FICHA TÉCNICA

Zscaler Private Access™

Capacite suas equipes com acesso rápido, seguro e confiável a aplicativos privados com o primeiro ZTNA com inteligência artificial do setor.

O Zscaler Private Access (ZPA) é uma solução nativa da nuvem que oferece acesso zero trust para todos os usuários com conectividade direta a aplicativos privados, minimizando a superfície de ataque, eliminando a movimentação lateral e protegendo contra ataques sofisticados.

As abordagens de segurança de rede legadas não atendem às necessidades das suas equipes de trabalho híbridas e do seu negócio.
Firewalls e VPNs tradicionais criam uma superfície de ataque massiva para invasores encontrarem e explorarem. Eles também colocam os usuários diretamente na sua rede, permitindo a propagação lateral de ameaças. Se as credenciais do seu usuário forem comprometidas, os invasores terão acesso fácil aos seus dados sigilosos. Usar uma VPN para acesso das suas equipes de trabalho híbridas e de terceiros aumenta o risco cibernético, cria experiências ruins para o usuário e aumenta a sobrecarga administrativa. Para fornecer acesso seguro aos usuários de qualquer dispositivo e local, você precisa de uma abordagem mais eficaz.

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

Benefícios:

- **Substitua soluções de VPN vulneráveis** Reduza a superfície de ataque e elimine a movimentação lateral conectando os usuários diretamente aos aplicativos, não à rede, elevando sua postura de segurança.
- **Evite ataques cibernéticos** Minimize o risco de violação com proteção de aplicativo privado contra ameaças da web e de identidade, proteção avançada contra ameaças com inspeção completa em linha e prevenção contra perda de dados.
- **Capacite suas equipes de trabalho híbridas** Estenda facilmente o acesso ultrarrápido a aplicativos privados entre usuários, sede, filiais e terceiros.
- **Reduza a complexidade operacional** Ofereça acesso seguro e otimizado, sem produtos pontuais caros e complexos, por meio de uma plataforma de ZTNA unificada e nativa da nuvem para usuários, cargas de trabalho e OT/TI

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
- **Os usuários comprometidos e as ameaças internas podem ignorar os controles tradicionais:** invasores habilidosos podem roubar credenciais e subverter a identidade para acessar aplicativos privados com ferramentas de acesso remoto legadas

É hora de repensar como conectamos usuários de forma segura e contínua aos aplicativos de que precisam e redefinir a segurança de aplicativos privados com uma solução de ZTNA.

Zscaler Private Access™ (ZPA)

Sendo o primeiro ZTNA com tecnologia de IA do setor, o Zscaler Private Access (ZPA) é uma solução nativa da nuvem que fornece acesso zero trust para todos os usuários com conectividade direta a aplicativos privados, ao mesmo tempo em que minimiza a superfície de ataque ao ocultar aplicativos por trás da Zero Trust Exchange, eliminando a movimentação lateral usando segmentação de usuário para aplicativo com tecnologia de IA e protegendo contra ataques sofisticados com inspeção de tráfego integrada, proteção de aplicativos e dados. Como um serviço nativo da nuvem resiliente construído em uma estrutura holística de Security Service Edge (SSE), o ZPA pode ser implantado em questão de horas para substituir VPNs e ferramentas de acesso remoto legadas para:

- **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
- **Aplicar acesso de privilégio mínimo:** o acesso aos aplicativos é determinado pela identidade e contexto, não por um endereço IP. 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
- **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

Até 2025, pelo menos 70% das novas implantações de acesso remoto serão realizadas predominantemente por ZTNA, em vez de serviços VPN, um aumento em relação aos 10% do final de 2021.*

— Gartner

*Gartner, tecnologias emergentes: informações sobre o crescimento da adoção do acesso à rede zero trust, Nat Smith, Mark Wah, Christian Canales. 8 de abril de 2022

Principais casos de uso

Proteger o acesso remoto (substituição de VPN)
As VPNs disponibilizadas na nuvem ou baseadas em dispositivos deixam você exposto a ataques cibernéticos. Elas são atormentadas por vulnerabilidades e regularmente exploradas por invasores. Seu design centrado na rede faz retorno do tráfego, expande a superfície de ataque e permite a movimentação lateral ao colocar os usuários diretamente na rede, levando a ataques de ransomware. As VPNs são inseguras, lentas e complexas de gerenciar.

