Folha de dados

Zscaler Private Access™

Capacite suas equipes de trabalho híbridas com acesso rápido, seguro e confiável a aplicativos privados com o único ZTNA de nova geração do setor.

A Zscaler redefine o acesso a aplicativos privados com recursos avançados de conectividade, segmentação e segurança para proteger sua empresa contra ameaças e oferecer uma excelente experiência de usuário.

As abordagens legadas de rede e segurança atendem às necessidades das equipes de trabalho híbridas atuais

Conectar usuários a aplicativos privados não deve ser algo lento, complicado ou arriscado. O trabalho híbrido e a transformação da nuvem derrubaram os modelos de segurança de rede baseados em perímetro, com aplicativos privados migrando para a nuvem e usuários acessando aplicativos pela internet pública, em qualquer dispositivo, de qualquer local. As abordagens tradicionais que dependem de VPNs e firewalls legados para controlar o acesso a aplicativos tornaram-se ineficazes em um mundo que prioriza a nuvem e a mobilidade.

Até 2025, pelo menos 70% das novas implantações de acesso remoto serão realizadas predominantemente por acesso à rede zero trust (ZTNA) em vez dos arcaicos serviços de VPN, que tiveram um aumento de menos de 10% no final de 2021, de acordo com a Gartner.

Benefícios:

- **Aumente a produtividade de equipes de trabalho híbridas** Obtenha acesso rápido e contínuo a aplicativos privados, quer seus usuários estejam em casa, no escritório ou em qualquer outro lugar
- **Mitigue os riscos de uma violação de dados** Minimize a superfície de ataque e a movimentação lateral, tornando os aplicativos invisíveis para a internet e, ao mesmo tempo, aplicando o acesso de privilégio mínimo
- **Detenha os adversários mais avançados** A proteção de aplicativos privados inédita e a inspeção completa de tráfego em linha minimizam o risco de usuários comprometidos e invasores ativos
- **Amplie a segurança zero trust em aplicativos, cargas de trabalho e dispositivos** A plataforma de ZTNA mais completa do mundo oferece acesso de privilégio mínimo a aplicativos privados, cargas de trabalho e dispositivos de TO/IIoT
- **Reduza a complexidade operacional** Nossa plataforma nativa da nuvem elimina soluções legadas de acesso remoto, como VPNs, que são difíceis de dimensionar, gerenciar e configurar

As abordagens de segurança de redes legadas podem ser facilmente contornadas por invasores que aproveitam a confiança inerente e o acesso exageradamente permissivo das arquiteturas tradicionais de castelo e fosso, pois:

- **A arquitetura legada não pode ser dimensionada ou oferecer uma experiência de usuário rápida e contínua:** as VPNs exigem o retorno do tráfego, o que apresenta custos, complexidade e muita latência para as atuais equipes de trabalho remotas
- **Firewalls tradicionais, VPNs, VDI e aplicativos privados criam uma enorme superfície de ataque:** os invasores podem descobrir e explorar recursos vulneráveis expostos externamente
- **O acesso total à rede permite a movimentação lateral livre:** as VPNs inserem usuários na sua rede, proporcionando aos invasores acesso fácil a dados sigilosos
- **Usuários comprometidos e ameaças internas podem ignorar os controles tradicionais:** invasores avançados podem roubar credenciais e adulterar a identidade para acessar aplicativos privados com ferramentas de acesso remoto legadas e ofertas de ZTNA de primeira geração

É hora de repensar como conectamos os usuários de forma segura e ininterrupta aos aplicativos necessários. É hora de redefinir a segurança de aplicativos privados com uma nova geração de ZTNA.

Zscaler Private Access™ (ZPA)

