I Percorsi dei Clienti

Approfondisci le storie vere sulla trasformazione ottenuta con lo zero trust e l'AI di Zscaler.

Scopri il modo in cui le aziende sono riuscite a migliorare il proprio profilo di sicurezza, favorire un'esperienza utente d'eccellenza, semplificare fusioni e acquisizioni e altro grazie allo zero trust con AI.

L'orientamento al cliente è uno dei valori fondamentali di Zscaler, ed è per questo che ci impegniamo a fornire il meglio dell'innovazione zero trust per aiutare le organizzazioni a raggiungere i propri obiettivi. Grazie alle funzionalità di Zero Trust Exchange, la nostra piattaforma basata sull'AI, abbiamo aiutato oltre 5.000 aziende in tutto il mondo ad abbattere i costi e a ridurre la complessità, semplificare le loro architetture di rete, proteggere i propri utenti e difendersi da minacce informatiche in continua evoluzione. In questo e-book, approfondirai i casi di studio di alcune delle organizzazioni di maggior successo al mondo e scoprirai il modo in cui sono riuscite a trasformare reti, sicurezza e operazioni insieme a Zscaler.

In quanto azienda pioniera del modello zero trust e con 15 anni di esperienza nel settore, Zscaler continua a impegnarsi per aiutare le organizzazioni di ogni dimensione e settore a raggiungere e superare i propri obiettivi zero trust. L'unica costante che conosciamo nella tecnologia è il "cambiamento" e, grazie alla nostra piattaforma Zero Trust Exchange, le aziende possono prepararsi ad affrontare qualsiasi situazione, continuando nel contempo a innovare e trasformare la propria infrastruttura IT.

Mike Rich
CRO e President of Global Sales

©2025 Zscaler, Inc. Tutti i diritti riservati.

Contenuti

Esplora le storie di successo dei clienti suddivise per settore

01 Edilizia

58 John Holland

02 Istruzione

28 Dipartimento dell'Istruzione di New York

03 Energia, petrolio, gas ed estrazione mineraria

70 Maxeon
30 Southwest Gas

04 Intrattenimento e ospitalità

22 MGM Resorts International

05 Federale e governativo

14 Pubblica amministrazione di D.C.
38 Capitale di Stato Magdeburgo

06
Servizi finanziari e assicurazioni

44 Capitec
20 Guaranteed Rate
24 Mercury Financial
36 Raiffeisen Bank International
66 The Bank of Saga

07
Settore alimentare, bevande e tabacco

26 Molson Coors

08
Settore sanitario e farmaceutico

8 AMN Healthcare
64 Keiju Medical Center
48 Sanitas

09
High Tech

16 DMI
62 Persistent Systems
52 Primetals Technologies

10
Settore manifatturiero

18 Eaton
42 Hydro
54 Unilever

11
Vendita al dettaglio e all'ingrosso

12 Cox Automotive
40 Cisalfa Sports

12
Servizi

60 Probe CX

13
Telecomunicazioni

10 ATN International
50 Colt

14
Servizi di trasporto

68 Cebu Pacific Air
46 Noatum
32 United Airlines

©2025 Zscaler, Inc. Tutti i diritti riservati.

AMS

Esplora le storie di successo dei clienti suddivise per area geografica

8 AMN Healthcare

10 ATN International

12 Cox Automotive

14 Pubblica amministrazione di D.C.

16 DMI

18 Eaton

20 Guaranteed Rate

22 MGM Resorts International

24 Mercury Financial

26 Molson Coors

28 Dipartimento dell'Istruzione di New York

30 Southwest Gas

32 United Airlines

©2025 Zscaler, Inc. Tutti i diritti riservati.

AMN Healthcare protegge gli utenti e i dati a livello globale con Zscaler Zero Trust Exchange

Zscaler protegge i modelli di lavoro da remoto offrendo esperienze ottimali a più di 5.000 utenti e tutela i dati dei pazienti dalle crescenti minacce informatiche che prendono di mira il settore sanitario

PANORAMICA SU AMN HEALTHCARE

Fornisce al personale sanitario soluzioni per migliorare i risultati dei pazienti

- Settore sanitario e farmaceutico
- Dallas, Texas, Stati Uniti
- Oltre 10.000 clienti in 24 sedi

1,2 MLD
transazioni web elaborate ogni mese

7 MLN
di minacce bloccate in tre mesi

Ore
per estendere la sicurezza all'edge ovunque

Sfide

- Un'infrastruttura di sicurezza legacy non era più compatibile con l'ecosistema operativo incentrato sul cloud in continua evoluzione dell'azienda
- Le VPN tradizionali non erano in grado di supportare le crescenti esigenze dell'accesso remoto e rendevano le risorse private ancora più vulnerabili alle minacce informatiche
- Un'architettura di sicurezza complessa, con soluzioni non integrate, limitava la visibilità e rendeva più complessa la risoluzione dei problemi.

Un percorso in fasi

1. **Ha implementato un accesso sicuro e diretto a Internet** per permettere a una forza lavoro distribuita a livello globale di lavorare in modo flessibile da qualsiasi luogo
2. **Ha introdotto l'accesso microsegmentato e zero trust alle applicazioni private** per sostituire in modo sicuro le VPN legacy
3. **Ha semplificato un set di soluzioni di monitoraggio e usufruito della visibilità completa end-to-end** per migliorare la risoluzione dei problemi degli utenti

Risultati

- **Protegge la connettività in uscita e in entrata di oltre 5.000 utenti**, migliorando le capacità e l'efficienza del lavoro da remoto a livello globale
- **Applica policy di accesso zero trust alle applicazioni private e ai prodotti digitali** utilizzati da oltre 10.000 clienti in tutto il mondo
- **Semplifica l'architettura e riduce i costi per la tecnologia** al fine di rafforzare il profilo di sicurezza abbattendo le spese generali

L'approccio di Zscaler è in linea con la nostra strategia zero trust complessiva, e la piattaforma Zero Trust Exchange rappresenta perfettamente la visione di architettura zero trust di AMN Healthcare.

Mani Masood
Head of Information Security,
AMN Healthcare

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

ATN International protegge le operazioni e migliora l'efficienza con Zscaler Zero Trust Exchange

Zscaler consente a più di 2.500 dipendenti di lavorare da remoto in modo ancora più efficiente, elimina i problemi degli utenti legati alla VPN e migliora la sicurezza delle operazioni di integrazione e onboarding durante fusioni e acquisizioni

PANORAMICA SU ATN INTERNATIONAL

Fornisce infrastrutture e servizi di comunicazione con competenza nei mercati in remoto

Telecomunicazioni

Beverly, Massachusetts, Stati Uniti

750.000 clienti a livello internazionale

100%

delle VPN eliminate e dei relativi ticket di assistenza

Tutti

i dipendenti protetti con Zscaler

Minuti

invece di ore per la mitigazione dei problemi degli utenti

Sfide

- L'infrastruttura di sicurezza on-premise non poteva supportare in modo efficiente le operazioni aziendali con base cloud o gli obiettivi futuri relativi a fusioni e acquisizioni.
- I dispositivi VPN legacy avevano difficoltà a supportare l'espansione del lavoro remoto, con un conseguente impatto negativo sulle esperienze utente e i rischi
- Le soluzioni di sicurezza tradizionali non offrivano le integrazioni cloud critiche per consentire la mitigazione proattiva dei problemi degli utenti

Un percorso in fasi

1. **Ha fornito un accesso diretto a Internet,** con funzionalità di ispezione e logging del traffico per prevenire le violazioni delle policy
2. **Ha sostituito i dispositivi VPN implementando un accesso zero trust a privilegi minimi** ad applicazioni e risorse private
3. **Ha sfruttato le funzionalità di Zscaler basate sull'AI e l'integrazione avanzata con Microsoft** per identificare e risolvere più rapidamente i problemi degli utenti

Risultati

- **Migliora l'esperienza di lavoro da remoto di oltre 2.500 utenti** ed elimina i problemi degli utenti relativi alle VPN, abbattendo del 100% il numero di ticket dell'assistenza
- **Accelera i tempi relativi a fusioni e acquisizioni e garantisce un onboarding più sicuro** per le aziende acquisite con un'architettura di sicurezza zero trust
- **Riduce a una manciata di minuti il tempo necessario per identificare e risolvere i problemi** grazie a funzionalità affidabili di reportistica e monitoraggio

Quando valuto infrastrutture e strumenti di sicurezza, cerco soluzioni che migliorino sia l'efficienza operativa che la protezione. Zscaler è la risposta a entrambe queste esigenze.

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

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Cox Automotive adotta lo zero trust attraverso un'implementazione a fasi grazie a Zscaler Zero Trust Exchange

Zscaler semplifica l'architettura di sicurezza, protegge la connettività degli utenti in cinque continenti e tutela i dati di milioni di acquirendi di auto online

PANORAMICA SU COX AUTOMOTIVE

Il più grande fornitore al mondo di servizi e tecnologie automobilistiche

- Vendita al dettaglio e all'ingrosso
- Atlanta, Georgia, Stati Uniti
- 2,3 miliardi di interazioni online all'anno

Oltre 30.000
membri del team protetti

40.000
clienti dei concessionari supportati

1
piattaforma unica che riduce la complessità

Sfide

- L'azienda era alla ricerca di una piattaforma compatibile con il cloud che potesse fare da base per un'architettura di sicurezza zero trust olistica
- I tradizionali dispositivi firewall risultavano inefficienti per l'ispezione del traffico Internet su larga scala per un gruppo di utenti distribuito in tutto il mondo
- Le VPN legacy non supportavano le policy di controllo degli accessi basate sull'identità, esponendo le applicazioni e i dati privati a un rischio maggiore

Un percorso in fasi

1. **Ha distribuito una piattaforma nativa del cloud, multitenant e zero trust** creata appositamente per integrarsi facilmente con altre soluzioni cloud
2. **Ha fornito una connettività sicura e diretta a Internet e alle app SaaS** con capacità di ispezione inline del traffico
3. **Ha sostituito le VPN con un accesso zero trust** per stabilire policy di sicurezza microsegmentate e a privilegi minimi per le app private

Risultati

- **Protegge un team che lavora in cinque continenti,** consentendogli di operare in modo flessibile da qualsiasi luogo e migliorando le esperienze degli utenti
- **Protegge le app e le risorse private critiche**, inclusi i dati di milioni di clienti, in modo più conveniente
- **Sostituisce le soluzioni di sicurezza legacy, inclusi firewall e VPN,** per semplificare i processi IT e accelerare l'onboarding in ambito di fusioni e acquisizioni

Una volta installati gli agenti sui dispositivi di tutti, sarà molto semplice integrare altre funzionalità di Zscaler nella nostra architettura. Ci basterà semplicemente attivarle.

