Jornadas de Clientes

Explore histórias reais de transformação, impulsionadas pelo zero trust da Zscaler + IA.

Veja como empresas elevaram suas posturas de segurança, promoveram experiências excepcionais para os usuários, simplificaram fusões e aquisições e mais com zero trust + IA.

A obsessão pelo cliente é um dos nossos principais valores na Zscaler e, como tal, estamos comprometidos em oferecer o melhor em inovação de zero trust para ajudar sua organização a atingir seus objetivos. Com os principais recursos aproveitados pela nossa plataforma Zero Trust Exchange, alimentada por IA, ajudamos mais de 5 mil empresas em todo o mundo a reduzir custos e complexidade, simplificar suas arquiteturas de rede, proteger seus usuários e se proteger contra ameaças cibernéticas em evolução. Neste e-book, você analisará os estudos de caso de algumas das organizações mais bem-sucedidas do mundo e como elas transformaram suas redes, segurança e operações com a Zscaler.

Com mais de 15 anos de pioneirismo em zero trust, a Zscaler continua comprometida em ajudar organizações de todos os tamanhos e setores a atingir e superar suas metas de zero trust. A única constante que conhecemos em tecnologia é a “mudança” e, com nossa plataforma Zero Trust Exchange, as empresas podem estar preparadas para qualquer coisa que surgir no caminho, enquanto continuam a inovar e transformar sua infraestrutura de TI.

Mike Rich
CRO e presidente de vendas globais

Índice

Explore as histórias de sucesso dos clientes por vertical

AMS

Explore as histórias de sucesso dos clientes por região

A AMN Healthcare protege usuários e dados globalmente com a Zscaler Zero Trust Exchange

A Zscaler assegura a experiência de trabalho remoto para mais de 5.000 usuários e protege os dados dos pacientes contra o aumento das ameaças cibernéticas direcionadas ao setor de saúde

RESUMO DA AMN HEALTHCARE

Fornecer aos clientes soluções de equipes de trabalho de saúde para melhorar os resultados dos pacientes

Saúde e farmacêutico

Dallas, Texas, EUA

Mais de 10 mil clientes em 24 locais

1,2 bilhão

de transações web processadas mensalmente

7 milhões

de ameaças bloqueadas em três meses

Horas

para implantar uma borda segura em qualquer lugar

Desafios

- Uma infraestrutura de segurança legada não era mais compatível com o ecossistema operacional na nuvem em evolução da empresa
- As VPNs tradicionais não conseguiam oferecer suporte às crescentes necessidades de acesso remoto, deixando os recursos privados mais vulneráveis a ameaças cibernéticas
- Uma arquitetura de segurança complexa com múltiplas soluções específicas tornava a visibilidade e a resolução de problemas difíceis de gerenciar

Jornada em fases

1. **Fornecimento de acesso seguro e direto à internet**, garantindo trabalho flexível de qualquer lugar para uma equipe de trabalho globalmente dispersa
2. **Introduziu acesso privado zero trust e microssegmentado a aplicativos**, fornecendo uma substituição segura para a VPN legada
3. **Simplificou a pilha de monitoramento e aproveitou a visibilidade abrangente de ponta a ponta** para melhorar a resolução de problemas do usuário

Resultados

- **Protege a conectividade de entrada e saída para mais de 5 mil usuários**, melhorando a capacidade e a eficiência do trabalho remoto global
- **Aplica políticas de acesso zero trust para aplicativos privados e produtos digitais** usados por mais de 10 mil clientes em todo o mundo
- **Simplifica a arquitetura e reduz os custos de tecnologia** para atingir uma postura de segurança mais robusta com menos sobrecarga

A abordagem da Zscaler está alinhada com nossa filosofia geral de zero trust, e a plataforma Zero Trust Exchange foi a personificação de nossa visão para uma arquitetura zero trust na AMN Healthcare.

Mani Masood
Chefe de segurança da informação, AMN Healthcare

Ver história de sucesso

A ATN International protege as operações e melhora a eficiência com a Zscaler Zero Trust Exchange

A Zscaler aprimora os recursos de trabalho remoto para mais de 2.500 funcionários, elimina problemas de usuários relacionados a VPN e garante uma integração mais segura em fusões e aquisições

RESUMO DA ATN INTERNACIONAL

Fornece infraestrutura e serviços de comunicação com expertise em mercados remotos

- Telecomunicações
- Beverly, Massachusetts, EUA
- 750 mil clientes internacionalmente

100%

de eliminação de VPNs e incidentes de ajuda com VPN

Todos

funcionários protegidos com a Zscaler

Minutos

vs. horas para mitigar problemas de usuário

Desafios

- A infraestrutura de segurança local não conseguia oferecer suporte eficiente às operações comerciais prioritárias na nuvem ou às metas futuras de fusões e aquisições
- Os dispositivos de VPN legados tiveram dificuldades de expansão com o aumento do trabalho remoto, o que levou a experiências de usuário insatisfatórias e maior risco
- As soluções de segurança tradicionais não ofereciam as integrações críticas na nuvem para permitir a mitigação proativa de problemas de usuário

Jornada em fases

1. **Forneceu acesso direto à internet,** aproveitando recursos de inspeção e registro de tráfego para evitar violações de políticas
2. **Substituiu dispositivos de VPN por acesso zero trust e de privilégio leste** para aplicativos e recursos privados
3. **Aproveitou os recursos da Zscaler com tecnologia de IA e a profunda integração com a Microsoft** para identificar e resolver problemas de usuário mais rapidamente

Resultados

- **Melhora a experiência de trabalho remoto para mais de 2.500 usuáriose** elimina problemas de usuários relacionados a VPN; incidentes de serviço caem em 100%
- **Acelera cronogramas de fusões e aquisições e garante uma integração mais segura** de empresas adquiridas com uma arquitetura de segurança zero trust
- **Reduz o tempo necessário para identificar e resolver problemas** para apenas alguns minutos com recursos robustos de relatórios e monitoramento

Uma das coisas que busco em ferramentas de infraestrutura e segurança é que elas ajudem você a ser mais eficiente operacionalmente e tragam mais segurança. A Zscaler preenche ambos os requisitos.

Richard Casselberry
Vice-presidente de segurança de TI, arquitetura e conformidade, ATN Internacional

Ver história de sucesso

COX AUTOMOTIVE

A Cox Automotive implementa o Zero Trust em fases com a Zscaler Zero Trust Exchange

A Zscaler simplifica a arquitetura de segurança, protege a conectividade para usuários em cinco continentes e protege os dados de milhões de compradores de carros online

RESUMO DA COX AUTOMOTIVE

A maior fornecedora mundial de serviços automotivos e tecnologia

- Varejo e atacado
- Atlanta, Geórgia, EUA
- 2,3 bilhões de interações online anualmente

Mais de 30 mil
membros da equipe protegidos

40 mil
clientes de concessionárias de automóveis com suporte

Uma
única plataforma reduz a complexidade

Desafios

- Queria uma plataforma compatível com a nuvem que pudesse servir como base para uma arquitetura de segurança zero trust holística
- Os dispositivos de firewall tradicionais tinham dificuldade para inspecionar o tráfego da internet em grande escala para um grupo de usuários dispersos globalmente
- As VPNs legadas não eram compatíveis com políticas de controle de acesso baseadas em identidade, colocando aplicativos e dados privados em maior risco

Jornada em fases

1. **Implantou uma plataforma zero trust multiusuário nativa na nuvem** desenvolvida especificamente para integrar-se facilmente com outras soluções de nuvem
2. **Forneceu conectividade direta e segura com a internet e aplicativos SaaS**, aproveitando os recursos de inspeção de tráfego em linha
3. **Substituiu VPNs por acesso zero trust** para estabelecer políticas de segurança microssegmentadas e de privilégio mínimo para aplicativos privados

Resultados

- **Assegura uma equipe trabalhando em cinco continentes,** proporcionando flexibilidade de trabalho em qualquer lugar e melhorando as experiências de usuário
- **Protege aplicativos e recursos privados críticos**, incluindo dados sobre milhões de clientes, de forma mais econômica
- **Desativa soluções de segurança legadas, incluindo firewalls e VPNs,** para otimizar os processos de TI e acelerar a integração em fusões e aquisições

Depois que os agentes estiverem instalados nos dispositivos de todos, será fácil integrar outros recursos da Zscaler à nossa arquitetura. Será apenas uma questão de ativar o interruptor.