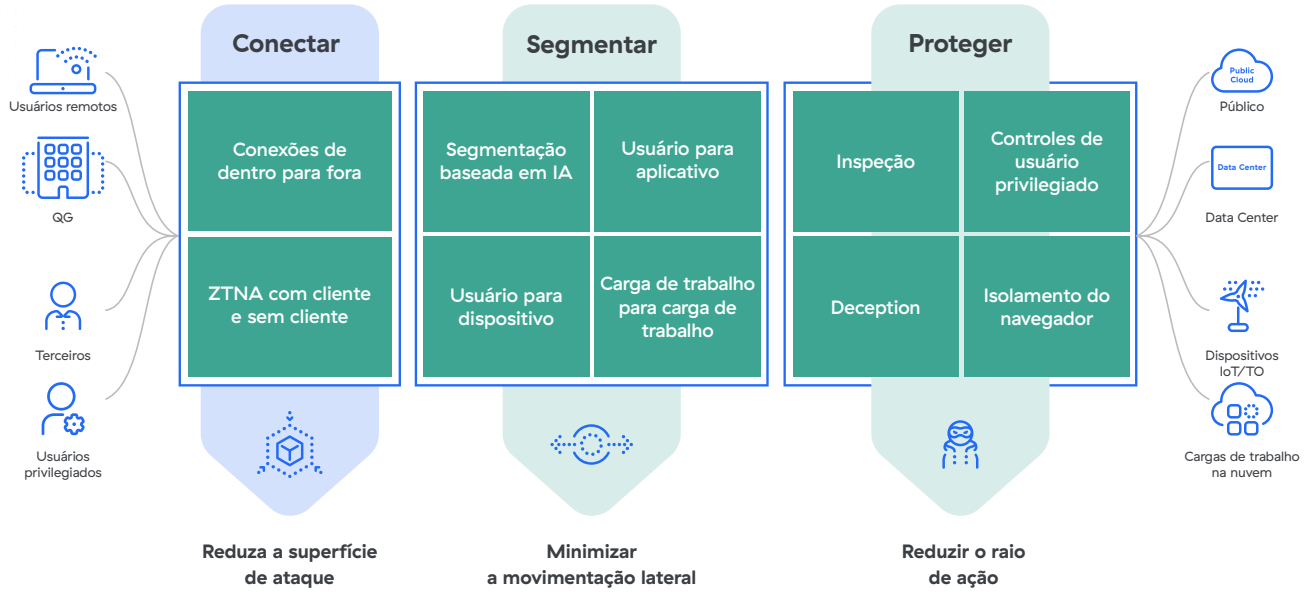
O ZPA é a plataforma de ZTNA mais implantada do mundo, que aplica os princípios de privilégio mínimo para oferecer aos usuários conectividade segura e direta a aplicativos privados executados localmente ou na nuvem pública, além de eliminar o acesso não autorizado e a movimentação lateral. Por ser um serviço nativo da nuvem desenvolvido sobre uma estrutura holística de borda de serviço de segurança (SSE), o ZPA pode ser implantado em questão de horas para substituir VPNs legadas e ferramentas de acesso remoto para:

- **Oferecer uma experiência de usuário superior:** conectar os usuários diretamente a aplicativos privados elimina o lento e caro retorno do tráfego em VPNs legadas, ao mesmo tempo em que monitora continuamente e soluciona proativamente problemas de experiência do usuário
- **Minimizar a superfície de ataque:** os aplicativos ficam invisíveis para a internet, evitando que usuários e dispositivos não autorizados os descubram. As conexões de dentro para fora entre usuário e aplicativo garantem que aplicativos e IPs nunca sejam expostos
- **Impor o acesso de privilégio mínimo:** o acesso ao aplicativo é determinado pela identidade e pelo contexto — não por um endereço IP — e os usuários nunca são colocados na rede para acesso
- **Eliminar a movimentação lateral:** os aplicativos são segmentados para que os usuários possam acessar apenas um aplicativo específico, ajudando a limitar a movimentação lateral
- **Interromper ataques cibernéticos com a inspeção completa:** o tráfego de aplicativos privados é inspecionado em linha para evitar as técnicas de ataques na web mais prevalentes
- **Evitar a perda de dados:** DLP integrada para aplicativos privados, resposta avançada a incidentes e classificação de dados para proteger os aplicativos mais importantes
- **Detectar usuários e dispositivos comprometidos:** as iscas integradas identificam e removem rapidamente usuários e dispositivos maliciosos

Até 2025, pelo menos 70% das novas implantações de acesso remoto serão realizadas predominantemente por acesso à rede zero trust (ZTNA).

— Gartner

Como o ZPA aborda casos de uso emergentes para ZTNA



Principais casos de uso

Alternativa à VPN
As VPNs não foram projetadas tendo em mente segurança, capacidade de dimensionamento ou experiência do usuário. Tradicionalmente, as VPNs transferem todo o tráfego de usuários remotos para data centers que podem estar a milhares de quilômetros de distância, resultando em latência e frustração do usuário. Uma vez conectadas, as VPNs encapsulam os usuários através do firewall e os colocam na mesma rede dos seus aplicativos, o que permite a movimentação lateral livre.