Jon Mahes
Sr. Manager, Cybersecurity,
Cox Automotive

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

La pubblica amministrazione del Distretto della Columbia consolida la sicurezza implementando Zscaler Zero Trust Exchange

Zscaler sostituisce i dispositivi VPN legacy per semplificare l'architettura di sicurezza, rafforzare la consapevolezza sui rischi in tempo reale e proteggere 15.000 utenti

PANORAMICA SULLA PUBBLICA AMMINISTRAZIONE DI D.C.

Supervisiona e gestisce tutti i servizi essenziali per i residenti del Distretto di Columbia

Federale e governativo

Washington, D.C., USA

Oltre 15.000 dipendenti

15.000
dipendenti pubblici protetti

~3 MLD
transazioni elaborate ogni mese

Oltre 200.000
di minacce alla sicurezza bloccate al mese

Sfide

- Un'infrastruttura di sicurezza obsoleta non era in grado di supportare il lavoro da remoto e contribuiva a generare inefficienze operative
- I dispositivi VPN tradizionali avevano esteso la rete aziendale ai dispositivi degli utenti finali, esponendo i dati sensibili al rischio di subire compromissioni
- I prodotti di sicurezza legacy limitavano la visibilità sulle minacce, rendendo più difficile la valutazione e la mitigazione dei rischi

Un percorso in fasi

1. **Ha fornito una connettività sicura e diretta a Internet e alle applicazioni SaaS**, consentendo di lavorare in modo flessibile da qualsiasi luogo
2. **Ha sostituito le VPN legacy con un accesso zero trust microsegmentato** per applicare policy di sicurezza uniformi alle risorse private
3. **Ha usato dati e approfondimenti basati sull'AI per rafforzare la consapevolezza sui rischi** e mitigare le potenziali minacce in tempo reale e su larga scala

Risultati

- **L'architettura zero trust migliora il profilo di sicurezza** elaborando circa 3 miliardi di transazioni e bloccando oltre 200.000 minacce ogni mese
- **Migliora l'esperienza utente da remoto di 15.000 utenti** e si integra in modo ottimale con le soluzioni di identità esistenti
- **L'azienda può concentrarsi in modo più approfondito sulla gestione del rischio,** con una migliore comprensione dei fattori di rischio e del profilo di sicurezza

La partnership con Zscaler si è rivelata essenziale per noi. Siamo riusciti a implementare la piattaforma a velocità record, integrando gli utenti in modo più efficace e migliorando la loro esperienza.

Suneel Cherukuri
CISO, Pubblica amministrazione di D.C.

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

DMI consente l'uso dei dispositivi personali su larga scala, migliora la protezione dei dati e ottiene considerevoli risparmi sui costi

Zscaler fornisce una connettività zero trust all'intera forza lavoro e consente ai dipendenti di operare in modo sicuro dal dispositivo che preferiscono

PANORAMICA SU DMI

DMI è un fornitore di servizi digitali leader a livello mondiale che opera tra il settore pubblico e quello privato

High Tech

McLean, Virginia, Stati Uniti

Oltre 2.100 dipendenti in 80 Paesi

Oltre 700.000 $
di risparmi annui

>2
settimane per la distribuzione

3%
di maggiore rapidità degli SLA dopo l'implementazione

Sfide

- L'installazione di nuovo hardware in un ambiente legacy introduceva periodi di inattività, obbligava a finestre di interruzione e richiedeva aggiornamenti periodici
- Richiedere agli utenti di lavorare dai dispositivi di DMI rendeva questi ultimi meno produttivi e aveva un impatto negativo sull'impronta di carbonio globale dell'organizzazione

Un percorso in fasi

1. **Ha protetto l'accesso a Internet e implementato una vera connettività zero trust** per dipendenti, collaboratori e terze parti senza lunghe configurazioni manuali dei dispositivi
2. **È stato consentito l'uso dei dispositivi personali, o BYOD (Bring Your Own Device) grazie all'isolamento del browser,** che ha permesso ai dipendenti di lavorare dai dispositivi che preferiscono

Risultati

- **Distribuisce lo zero trust in 2 settimane** senza alcun impatto sugli utenti e senza periodi di inattività
- **Risparmia 700.000 $ all'anno,** migliora le esperienze di onboarding e offboarding e riduce le tempistiche per la configurazione di nuovi uffici e dispositivi

Grazie al progetto BYOD siamo riusciti a risparmiare evitando di dover acquistare computer portatili per le persone che non ne avevano bisogno. Questo ha consentito a DMI di ottenere un risparmio annuo di oltre 700.000 dollari: una cifra enorme!

Mauricio Mendoza
Vice President, Global IT and Security, DMI

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Eaton protegge le operazioni globali con la segmentazione basata sull'AI

Zscaler aiuta i produttori globali a passare al cloud implementando una protezione avanzata dalle minacce, riducendo i rischi di subire violazioni e potenziando la visibilità tramite le integrazioni con i partner

PANORAMICA SU EATON

Produttore globale di apparecchiature elettriche per l'industria aerospaziale e altri settori

Settore manifatturiero

Cleveland, Ohio, Stati Uniti

Oltre 90.000 dipendenti e utenti in 170 Paesi in tutto il mondo

4 MLN

di minacce bloccate in un mese

90.000

dipendenti in tutto il mondo che si collegano a Internet e alle app private tramite lo zero trust

Diversi

partner dell'alleanza strategica che si integrano in modo ottimale

Sfide

- Le VPN e i firewall legacy ostacolavano la crescita e si sono rivelati inefficienti nel supportare gli oltre 30.000 dipendenti degli stabilimenti produttivi durante la pandemia e oltre
- L'architettura di sicurezza tradizionale, basata sul perimetro, era incompatibile con la strategia cloud dell'azienda e con le sue esigenze di segmentazione
- La mancanza di visibilità limitava l'identificazione delle minacce e rallentava i tempi di risoluzione

Un percorso in fasi

1. **Ha sostituito** gli strumenti per la sicurezza e l'accesso con una connettività zero trust a Internet e alle app private
2. **Ha adottato le innovazioni AI** per individuare e combattere le relative minacce e fornire una segmentazione per gli stabilimenti produttivi
3. **Ha potenziato la consapevolezza sugli attacchi** con azioni preventive e predittive di rilevamento e risposta alle violazioni

Risultati

- **Fornisce un'esperienza utente più sicura, affidabile e regolamentata** a dipendenti e terze parti
- **Sfrutta la potenza dell'AI per il rilevamento delle minacce**, la prevenzione della perdita dei dati, la correzione, la visibilità sull'utilizzo di ChatGPT e la segmentazione delle applicazioni
- **Rafforza il controllo degli accessi** tramite la segmentazione zero trust e l'integrazione con strumenti di EDR, CDR ed NDR

Zscaler è facile da usare, e le sue funzionalità sono integrate in un unico agente di endpoint. Siamo stati in grado di implementare rapidamente Zscaler nel nostro ambiente globale e di estenderne le funzionalità impiegando pochissime risorse.

Jason Koler
CISO, Eaton Corporation

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Guaranteed Rate blocca milioni di minacce e accelera l'integrazione di fusioni e acquisizioni da mesi a giorni

Zscaler sostituisce l'hardware di sicurezza, potenzia la resilienza, offre una sicurezza sempre attiva e riduce la superficie di attacco

PANORAMICA GUARANTEED RATE

Il secondo operatore più grande nel settore dei mutui residenziali negli Stati Uniti, con più di 500 filiali presenti in tutti i 50 Stati

Servizi finanziari e assicurativi

Chicago, Illinois, Stati Uniti

Oltre 6000 dipendenti

97%
di traffico cifrato ispezionato

2,5 milioni
minacce bloccate in 3 mesi

2–3x
accesso più rapido alle app

Sfide

- L'utilizzo delle VPN per connettersi a centinaia di app private in locale e su AWS estendeva la superficie di attacco
- Il backhauling del traffico da oltre 500 filiali al data center ostacolava le prestazioni e la produttività
- Il firewall legacy non era in grado di rilevare le minacce 0-day che entravano nella rete attraverso Internet e si muovevano lateralmente

Un percorso in fasi

1. **Ha reso sicuro l'accesso a Internet e SaaS dal cloud**, eliminando il backhauling da oltre 500 filiali
2. **Ha sostituito le VPN** offrendo agli utenti un accesso rapido e affidabile a oltre 500 app private nel data center e sul cloud
3. **Ha ottimizzato l'esperienza utente** identificando e risolvendo i problemi prestazionali in modo più rapido ed efficiente

Risultati

- **Riduce al minimo la superficie di attacco**, offre agli utenti un accesso diretto e a privilegi minimi e potenzia le attività di rilevamento e risposta
- **Riduce il rischio di subire compromissioni**, con il monitoraggio TLS/SSL inline del traffico e la protezione dalle minacce avanzate basata sull'AI
- **Impedisce il movimento laterale** attraverso la tecnologia di deception, per allontanare gli aggressori dalle risorse sensibili e contenere le minacce in tempo reale

Grazie a Risk360, siamo in grado di ottenere la massima visibilità sui punti ciechi che aumentano il rischio informatico. Questa visibilità ci consente di investire il nostro tempo in modo più oculato, così da riuscire ad affrontare e ridurre i rischi informatici più urgenti.