Jon Mahes
Gerente sênior de segurança cibernética, Cox Automotive

Ver história de sucesso

O Governo do Distrito de Colúmbia consolida a segurança na Zscaler Zero Trust Exchange

A Zscaler substitui dispositivos de VPN legados para otimizar a arquitetura de segurança, reforça a conscientização de riscos em tempo real e protege 15.000 usuários

RESUMO DO GOVERNO DO DISTRITO DE COLÚMBIA

Supervisiona e gerencia todos os serviços essenciais para os residentes do Distrito de Colúmbia

Governo e serviços federais

Washington, D.C., EUA

Mais de 15 mil funcionários

15 mil
funcionários do governo protegidos

Cerca de 3 bilhões
de transações processadas por mês

Mais de 200 mil
ameaças de segurança bloqueadas por mês

Desafios

- Uma infraestrutura de segurança desatualizada não oferecia suporte ao trabalho remoto e contribuía para ineficiências operacionais
- Os dispositivos de VPN tradicionais estenderam a rede corporativa aos dispositivos dos usuários finais, colocando dados sigilosos em risco de comprometimento
- Os produtos de segurança legados limitavam a visibilidade em torno das ameaças, tornando a avaliação e a mitigação de riscos mais desafiadoras

Jornada em fases

1. **Forneceu conectividade segura e direta à internet e aplicativos SaaS**, oferecendo flexibilidade para trabalhar de qualquer lugar
2. **Substituiu VPNs legadas por acesso zero trust microssegmentado** para aplicar políticas de segurança consistentes para recursos privados
3. **Aproveitou dados e insights baseados em IA para reforçar a conscientização sobre riscos** e mitigar ameaças potenciais em tempo real e em grande escala

Resultados

- **A arquitetura zero trust aprimora a postura de segurança:** processa cerca de 3 bilhões de transações e bloqueia mais de 200 mil ameaças mensalmente
- **Melhora a experiência remota de 15 mil usuários** e integra-se perfeitamente com soluções de identidade existentes
- **Oferece um foco mais abrangente na gestão de riscos**, impulsionado por melhores insights sobre fatores de risco e postura de segurança

A parceria com a Zscaler foi inestimável para nós. Implementamos a plataforma em velocidade recorde, integramos usuários de forma mais eficaz e aprimoramos a experiência do usuário.

Suneel Cherukuri
CISO, Governo do Distrito de Colúmbia

Ver história de sucesso

A DMI implementa o uso de dispositivos pessoais em larga escala, melhorando a proteção de dados e descobrindo economias substanciais de custos

A Zscaler fornece conectividade zero trust para todas as equipes de trabalho e capacita os funcionários a trabalhar com segurança no dispositivo de sua escolha

RESUMO DA DMI

A DMI é uma fornecedora líder global de serviços digitais que atua na intersecção dos setores público e privado

Alta tecnologia

McLean, Virgínia, EUA

Mais de 2.100 funcionários em 80 países

Mais de US$ 700.000

de economia anual

Menos de 2

semanas para implantar

3%

de melhoria na velocidade de resolução de SLA após a implantação

Desafios

- A instalação de novo hardware em um ambiente legado introduziu tempo de inatividade, causou janelas de interrupção e exigiu atualizações frequentes
- Exigir que os usuários trabalhem em dispositivos DMI tornou os funcionários menos produtivos e impactou negativamente a pegada de carbono global da organização

Jornada em fases

1. **Acesso seguro à Internet e conectividade zero trust real** para funcionários, prestadores de serviço e terceiros, sem configuração manual demorada de dispositivos
2. **Implementou a iniciativa de BYOD (traga seu próprio dispositivo) com suporte a isolamento do navegador,** permitindo que os funcionários trabalhem no dispositivo de sua escolha

Resultados

- **Implementa zero trust em duas semanas,** com impacto zero para os usuários e sem tempo de inatividade
- **Economiza US$ 700 mil anualmente,** melhora as experiências de integração e desligamento e reduz o tempo de configuração de novos escritórios e dispositivos

Com o projeto de BYOD, conseguimos economizar ao não precisar adquirir laptops para pessoas que não precisavam de um. Isso realmente nos rendeu uma economia anual de mais de US$ 700 mil para DMI, o que é muito!

Mauricio Mendoza
Vice-presidente de TI global e segurança, DMI

Ver história de sucesso

A Eaton protege as operações globais com segmentação alimentada por IA

A Zscaler ajuda a fabricante global a migrar para a nuvem com proteção avançada contra ameaças, redução de risco de violação e maior visibilidade por meio de integrações de parceiros

RESUMO DA EATON

Fabricante global de equipamentos elétricos para o setor aeroespacial e outros

Fabricação

Cleveland, Ohio, EUA

Mais de 90 mil funcionários e usuários em 170 países em todo o mundo

4M

de ameaças bloqueadas em um mês

90 mil

funcionários em todo o mundo se conectam à internet e a aplicativos privados por meio do zero trust

Vários

parceiros de aliança estratégica integram-se perfeitamente

Desafios

- VPNs e firewalls legados dificultavam o crescimento e não conseguiam dar suporte a mais de 30 mil funcionários de chão de fábrica durante a pandemia e depois dela
- A arquitetura de segurança tradicional baseada em perímetro era incompatível com a estratégia de priorização da nuvem e as necessidades de segmentação da empresa
- A falta de visibilidade limitou a descoberta de ameaças e atrasou o tempo de correção

Jornada em fases

1. **Substituiu** ferramentas de segurança e acesso por conectividade zero trust com a internet e aplicativos privados
2. **Adotou inovações de IA** para descobrir e combater ameaças baseadas em IA e fornecer segmentação para locais de fabricação
3. **Melhorou a conscientização sobre ataques** com detecção e resposta preventivas e preditivas de violações

Resultados

- **Oferece uma experiência de usuário mais segura, confiável e regulamentada** para funcionários e terceiros
- **Aproveita o poder da IA para detecção de ameaças**, prevenção contra perda de dados, correção, visibilidade do uso do ChatGPT e segmentação de aplicativos
- **Fortalece o controle de acesso** por meio de segmentação zero trust e integração com ferramentas de EDR, CDR e NDR

A Zscaler é fácil de usar e seus recursos são integrados em um único agente de terminal. Conseguimos implantar a Zscaler em nosso ambiente global rapidamente e expandir suas funcionalidades com poucos recursos necessários de nossa parte.

Jason Koler
CISO, Eaton Corporation

Ver história de sucesso

guaranteed Rate

A Guaranteed Rate bloqueia milhões de ameaças e acelera a integração de fusões e aquisições de meses para dias

A Zscaler substitui o hardware de segurança, oferecendo resiliência superior; segurança sempre ativa e uma superfície de ataque reduzida

RESUMO DA GUARANTEED RATE

Segunda maior líder em hipotecas de varejo nos EUA, com mais de 500 agências em 50 estados

Serviços financeiros e seguros

Chicago, Illinois, EUA

Mais de 6 mil funcionários

97%

do tráfego criptografado inspecionado

2,5 milhões

Ameaças bloqueadas em 3 meses

2–3x

mais velocidade de acesso a Aplicativos

Desafios

- O uso da VPN para conectar-se a centenas de aplicativos privados no local e na AWS expôs a superfície de ataque
- O tráfego de retorno de mais de 500 filiais para o data center prejudicou o desempenho e a produtividade
- O firewall legado não conseguiu detectar ameaças de dia zero entrando na rede pela internet e se movendo lateralmente

Jornada em fases

1. **Protegeu o acesso à internet e SaaS a partir da nuvem,** sem retorno do tráfego de mais de 500 filiais
2. **Substituiu a VPN**, dando aos usuários acesso rápido e confiável a mais de 500 aplicativos privados no data center e na nuvem
3. **Otimizou a experiência dos usuários** identificando e resolvendo problemas de desempenho de forma mais rápida e eficiente

Resultados

- **Minimiza a superfície de ataque**, dando aos usuários acesso direto e de privilégio mínimo, ao mesmo tempo em que aumenta a detecção e a resposta
- **Reduz o risco de comprometimento** com monitoramento em linha do tráfego em TLS/SSL e proteção avançada contra ameaças com tecnologia de IA
- **Impede a movimentação lateral** com tecnologia de deception para atrair invasores para longe de recursos sigilosos e conter ameaças em tempo real

Com o Risk360, podemos obter visibilidade dos pontos cegos com risco cibernético. Essa visibilidade nos permite focar mais em onde gastamos nosso tempo para abordar e reduzir os riscos cibernéticos mais urgentes.