O ZPA supera esses desafios fornecendo acesso rápido e direto a aplicativos por meio de mais de 150 pontos de presença (PoPs) distribuídos globalmente, sem os riscos de segurança inerentes à VPN. Sua conectividade de dentro para fora garante que o acesso aos aplicativos seja dissociado do acesso à rede, ao mesmo tempo que elimina a presença voltada à internet. O ZPA conecta os usuários a aplicativos, não a redes, e os usuários só podem acessar aplicativos específicos, não podendo mover-se lateralmente. O design nativo da nuvem do ZPA permite que as equipes de TI eliminem dispositivos de gateway de entrada, como balanceadores de carga, concentradores de VPN e outros dispositivos de segurança, reduzindo custos, complexidade e sobrecarga de gerenciamento.

Equipes de trabalho híbridas seguras
Nas equipes de trabalho modernas, os usuários trabalham de suas casas e outros locais remotos, filiais e sedes, desafiando os paradigmas da segurança legada. O ZPA oferece acesso contínuo e seguro a aplicativos privados de onde quer que eles precisem trabalhar, em qualquer dispositivo. Os usuários presenciais se beneficiam de uma experiência idêntica por meio do ZPA Private Service Edge.

O ZPA Private Service Edge permite que você implante o poder da nuvem em suas instalações, aplicando os mesmos controles de segurança dos seus usuários remotos com o mesmo alto desempenho. O ZPA agora é capaz de fornecer recursos de ZTNA universais para oferecer uma experiência de usuário rápida e consistente. Além disso, com o monitoramento da experiência digital, você obtém visibilidade em tempo real

sobre degradação de desempenho e interrupções, tornando o trabalho híbrido mais produtivo. Como faz parte da Zscaler Zero Trust Exchange™, os usuários se beneficiam de uma plataforma de SSE integrada para obter acesso seguro, rápido e direto à internet, SaaS, cargas de trabalho, dispositivos e aplicativos privados.

Alternativa ao acesso de terceiros/VDI
No passado, o acesso de terceiros dependia de uma infraestrutura de desktop virtual (VDI) desajeitada e cara ou de outros clientes de desktop remoto, como RDP, SSH ou VNC, que inseriam os usuários diretamente na sua rede e expunham os sistemas internos a dispositivos não confiáveis. Os recursos de acesso sem cliente do ZPA tornam o acesso de terceiros tão fácil quanto o acesso à web, reduzindo custos e minimizando riscos. Seus fornecedores, prestadores de serviços e parceiros podem usar livremente qualquer navegador da web em seus próprios dispositivos para se conectar a sites de intranet, sistemas internos e equipamentos, sem necessidade de clientes. Ele mantém usuários terceirizados e dispositivos não gerenciados isolados da sua rede e aplicativos, garantindo que os dados sigilosos nunca fiquem fora de seu controle e permaneçam protegidos contra ações não autorizadas de copiar/colar, impressão e upload/download. Com o acesso sem cliente, a TI pode oferecer uma experiência melhor e mais segura aos usuários sem incorrer nos custos de gerenciamento de VDIs legadas.

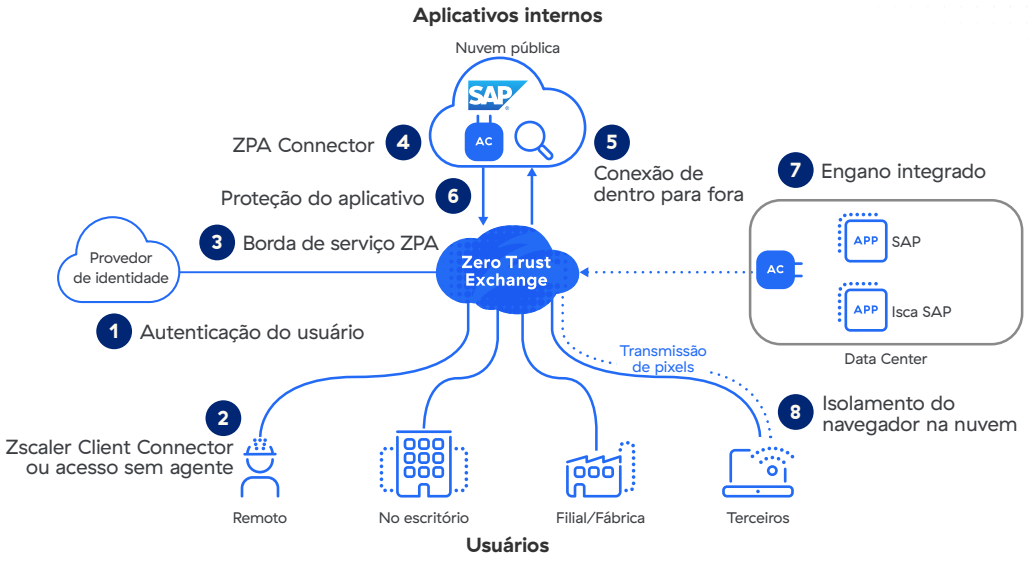
Fusões, aquisições e alienações
Os processos de fusões, aquisições e alienações muitas vezes exigem mesclar redes, o que pode ser um desafio devido à sobreposição de espaço de IP e à criação de firewalls entre as duas entidades. O ZPA melhora drasticamente a integração e o prazo de maturação após fusões e aquisições, acelerando o processo para questão de semanas em vez de meses. Ele fornece acesso contínuo a aplicativos privados, sem a necessidade de VPNs, e elimina a necessidade de convergir várias redes ou adquirir equipamentos de rede adicionais, liberando recursos para se concentrar em ações de alto impacto.