O ZPA resolve esses desafios fornecendo acesso zero trust para todos os usuários com conectividade direta a aplicativos privados, ao mesmo tempo em que minimiza a superfície de ataque ocultando aplicativos por trás da Zero Trust Exchange, eliminando a movimentação lateral usando segmentação de usuário para aplicativo com tecnologia de IA e protegendo contra ataques sofisticados com inspeção de tráfego integrada, proteção de aplicativos e dados. O ZPA oferece acesso rápido e direto a aplicativos por meio de mais de 160 pontos de presença (PoPs) distribuídos globalmente, sem os riscos de segurança inerentes à VPN. 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. O ZPA fornece acesso zero trust a todos os aplicativos, incluindo aplicativos conectados à rede, como Voz sobre IP (VoIP) e aplicativos de servidor para cliente, e até mesmo aplicativos hospedados por parceiros de negócios (extranet) onde os clientes não podem implantar os conectores de aplicativos da solução.

Proteger o acesso a aplicativos para usuários no escritório e híbridos
Nas equipes de trabalho modernas, os usuários trabalham em suas casas e outros locais remotos, filiais e sedes, desafiando paradigmas de segurança legados. As organizações precisam de acesso ininterrupto aos aplicativos, sem comprometer a segurança zero trust durante desastres ou períodos de acesso degradado à infraestrutura. Os padrões de conformidade e regulatórios devem ser atendidos para a continuidade dos negócios.

A borda de serviço privado do ZPA 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. Ao implantar as bordas de serviço privado da Zscaler com controladores de nuvem privada, o ZPA oferece suporte à troca totalmente automatizada para o modo de continuidade de negócios no caso de detecção de interrupção. As políticas e a autenticação são aplicadas mesmo que o ZPA Cloud não esteja acessível.

Acesso a usuários de dipositivos pessoais e terceiros
O acesso tradicional de terceiros dependia de soluções caras, complexas e arriscadas, como VDI, RDP, SSH ou VNC, que colocavam os usuários diretamente na rede e expunham os sistemas internos a dispositivos não confiáveis.

Os recursos de acesso sem cliente do ZPA facilitam o acesso de terceiros, reduzem custos e minimizam riscos. Terceiros, como prestadores de serviço, fornecedores e parceiros, podem usar qualquer navegador web em seus próprios dispositivos para se conectar a sites de intranet, sistemas internos e equipamentos, sem a necessidade de cliente. Ele mantém usuários terceirizados e dispositivos não gerenciados isolados da sua rede e aplicativos, garantindo que os dados sigilosos estejam protegidos contra área de transferência, impressão e upload/download não autorizados. A integração do ZPA e do Google Chrome Enterprise Browser aprimorará a segurança para dispositivos não gerenciados/pessoais ao verificar o Chrome Enterprise Browser e incorporar informações adicionais de postura nas verificações de política do ZPA. Com o Clientless Access, a TI pode oferecer uma experiência melhor e mais segura para os usuários sem incorrer nos custos de gerenciamento de VDI legado. Fusões, aquisições e alienações apresentam desafios de integração de rede, mas o ZPA acelera esse processo de meses para semanas. O ZPA oferece acesso contínuo a aplicativos privados, eliminando a necessidade de convergência de rede ou equipamentos adicionais.

Acesso remoto privilegiado para OT/TI
Os colaboradores e fornecedores terceirizados precisam acessar frequentemente os ativos de OT/TI para maximizar o tempo de atividade da produção e evitar interrupções devido a falhas de equipamentos e processos. O ZPA oferece acesso rápido, seguro e confiável aos ambientes OT/TI a partir de locais de campo, do chão de fábrica ou de qualquer outro lugar. O ZPA para OT/TI oferece acesso remoto a áreas de trabalho internas RDP, SSH e VNC totalmente isolado e sem cliente, sem exigir que os usuários instalem um cliente em seus dispositivos, utilizando jump hosts e VPNs legadas.

