-Appliances konnten die geschäftskritischen privaten Unternehmensressourcen nicht ausreichend schützen.
- VPN-Appliances hatten mit Performance- und Verbindungsproblemen zu kämpfen, was die Remotearbeit erschwerte und weniger sicher machte.

Schritte der Transformation

1. **Umstellung von einer Legacy-Sicherheitsarchitektur** auf eine umfassende, Cloud-native Zero-Trust-Plattform
2. **Bereitstellung eines sicheren, direkten Internetzugangs mit Advanced Threat Protection** zur besseren Unterstützung einer hybriden Belegschaft
3. **Umstellung von VPN-Appliances auf Zero-Trust-Zugriff,** um granulare Zugriffskontrollen für private Unternehmensanwendungen durchzusetzen

Ergebnisse

- **Sichert die ortsunabhängige Arbeitskonnektivität für 3.900 User mit einer sicheren VPN-Alternative**und verbessert die Userzufriedenheit um 90 %
- **Optimiert den Sicherheits-Stack und bietet robusten Schutz**— verarbeitet 733 Millionen Transaktionen pro Jahr
- **Verhindert 234 Millionen Richtlinienverstöße und blockiert 45.000 Sicherheitsbedrohungen in einem einzigen Quartal** und verbessert so den Sicherheitsstatus

Unsere Arbeitsumgebung ist dynamisch, und mit Zscaler können Mitarbeiter weiterhin produktiv arbeiten, ohne dass der Zugriff auf die benötigten Ressourcen beeinträchtigt oder die Sicherheit gefährdet wird.

Laureen Cansana
CIO, Cebu Pacific Air

Kundenreferenz anzeigen

maxeon

Maxeon Solar Technologies schließt mit Zscaler erfolgreich die digital Transformation nach einer Veräußerung ab

Führender Solarenergieanbieter stellt von Rechenzentren auf die Zero Trust Exchange um, um den Sicherheitsstatus und das Remote-Arbeitserlebnis für 5.000 globale User zu verbessern

MAXEON: KURZPORTRÄT

Führender globaler Hersteller von Solarmodulen mit Vertriebspräsenz in über 100 Ländern

Energie, Öl, Gas & Bergbau

Singapur

5.000 Mitarbeiter an 40 Standorten

134 %

mehr Traffic vierteljährlich abgewickelt

31 Mio.

Richtlinienverstöße in einem Quartal verhindert

2,9 Mio.

Bedrohungen in drei Monaten blockiert

Herausforderungen

- Herkömmliche Perimetersicherheit mit physischen Rechenzentren könnte die zunehmende Umstellung auf eine Cloud-First-Infrastruktur nicht unterstützen.
- Legacy-Firewalls konnten mit den steigenden Anforderungen an den Fernzugriff nicht skaliert werden, was zu schlechter Performance und einem höheren Risiko führte.
- Die bisherigen DLP-Lösungen waren schwierig zu verwalten und bargen das Risiko einer Kompromittierung von kritischem geistigen Eigentum und wichtigen IT-Assets

Schritte der Transformation

1. **Sichere Direktverbindungen zum Internet mit Inline-Verkehrsprüfung** zum Schutz der User überall dort, wo sie Online-Zugriff benötigen
2. **Implementierung einer speziell für Zero Trust entwickelten Experience-Monitoring-Lösung** zur Optimierung der Onboarding- und Lizenzierungsabläufe
3. **Einführung einer integrierten DLP-Lösung** zum Schutz kritischer Daten, zur Gewährleistung der Compliance und zur Verhinderung von Datenlecks

Ergebnisse

- **Beschleunigte digitale Transformation**— alle Rechenzentren wurden stillgelegt und 70 % der Workloads wurden in die Cloud migriert
- **Sicherer Remote-Zugriff** für eine geografisch verteilte Belegschaft in 16 Ländern
- **Schützt unternehmenskritische IP-Daten, darunter über 1.400 Patente**, verbessert den Sicherheitsstatus und gewährleistet die Geschäftskontinuität

Bei der Bewertung mehrerer namhafter Anbieter ist Zscaler aufgrund der Führungsposition im Gartner Magic Quadrant und seiner nachgewiesenen Fähigkeiten als klarer Sieger hervorgegangen.

Stephen Gani
CISO, Maxeon Solar Technologies

Kundenreferenz anzeigen