Acesso seguro do operador para TO e IIoT
Os funcionários e fornecedores terceirizados precisam acessar frequentemente os ativos de TO e IIoT para maximizar o tempo de atividade da produção, bem como evitar interrupções causadas por falhas de equipamentos e processos. O ZPA oferece acesso rápido, seguro e confiável a ambientes de TO e IIoT em locais de campo, no chão de fábrica ou em qualquer outro lugar. O ZPA para IoT e TO fornece acesso de desktop remoto totalmente isolado e sem clientes para sistemas de destino internos de RDP, SSH e VNC, sem exigir que os usuários instalem um cliente em seus dispositivos usando hosts de salto e VPNs legadas.

Conectividade segura entre cargas de trabalho
As organizações modernas exigem conectividade rápida e segura entre cargas de trabalho em ambientes privados, híbridos e multinuvem. O ZPA para cargas de trabalho reduz a complexidade e os custos operacionais, ao mesmo tempo que promove conectividade baseada em zero trust para cargas de trabalho em todos esses ambientes. Como as cargas de trabalho estão ocultas atrás do ZPA, elas são invisíveis para a internet e impossíveis de serem atacadas.

Conectividade zero trust para filiais
A conectividade zero trust para filiais conecta com segurança filiais, fábricas e data centers sem a complexidade das VPNs, garantindo acesso zero trust entre usuários, dipositivos de IoT/TO e aplicativos com base em políticas de negócios. Ela elimina a superfície de ataque e evita a movimentação lateral de ameaças, conectando usuários e dispositivos de IoT/TO a aplicativos por meio da Zero Trust Exchange. A conectividade zero trust para filiais simplifica drasticamente as comunicações das filiais, eliminando roteamentos complexos, VPNs e firewalls, ao mesmo tempo que oferece encaminhamentos flexíveis e gerenciamento simples de políticas com a estrutura de política comprovada do ZIA e ZPA.

O ZPA amplia o acesso de privilégio mínimo para toda a empresa



Como funciona

Quando um usuário (funcionário, fornecedor, parceiro ou prestador de serviços) tenta acessar um aplicativo interno, o ZPA fornece conectividade segura e direta seguindo essas etapas:

1. O usuário se autentica com o IdP usando as credenciais SAML SSO existentes.
2. A postura do dispositivo do usuário é verificada com o Zscaler Client Connector, um agente leve de encaminhamento instalado no laptop ou dispositivo móvel do usuário. O ZPA também pode assimilar a postura do dispositivo por meio de uma integração terceirizada com todos os principais provedores de EPP/EDR/XDR (por exemplo, Crowdstrike, Microsoft Defender, SentinelOne).
3. O aplicativo da Zscaler encaminha o tráfego do usuário para a Borda de serviço ZPA mais próxima, que atua como um agente, com a verificação das políticas de segurança e acesso do usuário.
4. Depois, a Borda de serviço ZPA determina a aplicação mais próxima ao usuário e estabelece uma conexão segura com o ZPA App Connector, uma máquina virtual leve instalada no ambiente que hospeda servidores e aplicativos.
5. Dois túneis de saída, um do Client Connector no dispositivo e outro do App Connector, são unidos pela Borda de serviço ZPA.
6. Assim que a conexão é estabelecida entre o dispositivo do usuário e o aplicativo, o App Connector inspeciona automaticamente o tráfego em linha para detectar e interromper possíveis ameaças de usuários ou dispositivos que possam estar comprometidos.
7. O Zscaler Deception integrado detecta usuários comprometidos acessando aplicativos iscas e pode desativar o acesso a recursos internos na Zscaler Zero Trust Exchange.
8. Além disso, os usuários terceirizados podem se conectar a aplicativos privados com o acesso integrado pelo navegador ou com o isolamento do navegador na nuvem, para acesso sem cliente em dispositivos não gerenciados.