Darin Hurd
CISO presso Guaranteed Rate

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

MGM Resorts International continua a investire su un'architettura zero trust nativa del cloud

Zscaler ci ha portato un Time to value impareggiabile, offrendoci una segmentazione zero trust, la protezione dalla perdita di dati e informazioni utili e concrete da tutta l'azienda

PANORAMICA SU MGM RESORTS INTERNATIONAL

Leader nel settore del gioco, dell'intrattenimento e dell'ospitalità che conta 31 resort in tutto il mondo

Intrattenimento e ospitalità

Las Vegas, Nevada, Stati Uniti

70.000 dipendenti in tutto il mondo

1° giorno
valore immediato dalla piattaforma

Oltre 275.000
minacce bloccate ogni mese

50%
utilizzo più efficiente dei dispositivi da parte del personale

Sfide

- La sicurezza basata sul modello “Castle and moat” aumentava il rischio associato al movimento laterale, in quanto concedeva agli utenti un ampio accesso alla rete
- I gateway VPN tradizionali creavano colli di bottiglia nel traffico e portavano a un’esperienza utente scadente
- Gli strumenti di sicurezza legacy offrivano una visibilità limitata sulle attività di navigazione dell’intera base di utenti

Un percorso in fasi

1. **Ha sostituito le VPN e implementato la segmentazione zero trust** per tutta la forza lavoro
2. **Ha implementato rapidamente** una serie di soluzioni per l’accesso privato, l’esperienza digitale e la protezione dei dati
3. **Ha adottato la tecnologia di deception** per proteggersi dalla compromissione da parte degli aggressori attivi

Risultati

- **Migliora l’esperienza dei dipendenti** offrendo prestazioni e connettività più rapide in tutto l’ambiente
- **Rimane al passo con le minacce emergenti** con una soluzione DLP completa, l’accesso privato e la segmentazione zero trust
- **Rafforza il profilo di sicurezza aziendale** contribuendo ad accelerare il business con un approccio incentrato sul cloud

Abbiamo implementato la segmentazione zero trust per tutta la nostra forza lavoro in tempi record, e ora riusciamo a gestire la soluzione quotidianamente, garantendo una protezione dalla perdita dei dati e la massima visibilità sulle nostre applicazioni. Per noi sono state grandi vittorie ottenute in modo semplice e veloce.

Stephen Harrison
CISO, MGM Resorts International

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Mercury Financial migliora la sicurezza e l'efficienza con Zscaler Zero Trust Exchange

Zscaler offre integrazioni fluide e funzionalità di AI per consentire alla forza lavoro di operare da remoto in modo più sicuro e proteggere i dati finanziari sensibili dalle minacce

PANORAMICA SU MERCURY FINANCIAL

Una società di servizi finanziari non bancari che aiuta i clienti a creare e gestire il credito

Servizi finanziari e assicurativi

Austin, Texas, Stati Uniti

Oltre 500 dipendenti

100%

di esperienza ottimizzata per i lavoratori da remoto

76%

di riduzione dei ticket di supporto IT

Zero

periodi di inattività dovuti ai malware

Sfide

- Le soluzioni di sicurezza tradizionali non consentivano un'ispezione completa del traffico inline; questo inibiva il rilevamento e la prevenzione delle minacce
- Le VPN legacy erano incompatibili con le esigenze incentrate sul cloud di una forza lavoro distribuita e davano origine a esperienze utente scadenti
- I dati limitati sulle attività degli utenti e sul profilo di sicurezza dei dispositivi rendevano difficile la diagnosi e la risoluzione dei problemi per una forza lavoro in remoto

Un percorso in fasi

1. **Ha ottenuto una connettività sicura e diretta a Internet** utilizzando funzionalità di contenimento delle minacce basate sull'AI per prevenire la compromissione dei dati
2. **Ha sostituito le VPN con l'accesso zero trust microsegmentato** alle app private, per garantire connessioni in remoto controllate e sicure
3. **Ha impiegato integrazioni e informazioni più granulari sugli utenti**, per snellire le spese e il carico amministrativo senza aumentare i rischi

Risultati

- **Riduce la superficie di attacco**, con l'azzeramento dei periodi di inattività dovuti a malware o ransomware dopo la distribuzione di Zscaler
- **Limita il movimento laterale e riduce il raggio d'impatto** se una minaccia entra nel set di soluzioni di sicurezza, garantendo anche un ripristino più rapido
- **Le integrazioni con AWS, Crowdstrike e Okta semplificano l'infrastruttura di sicurezza** e rafforzano la conformità alle normative

Consideriamo Zscaler tra i leader di questo settore perché offre una soluzione completa che copre ogni aspetto dello zero trust. Per ottenere le stesse funzionalità che ci offre Zscaler, dovremmo implementare molte soluzioni distinte di fornitori diversi.

Arjun Thusu
CIO,
Mercury Financial

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Molson Coors offre un'esperienza utente ottimale grazie a Zscaler Zero Trust Exchange

Zscaler elimina la necessità di ricorrere ai dispositivi VPN, protegge la connettività per una forza lavoro globale e fornisce informazioni utili che consentono di risolvere i problemi più rapidamente

PANORAMICA SU MOLSON COORS

Terzo produttore di birra al mondo e innovatore globale nel settore del beverage

Alimentari, bevande e tabacco

Chicago, Illinois, Stati Uniti

Oltre 17.000 dipendenti
Oltre 42 birrifici

17.000
utenti protetti con lo zero trust

96%
maggiore rapidità di risoluzione dei problemi degli utenti

Milioni
di minacce bloccate ogni giorno

Sfide

- Le apparecchiature firewall non erano in grado di adattarsi alla domanda di accesso remoto a Internet e avevano difficoltà a ispezionare il traffico inline
- La mancanza di visibilità sulle attività degli utenti e sul profilo di sicurezza dei dispositivi rendeva difficile identificare e risolvere i problemi prestazionali
- Un'architettura di sicurezza legacy, basata su dispositivi VPN, creava un ambiente di rete piatto e una superficie di attacco più estesa

Un percorso in fasi

1. **Ha implementato un accesso diretto a Internet con funzionalità avanzate di rilevamento delle minacce** per proteggere gli utenti in remoto e le terze parti
2. **Ha utilizzato una visibilità end-to-end su utenti e dispositivi** per semplificare la gestione della sicurezza e risolvere più rapidamente i problemi degli utenti
3. **Ha sostituito le VPN tradizionali con un accesso zero trust alle applicazioni private** per proteggere le risorse e migliorare l'esperienza utente

Risultati

- **Garantisce un'esperienza utente ottimale ai dipendenti** che lavorano in 42 birrifici in tutto il mondo e ai partner terzi
- **Migliora il tempo medio di risoluzione dei problemi degli utenti**, individuandone le cause e automatizzandone la mitigazione nel giro di minuti, non ore
- **Blocca le minacce avanzate** ed elimina il movimento laterale per proteggere le applicazioni private e i dati aziendali sensibili

Le minacce intercettate da Zscaler sono costantemente nell'ordine delle centinaia di migliaia o addirittura milioni, a seconda della giornata. È una soluzione semplice e facile da usare. Basta poco per imparare a usarla, e non ci sono limitazioni.

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

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Il Dipartimento dell'Istruzione di New York City passa dalle VPN allo zero trust

Zscaler aiuta a proteggere l'accesso a Internet e alle applicazioni private per oltre 1 milione di utenti e più di 2 milioni di dispositivi

PANORAMICA SUL DIPARTIMENTO DELL'ISTRUZIONE DI NEW YORK

Il Dipartimento dell'Istruzione della Città di New York (NYC DOE) è il più grande sistema scolastico degli Stati Uniti e uno dei più grandi al mondo. Serve oltre 1 milione di studenti, dalla scuola materna agli istituti superiori, con uno staff di oltre 150.000 insegnanti e dirigenti in tutti e cinque i distretti di New York

Istruzione

New York City, New York, USA

Oltre 1 milione di utenti e più di 2 milioni di dispositivi

Oltre 2 MLN

di dispositivi di studenti e dipendenti protetti

15%

di diminuzione degli attacchi

40%

di minacce in più bloccate

Sfide

- L'infrastruttura legacy non era in grado di scalare per fornire esperienze sicure e uniformi a oltre 1 milione di utenti
- L'approccio tradizionale basato su VPN e firewall non risultava efficace nel bloccare le minacce informatiche avanzate
- La scarsa visibilità sugli endpoint rendeva difficile la manutenzione e il monitoraggio dei dispositivi per l'apprendimento da remoto del dipartimento

Un percorso in fasi

1. **Ha implementato un accesso sicuro a Internet e SaaS** con un'architettura proxy zero trust che ispeziona il 100% del traffico TLS/SSL su larga scala
2. **Ha sostituito le VPN con lo ZTNA (Zero Trust Network Access)** per offrire agli utenti una connettività veloce e senza interruzioni
3. **Ha migliorato la visibilità** su reti e dispositivi sfruttando il monitoraggio end-to-end dell'esperienza digitale

Risultati

- **Estende l'accesso rapido, affidabile e sicuro** alle applicazioni di apprendimento per studenti e dipendenti, ovunque e su qualsiasi dispositivo
- **Filtra il traffico in base al contenuto**, oltre al semplice blocco degli URL, per supportare la conformità al CIPA sui dispositivi di apprendimento
- **Migliora le prestazioni della rete** grazie all'individuazione e alla risoluzione dei problemi relativi a rete e DNS nell'ambiente

Penso che Zscaler sarà un buon partner per aiutarci a capire dove ci porterà l'impiego dell'AI e ad agire più rapidamente nella risposta agli incidenti e l'individuazione dei problemi.

Demond Waters
CISO, Dipartimento dell'Istruzione della Città di New York

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Southwest Gas usa Zscaler Zero Trust Exchange per offrire un'esperienza utente ottimizzata e sicura

Zscaler elimina la dipendenza dalle soluzioni di sicurezza legacy per offrire una connettività più rapida e affidabile a 2.300 dipendenti ibridi e 50 uffici sul campo

PANORAMICA SU SOUTHWEST GAS

Società che opera nel settore energetico, che fornisce gas naturale ad Arizona, Nevada e California.