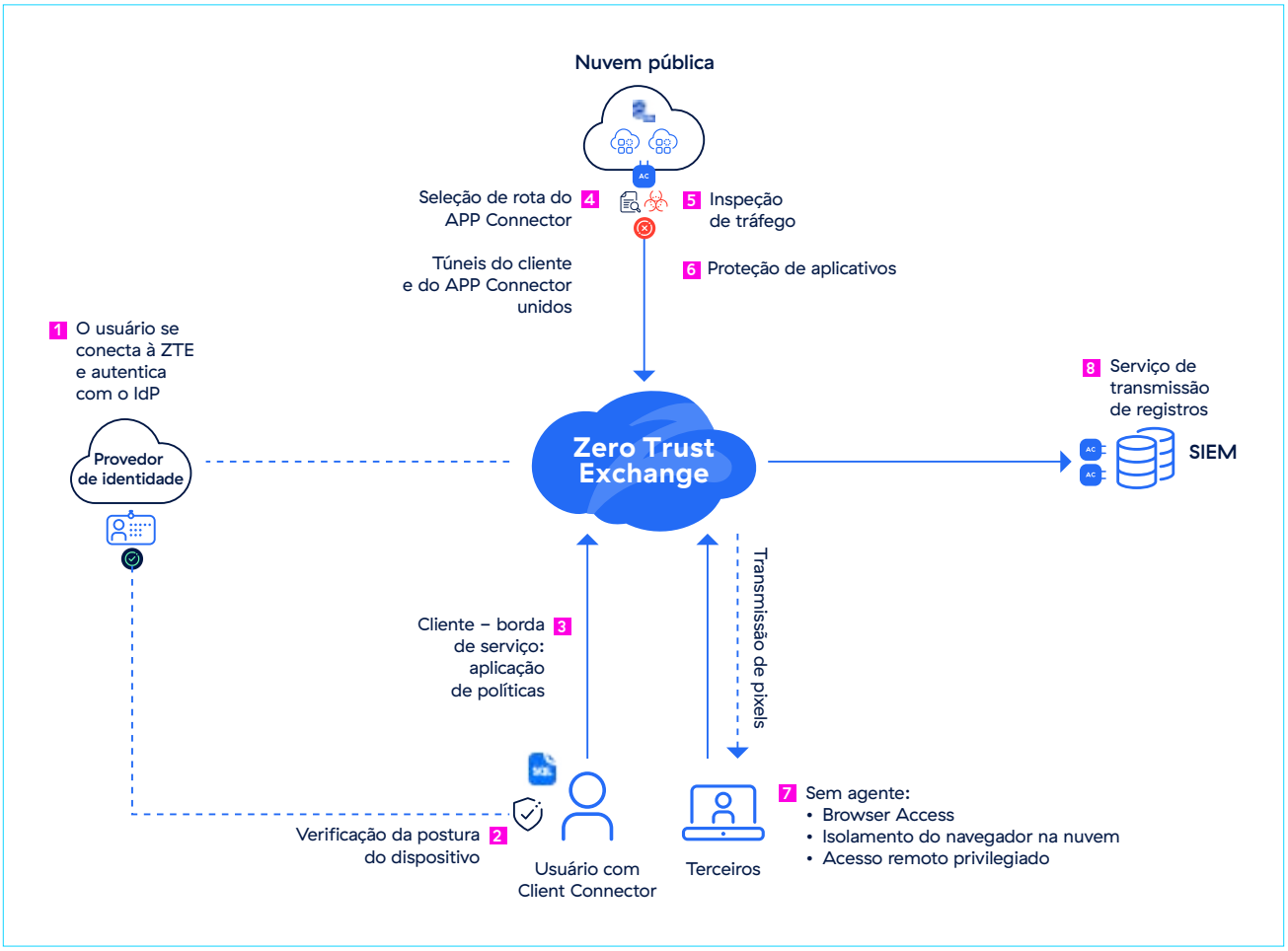
Alternativa à VDI
As equipes de TI e segurança não têm controle sobre dispositivos não gerenciados, criando riscos comerciais. Para dar suporte ao acesso a aplicativos em dispositivos não gerenciados, as organizações tradicionalmente usam VDI. As VDIs colocam os usuários diretamente na rede, expondo aplicativos internos a terminais não gerenciados. Além disso, as VDIs são caras, complicadas de gerenciar e não são dimensionáveis. Na esteira da transformação digital, os aplicativos modernizados são normalmente baseados na web ou no navegador, e transmitir um desktop inteiro via VDI não fornece uma experiência muito boa para o usuário final.