Uma borda de serviço do ZPA pode ser hospedada pela Zscaler na nuvem (borda de serviço público ZPA) ou executada localmente, dentro da infraestrutura do cliente (borda de serviço privado ZPA). De qualquer modo, elas são gerenciadas pela Zscaler, sem a exigência de dispositivos.

Principais recursos

Mecanismo de políticas baseadas em risco	Valide continuamente as políticas de acesso baseadas em usuário, dispositivo, conteúdo e postura de risco do aplicativo com um poderoso mecanismo nativo de políticas, para garantir que somente usuários válidos e autenticados possam acessar aplicativos privados.
Acesso unificado com cliente e sem cliente	Escolha o método de proteção ideal para o seu ambiente híbrido. O acesso com cliente garante que os usuários gerenciados permaneçam protegidos mesmo quando estiverem fora da rede corporativa através de um agente leve, o Zscaler Client Connector. O acesso sem cliente fornece aos usuários não gerenciados acesso sem atrito a aplicativos, de qualquer dispositivo e navegador web.
Acesso pelo navegador	Permita que usuários de dispositivos pessoais e terceirizados usem livremente seus dispositivos para acessar aplicativos internos de maneira direta e segura, utilizando qualquer navegador web, sem a necessidade de instalar um cliente.
ZTNA local	Ofereça o ZTNA para usuários locais, conectando com segurança usuários em escritórios a aplicativos. O ZTNA universal garante acesso e políticas consistentes para os usuários, independentemente de seu local e aplicativo.
Recuperação de desastres	Garanta o acesso ininterrupto a aplicativos essenciais, mesmo durante um evento de cisne negro, com uma solução de continuidade de negócios controlada pelo cliente, criando uma rota de acesso a aplicativos privados importantes por meio da Private Service Edge (borda de serviço privado) do ZPA.
Descoberta de aplicativos	Descubra e catalogue automaticamente os aplicativos que usam nomes de domínio específicos e sub-redes IP para obter uma visão granular do seu patrimônio de aplicativos privados, bem como da sua possível superfície de ataque.
Segmentação de aplicativos baseada em IA	Aplique as recomendações de segmentação baseadas em aprendizado de máquina distribuídas automaticamente para você no ZPA, agilizando e facilitando a identificação dos segmentos de aplicativo corretos e a criação das políticas de acesso corretas. Baseada em modelos de aprendizado de máquina continuamente treinados com milhões de sinais de clientes e seus padrões exclusivos de acesso a aplicativos, a segmentação baseada em ML pode ajudar a minimizar sua superfície de ataque interna.
Segmentação Usuário para app	Garanta que todo o acesso a aplicativos seja concedido conforme a necessidade e com privilégios mínimos, com a segmentação de usuário para aplicativo. Ofereça aos usuários autorizados acesso seguro a aplicativos específicos sem a necessidade de inseri-los na rede. Evite a necessidade de segmentações de rede complexas com firewalls internos.
Segmentação Usuário para dispositivo	Garanta que todo acesso a equipamentos e sistemas de TO/IIoT seja concedido com base no privilégio mínimo, com a segmentação de usuário para dispositivo. Permita que fornecedores terceirizados e usuários remotos se conectem de qualquer local a equipamentos com o ZPA para IoT e TO.
Segmentação de carga de trabalho para carga de trabalho	Garanta a conectividade e a comunicação segura de carga de trabalho para carga de trabalho em ambientes híbridos e multinuvem com o ZPA for cargas de trabalho.
Proteção de aplicativos	Proteja os aplicativos privados e a infraestrutura contra os ataques mais comuns com a inspeção de segurança integrada de alto desempenho de toda carga de aplicativos que expõe ameaças. Identifique e bloqueie os riscos conhecidos de segurança web, como o OWASP Top 10, e as vulnerabilidades emergentes de dia zero que podem contornar os controles de segurança de rede tradicionais.
Engano integrado	Detecte e detenha os mais sofisticados invasores e ameaças internas com o engano do aplicativo nativo, incluindo a contenção automatizada de usuários comprometidos por toda a Zero Trust Exchange.
Isolamento integrado do navegador na nuvem	Ofereça acesso isolado e sem cliente a aplicativos web essenciais para prestadores de serviço e funcionários que usam dispositivos pessoais. Garanta que terminais não gerenciados com vulnerabilidades ou infecções de malware não comprometam sua rede ou aplicativos. Aplique controles de exfiltração de dados (copiar/colar, imprimir, upload/download) para evitar a perda de dados sigilosos.
Acesso remoto privilegiado	Permita que administradores e operadores com privilégios se conectem com segurança a sites da intranet, sistemas internos e equipamentos sem a necessidade de VPNs, VDIs ou clientes de área de trabalho remota como RDP, SSH e VNC.
Proteção dos dados contra ameaças	Reduza o risco de ameaças com a inspeção completa de conteúdo. Encontre e controle dados sigilosos na conexão entre usuário e aplicativo.
SD-WAN Zero Trust	Conecte filiais, fábricas e data centers com segurança sem a complexidade das VPNs, garantindo acesso zero trust entre usuários, dispositivos de IoT/TO e aplicativos com base em políticas de negócios.