Energia, petrolio, gas ed estrazione mineraria

Las Vegas, Nevada, Stati Uniti

2 milioni di clienti

4–6

settimane per la distribuzione completa dello zero trust

95%

di casi d'uso implementati con successo

1

piattaforma single-vendor per massimizzare la semplicità

Sfide

- Un'infrastruttura di sicurezza tradizionale non era in grado di adattarsi alla trasformazione cloud o al passaggio al lavoro ibrido
- Fornire una connettività a Internet veloce e affidabile agli uffici sul campo e ai dipendenti in remoto nelle aree rurali era una vera e propria sfida
- Le VPN legacy non consentivano l'impiego di policy di accesso basate sull'identità, e questo rendeva le app e i dati privati più vulnerabili alle minacce

Un percorso in fasi

1. **Ha implementato una piattaforma zero trust multitenant**, semplificando il set di soluzioni di sicurezza e ottimizzando gli ambienti di lavoro da remoto
2. **Ha implementato un accesso diretto a Internet e alle app SaaS** con una protezione costante contro le minacce, indipendentemente dalla posizione
3. **Ha sostituito le VPN con un accesso zero trust alle applicazioni private** per ridurre la superficie di attacco ed eliminare la perdita dei dati

Risultati

- **Consente a 2.300 dipendenti ibridi di lavorare in modo flessibile e sicuro da qualsiasi luogo** e protegge utenti e dati in 50 uffici sul campo
- **Consente l'uso di policy di controllo degli accessi microsegmentate e con privilegi minimi** per le applicazioni private, al fine di tutelare i dati critici
- **Accelera l'adozione dello zero trust**, elimina la complessità della gestione della sicurezza e riduce le richieste di supporto tecnico

Dopo un'attenta valutazione del valore aggiunto (Proof of Value), abbiamo scelto Zscaler grazie alla sua architettura innovativa, che ci ha consentito di migrare la sicurezza sul cloud e migliorare l'efficienza del lavoro da remoto.

David Petroski
Senior Infrastructure Architect,
Southwest Gas

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

United Airlines rileva e blocca le minacce in evoluzione con Zscaler Zero Trust Exchange

Zscaler elimina il 40% di minacce in più rispetto alle precedenti soluzioni legacy, proteggendo 80.000 utenti globali e offrendo viaggi più sicuri a 143 milioni di passeggeri

PANORAMICA SU UNITED AIRLINES

Compagnia aerea americana, terza al mondo per grandezza, operante in 48 Paesi

- Servizi di trasporto
- Chicago, Illinois, Stati Uniti
- Oltre 80.000 dipendenti in più di 350 sedi

6
mesi per la trasformazione zero trust

1 PB
di traffico TLS ispezionato

Oltre 3 MLN $
di risparmi sui costi rispetto alle soluzioni legacy

Sfide

- Un'architettura tradizionale, basata sul perimetro e sui data center, non era in grado di supportare una trasformazione digitale rapida
- I firewall e le VPN legacy non avevano l'agilità necessaria per adattarsi all'incremento del lavoro da remoto, e di conseguenza mettevano a rischio utenti e dati
- I precedenti prodotti di sicurezza non disponevano di funzionalità avanzate per il rilevamento delle minacce, comportando l'esposizione di una superficie di attacco più estesa

Un percorso in fasi

1. **Ha implementato una connettività sicura e diretta a Internet e alle app SaaS** per garantire una protezione costante degli utenti, ovunque
2. **Ha sostituito le VPN con policy di accesso a privilegi minimi e zero trust** per proteggere le app e i dati privati dalle compromissioni
3. **Ha sfruttato le integrazioni con il cloud e le funzionalità di monitoraggio dell'esperienza** per aumentare la visibilità in tempo reale sulle minacce

Risultati

- **Consente a 80.000 dipendenti di lavorare in sicurezza da qualsiasi luogo** e offre un accesso remoto sicuro a oltre 2.000 app private critiche
- **Riduce la complessità e i costi per l'architettura** eliminando i firewall negli aeroporti e 6 prodotti di sicurezza indipendenti
- **Unifica l'ecosistema di sicurezza e applica dinamicamente le policy** per bloccare il 40% di minacce in più e potenziare la sicurezza

Con Zscaler, possiamo operare con serenità sapendo che il traffico sarà sempre sicuro, indipendentemente dall'infrastruttura di rete sottostante, per tutti i nostri dipendenti, clienti e partner.

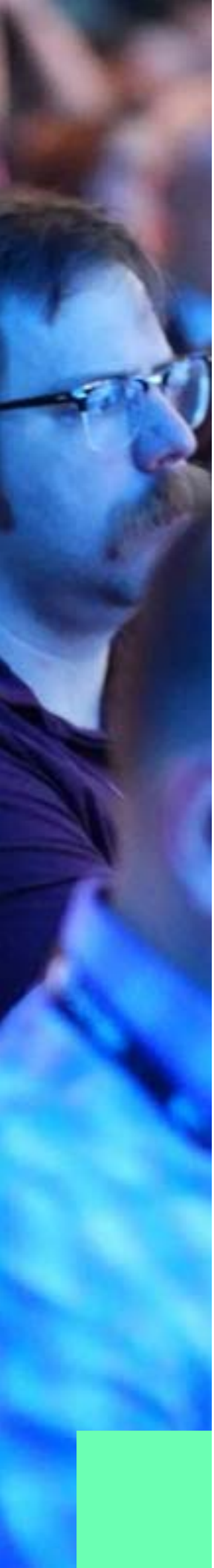
Deneen DeFiore
Vice President and Chief Information Security Officer, United Airlines

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

EMEA

Esplora le storie di successo dei clienti suddivise per area geografica



01 Austria

36 Raiffeisen Bank

02 Germania

38 Capitale di Stato Magdeburgo

03 Italia

40 Cisalfa Sports

04 Norvegia

42 Hydro

05 Sudafrica

44 Capitec

06 Spagna

46 Noatum

48 Sanitas

07 Regno Unito

50 Colt

52 Primetals Technologies

54 Unilever

©2025 Zscaler, Inc. Tutti i diritti riservati.

Raiffeisen Bank International

Raiffeisen Bank International trasforma la sicurezza grazie a Zscaler Zero Trust Exchange

Zscaler sostituisce le apparecchiature legacy per fornire una protezione completa dalle minacce, permettere di lavorare con la massima flessibilità da qualsiasi luogo e ridurre i costi per la sicurezza informatica

PANORAMICA SU RAIFFEISEN BANK

Una delle principali banche austriache operante in ambito corporate e negli investimenti

Servizi finanziari e assicurativi

Vienna, Austria

Milioni di clienti in 12 mercati

44.000
dipendenti protetti con lo zero trust

18,6 MLN
di clienti godono di servizi bancari sicuri

1
piattaforma fornisce lo zero trust a livello globale

Sfide

- Un'infrastruttura di sicurezza tradizionale non era compatibile con un approccio incentrato sul cloud e metteva a rischio utenti e workload
- I dispositivi di sicurezza legacy non consentivano di lavorare con la massima flessibilità da qualsiasi luogo, generando latenza e prestazioni scadenti
- Le VPN non consentivano di implementare l'accesso basato sulle identità alle app private, portando ad avere policy incoerenti e una superficie di attacco più estesa

Un percorso in fasi

1. **Ha implementato una piattaforma completa zero trust** sfruttando i vantaggi dei service edge pubblici e privati, per proteggere gli utenti ovunque
2. **Ha introdotto una connettività sicura e diretta a Internet, senza ricorrere al backhauling**, per offrire esperienze utente uniformi a una forza lavoro ibrida
3. **Ha sostituito i dispositivi VPN implementando un accesso zero trust alle applicazioni private** e policy di accesso ottimizzate basate sull'identità

Risultati

- **Protegge la connettività in uscita e in entrata per una forza lavoro ibrida**, offrendo una protezione uniforme in ogni sede
- **Riduce la latenza e migliora le prestazioni delle applicazioni SaaS e private** per migliorare le esperienze degli utenti in ufficio e da remoto
- **Semplifica l'architettura di sicurezza e offre una protezione completa contro le minacce**, riducendo al contempo la spesa per la sicurezza

La partnership con Zscaler ci ha consentito di potenziare la sicurezza, abbattere i costi e migliorare l'esperienza utente applicando i nostri principi zero trust.

Peter Gerdenitsch
CISO del Gruppo, Raiffeisen Bank International

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Il Consiglio cittadino di Magdeburgo protegge la sua trasformazione digitale con Zscaler Zero Trust Exchange

La capitale dello Stato tedesco sostituisce gli apparecchi VPN e supporta una forza lavoro ibrida, gettando allo stesso tempo le basi per proseguire la sua evoluzione digitale con Zscaler

PANORAMICA SULLA CAPITALE MAGDEBURGO

Fornisce servizi amministrativi ai residenti della capitale della Sassonia-Anhalt

Federale e governativo

Magdeburgo, Germania

2.500 dipendenti

2.500
dipendenti ibridi protetti

230.000
residenti della città supportati

1
soluzione single-vendor per semplificare la sicurezza

Sfide

- Un'architettura di sicurezza tradizionale, basata su hardware, non era sufficientemente agile per supportare gli obiettivi di trasformazione digitale
- Le soluzioni proxy e firewall legacy non erano in grado di adattarsi e proteggere la connettività a Internet di una forza lavoro sempre più ibrida
- Le VPN non consentivano un controllo granulare degli accessi, esponendo di conseguenza le app private a un rischio maggiore e limitando la produttività e l'efficienza del lavoro da remoto

Un percorso in fasi

1. **Ha distribuito una piattaforma zero trust nativa del cloud** per modernizzare l'architettura di sicurezza e consentire il proseguimento della trasformazione digitale
2. **Ha introdotto una connettività sicura e diretta a Internet** con funzionalità integrate di ispezione del traffico per gestire le minacce
3. **Ha implementato un accesso sicuro alle app private con controlli basati sull'identità e zero trust**, garantendo una protezione uniforme per i dati critici

Risultati

- **Consente di offrire esperienze utente ottimali a una forza lavoro ibrida** e di proteggere il lavoro remoto di fino a 1.500 utenti al mese
- **Riduce i costi per la sicurezza e la complessità di gestione** con un'architettura che elimina i prodotti di sicurezza legacy
- **Accelera il proseguimento della trasformazione digitale** attraverso un'architettura di sicurezza zero trust completa e scalabile

Volevamo essere un punto di riferimento per gli altri comuni e incoraggiarli a valutare e implementare soluzioni ideali per il business, proprio come abbiamo fatto noi adottando una soluzione di sicurezza con base cloud.