O ZPA é uma alternativa eficaz à VDI, oferecendo acesso seguro, sem agentes e baseado no navegador em dispositivos não gerenciados. Os usuários obtêm acesso rápido e contínuo a aplicativos privados intermediados pela borda de serviço mais próxima. A arquitetura do ZPA fornece acesso direto aos aplicativos, sem colocar o usuário na rede, tornando o acesso a aplicativos privados seguro. O ZPA Browser Access permite que os usuários utilizem um navegador web para autenticação de usuários e acesso a aplicativos, sem precisar instalar o Zscaler Client Connector em seus dispositivos. O ZPA integrou o isolamento do navegador, e como apenas os pixels são transmitidos para o dispositivo do usuário final, em vez do conteúdo real, os dados nos aplicativos permanecem seguros. O ZPA permite que os administradores criem políticas de isolamento para definir como um usuário pode interagir dentro do ambiente isolado.

Microsegmentação
Soluções de acesso remoto, como VPNs, concedemacesso total à rede e expõem IPs e aplicativos à internet. As VPNs estendem a rede interna para dispositivos remotos e, por design, exigem tráfego de entrada, expondo uma superfície de ataque pública. Sem segmentação de rede adequada, uma violação em um segmento pode comprometer toda a rede da organização. Dito isso, implementar a segmentação requer regras de firewall complexas que são difíceis de manter, frequentemente interrompem aplicativos e podem complicar o acesso para usuários de VPN. Em grandes organizações, isso geralmente requer alta disponibilidade, roteamento complexo e links privados caros.

A segmentação de aplicativos com tecnologia de IA da Zscaler oferece segmentação precisa de usuário para aplicativo e uma solução robusta para implementar facilmente políticas consistentes em escala e eliminar a movimentação lateral de ameaças. Ela ajuda você a descobrir todos os aplicativos dentro da sua organização e fornece insights visuais sobre quais usuários têm acesso a quais aplicativos. Ela gera automaticamente recomendações para segmentos de aplicativos e políticas com base em modelos de aprendizado de máquina, simplificando a implementação.

Como funciona o ZPA



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 conecta à Zero Trust Exchange com o Client Connector e se autentica com o provedor de identidade (IdP). Após a autenticação bem-sucedida, ele se reconecta à borda de serviço público, estabelecendo uma conexão TLS única e permanente com a borda de serviço.

2 Após a autenticação do usuário e o estabelecimento do túnel para a borda de serviço, o conector do cliente baixa sua configuração, incluindo a verificação de postura do dispositivo.

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 Dois túneis de saída, um do Client Connector no dispositivo e outro do App Connector, são unidos pela borda de serviço.

5 Uma vez estabelecida a conexão entre o dispositivo do usuário e o aplicativo, o App Connector inspeciona automaticamente o tráfego em linha para detectar e interromper possíveis ameaças provenientes de usuários ou dispositivos que possam ter sido comprometidos.

6 O Zscaler AppProtection protege aplicativos privados da web e baseados em identidade por meio de uma inspeção abrangente da Camada 7, aprimorando a postura geral de segurança.

7 Os usuários terceirizados podem se conectar a aplicativos privados com acesso integrado baseado em navegador ou no Zscaler Browser Isolation para obter acesso sem cliente em dispositivos não gerenciados.

8 O Log Streaming Service (LSS) transmite vários logs, incluindo a atividade do usuário para o SIEM

Uma borda de serviço do ZPA pode ser hospedada pela Zscaler na nuvem (borda de serviço público do ZPA) ou executada localmente dentro da sua infraestrutura (borda de serviço privado do ZPA), proporcionando um caminho mais curto para aplicativos locais e apoiando o Planejamento de Continuidade de Negócios.

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.
Continuidade de negócios e recuperação de desastres	Garanta acesso ininterrupto a aplicativos críticos, mesmo durante um evento cisne negro, com uma solução de continuidade de negócios controlada pelo cliente ou totalmente gerida, criando a rota de acesso a aplicativos privados críticos através da 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.
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.

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.
Identidade e logon único (SSO)	Integre facilmente à sua infraestrutura existente de identidade e autenticação, aproveitando o SSO para reduzir ainda mais a complexidade.
Acesso seguro a aplicativos de rede	Ofereça acesso seguro a aplicativos conectados à rede legada, como VoIP e aplicativos de servidor para cliente.
Conectividade IPsec	Ofereça acesso zero trust a aplicativos de parceiros de negócios e fornecedores (aplicativo de extranet) hospedados em suas redes

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.

Elimine a movimentação lateral
A conectividade baseada no acesso de privilégio mínimo garante que o acesso ao aplicativo seja concedido individualmente de um usuário autorizado para aplicativos nomeados, em vez de acesso total à rede. Portanto, a movimentação lateral entre aplicativos ou pela 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.