Benefícios

Minimize a superfície de ataque
Eliminar VPNs vulneráveis e tornar os aplicativos invisíveis para a internet impossibilita que usuários não autorizados os encontrem e ataquem. O ZPA cria um segmento entre um usuário autorizado e um aplicativo privado específico, removendo toda a conectividade de entrada e permitindo apenas conexões de dentro para fora por meio de microtúneis criptografados para os dispositivos dos usuários. Os administradores podem descobrir e segmentar automaticamente aplicativos, serviços e cargas de trabalho não autorizados usando a descoberta de aplicativos, reduzindo ainda mais a superfície de ataque.

Minimize a movimentação lateral
A conectividade baseada no acesso de privilégio mínimo garante que o acesso aos aplicativos seja concedido individualmente de um usuário autorizado para aplicativos específicos, em vez de acesso total à rede. Portanto, a movimentação lateral entre aplicativos ou na rede é impossível. Como o ZPA não é baseado em endereços IP, a necessidade de configurar e gerenciar segmentações de rede complexas, listas de controle de acesso (ACLs), políticas de firewall ou traduções de endereços de rede é eliminada. Os recursos de deception integrados do ZPA permitem que as equipes de segurança detectem e isolem imediatamente um usuário mal-intencionado ou um dispositivo comprometido que tente se mover lateralmente pela organização.

Evite usuários comprometidos, ameaças internas e invasores avançados
A primeira proteção de aplicativos privados de seu tipo, com recursos integrados de inspeção, deception e prevenção contra perda de dados, minimiza o risco de usuários comprometidos e invasores ativos. O ZPA interrompe automaticamente ataques na web com cobertura completa para as técnicas mais prevalentes, incluindo o OWASP Top 10, e compatibilidade completa com assinaturas personalizadas para correção virtual imediata contra vulnerabilidades de dia zero. O ZPA minimiza os riscos de terceiros e de dispositivos pessoais com acesso totalmente isolado a aplicativos que mantém dados sigilosos fora de dispositivos não gerenciados usando o isolamento integrado do navegador na nuvem. A tecnologia de deception integrada que utiliza aplicativos iscas permite que as equipes de segurança contenham ameaças ativas na rede, impedindo o acesso de usuários comprometidos aos recursos.

Ofereça uma experiência de usuário excepcional
A conectividade sempre rápida que não exige login e logout de clientes em VPNs oferece aos usuários remotos uma experiência de acesso mais segura e eficiente. Prestadores de serviço, fornecedores e parceiros terceirizados se beneficiam do acesso sem atrito a partir de qualquer dispositivo e navegador da web, sem a necessidade de instalar um cliente. Os usuários se inscrevem com suas credenciais de SSO existentes (Azure AD, Okta, Ping, etc.). Além disso, os administradores podem manter os usuários produtivos detectando e solucionando proativamente problemas de desempenho do usuário final causados por dificuldades de acesso a aplicativos privados, interrupções na rota da rede ou congestionamentos da rede.