Dott. Tim Hoppe
Ufficio statistiche, elezioni
e digitalizzazione, Città di Magdeburgo

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Cisalfa Sport rafforza il proprio profilo di sicurezza implementando Zscaler in meno di tre mesi

La piattaforma zero trust riduce la superficie di attacco e garantisce un'esperienza utente fluida a dipendenti e utenti terzi

PANORAMICA SU CISALFA SPORT

Il principale rivenditore omnicanale di articoli sportivi in Italia

- Vendita al dettaglio e all'ingrosso
- Curno (BG), Italia
- Oltre 3.600 dipendenti

2,5

mesi per la distribuzione di Zscaler in tutta l'azienda

Oltre 130

partner e collaboratori terzi accedono in modo sicuro ad app private e infrastruttura on-premise

70%

di utenti integrati in 2 settimane di distribuzione

Sfide

- La VPN consentiva a tutti i dipendenti e alle terze parti di accedere, senza segmentazione, all'intera rete aziendale, aumentando di conseguenza il rischio e il raggio d'impatto dei potenziali attacchi
- Due soluzioni VPN legacy presentavano policy e configurazioni divergenti, con conseguenti incoerenze nella sicurezza e nella gestione
- L'accesso alle app tramite VPN generava prestazioni lente e un volume elevato di ticket all'assistenza da parte di utenti interni ed esterni

Un percorso in fasi

1. **Ha ridotto la superficie di attacco** sostituendo le VPN vulnerabili con un accesso diretto dall'utente all'app privata
2. **Ha bloccato il movimento laterale delle minacce** mediante l'applicazione di policy di accesso con privilegi minimi per tutti gli utenti
3. **Ha ottimizzato l'esperienza utente** migliorando le prestazioni e l'affidabilità delle app ed eliminando le interruzioni o le diverse procedure di log in tramite VPN per accedere alle risorse

Risultati

- **Potenzia la sicurezza complessiva** fornendo un accesso diretto utente-app a tutti gli utenti e un'applicazione coerente delle policy
- **Concede a partner e collaboratori un accesso clientless trasparente e fluido** alle app private e ai dati
- **Riduce i ticket dell'assistenza relativi alla latenza**, offrendo una connettività ultra veloce fornita tramite il punto di presenza più vicino

Zscaler Zero Trust Exchange [...] soddisfa tutte le nostre esigenze, offrendoci un accesso più rapido e sicuro alle app senza la necessità di ricorrere alle VPN, una riduzione del rischio dell'intero ambiente e un percorso ben definito per espandere lo zero trust.

Fabio Freti
IT Operations and Infrastructure
Cisalfa Sport

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Hydro potenzia il suo profilo di sicurezza e le sue attività per la sostenibilità grazie a Zscaler Zero Trust Exchange

Zscaler riduce la superficie di attacco e l'impronta di carbonio del fornitore di energia rinnovabile per eliminare l'hardware legacy e adottare un approccio integralmente incentrato sul cloud

PANORAMICA SU HYDRO

Una delle più grandi aziende nel campo delle energie rinnovabili al mondo, presente in 40 Paesi

Settore manifatturiero

Oslo, Norvegia

31.000 dipendenti

33.000

dipendenti protetti con lo zero trust

1

approccio single-vendor per ridurre i costi e la complessità

100%

Operazioni cloud Obiettivo

Sfide

- L'infrastruttura di sicurezza e l'hardware legacy richiedevano molta energia e non erano in linea con gli obiettivi di sostenibilità dell'azienda
- Una rete MPLS a bassa larghezza di banda non era in grado di supportare un aumento del traffico dei dati sul cloud, con conseguenti prestazioni scadenti
- Le VPN tradizionali con policy di accesso altamente limitate, basate sull'accesso "a tutto o a niente", hanno messo a rischio la rete, portando a un costoso attacco ransomware

Un percorso in fasi

1. **Ha implementato una connettività sicura e diretta a Internet**, eliminando il backhauling del traffico e migliorando l'affidabilità dell'accesso
2. **Ha sostituito le VPN legacy con l'accesso zero trust basato su policy** alle applicazioni private per tutelare i dati dagli attacchi informatici
3. **Ha implementato una soluzione per il monitoraggio dell'esperienza creata appositamente per il traffico del cloud,** in modo consentire una risoluzione più rapida dei problemi degli utenti

Risultati

- **Elimina la dipendenza dai prodotti legacy** e riduce l'impatto ambientale attraverso una piattaforma di sicurezza multitenant e nativa del cloud
- **Migliora le prestazioni delle applicazioni SaaS** ottimizzando l'esperienza utente di 33.000 dipendenti in 140 sedi
- **Riduce i costi e la complessità di gestione migliorando al contempo la sicurezza, il tutto** grazie a una soluzione single-vendor per lo zero trust

Con Zscaler Private Access, gli utenti non hanno più bisogno di connettersi alla rete per utilizzare le nostre applicazioni private. E oggi, mentre continuiamo a impegnarci per modernizzare il nostro ambiente di lavoro, ci stiamo muovendo verso l'abbandono definitivo della VPN.

Armin Auth
Head of I&T Strategic Programs

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Capitec accelera la trasformazione digitale e protegge i dati finanziari con Zscaler

La più grande banca del Sudafrica implementa la sicurezza zero trust in tre mesi, proteggendo 17.000 utenti e bloccando 745.000 minacce grazie a Zero Trust Exchange

PANORAMICA SU CAPITEC

La più grande banca del Sudafrica, con 21 milioni di clienti e classificata al primo posto per la soddisfazione dei clienti

Servizi finanziari e assicurativi

Città del Capo, Sudafrica

15.450 dipendenti in 860 filiali

3
secondi per migrare le app private su AWS

125 MLN
di violazioni delle policy prevenute in un anno

3
mesi per l'implementazione completa dello zero trust

Sfide

- L'architettura di sicurezza basata sul perimetro non era in grado di proteggere efficacemente i dati finanziari di alto valore da compromissioni e perdite
- I dispositivi di sicurezza legacy, come firewall e VPN, erano complessi da gestire e danneggiavano la produttività degli utenti
- La visibilità limitata sull'esperienza utente impediva di adottare un approccio proattivo all'identificazione e alla risoluzione dei problemi

Un percorso in fasi

1. **Ha implementato una connettività diretta e sicura a Internet e alle app SaaS** con l'ispezione del traffico per prevenire la compromissione dei dati
2. **Ha sostituito i dispositivi VPN legacy, introducendo l'accesso zero trust** alle applicazioni private e ai dati finanziari sensibili
3. **Ha impiegato funzionalità avanzate per ottimizzare l'esperienza digitale e informazioni concrete** per risolvere annosi problemi legati all'esperienza utente

Risultati

- **Protegge l'accesso a Internet e alle applicazioni cloud di 17.000 utenti**, prevenendo 125 milioni di violazioni delle policy all'anno
- **Protegge un'applicazione di private banking a cui accedono oltre 11 milioni di clienti** attraverso un accesso basato su policy e zero trust
- **Consente una trasformazione digitale più rapida:** bastano pochi secondi per migrare le app su AWS senza periodi di inattività e problemi di sicurezza

Abbiamo introdotto Zero Trust Exchange nel nostro ambiente, e i nostri agenti software di sicurezza zero trust sono stati distribuiti a tutti gli utenti nel giro di tre mesi.

Andrew Baker
CTO, Capitec

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Noatum implementa una suite di tecnologie di Zscaler per supportare una varietà di casi d'uso

Tra cui accesso sicuro a Internet, SaaS e app private, rilevamento più efficiente delle minacce informatiche ed esperienze utente ottimizzate

PANORAMICA SU NOATUM

Noatum è un gruppo multinazionale leader nel settore dei servizi di trasporto e della logistica

Servizi di trasporto

Barcellona, Spagna

Oltre 4.300 dipendenti

1° giorno

valore immediato dalla piattaforma

Zero

dipendenza da VPN e firewall

360

gradi di quantificazione del rischio

Sfide

- Le VPN tradizionali lasciavano l'organizzazione troppo esposta agli attacchi informatici, quando gli utenti accedevano a Internet
- Le misure di sicurezza legacy, come i firewall, impedivano all'organizzazione di ispezionare il traffico cifrato
- Le architetture basate sul perimetro rendevano l'onboarding associato a fusioni e acquisizioni molto più lento

Un percorso in fasi

1. **Ha sostituito le VPN** con una piattaforma cloud, consentendo un accesso sicuro a Internet e alle app private
2. **Ha creato un hub di monitoraggio consolidato dell'esperienza sul cloud** con ZDX
3. **Valuta il rischio aziendale** in modo olistico con Zscaler Risk360

Risultati

- **Supporta il lavoro da qualsiasi luogo** in totale sicurezza, offrendo un accesso sicuro e fluido agli utenti
- **Riduce al minimo gli incidenti degli utenti** e migliora l'analisi delle cause, fornendo informazioni utili e massimizzando l'agilità
- **Migliora la valutazione del rischio** e la difesa dalle minacce nascondendo i sistemi e le app da Internet

Il problema risiedeva nella VPN tradizionale, nell'esposizione dei servizi Internet e nel costante rischio di subire attacchi; questo è stato il vero motivo per cui abbiamo cercato una soluzione come Zscaler.