Evite usuários comprometidos, ameaças internas e invasores avançados
Os recursos integrados de inspeção em linha e DLP minimizam o risco de usuários comprometidos e invasores ativos. O ZPA interrompe automaticamente os ataques da web com cobertura completa para as técnicas mais prevalentes, incluindo o OWASP Top 10, e suporte completo de assinatura personalizada para aplicação imediata de correções virtuais contra vulnerabilidades de dia zero. O ZPA minimiza os riscos de terceiros e dispositivos pessoais com acesso totalmente isolado a aplicativos que mantém dados sigilosos fora de dispositivos não gerenciados usando isolamento de navegador de nuvem integrado.

Forneça uma experiência de usuário excepcional
Conectividade consistentemente rápida que não requer login e logout de clientes de VPN oferece aos usuários remotos uma experiência de acesso mais segura e eficiente. Prestadores de serviço, fornecedores e parceiros terceirizados se beneficiam de um acesso sem atritos de qualquer dispositivo e navegador web, sem a necessidade de instalar um cliente. Os usuários utilizam suas credenciais de SSO existentes (Azure AD, Okta, Ping, etc.) Além disso, os administradores podem manter os usuários produtivos detectando e resolvendo proativamente problemas de desempenho do usuário final causados por dificuldades de acesso a aplicativos privados, quedas de rota de rede ou congestionamento de rede.

Uma plataforma unificada para proteger o acesso de aplicativos, cargas de trabalho e dispositivos.
Estenda o zero trust em aplicativos privados e dispositivos de OT/TI para simplificar e integrar diversas ferramentas de acesso remoto desconexas, unificando políticas de segurança e acesso para impedir violações e reduzir a complexidade operacional.

Opções de pacotes do Zscaler Private Access

	Plataforma Zscaler Essentials (ZS-ESS-PLATFORM)	Plataforma Zscaler Private Access (ZS-ZPA-PLATFORM)	Plataforma Zscaler (ZS-PLATFORM)
Serviços da plataforma Private Access	✔ 1 usuário para cada 20 usuários inscritos (Mínimo: 500 usuários inscritos)	✔	✔
Controle de acesso granular por usuário, grupo e portas			
Serviço de transmissão de registros			
Monitoramento contínuo da integridade de todos os aplicativos			
Ancoragem de IP de origem			
App Connector	$	Tantos quantos forem necessários, até o máximo do sistema	Tantos quantos forem necessários, até o máximo do sistema
Borda de serviço privado ZPA			
Acesso de terceiros	$	✔ PRA para mais de 500 usuários	✔ PRA para mais de 500 usuários
Acesso pelo navegador			
Portal do usuário			
Acesso remoto privilegiado (PRA) Standard			
Monitoramento da experiência digital	$	✔	✔
Padrão ZDX			
Segurança para aplicativos privados	$	$	✔ Decepction para mais de 500 usuários
Proteção de dados para aplicativos privados			
Gestão de riscos: deception			
Segmentação	20 segmentos de aplicativos (10 recomendações/ 90 dias, retrospectiva limitada)	20 segmentos de aplicativos (10 recomendações/ 90 dias, retrospectiva limitada)	20 segmentos de aplicativos (10 recomendações/ 90 dias, retrospectiva limitada)
Segmentos de aplicativos e visualização de segmentação			
Complemento de segmentação	✔ 100 recs/ 14 dias Relatórios semanais sob demanda, baixe e analise até 30 dias de dados Importe aplicativos do sistema interno ou de fontes de terceiros (Qualys, Tenable, ServiceNow)	✔ 100 recs/ 14 dias Relatórios semanais sob demanda, baixe e analise até 30 dias de dados Importe aplicativos do sistema interno ou de fontes de terceiros (Qualys, Tenable, ServiceNow)	✔ 100 recs/ 14 dias Relatórios semanais sob demanda, baixe e analise até 30 dias de dados Importe aplicativos do sistema interno ou de fontes de terceiros (Qualys, Tenable, ServiceNow)
Segmentos de aplicativos ilimitados			
Segmentação baseada em IA			
Insights de segmentação			
Importação de segmentos de aplicativos (de arquivos de dados estruturados)			
Complemento AppProtection	Complemento	Complemento	Complemento
Visibilidade de ataque de aplicativo			
Defesa OWASP Top 10: injeção de SQL, cross-site scripting, verificação de ambientes e portas			
Proteção contra ameaças de dia zero			
Monitoramento de usuários de alto risco			