Uma plataforma unificada para acesso seguro entre aplicativos, cargas de trabalho e dispositivos
Estenda o zero trust para aplicativos privados, cargas de trabalho e dispositivos TO/IIoT para simplificar e integrar múltiplas ferramentas de acesso remoto desconexas, unificando políticas de segurança e acesso para impedir violações e reduzir a complexidade operacional.

Zscaler Private Access Editions

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Serviços da plataforma	Ancoragem de IP de origem, IdP múltiplo, LSS	(+) Acesso estendido ao DC	(+) Ambiente de testes, PKI do cliente	(+) Ambiente de testes, PKI do cliente
Segmentação de usuário para aplicativo	10 Segmentos de aplicativos	500 segmentos de aplicativos	Segmentos de aplicativos ilimitados	Segmentos de aplicativos ilimitados
App Connector	20 pares	50 pares	Pares ilimitados	Pares ilimitados
ZTNA local[1]	1 par (virtual)	1 par de borda de serviço privado por 5 mil usuários	1 par de borda de serviço privado por 2 mil usuários	1° par de Borda de serviço privado incluído, par adicional para cada mil usuários
Acesso sem cliente[2]	—	✓	✓	✓
Monitoramento integrado da experiência digital	—	Padrão	Padrão	Padrão
Engano integrado	—	Padrão	Avançado	Advanced Plus
Proteção de aplicativos	—	—	✓	✓
Isolamento integrado	—	—	Padrão	Advanced Plus
Proteção de dados (aplicativos privados)	—	—	—	✓
Suporte premium	—	—	—	✓

Principais diferenciais

Por ser a única plataforma de ZTNA de nova geração no setor, o Zscaler Private Access fornece segurança superior com uma experiência de usuário incomparável:

- **Criada do zero visando o acesso de privilégio mínimo:** Permita que usuários autorizados se conectem apenas a recursos aprovados, não à sua rede — algo impossível de fazer com VPNs legadas
- **Os aplicativos tornam-se invisíveis e inacessíveis aos invasores:** impeça o comprometimento de aplicativos, o roubo de dados e a movimentação lateral, tornando aplicativos, cargas de trabalho e dispositivos privados invisíveis para a internet pública
- **Inspeção completa em linha:** proteja seus aplicativos identificando e interrompendo a exploração de aplicativos privados, impedindo automaticamente os ataques mais comuns na web e protegendo seus dados com a DLP líder do setor
- **Deception integrado:** impeça tentativas de movimentação lateral e a propagação de ransomware com a única solução de ZTNA com deception de aplicativo nativo
- **Acesso sem cliente:** aproveite o acesso baseado no navegador para terceiros com DLP integrada
- **Produtividade aprimorada:** mantenha visibilidade completa do acesso a aplicativos privados para detectar problemas do usuário que afetam a experiência do usuário
- **Presença global na borda:** obtenha segurança e experiência de usuário incomparáveis com mais de 150 locais de borda na nuvem em todo o mundo, bem como uma borda de serviço local opcional para estender o zero trust à sua sede
- **Base nativa da nuvem:** aproveite a capacidade de dimensionamento de uma plataforma disponibilizada na nuvem sem dispositivos locais dispendiosos ou infraestrutura complexa à medida que sua empresa cresce

[1]O ZPA Business Edition oferece suporte a até 5 pares de Private Service Edge; é necessário adquirir pares adicionais após 50 mil usuários.
O ZPA Transformation Edition oferece suporte a até 10 pares de Borda de serviço privado; é necessário adquirir pares adicionais após 50 mil usuários.
O ZPA Unlimited Edition oferece suporte a até 50 pares de Private Service Edge; é necessário adquirir pares adicionais após 50 mil usuários.

[2]O acesso sem cliente inclui o acesso pelo navegador e o acesso remoto privilegiado (para até 10 sistemas).

- **Plataforma ZTNA unificada para usuários, cargas de trabalho e dispositivos:** conecte-se com segurança a aplicativos privados, serviços e dispositivos TO com a plataforma ZTNA mais abrangente do setor
- **Parte de uma plataforma zero trust extensível:** proteja e capacite seus negócios com a Zero Trust Exchange, desenvolvida em uma estrutura de SSE completa

Componentes básicos

Zscaler Client Connector
O Client Connector é um aplicativo leve que roda em laptops e dispositivos móveis dos usuários. Ao encaminhar automaticamente o tráfego do usuário para a Zscaler Service Edge mais próxima, ele garante que as políticas de segurança e acesso sejam aplicadas em todos os dispositivos, locais e aplicativos.