Josep Pou
CISO, Noatum

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Sanitas offre una connettività sicura e fluida grazie a Zscaler Internet Access

Implementare protezioni per Internet, SaaS e applicazioni private per oltre 12.000 utenti, ovunque

PANORAMICA SU SANITAS

Sanitas è un'azienda leader nel settore delle assicurazioni sanitarie e in rapida espansione

Settore sanitario e farmaceutico

Madrid, Spagna

Oltre 11.700 dipendenti in Spagna, Europa e Sudamerica

2,5

mesi per la distribuzione a tutti gli utenti

12–15.000

di utenti protetti dalla nostra piattaforma

Zero

necessità di connettersi a un data center

Sfide

- Le unità aziendali separate avevano strumenti di sicurezza separati, senza un modello con base cloud
- Le VPN comportavano un processo di autenticazione estenuante per gli utenti e fornivano una sicurezza scadente
- Gli uffici partner non erano in grado di connettersi ai data center e non potevano accedere alle applicazioni

Un percorso in fasi

1. Distribuisce un approccio zero trust omogeneo e con base cloud per proteggere l'intera organizzazione su larga scala
2. Ha sostituito le VPN con un modello zero trust per migliorare la connettività di tutti gli utenti indipendentemente dalla posizione
3. Fornisce a tutti gli utenti, compresi i partner, un accesso sicuro e fluido alle applicazioni

Risultati

- Protegge 12.000–15.000 utenti in 2,5 mesi con Zscaler Internet Access
- Consente di lavorare da qualsiasi luogo, favorendo la flessibilità e l'agilità del business e offrendo un'esperienza analoga a quella in sede ovunque
- Fornisce un accesso sicuro ai workload e alle applicazioni

Oggi, i dipendenti possono lavorare da casa proprio come se fossero in ufficio, in modo trasparente, flessibile, estremamente agile e senza le barriere che incontravamo con altre soluzioni.

Antonio Cerezo
Head of Cybersecurity, Europe and LATAM

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Colt Technology Services migliora la sicurezza e l'esperienza digitale con Zero Trust Exchange

La partnership con Zscaler ha permesso di implementare un'architettura zero trust in tre mesi, consentendo all'azienda di aiutare altre imprese a supportare la trasformazione della sicurezza

PANORAMICA SU COLT TECHNOLOGY SERVICES

Offre soluzioni per reti, comunicazioni vocali e data center a più di 25.000 imprese a livello globale

Telecomunicazioni

Londra, Regno Unito

Oltre 5.000 dipendenti in 60 uffici globali

5.000

dipendenti ibridi protetti

83%

maggiore rapidità di distribuzione rispetto alle soluzioni legacy

100 MLN

di violazioni delle policy bloccate ogni trimestre

Sfide

- L'accelerazione della migrazione al cloud per supportare un ambiente di lavoro ibrido aveva esteso la superficie di attacco e il rischio di subire compromissioni
- Una soluzione proxy obsoleta non era in grado di gestire l'ispezione inline del traffico cifrato, creando punti ciechi sfruttabili dai malware
- I dispositivi VPN legacy non consentivano l'applicazione di policy di accesso dinamiche alle applicazioni private, con un conseguente impatto sul lavoro da remoto

Un percorso in fasi

1. **Ha implementato un'architettura di sicurezza nativa del cloud e zero trust** per supportare le operazioni aziendali incentrate sul cloud e il lavoro ibrido
2. **Ha fornito un accesso sicuro e diretto a Internet**, ispezionando tutto il traffico cifrato per fermare le minacce e la perdita dei dati
3. **Ha sostituito i dispositivi VPN legacy con un accesso zero trust alle applicazioni private**, rendendo il lavoro da remoto più semplice e sicuro

Risultati

- **Fornisce esperienze digitali impeccabili a oltre 5.000 dipendenti ibridi,** proteggendo contemporaneamente il traffico in uscita e in entrata
- **Ispeziona il traffico Internet su larga scala**, elaborando 6,7 miliardi di transazioni e bloccando 476.000 minacce alla sicurezza ogni trimestre
- **Supporta l'accesso microsegmentato e basato su policy alle applicazioni private**, un risultato impossibile da ottenere con le VPN tradizionali

Zscaler ci aiuta a migliorare sia l'esperienza utente che la sicurezza. La piattaforma nativa del cloud di Zscaler protegge i nostri dipendenti ovunque, indipendentemente dai dispositivi che utilizzano.

Ash Surti
Chief Digital and Information Officer,
Colt Technology Services

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Primetals Technologies crea un ambiente di lavoro ibrido sicuro con Zscaler Zero Trust Exchange

Il leader mondiale nella produzione di metalli abbandona i data center e consolida un set di soluzioni di sicurezza legacy per accelerare la trasformazione digitale con Zscaler

PANORAMICA SU PRIMETALS TECHNOLOGIES

Leader mondiale nelle soluzioni per gli impianti metallurgici, specializzato nella produzione di acciaio

High Tech

Londra, Regno Unito

Oltre 7.500 dipendenti

7.500
utenti protetti con lo zero trust

Fino al 35%
di riduzione dei costi infrastrutturali

4,53/5
valutazione della soddisfazione dei dipendenti

Sfide

- Un set di soluzioni di sicurezza tradizionale, basato sui data center, non era in grado di offrire scalabilità per supportare la trasformazione digitale con base cloud
- Le apparecchiature di sicurezza legacy, inclusi firewall e VPN, non erano sufficientemente agili per supportare una nuova riprogettazione della rete SD-WAN
- Le apparecchiature VPN obsolete non proteggevano efficacemente la connettività da remoto di una forza lavoro ibrida e distribuita a livello globale

Un percorso in fasi

1. **Ha distribuito una connettività compatibile con la SD-WAN e diretta a Internet** per semplificare l'infrastruttura e migliorare le prestazioni
2. **Ha sostituito le VPN con un accesso zero trust alle applicazioni private**, per consentire agli utenti in tutto il mondo di lavorare in sicurezza da qualsiasi luogo
3. **Ha approfittato delle funzionalità avanzate per il monitoraggio dell'esperienza utente** al fine di garantire che gli strumenti di collaborazione per il personale funzionassero perfettamente

Risultati

- **Semplifica il set di soluzioni di sicurezza**, riduce la dipendenza dai data center e abbatte i costi infrastrutturali complessivi
- **Garantisce una connettività in uscita e in entrata senza interruzioni** a un gruppo di utenti ibrido, composto per il 25% da personale completamente in remoto
- **Riduce il volume dei ticket di assistenza e risolve i problemi più rapidamente**, migliorando l'esperienza degli utenti finali e snellendo le spese generali amministrative

Il passaggio al cloud ha richiesto di modernizzare il nostro set di soluzioni di sicurezza [...]; Zscaler Zero Trust Exchange ha svolto un ruolo cruciale nel trasformare questa visione in realtà.

Ralph Deleja-Hotko
Head of Backend and Cloud Solutions, Primetals Technologies

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Unilever migliora la sicurezza globale e garantisce un accesso controllato alle app grazie allo zero trust

Zscaler consente a Unilever di eliminare le VPN, di fornire agli utenti una connettività diretta e sicura alle app e a Internet e di semplificare le operazioni in 190 Paesi

PANORAMICA SU UNILEVER

Azienda globale di beni di consumo con prodotti utilizzati da 3,4 miliardi di persone ogni giorno

Settore manifatturiero

Londra, Regno Unito

Vendite in 190 Paesi

Oltre 3 MLD

di transazioni al dettaglio rese sicure ogni settimana

99,9%

di uptime durante l'elaborazione di 220 TB di dati in due mesi

Oltre 1.500

di applicazioni gestite garantendo un accesso zero trust controllato

Sfide

- Le VPN legacy avevano una flessibilità limitata e non si adattavano alla strategia cloud globale di Unilever
- Il modello di sicurezza tradizionale aumentava i rischi a causa di un controllo degli accessi e di una visibilità insufficienti
- La crescente necessità di ricorrere all'accesso remoto metteva a dura prova l'infrastruttura VPN, influenzando negativamente l'esperienza utente

Un percorso in fasi

1. **Ha abilitato l'accesso sicuro degli utenti a Internet e SaaS** grazie all'ispezione completa del traffico TLS/SSL e la protezione dalle minacce avanzate
2. **Ha sostituito le VPN** con un accesso zero trust alle applicazioni private
3. **Ha migliorato l'esperienza utente** implementando il monitoraggio dell'esperienza digitale per identificare e risolvere rapidamente i problemi prestazionali

Risultati

- **Riduce i rischi** con un accesso sicuro e diretto alle applicazioni, eliminando le limitazioni e le vulnerabilità delle VPN
- **Migliora l'efficienza operativa** elaborando il traffico dati su larga scala con un uptime del 99,99%
- **Supporta la strategia cloud globale** fornendo un accesso remoto sicuro in 190 Paesi, offrendo la massima flessibilità alla forza lavoro di Unilever

L'approccio zero trust di Zscaler ha trasformato la sicurezza di Unilever. L'eliminazione dei colli di bottiglia delle VPN consente alla nostra forza lavoro globale di accedere in modo sicuro alle applicazioni, migliorando le prestazioni, la flessibilità e la resilienza.

Richard Mardling
Access and Connectivity Director, Unilever

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Asia-Pacifico e Giappone

Esplora le storie di successo dei clienti suddivise per area geografica

01 Australia

58 John Holland
60 Probe CX

02 India

62 Persistent Systems

03 Giappone

64 Keiju Medical Center
66 The Bank of Saga

04 Filippine

68 Cebu Pacific Air

05 Singapore

70 Maxeon

©2025 Zscaler, Inc. Tutti i diritti riservati.