Darin Hurd
CISO, Guaranteed Rate

Ver história de sucesso

A MGM Resorts International dobra a aposta em uma arquitetura Zero Trust nativa da nuvem

A Zscaler oferece tempo de retorno incomparável com segmentação zero trust, proteção contra perda de dados e insights práticos detalhados em todo o negócio

RESUMO DA MGM RESORTS INTERNATIONAL

Líder em jogos, entretenimento e hospitalidade com 31 destinos de resort em todo o mundo

Entretenimento e hospitalidade

Las Vegas, Nevada, EUA

70 mil funcionários em todo o mundo

Dia 1

valor imediato da plataforma

Mais de 275 mil

Ameaças bloqueadas cada mês

50%

mais eficiência no uso de dispositivos pela equipe

Desafios

- A segurança do tipo castelo e fosso aumentou o risco de movimentação lateral ao dar aos usuários amplo acesso à rede
- Os gateways de VPN tradicionais criaram gargalos de tráfego, levando a uma experiência ruim para o usuário
- As ferramentas de segurança legadas ofereciam informações limitadas sobre a atividade de navegação na base de usuários

Jornada em fases

1. **Substituiu VPNs e implementou segmentação zero trust** para todas as equipes de trabalho
2. **Implantou rapidamente** um conjunto de soluções de acesso privado, experiência digital e proteção de dados
3. **Adotou tecnologia de deception** para proteger contra comprometimento por invasores ativos

Resultados

- **Melhora a experiência dos funcionários** com desempenho e conectividade mais rápidos em todo o ambiente
- **Fica à frente das ameaças emergentes** com DLP abrangente, acesso privado e segmentação zero trust
- **Fortalece a postura de segurança empresarial** ao mesmo tempo em que ajuda a acelerar os negócios com uma abordagem que prioriza a nuvem

Alcançamos a segmentação zero trust em nossas equipes de trabalho em tempo recorde, e a manutenção diária da solução com proteção contra perda de dados com insights sobre nossos aplicativos. Essas foram vitórias muito rápidas e fáceis, do nosso ponto de vista.

Stephen Harrison
CISO, MGM Resorts Internacional

Ver história de sucesso

A Mercury Financial melhora a segurança e a eficiência com a Zscaler Zero Trust Exchange

A Zscaler oferece integrações perfeitas e recursos de IA para oferecer suporte a um trabalho remoto mais seguro de qualquer local e proteger dados financeiros sigilosos contra ameaças

RESUMO DA MERCURY FINANCIAL

Uma empresa de serviços financeiros não bancários que ajuda os clientes a construir e gerenciar crédito

Serviços financeiros e seguros

Austin, Texas, EUA

Mais de 500 funcionários

100%

experiência perfeita para trabalhadores remotos

76%

de redução em incidentes de suporte de TI

Zero

tempo de inatividade devido a malware

Desafios

- As soluções de segurança tradicionais não permitiam a inspeção completa do tráfego em linha, inibindo a detecção e prevenção de ameaças
- As VPNs legadas eram incompatíveis com as necessidades de priorização da nuvem de uma equipe de trabalho distribuída, resultando em experiências ruins para os usuários
- Dados limitados sobre a atividade dos usuários e a postura dos dispositivos tornaram desafiadores o diagnóstico e a resolução de problemas para uma equipe de trabalho remota

Jornada em fases

1. **Protegeu a conectividade direta à internet**, usando recursos de contenção de ameaças com tecnologia de IA para evitar o comprometimento de dados
2. **Substituiu VPNs por acesso zero trust microssegmentado** para aplicativos privados para garantir que as conexões remotas sejam controladas e seguras
3. **Aproveitou integrações importantes e insights mais robustos de usuários** para aliviar a sobrecarga administrativa sem aumentar os riscos

Resultados

- **Reduz a superfície de ataque:** tempo de inatividade zero causado por malware ou ransomware desde a implantação da Zscaler
- **Limita a movimentação lateral e reduz o raio de ação** se uma ameaça entrar na pilha de segurança, garantindo uma correção mais rápida
- **Integrações com AWS, Crowdstrike e Okta otimizam a infraestrutura de segurança** e reforçam a conformidade regulatória

Vemos a Zscaler como líder nesse espaço porque ela é completa e abrange todas as facetas do zero trust. Para obter a mesma funcionalidade que obtemos da Zscaler em outros lugares, teríamos que implantar soluções de vários fornecedores.

Arjun Thusu
Diretor de informação,
Mercury Financial

Ver história de sucesso

A Molson Coors serve uma ótima experiência do usuário com a Zscaler Zero Trust Exchange

A Zscaler elimina a necessidade de dispositivos de VPN, protege a conectividade para uma equipe de trabalho global e fornece insights que resolvem problemas mais rapidamente

RESUMO DA MOLSON COORS

Terceira maior cervejaria do mundo e inovadora global na indústria de bebidas

Alimentos, bebidas e tabaco

Chicago, Illinois, EUA

Mais de 17 mil funcionários, mais de 42 cervejarias

17 mil

de usuários protegidos com zero trust

96%

mais velocidade de resolução de problemas do usuário

Milhões

de ameaças bloqueadas diariamente

Desafios

- Os dispositivos de firewall não conseguiam acompanhar a demanda por acesso remoto à internet e tinham dificuldade para inspecionar o tráfego em linha
- A falta de visibilidade em torno das atividades dos usuários e da postura dos dispositivos tornou desafiadora a identificação e a resolução de problemas de desempenho
- Uma arquitetura de segurança legada, dependente de dispositivos de VPN, criou um ambiente de rede plano e uma superfície de ataque mais ampla

Jornada em fases

1. **Provisionou acesso direto à internet com recursos avançados de detecção de ameaças** para manter usuários remotos e de terceiros seguros
2. **Aproveitou a visibilidade de ponta a ponta entre usuários e dispositivos** para simplificar o gerenciamento de segurança e resolver problemas de usuário mais rapidamente
3. **Substituiu as VPNs tradicionais por acesso zero trust para aplicativos privados** para proteger recursos e melhorar a experiência dos usuários

Resultados

- **Garante uma ótima experiência de usuário para funcionários** que trabalham em 42 cervejarias em todo o mundo, bem como para parceiros terceirizados
- **Melhora o tempo médio de resolução de problemas do usuário**ao identificar as causas-raiz e automatizar a mitigação em minutos, não horas
- **Bloqueia ameaças avançadas** e elimina a movimentação lateral para manter aplicativos privados e dados corporativos sigilosos mais seguros

Quantas ameaças foram bloqueadas somente pela Zscaler? São sempre centenas de milhares ou milhões, dependendo do dia. É simples e fácil de usar. Você pode treinar imediatamente. Não há limitações.

Jeremy Bauer
Diretor sênior de segurança da informação (CISO), Molson Coors Beverage Company

Ver história de sucesso

O Departamento de Educação da Cidade de Nova York migra da VPN para o Zero Trust

A Zscaler ajuda a proteger o acesso à internet e a aplicativos privados para mais de 1 milhão de usuários e mais de 2 milhões de dispositivos

RESUMO DO DEPARTAMENTO DE EDUCAÇÃO DE NYC

O Departamento de Educação da Cidade de Nova York (NYC DOE) é o maior sistema escolar dos Estados Unidos e um dos maiores do mundo. Ele atende mais de 1 milhão de alunos do jardim de infância ao 3º ano do ensino médio, com uma equipe de mais de 150 mil professores e administradores em todos os cinco distritos de Nova York.

Educação

Cidade de Nova York, Nova York, EUA

Mais de 1 milhão de usuários e mais de 2 milhões de dispositivos

Mais de 2 milhões

de dispositivos de alunos e funcionários protegidos

15%

de redução em ataques

40%

mais ameaças bloqueadas

Desafios

- A infraestrutura legada não conseguiu ser dimensionada para fornecer experiências seguras e consistentes para mais de 1 milhão de usuários
- A abordagem tradicional de VPN e firewall foi ineficaz no bloqueio de ameaças cibernéticas avançadas
- A baixa visibilidade de terminais dificultou a manutenção e o monitoramento dos dispositivos de aprendizagem remota do departamento

Jornada em fases

1. **Protegeu o acesso à internet e SaaS** com uma arquitetura de proxy zero trust que inspeciona 100% do tráfego em TLS/SSL em larga escala
2. **Substituiu a VPN por acesso à rede zero trust (ZTNA)** para oferecer conectividade rápida e contínua aos usuários
3. **Aprimorou a visibilidade** em redes e dispositivos com monitoramento da experiência digital de ponta a ponta

Resultados

- **Estende acesso rápido, confiável e seguro** a aplicativos de aprendizagem para alunos e funcionários em qualquer lugar, em qualquer dispositivo
- **Filtra o tráfego com base no conteúdo**, além do simples bloqueio de URL, para oferecer suporte à conformidade com a CIPA em dispositivos de aprendizagem
- **Melhora o desempenho da rede** ao encontrar e resolver problemas de rede e DNS no ambiente

Acredito que a Zscaler pode ser uma boa parceira para nos ajudar a entender o que estamos fazendo com a IA e nos ajudar a avançar mais rapidamente quando se trata de resposta a incidentes e encontrar uma agulha no palheiro.