Zscaler Branch Connector
O Branch Connector, disponível em formato de dispositivo físico e virtual, melhora o desempenho dos aplicativos, eliminando o retorno do tráfego e encaminhando todo o tráfego de filiais e data centers diretamente para o local de borda da Zscaler mais próximo, minimizando a latência. Ele permite a comunicação bidirecional entre usuários, servidores e dispositivos de IoT/TO, onde o Client Connector não pode ser instalado, e aplicativos, em qualquer rede por meio da Zero Trust Exchange.

Zscaler Clientless Access
Os usuários podem se conectar com segurança a aplicativos, cargas de trabalho e dispositivos de TO por meio do acesso integrado baseado em navegador (web, RDP, SSH, VNC) ou Zscaler Browser Isolation para acesso sem cliente em dispositivos não gerenciados.

ZPA App Connector
Os App Connectors são máquinas virtuais leves que ficam na frente de aplicativos privados implantados no data center ou na nuvem pública, intermediando a conectividade de segurança entre um usuário autorizado e um aplicativo nomeado com uma conexão de dentro para fora que não expõe os aplicativos na internet.

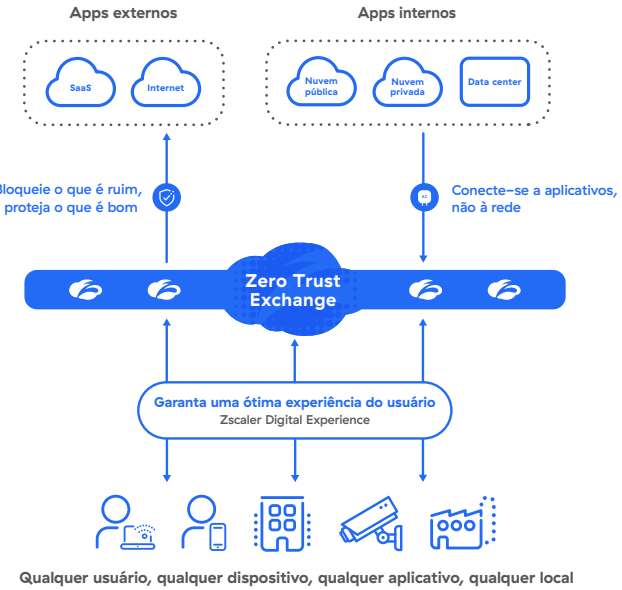
Bordas de serviço do ZPA
As bordas de serviço aplicam políticas de segurança e acesso, unindo a conexão de dentro para fora entre um usuário autorizado (por meio do Client Connector e acesso do navegador) e um aplicativo privado específico (por meio do App Connector). A maioria dos clientes usa nossas bordas de serviço público, que estão hospedados em mais de 150 agentes em todo o mundo e gerenciam milhões de usuários simultâneos para as maiores organizações do mundo. As bordas de serviço privado, gerenciadas pela Zscaler, também estão disponíveis para serem hospedadas localmente e fornecer aos usuários locais a rota mais curta para aplicativos locais sem sair da rede local.

O ZPA faz parte da holística Zero Trust Exchange

A Zscaler Zero Trust Exchange é uma plataforma nativa da nuvem que alimenta uma borda de serviço de segurança (SSE) completa para conectar usuários, cargas de trabalho e dispositivos sem inseri-los na rede corporativa. Ela reduz os riscos e a complexidade associados às soluções de segurança baseadas em perímetro, que estendem a rede, expandem a superfície de ataque, aumentam o risco de movimentação lateral e não conseguem evitar a perda de dados.

Como a Zscaler fornece a estratégia zero trust a usuários, cargas de trabalho e IIoT/TO

Implante em semanas para melhorar a proteção cibernética e a experiência do usuário



Especificações técnicas

Componente Zscaler	Plataformas e sistemas compatíveis	
Client Connector	iOS 9 ou posterior Android 5 ou posterior Windows 7 ou posterior	macOSX 10.10 ou posterior CentOS 8 Ubuntu 20.04
Branch Connector	CentOS, RedHat	VMware vCenter ou vSphere Hypervisor
Acesso sem cliente	Navegadores web modernos: (compatível com HTML 5)	Chrome Edge Firefox
App Connector	AWS Centos, Oracle e Red hat Microsoft Azure	Microsoft Hyper-V VMware vCenter ou vSphere Hypervisor Docker host

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com.br** ou siga-nos no Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com.br