John Holland riduce i costi di rete del 50% utilizzando Zscaler Zero Trust Exchange

Zscaler semplifica la transizione alla SD-WAN e consente di sostituire centinaia di firewall, migliorando l'efficienza operativa e la sicurezza

PANORAMICA SU JOHN HOLLAND

Azienda integrata specializzata in infrastrutture, edilizia, ferrovie e trasporti multimodali

Edilizia

Melbourne, Victoria, Australia

Oltre 5.000 dipendenti in più di 120 sedi

1 settimana
per l'implementazione dello dello zero trust

6.000
utenti protetti tra personale e collaboratori

122.000
minacce bloccate in tre mesi

Sfide

- Un'architettura di sicurezza perimetrale tradizionale non era in grado di supportare operazioni aziendali sempre più orientate al cloud
- Una rete MPLS obsoleta faceva affidamento su significativo backhauling del traffico, rallentando la velocità dei servizi IT e incrementando i costi
- I dispositivi firewall legacy non disponevano dell'agilità necessaria per ispezionare il traffico cifrato inline, aumentando di conseguenza la vulnerabilità alle minacce

Un percorso in fasi

1. **Ha implementato una piattaforma di sicurezza zero trust completa e nativa del cloud** per creare un ambiente IT più agile e scalabile
2. **Ha ridotto la dipendenza da dispositivi firewall e i costi di rete** grazie a un accesso sicuro e diretto a Internet e alle app SaaS
3. **Ha approfittato delle funzionalità avanzate per il rilevamento delle minacce per semplificare l'ecosistema di sicurezza** ed eliminare il rischio di subire compromissioni dei dati

Risultati

- **Ha implementato lo zero trust per il 100% degli utenti in una settimana** e consente un provisioning più rapido per l'accesso alla rete in oltre 120 siti operativi
- **Elimina centinaia di dispositivi firewall legacy grazie alla connettività zero trust**, con un abbattimento dei costi di rete del 50%
- **Protegge la connettività degli utenti** elaborando 400 TB di traffico e prevenendo 98 milioni di violazioni delle policy ogni trimestre

Zscaler completa la nostra strategia di sicurezza semplificando i nostri processi, e di conseguenza ci ha resi molto più sicuri.

Kier Morrison
General Manager, IT Technology Operations, John Holland

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Probe CX elimina gradualmente le VPN per proteggere 7.600 dipendenti e le app critiche tramite Zscaler Zero Trust Exchange

Zscaler snellisce il set di soluzioni di sicurezza, semplifica la gestione delle policy e riduce la spesa per la tecnologica ottimizzando al contempo la sicurezza

PANORAMICA SU PROBE CX

Uno dei maggiori provider australiani di servizi per l'esperienza dei clienti e outsourcing dei processi aziendali

Servizi

Melbourne, Victoria, Australia

19.000 dipendenti, con un'operatività in 32 sedi di consegna

100%
di VPN eliminate

8,1 MLD
di transazioni elaborate in un trimestre

3,1 MLN
minacce bloccate in tre mesi

Sfide

- Un'architettura di sicurezza tradizionale non era scalabile per supportare una forza lavoro in rapida crescita o un approccio incentrato sul cloud
- Le VPN legacy non supportavano le policy di controllo di accesso microsegmentato, esponendo le applicazioni e i dati privati a un rischio maggiore
- La visibilità limitata sull'esperienza utente e sulle prestazioni delle applicazioni rendeva la mitigazione dei problemi complicata e dispendiosa in termini di tempo

Un percorso in fasi

1. **Ha implementato una connettività diretta e sicura a Internet e alle applicazioni SaaS** ispezionando il traffico inline ed eliminando così la necessità di ricorrere al backhauling
2. **Ha sostituito le VPN con un accesso zero trust alle applicazioni private** per proteggere al meglio la proprietà intellettuale e i dati critici
3. **Ha approfittato delle funzionalità avanzate per l'esperienza utente** al fine di risolvere i problemi più rapidamente e ottimizzare l'esperienza di lavoro da remoto

Risultati

- **Offre a 7.600 utenti in cinque Paesi la flessibilità di poter lavorare da qualsiasi luogo con i principi dello zero trust**
- **Elabora circa 285 TB di traffico ogni trimestre**, applicando policy di sicurezza coerenti e riducendo al minimo la superficie di attacco
- **Semplifica la gestione della sicurezza con una piattaforma multitenant** che offre una sicurezza zero trust a un TCO inferiore

Uno dei principali vantaggi che abbiamo ottenuto con questa tecnologia è stato quello di poter eliminare il 100% delle VPN presenti nel nostro ambiente.

Rohan Khanna
Chief Technology Officer, Probe CX

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Persistent potenzia la sicurezza con un risparmio sui costi Capex/Opex pari a 2 milioni di dollari su base annua

Lo zero trust protegge i dati sensibili dei clienti e la proprietà intellettuale, favorisce l'innovazione, riduce la complessità e supporta gli obiettivi ambientali, sociali e di governance (ESG)

PANORAMICA SU PERSISTENT

Un partner globale per l'ingegneria digitale e la modernizzazione aziendale che aiuta le imprese a promuovere l'innovazione

High Tech

Pune, India

23.000 dipendenti in 21 Paesi

85%

di miglioramento del profilo di sicurezza eliminando la VPN

Oltre 80

attacchi ad alta priorità intercettati in 90 giorni attraverso la deception

4x

accesso più rapido alle app private rispetto alla VPN

Sfide

- Fornire ai lavoratori da remoto di 21 Paesi una connettività veloce e un'esperienza utente più produttiva
- Proteggere la proprietà intellettuale e i dati sensibili dei clienti nell'ambiente cloud
- Semplificare un'infrastruttura complessa
- Ridurre i costi hardware e operativi in tutto l'ambiente
- Trovare un partner a lungo termine per lo zero trust con una soluzione scalabile in grado di supportare una rapida espansione
- Ridurre al minimo l'impatto ambientale abbattendo l'impronta di carbonio

Un percorso in fasi

1. **Ha potenziato la sicurezza** implementando connessioni sicure e dirette a Internet, SaaS e app private
2. **Ha ridotto la latenza, abbattuto i costi e migliorato l'esperienza utente** eliminando le VPN e i firewall inaffidabili e non sicuri
3. **Ha protetto la proprietà intellettuale e i dati di valore dei clienti implementando** tecnologie avanzate di prevenzione della perdita di dati (DLP) e deception

Risultati

- **Migliora e accelera l'accesso remoto** di 4 volte per 23.000 lavoratori distribuiti a livello globale
- **Elimina la complessità** e migliora l'efficacia e l'efficienza della sicurezza
- **Accelera il rilevamento e la risposta** tramite l'integrazione con CrowdStrike, Microsoft Entra ID e Securonix
- **Amplia il portafoglio di soluzioni offerte dall'azienda** ai propri clienti con una pratica di sicurezza incentrata su Zscaler

Zscaler DLP offre al team di sicurezza una visibilità granulare sull'utilizzo delle applicazioni shadow di AI generativa, inclusi i prompt immessi, e applica il blocco di DLP in tempo reale e l'isolamento delle applicazioni

Debashis Singh
Chief Information Officer, Persistent

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

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

Il Keiju Medical Center trasforma l'assistenza sanitaria digitale dei pazienti grazie a Zscaler Zero Trust Exchange

Zscaler fornisce una soluzione per l'accesso mobile sicuro ai dati delle cartelle cliniche elettroniche, consente ai medici di collaborare da qualsiasi luogo e migliora l'esperienza dei pazienti

PANORAMICA SUL KEIJU MEDICAL CENTER

L'ospedale di riferimento per il supporto medico nel territorio di Noto, riconosciuto come leader digitale

- Settore sanitario e farmaceutico
- Città di Nanao, prefettura di Ishikawa, Giappone
- Oltre 800 dipendenti per più di 400 posti letto

800
membri del personale medico protetto

Centinaia
di dispositivi mobili connessi in modo sicuro

1
piattaforma per la sicurezza zero trust

Sfide

- Un'architettura di sicurezza perimetrale non era in grado di adattarsi alla crescente richiesta di servizi di assistenza sanitaria digitale e di telemedicina
- I firewall legacy non erano in grado di proteggere la connettività da remoto a Internet, limitando il reclutamento dei medici a un'area locale circoscritta
- Le VPN tradizionali esponevano le applicazioni e le risorse private, compresi i dati sensibili dei pazienti, a un rischio maggiore di subire compromissioni

Un percorso in fasi

1. **Ha implementato un'architettura di sicurezza nativa del cloud e zero trust** per supportare modalità alternative di assistenza digitale ai pazienti
2. **Ha introdotto una connettività sicura e diretta a Internet** che consente al personale medico di lavorare in modo flessibile e sicuro da qualsiasi luogo
3. **Ha eliminato le apparecchiature VPN e adottato l'accesso zero trust** alle applicazioni private per tutelare l'accesso remoto ai dati delle cartelle elettroniche dei pazienti

Risultati

- **Consente al personale medico di lavorare da qualsiasi luogo con la massima flessibilità** ed espande il bacino di selezione per reclutare medici qualificati
- **Protegge le cartelle cliniche sensibili dei pazienti dalle minacce** durante l'accesso remoto: oltre 500 dispositivi mobili si collegano in modo sicuro ai dati delle cartelle cliniche elettroniche
- **Elimina la necessità di ricorrere ai dispositivi di sicurezza legacy** e ottimizza l'efficienza operativa, migliorando l'assistenza ai pazienti

La trasformazione digitale è essenziale per garantire al personale di poter lavorare in modo efficiente anche con risorse limitate. Molti medici vivono lontano [...], e per questo avevamo bisogno di un ambiente per l'accesso remoto sicuro e facile da usare.

Mr. Masahiro Kamino
Chairman of the Board of Directors,
Keiju Medical Center

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

このまちで、あなたと
佐賀銀行

The Bank of Saga supporta la trasformazione digitale con Zscaler Zero Trust Exchange

Zscaler semplifica l'infrastruttura, riduce la dipendenza dalle soluzioni legacy e rafforza la sicurezza mentre le operazioni bancarie si spostano sul cloud

PANORAMICA SU THE BANK OF SAGA

Fornitore di servizi finanziari incentrati sulla comunità, impegnato nell'innovazione per il miglioramento dell'esperienza dei clienti

Servizi finanziari e assicurativi

Città di Saga, prefettura di Saga, Giappone

Oltre 1.200 dipendenti

Circa 33%
di riduzione dei costi per la comunicazione

1.800
utenti protetti con lo zero trust

1
piattaforma per il single sign-on che incrementa la produttività

Sfide

- Un'architettura di sicurezza tradizionale e basata sul perimetro non supportava le continue attività di migrazione sul cloud della banca
- Le apparecchiature di sicurezza legacy non disponevano dell'agilità necessaria per adattarsi alle crescenti esigenze di connettività diretta e affidabile a Internet
- Le VPN erano costose da gestire ed estendevano la superficie di attacco, rendendo app e dati privati vulnerabili alle minacce

Un percorso in fasi

1. **Ha implementato una piattaforma zero trust completa e nativa del cloud** per applicare policy di sicurezza uniformi in tutta l'azienda
2. **Ha introdotto una connettività diretta a Internet** e approfittato dell'ispezione del traffico inline per proteggere l'accesso alle app SaaS pubbliche
3. **Ha sostituito le VPN con un accesso zero trust alle app private**, con opzioni di configurazione granulari per proteggere i dati critici

Risultati

- **Protegge la connettività in uscita e in entrata per i dipendenti**, applicando policy di accesso uniformi indipendentemente dalla posizione
- **Tutela le applicazioni di private banking e i dati critici dalle compromissioni**, proteggendo e migliorando le esperienze dei clienti
- **Ottimizza il set di soluzioni di sicurezza e sostituisce le apparecchiature legacy**, rendendo più semplice la gestione delle policy e riducendo i costi

Per supportare la trasformazione digitale è necessario passare al cloud. [Ma] la sicurezza perimetrale tradizionale non consente di approfittare appieno della praticità offerta dai servizi SaaS e dal web. La sicurezza zero trust era essenziale.