Demond Waters
CISO, Departamento de Educação da Cidade de Nova York

Ver história de sucesso

A Southwest Gas utiliza a Zscaler Zero Trust Exchange para otimizar uma experiência de usuário segura

A Zscaler elimina a dependência de soluções de segurança legadas para fornecer conectividade mais rápida e confiável para 2.300 funcionários híbridos e 50 escritórios de campo

RESUMO DA SOUTHWEST GAS

Empresa de energia que fornece serviços de gás natural no Arizona, Nevada e Califórnia

Energia, petróleo, gás e mineração

Las Vegas, Nevada, EUA

2 milhões de clientes

4–6
semanas para implantar zero trust Zero Trust

95%
dos casos de uso atendidos

Uma
plataforma de fornecedor único para simplicidade

Desafios

- Uma infraestrutura de segurança tradicional não poderia ser dimensionada para oferecer suporte à transformação para a nuvem ou à mudança para o trabalho híbrido
- Era um desafio fornecer conectividade de internet rápida e confiável para escritórios de campo e funcionários remotos em áreas rurais
- As VPNs legadas não permitiam políticas de acesso baseadas em identidade, deixando aplicativos e dados privados mais vulneráveis a ameaças

Jornada em fases

1. **Implantou uma plataforma zero trust multiusuário**, simplificando a pilha de segurança e otimizando ambientes de trabalho remoto
2. **Provisionou acesso direto à internet e aplicativos SaaS** com proteção consistente contra ameaças, independentemente da localização
3. **Substituiu VPNs por acesso zero trust a aplicativos privados** para reduzir a superfície de ataque e eliminar a perda de dados

Resultados

- **Garante flexibilidade de trabalho de qualquer lugar para 2.300 funcionários híbridos** e protege usuários e dados em 50 escritórios de campo
- **Oferece políticas de controle de acesso microssegmentadas e de privilégio mínimo** para aplicativos privados, mantendo os dados críticos seguros
- **Acelera a adoção do zero trust**, elimina a complexidade do gerenciamento de segurança e reduz as solicitações de suporte técnico

Após realizar uma prova de valor (PoV), selecionamos a Zscaler por sua arquitetura moderna, o que nos permitiu migrar nossa pilha de segurança para a nuvem e otimizar uma equipe de trabalho remota.

David Petroski
Arquiteto sênior de infraestrutura, Southwest Gas

Ver história de sucesso

A United Airlines detecta e bloqueia ameaças em evolução com a Zscaler Zero Trust Exchange

A Zscaler elimina 40% mais ameaças do que as soluções legadas anteriores para proteger 80 mil usuários globais e oferecer viagens mais seguras para 143 milhões de passageiros

RESUMO DA UNITED AIRLINES

Empresa de aviação americana e terceira maior companhia aérea do mundo, operando em 48 países

Serviços de transporte

Chicago, Illinois, EUA

Mais de 80 mil funcionários em mais de 350 locais

6
meses para transformação zero trust

1 PB
de tráfego em TLS inspecionado

Mais de US$ 3 milhões
em economia de custos em relação às soluções legadas

Desafios

- Uma arquitetura tradicional baseada em perímetro e dependente de data centers não seria compatível com uma transformação digital acelerada
- Firewalls e VPNs legados não tinham agilidade para escalar com o aumento do trabalho remoto, colocando usuários e dados em risco
- Os produtos de segurança anteriores não tinham recursos avançados de detecção de ameaças, expondo uma superfície de ataque mais ampla

Jornada em fases

1. **Forneceu conectividade segura e direta à internet e aplicativos SaaS** para garantir proteção consistente para usuários em qualquer lugar
2. **Substituiu VPNs por políticas de acesso zero trust e de privilégio mínimo** para proteger aplicativos e dados privados contra comprometimento
3. **Aproveitou integrações de nuvem e recursos de monitoramento de experiência** para aumentar a visibilidade em tempo real das ameaças

Resultados

- **Permite que 80.000 funcionários trabalhem com segurança de qualquer local** e protege o acesso remoto para mais de 2.000 aplicativos privados essenciais
- **Reduz a complexidade e o custo da arquitetura:** zero firewalls necessários em aeroportos e seis produtos de segurança específicos eliminados
- **Unifica o ecossistema de segurança e aplica dinamicamente políticas** para bloquear 40% mais ameaças e melhorar a postura de segurança

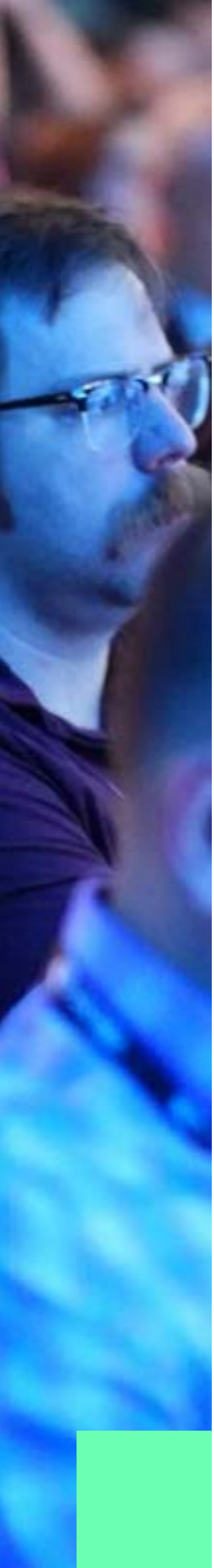
A Zscaler nos dá a tranquilidade de que o tráfego estará protegido, independentemente da rede subjacente, para nossos funcionários, clientes e parceiros.

Deneen DeFiore
Vice-presidente e diretora de segurança da informação, United Airlines

Ver história de sucesso

EMEA

Explore as histórias de sucesso dos clientes por região



Raiffeisen Bank International

O Raiffeisen Bank International transforma a segurança na Zscaler Zero Trust Exchange

A Zscaler substitui dispositivos legados para fornecer proteção abrangente contra ameaças, oferecer flexibilidade de trabalho de qualquer lugar e reduzir custos de segurança

RESUMO DO RAIFFEISEN BANK

Um dos principais bancos corporativos e de investimento da Áustria

Serviços financeiros e seguros

Viena, Áustria

Milhões de clientes em 12 mercados

44 mil

funcionários protegidos por zero trust

18,6 milhões

de clientes desfrutam de serviços bancários seguros

Uma

plataforma entrega zero trust total

Desafios

- Uma infraestrutura de segurança tradicional não era compatível com uma abordagem que priorizasse a nuvem, colocando usuários e cargas de trabalho em risco
- Os dispositivos de segurança legados não ofereciam suporte à flexibilidade do trabalho de qualquer lugar, resultando em latência e baixo desempenho
- As VPNs não permitiam o acesso baseado em identidade para aplicativos privados, levando a políticas inconsistentes e uma superfície de ataque mais ampla

Jornada em fases

1. **Implementou uma plataforma zero trust abrangente**, aproveitando as vantagens de serviços públicos e privados para proteger os usuários em qualquer local
2. **Protegeu a conectividade direta à internet, sem retorno do tráfego,** para garantir experiências de usuário consistentes para uma equipe de trabalho híbrida
3. **Substituiu dispositivos de VPN por acesso zero trust para aplicativos privados** e refinou políticas de acesso baseadas em identidade

Resultados

- **Protege a conectividade de entrada e saída para uma equipe de trabalho híbrida**, oferecendo proteção consistente em todos os locais
- **Reduz a latência e melhora o desempenho de aplicativos privados e SaaS** para melhorar as experiências de usuário no escritório e remotamente
- **Simplifica a arquitetura de segurança e oferece proteção abrangente contra ameaças,** ao mesmo tempo que reduz os gastos com segurança

A parceria com a Zscaler nos trouxe mais segurança, menos custos e uma melhor experiência de usuário ao aplicar nossos princípios de zero trust.