Principais diferenciais

Como a primeira solução de ZTNA com tecnologia de IA do setor, o ZPA oferece 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 se tornam invisíveis e inacessíveis para invasores:** impeça a violação de aplicativos, roubo de dados e movimentação lateral tornando aplicativos privados, cargas de trabalho e dispositivos 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
- **Ofereça a continuidade global dos negócios sem comprometer a segurança:** minimize o impacto das interrupções e aplique acesso zero trust para atender aos requisitos de conformidade rigorosos, mesmo quando a nuvem da Zscaler estiver inacessível
- **Acesso sem cliente:** aproveite o acesso baseado no navegador para terceiros com DLP integrada
- **Elimine a movimentação lateral com segmentação baseada em IA:** fornece segmentação precisa de usuário para aplicativo, visualiza o acesso e ajusta as políticas usando aprendizado de máquina para minimizar superfícies de ataque e evitar ameaças laterais
- **Presença global na borda:** obtenha segurança e experiência de usuário incomparáveis com mais de 160 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
- **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

**Gartner, Magic Quadrant para Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15 de abril de 2024

A Gartner não endossa nenhum fornecedor, produto ou serviço descrito em suas publicações de pesquisa, e não aconselha os usuários de tecnologia a selecionar somente os fornecedores com as mais altas pontuações ou outra designação. As publicações de pesquisa da Gartner consistem em opiniões da empresa de pesquisa da Gartner e não devem ser interpretadas como declarações de fato. A Gartner renuncia a todas as garantias, expressas ou implícitas, com respeito a esta pesquisa, incluindo quaisquer garantias de comercialização ou adequação a um determinado propósito.

GARTNER é uma marca registrada e marca de serviço da Gartner, Inc. e/ou suas afiliadas nos EUA e internacionalmente, e MAGIC QUADRANT é uma marca registrada da Gartner, Inc. e/ou suas afiliadas e são usadas aqui com a devida permissão. Todos os direitos reservados.

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 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.

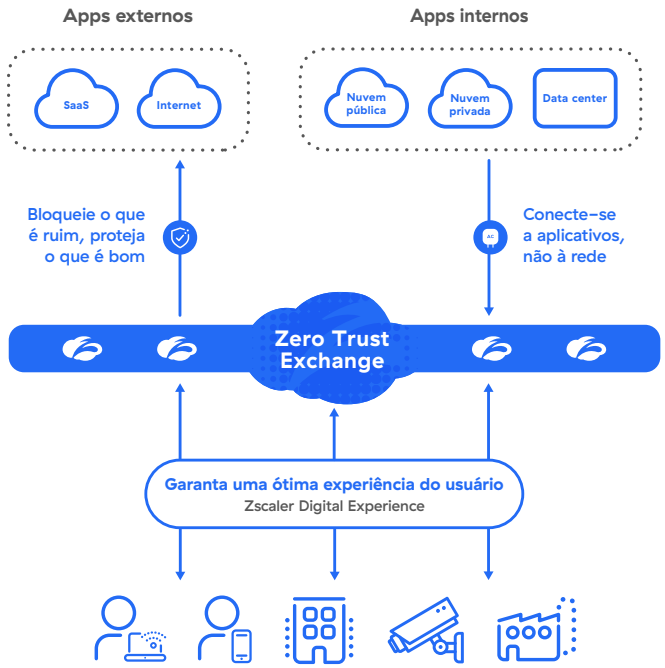
Bordas de serviço do ZPA
As bordas de serviço aplicam políticas de segurança e acesso, conectando o usuário autorizado (via Client Connector e acesso do navegador) a um aplicativo privado específico (via App Connector). A maioria dos clientes utiliza nossas bordas de serviço públicas, que estão hospedadas em mais de 160 pontos de presença (PoPs) ao redor do mundo e atendem a milhões de usuários simultâneos para as maiores organizações do mundo. As bordas de serviço privadas, gerenciadas pela Zscaler, também estão disponíveis para serem hospedadas localmente, proporcionando aos usuários locais a rota mais curta para aplicativos locais sem sair da rede local. Isso também garante a continuidade dos negócios com acesso ininterrupto a aplicativos críticos, mesmo durante um evento de cisne negro.

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 oferece zero trust para usuários, cargas de trabalho e OT/TI

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



Qualquer usuário, qualquer dispositivo, qualquer aplicativo, qualquer local

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
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