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

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Cebu Pacific Air protegge la sua forza lavoro ibrida con Zscaler Zero Trust Exchange

Zscaler migliora l'esperienza di lavoro da remoto di 3.900 dipendenti e protegge le operazioni aziendali critiche in sette hub strategici in Asia

PANORAMICA SU CEBU PACIFIC AIR

Compagnia aerea leader nelle Filippine, che opera voli verso oltre 60 destinazioni

- Servizi di trasporto
- Metro Manila, Filippine
- 3.900 dipendenti in sette hub strategici

234 MLN

di violazioni delle policy bloccate ogni trimestre

90%

incremento della soddisfazione degli utenti

2

settimane per implementare l'accesso remoto zero trust alle app

Sfide

- Un'infrastruttura di sicurezza legacy rallentava la trasformazione digitale e intensificava i rischi di subire compromissioni e minacce
- I dispositivi di sicurezza tradizionali non erano in grado di proteggere adeguatamente le risorse private fondamentali per le operazioni aziendali
- Le apparecchiature VPN presentavano problemi in termini di prestazioni e connettività, rendendo il lavoro da remoto più complesso e meno sicuro

Un percorso in fasi

1. **Ha eliminato l'architettura di sicurezza legacy obsoleta** implementando una piattaforma zero trust completa e nativa del cloud
2. **Ha fornito un accesso sicuro e diretto a Internet con funzionalità di protezione dalle minacce avanzate**, per supportare al meglio la forza lavoro ibrida
3. **Ha sostituito i tradizionali dispositivi VPN con un accesso zero trust** per applicare controlli granulari degli accessi alle applicazioni private

Risultati

- **Protegge la connettività per consentire a 3.900 utenti di lavorare da qualsiasi luogo, implementando un'alternativa sicura alla VPN** e migliorando la soddisfazione degli utenti del 90%
- **Semplifica il set di soluzioni di sicurezza pur continuando a fornire una solida protezione** ed elabora 733 milioni di transazioni all'anno
- **Ha prevenuto 234 milioni di violazioni delle policy e bloccato 45.000 minacce alla sicurezza in un solo trimestre**, potenziando al contempo il profilo di sicurezza

Il nostro è un ambiente di lavoro dinamico e, grazie a Zscaler, i dipendenti possono continuare a lavorare in modo produttivo, senza ostacoli alla capacità di connettersi alle risorse di cui hanno bisogno e senza compromettere la sicurezza.

Laureen Cansana
CIO, Cebu Pacific Air

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.

Maxeon Solar Technologies realizza la sua trasformazione digitale grazie a Zscaler dopo una cessione

Il leader nel campo dell'energia solare elimina i data center per potenziare la sicurezza e migliorare le esperienze di lavoro da remoto di 5.000 utenti globali grazie a Zero Trust Exchange

PANORAMICA SU MAXEON

Leader mondiale nella produzione di pannelli solari con una presenza commerciale in oltre 100 Paesi

Energia, petrolio, gas ed estrazione mineraria

Singapore

5.000 dipendenti in 40 sedi

134%

di traffico in più elaborato ogni trimestre

31 MLN

di violazioni delle policy prevenute in un trimestre

2,9 MLN

minacce bloccate in tre mesi

Sfide

- La sicurezza perimetrale tradizionale, costruita attorno ai data center, non supportava un'infrastruttura in continua evoluzione e incentrata sul cloud
- I firewall legacy non erano scalabili per adattarsi alle crescenti esigenze di accesso remoto, portando a prestazioni scadenti e rischi più elevati
- Le precedenti soluzioni di DLP erano difficili da gestire, mettendo la proprietà intellettuale e le risorse critiche a rischio di subire compromissioni

Un percorso in fasi

1. **Ha implementato una connettività diretta e sicura a Internet con ispezione del traffico inline** per proteggere gli utenti ovunque abbiano bisogno di accedere online
2. **Ha implementato una soluzione per il monitoraggio dell'esperienza creata ad hoc per lo zero trust** al fine di semplificare i processi di onboarding e la gestione delle licenze
3. **Ha introdotto una soluzione integrata di DLP** per tutelare le informazioni critiche, garantire la conformità e prevenire le violazioni dei dati

Risultati

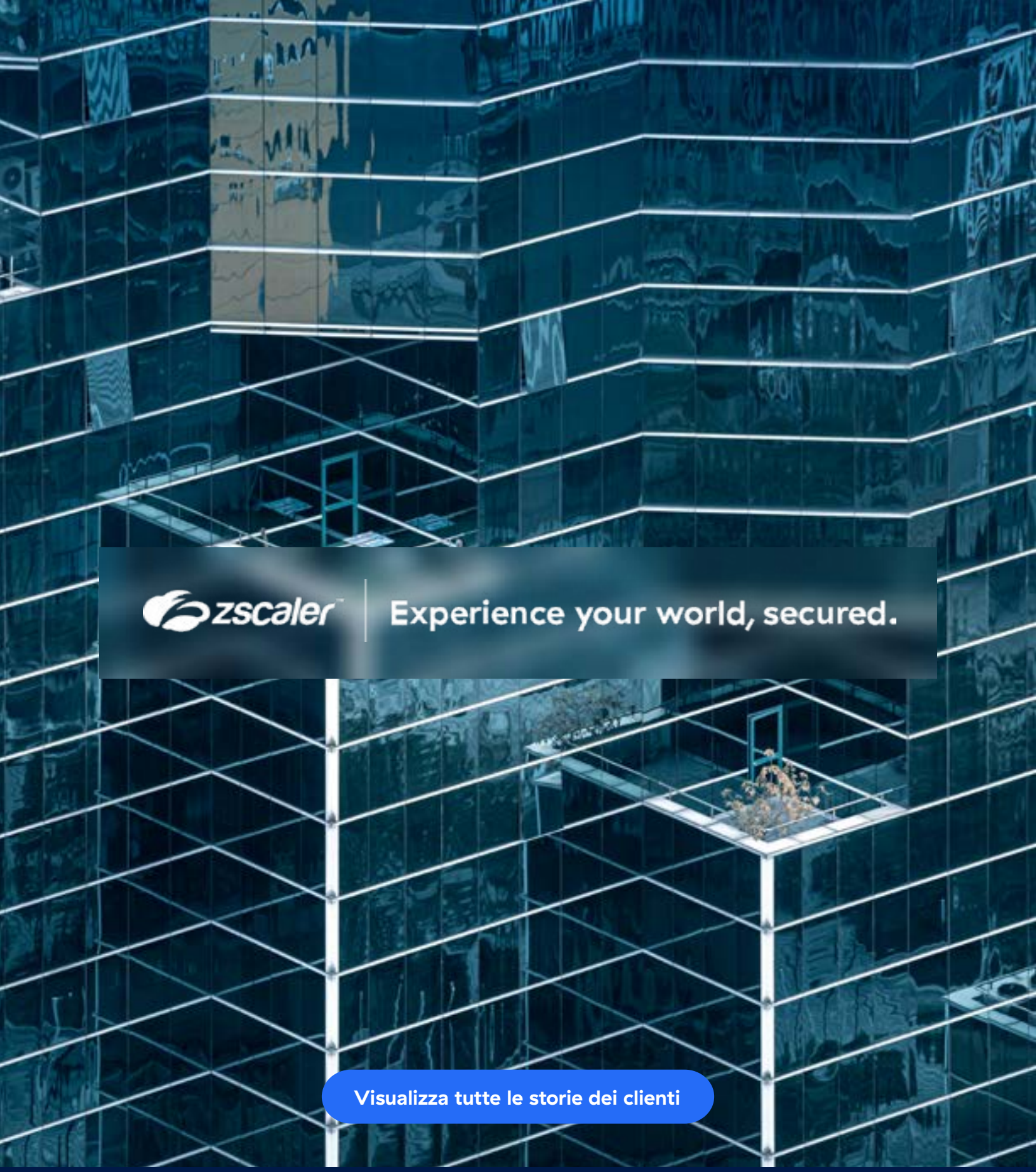
- **Accelera la trasformazione digitale:** tutti i data center sono stati eliminati e il 70% dei workload è stato spostato sul cloud
- **Consente di lavorare da qualsiasi luogo offrendo la massima flessibilità e sicurezza** a un gruppo di utenti altamente distribuito che opera da 16 Paesi
- **Protegge i dati IP critici per il business, tra cui oltre 1.400 brevetti**, potenziando la sicurezza e garantendo la continuità operativa

Dopo aver valutato diversi fornitori molto popolari, Zscaler si è rivelata la vincitrice indiscussa grazie alla sua posizione di leadership nel Gartner Magic Quadrant e alle sue comprovate competenze.

Stephen Gani
CISO, Maxeon Solar Technologies

Scopri questa storia di successo

©2025 Zscaler, Inc. Tutti i diritti riservati.



©2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su zscaler.com/it/legal/trademarks sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Eventuali altri marchi commerciali appartengono ai rispettivi proprietari.