Peter Gerdenitsch
CISO do grupo,
Raiffeisen Bank International

Ver história de sucesso

O Conselho Municipal de Magdeburg garante sua transformação digital com a Zscaler Zero Trust Exchange

A capital do estado alemão substitui dispositivos de VPN e capacita uma equipe de trabalho híbrida ao mesmo tempo em que estabelece as bases para a evolução digital contínua com a Zscaler

RESUMO DA CAPITAL ESTADUAL MAGDEBURGO

Fornece serviços administrativos aos residentes da capital da Saxônia–Anhalt

- Governo e serviços federais
- Magdeburgo, Alemanha
- 2.500 funcionários

2,5 mil
funcionários híbridos protegidos

230 mil
moradores da cidade com suporte

Uma
solução de fornecedor único para simplificar a segurança

Desafios

- Uma arquitetura de segurança tradicional baseada em hardware não era ágil o suficiente para dar suporte às metas de transformação digital
- As soluções de proxy e firewall legadas não conseguiam expandir para proteger a conectividade de internet para uma equipe de trabalho cada vez mais híbrida
- As VPNs não permitiam o controle de acesso granular, colocando os aplicativos privados em maior risco e limitando as capacidades de trabalho remoto

Jornada em fases

1. **Implantou uma plataforma zero trust nativa na nuvem** para modernizar a arquitetura de segurança e permitir uma maior transformação digital
2. **Introduziu conectividade de internet segura e direta**, aproveitando a funcionalidade de inspeção de tráfego integrada para gerenciar ameaças
3. **Protegeu o acesso a aplicativos privados com controles zero trust baseados em identidade**, garantindo proteção consistente para dados críticos

Resultados

- **Melhora as experiências de usuário para uma equipe de trabalho híbrida** e permite o trabalho remoto seguro para até 1.500 usuários mensalmente
- **Reduz os custos de segurança e a complexidade de gerenciamento** com uma arquitetura que desativa produtos de segurança legados
- **Acelera os esforços futuros de transformação digital** com uma arquitetura de segurança zero trust abrangente e dimensionável

Queríamos ser um exemplo para outros municípios e incentivá-los a avaliar e implementar boas soluções para o negócio, assim como fizemos com uma solução de segurança baseada na nuvem.

Dr. Tim Hoppe
Escritório de Estatísticas, Eleições e Digitalização, Cidade de Magdeburgo

Ver história de sucesso

A Cisalfa Sport fortalece sua postura de segurança acelerando a implantação da Zscaler em menos de três meses

A plataforma zero trust reduz a superfície de ataque e garante uma experiência de usuário perfeita para funcionários e usuários terceirizados

RESUMO DA CISALFA SPORT

Principal varejista esportivo omnicanal da Itália

Varejo e atacado

Curno (BG), Itália

Mais de 3.600 funcionários

2,5
meses para implantação da Zscaler em toda a empresa

Mais de 130
parceiros e prestadores de serviço terceirizados acessam com segurança aplicativos privados e infraestrutura local

70%
dos usuários integrados em duas semanas após a implantação

Desafios

- A VPN permitia que todos os funcionários e terceiros tivessem acesso não segmentado a toda a rede corporativa, aumentando o risco e o raio de ação de possíveis ataques
- Duas soluções de VPN legadas tinham políticas e configurações conflitantes, resultando em problemas de segurança inconsistente e gerenciamento de segurança
- O acesso a aplicativos via VPN resultou em desempenho lento e um alto volume de incidentes de suporte técnico de usuários internos e externos

Jornada em fases

1. **Reduziu a superfície de ataque** substituindo VPNs vulneráveis por acesso direto do usuário ao aplicativo privado
2. **Impediu a movimentação lateral de ameaças** por meio da aplicação de políticas de acesso de privilégio mínimo para todos os usuários
3. **Melhorou a experiência do usuário** com desempenho e confiabilidade aprimorados do aplicativo, sem mais interrupções ou vários logins de VPN para acessar recursos

Resultados

- **Aumenta a postura geral de segurança** ao fornecer acesso direto do usuário ao aplicativo para todos os usuários e aplicação consistente de políticas
- **Permite acesso transparente e sem cliente** a aplicativos e dados privados para parceiros e prestadores de serviço
- **Reduz os incidentes de suporte técnico relacionados à latência** com conectividade extremamente rápida fornecida pelo ponto de presença mais próximo

A Zscaler Zero Trust Exchange... cobre todas as bases: acesso mais rápido e seguro a aplicativos sem a necessidade de VPN, redução de risco em todo o ambiente e um caminho explícito para expansão do zero trust.

Fabio Freti
Gerente de operações de TI
e infraestrutura, Cisalfa Sport

Ver história de sucesso

A Hydro reforça sua postura de segurança e esforços de sustentabilidade na Zscaler Zero Trust Exchange

A Zscaler reduz a superfície de ataque e a pegada de carbono à medida que o provedor de energia renovável pretende aposentar o hardware legado e se tornar 100% cloud-first

RESUMO DA HYDRO

Uma das maiores empresas de energia renovável do mundo, com presença em 40 países

Fabricação

Oslo, Noruega

31 mil funcionários

33 mil

funcionários protegidos com zero trust

Um

único fornecedor para redução de custos e complexidade

100%

Operações na nuvem meta

Desafios

- A infraestrutura e o hardware de segurança legados consumiam muita energia e não estavam alinhados com as metas de sustentabilidade corporativa
- Uma rede MPLS de baixa largura de banda não poderia ser dimensionada para dar suporte ao aumento no tráfego de dados vinculado à nuvem, resultando em baixo desempenho
- As VPNs tradicionais com políticas de acesso do tipo “tudo ou nada” colocavam a rede em risco, resultando em um dispendioso ataque de ransomware

Jornada em fases

1. **Provisionou conectividade segura e direta à internet**, eliminando o retorno de tráfego e melhorando a confiabilidade do acesso
2. **Substituiu VPNs legadas por acesso zero trust baseado em políticas** para aplicativos privados para proteger dados de ataques cibernéticos
3. **Implantou uma solução de monitoramento da experiência desenvolvida especificamente para tráfego na nuvem** para permitir uma resolução mais rápida dos problemas do usuário

Resultados

- **Elimina a dependência de produtos específicos legados** e reduz a pegada de carbono com uma plataforma de segurança multiusuário nativa da nuvem
- **Aprimora o desempenho de aplicativos SaaS**, melhorando as experiências de usuário para 33 mil funcionários em 140 locais
- **Reduz custos e complexidade de gerenciamento ao mesmo tempo em que melhora a postura de segurança** usando uma solução de provedor único para zero trust

Com o Zscaler Private Access, os usuários não precisam mais se conectar à rede para usar nossos aplicativos privados. Agora, à medida que continuamos a evoluir nosso ambiente de trabalho moderno, estamos caminhando para aposentar a VPN.

Armin Auth
Chefe de programas estratégicos de TI

Ver história de sucesso

A Capitec acelera a transformação digital e protege dados financeiros com a Zscaler

O maior banco da África do Sul implementa segurança zero trust em três meses, protegendo 17 mil usuários e bloqueando 745 mil ameaças na Zero Trust Exchange

RESUMO DA CAPITEC

Maior banco da África do Sul, atendendo 21 milhões de pessoas e classificado como n.º 1 em satisfação do cliente

Serviços financeiros e seguros

Cidade do Cabo, África do Sul

15.450 funcionários em 860 filiais

3
segundos para migrar aplicativos privados para a AWS

125 milhões
de violações de políticas evitadas em um ano

3
meses para a implementação abrangente Zero Trust

Desafios

- A arquitetura de segurança baseada em perímetro não conseguiu proteger com eficácia dados financeiros de alto valor contra comprometimento e perda
- Dispositivos de segurança legados, como firewalls e VPNs, eram complexos de gerenciar e a produtividade do usuário era prejudicada
- A visibilidade limitada sobre a experiência de usuário impediu uma abordagem proativa para identificação e resolução de problemas

Jornada em fases

1. **Protegeu a conectividade direta à internet e aplicativos SaaS**, aproveitando a inspeção de tráfego para evitar o comprometimento de dados
2. **Substituiu dispositivos de VPN legados, introduzindo acesso zero trust** para aplicativos privados e dados financeiros sigilosos
3. **Aproveitou recursos avançados de experiência digital e insights práticos** para resolver problemas de longa data de experiência do usuário

Resultados

- **Garante o acesso à internet e aos aplicativos na nuvem para 17 mil usuários**, evitando 125 milhões de violações de políticas por ano
- **Protege um aplicativo bancário privado acessado por mais de 11 milhões de clientes** com acesso zero trust baseado em política
- **Permite uma transformação digital mais rápida:** apenas alguns segundos para migrar aplicativos para a AWS com tempo de inatividade zero e sem falhas de segurança

Trouxemos a Zero Trust Exchange para nosso ambiente, e nossos agentes de software de segurança zero trust foram lançados para todos os nossos usuários em três meses.

Andrew Baker
CTO, Capitec

Ver história de sucesso

A Noatum implementa um conjunto de tecnologia Zscaler para dar suporte a uma variedade de casos de uso

Incluindo acesso seguro à Internet, SaaS e aplicativos privados, detecção aprimorada de ameaças cibernéticas e experiências de usuário otimizadas

RESUMO DA NOATUM

A Noatum é um grupo multinacional líder em serviços de transporte e logística

Serviços de transporte

Barcelona, Espanha

Mais de 4.300 funcionários

Dia 1
Valor imediato da plataforma

Zero
dependência de VPNs e firewalls

360
graus de quantificação de riscos

Desafios

- As VPNs tradicionais deixaram a organização muito exposta a ataques cibernéticos quando os usuários acessavam a internet
- A segurança legada, como firewalls, deixou a organização incapaz de inspecionar o tráfego criptografado
- Arquiteturas baseadas em perímetro tornaram a integração de fusões e aquisições muito mais demorada do que deveria

Jornada em fases

1. **Substituiu VPNs** por uma plataforma de nuvem para oferecer acesso seguro à internet e a aplicativos privados
2. **Criou um hub único de monitoramento da experiência baseado na nuvem** com a ZDX
3. **Avalia o risco empresarial** de forma holística com o Zscaler Risk360

Resultados

- **Permite trabalhar de qualquer lugar** com confiança, com acesso seguro e contínuo dos usuários
- **Minimiza incidentes de usuário** e melhora a análise da causa-raiz, fornecendo conhecimento e agilidade
- **Melhora a avaliação de riscos**, bem como a defesa contra ameaças, ocultando sistemas e aplicativos da internet

A VPN tradicional era o problema. A exposição que tínhamos nos serviços de internet e o risco de receber ataques constantemente, isso foi realmente o catalisador para procurarmos uma solução como a Zscaler.

Josep Pou
CISO, Noatum

Ver história de sucesso

Sanitas
Parte de Bupa

A Sanitas oferece conectividade segura e contínua com o Zscaler Internet Access

Implementando proteções para internet, SaaS e aplicativos privados para mais de 12 mil usuários, onde quer que trabalhem

RESUMO DA SANITAS

A Sanitas é uma grande seguradora médica de alto crescimento

Saúde e farmacêutico

Madri, Espanha

Mais de 11.700 mil funcionários na Espanha, Europa e América Latina

2,5
meses para implantar para todos os usuários

12–15 mil
usuários protegidos pela nossa plataforma

Zero
necessidade de se conectar a um centro de dados

Desafios

- Unidades de negócios separadas significavam meios separados de segurança sem um modelo baseado na nuvem
- As VPNs criaram um processo tedioso de autenticação de usuários com segurança fraca
- Os escritórios parceiros não conseguiam se conectar aos data centers e não conseguiam acessar os aplicativos

Jornada em fases

1. Implementa zero trust homogêneo e baseado na nuvem para proteger toda a organização em escala
2. Substituiu VPNs por um modelo zero trust para melhorar a conectividade para todos os usuários, independentemente da localização
3. Oferece acesso seguro e contínuo aos aplicativos para todos os usuários, incluindo parceiros

Resultados

- Protege entre 12 mil e 15 mil usuários em 2,5 meses com o Zscaler Internet Access
- Permite trabalhar de qualquer lugar, possibilitando negócios flexíveis e ágeis com uma experiência semelhante à de um escritório
- Oferece acesso seguro a cargas de trabalho e aplicativos

Hoje, os funcionários podem trabalhar de casa da mesma forma que trabalham no escritório, de forma transparente, flexível, ágil e sem as barreiras que tínhamos com outras soluções.

Antonio Cerezo
Chefe de segurança cibernética na Europa e América Latina

Ver história de sucesso

A Colt Technology Services melhora a segurança e a experiência digital com a Zero Trust Exchange

A parceria com a Zscaler para implantar uma arquitetura zero trust em três meses permite que a empresa ajude outras empresas a alcançar a transformação da segurança

RESUMO DA COLT TECHNOLOGY SERVICES

Fornece serviços de rede, voz e data center para mais de 25.000 empresas em todo o mundo

Telecomunicações

Londres, Reino Unido

Mais de 5 mil funcionários em 60 escritórios globais

5 mil
funcionários híbridos protegidos

83%
mais velocidade de implantação do que soluções legadas

100 milhões
de violações de política evitadas trimestralmente

Desafios

- Acelerar a migração para a nuvem para dar suporte a um ambiente de trabalho híbrido aumentou a superfície de ataque e o risco de comprometimento
- Uma solução de proxy ultrapassada não conseguia gerenciar a inspeção em linha do tráfego criptografado, resultando em pontos cegos para malware
- Os dispositivos de VPN legados não permitiam políticas dinâmicas de acesso a aplicativos privados, tornando a sustentabilidade do trabalho remoto desafiadora

Jornada em fases

1. **Implantou uma arquitetura de segurança nativa da nuvem e zero trust** para dar suporte a operações comerciais que priorizam a nuvem e o trabalho híbrido
2. **Forneceu acesso seguro e direto à internet**, inspecionando todo o tráfego criptografado para impedir ameaças e perda de dados
3. **Substituiu dispositivos de VPN legados por acesso zero trust para aplicativos privados**, tornando o trabalho remoto mais fácil e seguro

Resultados

- **Oferece experiências digitais excepcionais para mais de 5 mil funcionários híbridos,** ao mesmo tempo em que protege o tráfego de entrada e saída
- **Inspeciona o tráfego da internet em grande escala**, processando 6,7 bilhões de transações e bloqueando 476 mil ameaças de segurança trimestralmente
- **Utiliza políticas de acesso a aplicativos privados microssegmentadas e baseadas em políticas,** o que não é possível com VPNs tradicionais

A Zscaler nos ajuda a melhorar tanto a experiência de usuário quanto a segurança. A plataforma nativa da nuvem da Zscaler protege nossos funcionários, não importa onde eles trabalhem e independentemente dos dispositivos que eles usem.

Ash Surti
Diretor de digital e informação,
Colt Technology Services

Ver história de sucesso

A Primetals Technologies cria um ambiente de trabalho híbrido seguro com a Zscaler Zero Trust Exchange

Líder global em produção de metais abandona data centers e consolida uma pilha de segurança legada para acelerar a transformação digital com a Zscaler

RESUMO DA PRIMETALS TECHNOLOGIES

Líder global em soluções para plantas metalúrgicas, especializada em produção de aço

Alta tecnologia

Londres, Reino Unido

Mais de 7.500 mil funcionários

7,5 mil
usuários protegidos com zero trust

Até 35%
de redução nos custos de infraestrutura

4,53/5
classificação de satisfação dos funcionários

Desafios

- Uma pilha de segurança tradicional construída em torno de data centers não poderia ser dimensionada para dar suporte à transformação digital que prioriza a nuvem
- Os dispositivos de segurança legados, incluindo firewalls e VPNs, não eram ágeis o suficiente para oferecer suporte a um novo design de rede SD-WAN
- Os dispositivos de VPN desatualizados não protegiam efetivamente a conectividade remota para uma equipe de trabalho híbrida e globalmente dispersa

Jornada em fases

1. **Implantou conectividade direta à internet compatível com SD-WAN** para otimizar a infraestrutura e melhorar o desempenho
2. **Substituiu VPNs por acesso zero trust para aplicativos privados** para oferecer segurança ao trabalho de qualquer lugar para usuários em todo o mundo
3. **Aproveitou os recursos avançados de monitoramento da experiência do usuário** para garantir que as ferramentas de colaboração da equipe estivessem funcionando de maneira ideal

Resultados

- **Simplifica a pilha de segurança**, reduz a dependência de data centers e diminui os gastos com custos gerais de infraestrutura
- **Garante conectividade perfeita de entrada e saída** para um grupo de usuários híbridos, 25% dos quais trabalham totalmente remotos
- **Reduz o volume de incidentes de suporte técnico e resolve problemas mais rapidamente**, melhorando a experiência do usuário final e aliviando a sobrecarga administrativa

No curso da transição para a nuvem, foi necessário modernizar a pilha de segurança... a Zscaler Zero Trust Exchange (ZTE) desempenhou um papel fundamental para tornar essa visão uma realidade.

Ralph Deleja-Hotko
Chefe de soluções de backend e nuvem, Primetals Technologies

Ver história de sucesso

A Unilever aprimora a segurança global e obtém acesso “just enough” a aplicativos com Zero Trust

A Zscaler permite que a Unilever elimine VPNs, forneça aos usuários conectividade direta e segura a aplicativos e à internet e simplifique as operações em 190 países

RESUMO DA UNILEVER

Empresa global de bens de consumo com produtos usados por 3,4 bilhões de pessoas diariamente

Fabricação

Londres, Reino Unido

Vendas em 190 países

Mais de 3 bilhões

de transações protegidas semanalmente

99,9%

de tempo de atividade durante o processamento de 220 TB de dados em dois meses

Mais de 1.500

aplicativos gerenciados com acesso zero trust “just enough”

Desafios

- As VPNs legadas tinham flexibilidade limitada e não conseguiam escalar com a estratégia global de nuvem da Unilever
- O modelo de segurança tradicional aumentou o risco devido ao controle de acesso e visibilidade insuficientes
- A crescente demanda por acesso remoto sobrecarregou a infraestrutura de VPN, impactando a experiência de usuário

Jornada em fases

1. **Permitiu acesso seguro do usuário à internet e SaaS** com inspeção total do tráfego em TLS/SSL e proteção avançada contra ameaças
2. **Substituiu a VPN** por acesso zero trust para aplicativos privados
3. **Melhorou a experiência de usuário** ao fornecer monitoramento da experiência digital para identificar e resolver problemas de desempenho rapidamente

Resultados

- **Reduz os riscos** com acesso seguro e direto aos aplicativos, sem as limitações e vulnerabilidades da VPN
- **Aumenta a eficiência operacional** processando tráfego de dados em larga escala com 99,99% de tempo de atividade
- **Oferece suporte à estratégia global de nuvem**, fornecendo acesso remoto seguro em 190 países, mantendo a flexibilidade para a equipe de trabalho da Unilever

A abordagem zero trust da Zscaler transformou a segurança na Unilever. A eliminação de gargalos de VPN permite que nossa equipe de trabalho global acesse aplicativos com segurança, melhorando o desempenho, a flexibilidade e a resiliência.

Richard Mardling
Diretor de acesso
e conectividade, Unilever

Ver história de sucesso

APJ

Explore as histórias de sucesso dos clientes por região

A John Holland reduz os custos de rede em 50% usando a Zscaler Zero Trust Exchange

A Zscaler facilita a transição para a SD-WAN e permite desativar centenas de firewalls, melhorando a eficiência operacional e a postura de segurança

RESUMO DA JOHN HOLLAND

Empresa de infraestrutura integrada, construção, ferrovia e transporte multimodal

Construção

Melbourne, Victoria, Austrália

Mais de 5.000 funcionários em mais de 120 locais

1 semana
para implantar Zero Trust

6 mil
funcionários e prestadores de serviço protegidos

122 mil
ameaças bloqueadas em três meses

Desafios

- Uma arquitetura de segurança de perímetro tradicional não poderia ser dimensionada para oferecer suporte a operações comerciais cada vez mais focadas na nuvem
- Uma rede MPLS desatualizada dependia de um retorno de tráfego significativo, diminuindo a velocidade dos serviços de TI e aumentando os custos
- Os dispositivos de firewall legados não tinham agilidade para inspecionar o tráfego criptografado em linha, aumentando a vulnerabilidade a ameaças

Jornada em fases

1. **Implantou uma plataforma de segurança zero trust abrangente e nativa da nuvem** para criar um ambiente de TI mais ágil e dimensionável
2. **Reduziu a dependência de dispositivos de firewall e custos de rede** com acesso direto e seguro à internet e aplicativos SaaS
3. **Aproveitou recursos avançados de detecção de ameaças para otimizar o ecossistema de segurança** e eliminar o risco de comprometimento de dados

Resultados

- **Migra 100% dos usuários para zero trust em uma semana** e oferece provisionamento de acesso de rede mais rápido em mais de 120 locais de projetos
- **Desativa centenas de dispositivos de firewall legados com conectividade zero trust**, obtendo uma redução de 50% nos custos de rede
- **Protege a conectividade para usuários**, processando 400 TB de tráfego e prevenindo 98 milhões de violações de políticas trimestralmente

A Zscaler fornece o restante da nossa segurança que simplificou nossos processos e, por meio dessa simplificação, nos tornou muito mais seguros.

Kier Morrison
Gerente geral de operações de tecnologia de TI, John Holland

Ver história de sucesso

A Probe CX elimina as VPNs para proteger 7.600 funcionários e aplicativos essenciais na Zscaler Zero Trust Exchange

A Zscaler otimiza a pilha de segurança, simplifica o gerenciamento de políticas e reduz os gastos com tecnologia, enquanto mantém a borda de segurança robusta

RESUMO DA PROBE CX

Uma das maiores terceirizadoras de experiência do cliente e processos de negócios da Austrália

Serviços

Melbourne, Victoria, Austrália

19 mil funcionários, operações em 32 locais de entrega

100%
de VPNs sendo desativadas

8,1 bilhões
de transações processadas em um trimestre

3,1 milhões
Ameaças bloqueadas em três meses

Desafios

- Uma arquitetura de segurança tradicional não poderia ser dimensionada junto com uma equipe de trabalho em rápido crescimento ou uma abordagem em evolução que prioriza a nuvem
- As VPNs legadas não permitiam políticas de controle de acesso microssegmentadas, colocando os aplicativos privados em maior risco
- A visibilidade limitada da experiência de usuário e do desempenho de aplicativos tornou a mitigação de problemas complicada e demorada

Jornada em fases

1. **Protegeu a conectividade direta à internet e aplicativos SaaS**, inspecionando o tráfego em linha, sem necessidade de retorno do tráfego
2. **Substituiu VPNs por acesso zero trust para aplicativos privados** para proteger melhor a propriedade intelectual e dados críticos
3. **Aproveitou os recursos avançados de experiência do usuário** para resolver problemas mais rapidamente e oferecer uma experiência de trabalho remoto perfeita

Resultados

- **Oferece flexibilidade de trabalho em qualquer lugar, apoiada por princípios zero trust** para 7.600 usuários em cinco países
- **Processa aproximadamente 285 TB de tráfego por trimestre**, aplicando políticas de segurança consistentes e minimizando a superfície de ataque
- **Simplifica o gerenciamento da segurança com uma plataforma multilusuário** que oferece segurança zero trust com um TCO menor

Um dos principais benefícios que obtivemos ao implementar essa tecnologia agora é que conseguimos nos livrar de 100% dessas VPNs no ambiente.

Rohan Khanna
Diretor de tecnologia, Probe CX

Ver história de sucesso

Persistent

A Persistent aumenta a segurança ao mesmo tempo em que economiza US$ 2 milhões em custos de Capex/Opex ano a ano

O zero trust protege dados sigilosos de clientes e de propriedade intelectual, permite a inovação, reduz a complexidade e oferece suporte a metas ambientais, sociais e de governança (ESG)

RESUMO DA PERSISTENT

Um parceiro global de engenharia digital e modernização empresarial que ajuda as empresas a promover a inovação

Alta tecnologia

Pune, Índia

23 mil funcionários em 21 países

85%

de melhoria na postura de segurança com a eliminação da VPN

Mais de 80

ataques de alta prioridade interceptados em 90 dias com deception

4X

acesso mais rápido a aplicativos privados do que com a VPN

Desafios

- Fornecer conectividade rápida e uma experiência de usuário mais produtiva aos trabalhadores remotos em 21 países
- Proteger a propriedade intelectual e os dados sigilosos do cliente no ambiente de nuvem
- Simplificar uma infraestrutura complexa
- Reduzir custos operacionais e de hardware em todo o ambiente
- Encontrar um parceiro de zero trust de longo prazo com uma solução dimensionável que promova uma expansão rápida
- Minimizar o impacto ambiental reduzindo a pegada de carbono

Jornada em fases

1. **Aprimorou a postura de segurança** com conexões diretas e seguras à internet, SaaS e aplicativos privados
2. **Reduziu a latência, diminuiu custos e aprimorou a experiência de usuário** eliminando VPNs e firewalls não confiáveis e inseguros
3. **Protegeu propriedades intelectuais valiosas e dados de clientes com** prevenção avançada de perda de dados (DLP) e tecnologia de deception

Resultados

- **Melhora e acelera o acesso remoto** em quatro vezes para 23 mil trabalhadores distribuídos globalmente
- **Remove a complexidade** e melhora a eficácia e a eficiência da segurança
- **Acelera a detecção e a resposta** por meio da integração com CrowdStrike, Microsoft Entra ID e Securonix
- **Aumenta o portfólio de ofertas da empresa** com uma prática de segurança focada na Zscaler para seus próprios clientes

A Zscaler DLP fornece à equipe de segurança uma visão granular do uso de aplicativos de IA generativa ocultos, incluindo prompts de entrada, e impõe bloqueio de DLP em tempo real e isolamento de aplicativos

Debashis Singh
Diretor de informação, Persistent

Ver história de sucesso

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

O Keiju Medical Center transforma o atendimento digital ao paciente na Zscaler Zero Trust Exchange

A Zscaler fornece uma solução para acesso móvel seguro aos dados de EMR, permite que os médicos colaborem de qualquer lugar e aprimora as experiências dos pacientes

RESUMO DO KEIJU MEDICAL CENTER

O único hospital de apoio médico na região de Noto, reconhecido como líder digital

- Saúde e farmacêutico
- Cidade de Nanao, província de Ishikawa, Japão
- Mais de 800 funcionários para mais de 400 leitos

800
funcionários hospitalares protegidos

100s
de dispositivos móveis conectados com segurança

Uma
plataforma para segurança zero trust

Desafios

- Uma arquitetura de segurança em perímetro não conseguiu se adaptar à crescente necessidade de atendimento digital a pacientes e telemedicina
- Os firewalls legados não conseguiam proteger a conectividade à internet remotamente, limitando o recrutamento de médicos a uma pequena área local
- As VPNs tradicionais colocam aplicativos e recursos privados, incluindo dados sigilosos de pacientes, em maior risco de comprometimento

Jornada em fases

1. **Implantou uma arquitetura de segurança zero trust nativa da nuvem** para oferecer suporte a formas alternativas de fornecer atendimento digital a pacientes
2. **Introduziu conectividade segura e direta à internet**, permitindo que a equipe médica trabalhe de forma flexível e segura em qualquer lugar
3. **Eliminou dispositivos de VPN e adotou acesso zero trust** para aplicativos privados para proteger o acesso remoto aos dados de EMR

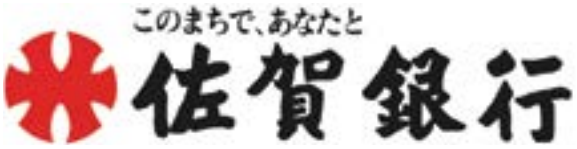
Resultados

- **Oferece a flexibilidade do trabalho de qualquer lugar para a equipe médica** e expande a abertura de recrutamento para médicos qualificados
- **Protege registros sigilosos de pacientes contra ameaças** quando acessados remotamente; mais de 500 dispositivos móveis se conectam com segurança aos dados de EMR
- **Elimina a necessidade de dispositivos de segurança legados** e melhora a eficiência operacional, resultando em melhor atendimento a pacientes

A transformação digital é essencial para garantir que a equipe possa trabalhar de forma eficiente com recursos limitados. Muitos médicos moram mais longe... então precisávamos de um ambiente de acesso remoto seguro e fácil de usar.

Sr. Masahiro Kamino
Presidente do Conselho de Administração, Keiju Medical Center

Ver história de sucesso



O Bank of Saga apoia a transformação digital com a Zscaler Zero Trust Exchange

A Zscaler otimiza a infraestrutura, reduz a dependência de soluções legadas e fortalece a postura de segurança à medida que as operações bancárias migram para a nuvem

RESUMO DO BANK OF SAGA

Provedor de serviços financeiros focado na comunidade trabalhando para melhorar a conveniência do cliente

- Serviços financeiros e seguros
- Cidade de Saga, Prefeitura de Saga, Japão
- Mais de 1.200 funcionários

Cerca de 33%
menos custos de comunicação

1,8 mil
de usuários protegidos com zero trust

Um
login único aumenta a produtividade

Desafios

- Uma arquitetura de segurança tradicional baseada em perímetro não seria compatível com os esforços contínuos de migração para a nuvem do banco
- Os dispositivos de segurança legados não tinham agilidade para expandir com as crescentes necessidades de conectividade direta e confiável à internet
- As VPNs eram caras de manter e aumentavam a superfície de ataque, deixando aplicativos e dados privados vulneráveis a ameaças

Jornada em fases

1. **Implantou uma abrangente plataforma zero trust nativa na nuvem** para aplicar políticas de segurança consistentes em toda a empresa
2. **Introduziu conectividade direta à internet** e aproveitou a inspeção de tráfego em linha para proteger o acesso a aplicativos SaaS públicos
3. **Substituiu VPNs por acesso zero trust para aplicativos privados**, aproveitando opções de configuração granular para proteger dados críticos

Resultados

- **Protege a conectividade de entrada e saída para funcionários**, aplicando políticas de acesso consistentes, independentemente da localização
- **Protege aplicativos bancários privados e dados críticos contra comprometimento**, assegurando e melhorando as experiências do cliente
- **Simplifica a pilha de segurança e substitui dispositivos legados**, simplificando o gerenciamento de políticas e reduzindo custos

Uma mudança para a nuvem é necessária para a transformação digital. ... [No entanto,] a segurança de limites convencional não permite que a conveniência do SaaS e dos serviços web seja totalmente utilizada. A segurança zero trust era essencial.

Sr. Hiroaki Hayashida
Diretor adjunto do Grupo de Planejamento e Desenvolvimento de Sistemas, Departamento de Sistemas, Sede de Gestão Empresarial, The Bank of Saga

Ver história de sucesso

A Cebu Pacific Air protege sua equipe de trabalho híbrida com a Zscaler Zero Trust Exchange

A Zscaler melhora a experiência de trabalho remoto para 3.900 funcionários e protege operações comerciais críticas em sete centros estratégicos na Ásia

RESUMO DA CEBU PACIFIC AIR

Principal companhia aérea das Filipinas, operando voos para mais de 60 destinos

- Serviços de transporte
- Metro Manila, Filipinas
- 3.900 funcionários em sete centros estratégicos

234 milhões
de violações de política evitadas trimestralmente

90%
de aumento na satisfação dos usuários

2
semanas para implantar acesso remoto zero trust a aplicativos

Desafios

- Uma infraestrutura de segurança legada retardou os esforços de transformação digital e aumentou o risco de comprometimento e ameaças
- Os dispositivos de segurança tradicionais não conseguiam proteger adequadamente os recursos privados essenciais para as operações comerciais
- Os dispositivos de VPN enfrentaram problemas de desempenho e conectividade, tornando o trabalho remoto mais difícil e menos seguro

Jornada em fases

1. **Aposentou uma arquitetura de segurança legada desatualizada**e, em seu lugar, implantou uma abrangente plataforma zero trust nativa na nuvem
2. **Forneceu acesso seguro e direto à internet com recursos avançados de proteção contra ameaças** para oferecer melhor suporte a uma equipe de trabalho híbrida
3. **Substituiu os dispositivos de VPN tradicionais por acesso zero trust** para aplicar controles granulares de acesso a aplicativos privados

Resultados

- **Protege a conectividade de trabalho de qualquer lugar para 3.900 usuários com uma alternativa segura à VPN**, melhorando a satisfação dos usuários em 90%
- **Simplifica a pilha de segurança, ao mesmo tempo que fornece proteção robusta:** processa 733 milhões de transações por ano
- **Previne 234 milhões de violações de políticas e bloqueia 45.000 ameaças de segurança em um único trimestre**, melhorando a postura de segurança

Nosso ambiente de trabalho é dinâmico e, com a Zscaler, os funcionários podem continuar a trabalhar de forma produtiva sem prejudicar sua capacidade de se conectar aos recursos de que precisam, sem comprometer a segurança.

Laureen Cansana
CIO, Cebu Pacific Air

Ver história de sucesso

maxeon

A Maxeon Solar Technologies alcança a transformação digital com a Zscaler após uma alienação

Líder em energia solar elimina data centers para melhorar a postura de segurança e as experiências de trabalho remoto para 5.000 usuários globais na Zero Trust Exchange

RESUMO DA MAXEON

Líder global em fabricação de painéis solares com presença de vendas em mais de 100 países

Energia, petróleo, gás e mineração

Singapura

5.000 funcionários em 40 locais

134%

mais tráfego processado trimestralmente

31 milhões

de violações de políticas evitadas em um trimestre

2,9 milhões

de ameaças bloqueadas em três meses

Desafios

- A segurança de perímetro tradicional construída em torno de data centers não era compatível com uma infraestrutura em evolução e que prioriza a nuvem
- Os firewalls legados não conseguiam acompanhar as crescentes necessidades de acesso remoto, o que resultava em baixo desempenho e maior risco
- As soluções de DLP anteriores eram difíceis de gerenciar, deixando a propriedade intelectual e os ativos críticos em risco de comprometimento

Jornada em fases

1. **Protegeu a conectividade direta à internet com inspeção de tráfego em linha** para proteger os usuários em qualquer lugar onde precisem de acesso online
2. **Implantou uma solução de monitoramento da experiência desenvolvida especificamente para zero trust** para agilizar os processos de integração e licenciamento
3. **Introduziu uma solução de DLP integrada** para proteger informações críticas, garantir a conformidade e evitar violações de dados

Resultados

- **Acelera a transformação digital:** todos os data centers foram desativados e 70% das cargas de trabalho migraram para a nuvem
- **Protege a flexibilidade do trabalho de qualquer lugar** para um grupo de usuários geograficamente dispersos que trabalham em 16 países
- **Protege dados críticos de PI, incluindo mais de 1.400 patentes,** melhorando a postura de segurança e garantindo a continuidade dos negócios

Embora tenhamos avaliado vários fornecedores de renome, a Zscaler saiu como uma clara vencedora devido à sua posição de liderança no Gartner Magic Quadrant e seus recursos comprovados.

Stephen Gani
CISO, Maxeon Solar Technologies

Ver história de sucesso