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 tradicionais de segurança de rede não atendem às necessidades das suas equipes híbridas e da sua empresa.
Os firewalls e as VPNs tradicionais criam uma enorme superfície de ataque que os invasores podem encontrar e explorar. Além disso, eles colocam os usuários diretamente na sua rede, permitindo a propagação lateral de ameaças. Se as credenciais dos seus usuários forem comprometidas, os invasores terão acesso fácil aos seus dados sigilosos. Usar uma VPN para oferecer acesso às suas equipes híbridas e a terceiros aumenta o risco cibernético, cria experiências insatisfatórias para os usuários e aumenta a sobrecarga administrativa. Para fornecer acesso seguro aos usuários de qualquer dispositivo e local, você precisa de uma abordagem mais eficaz.

De acordo com o Relatório de riscos da VPN de 2025 da Zscaler ThreatLabz, 92% dos entrevistados compartilham a preocupação de que falhas não corrigidas em VPNs possam levar diretamente a incidentes de ransomware, o que destaca a dificuldade de manter as VPNs atualizadas continuamente.

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.
- **Previna ataques cibernéticos**
  Minimize o risco de violações com proteção de aplicativos privados contra ameaças à web e à identidade, proteção avançada contra ameaças com inspeção inline completa e prevenção contra perda de dados.
- **Capacite suas equipes híbridas**
  Amplie o acesso ultrarrápido a aplicativos privados para usuários, sede, filiais e terceiros de forma integrada.
- **Reduza a complexidade operacional**
  Ofereça acesso seguro e otimizado, sem produtos caros e complexos para fins específicos, por meio de uma plataforma de ZTNA unificada e nativa em nuvem para usuários, cargas de trabalho e OT/TI.

©2025 Zscaler, Inc. Todos os direitos reservados.

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 direta aos aplicativos de que precisam e redefinir a segurança de aplicativos privados com uma solução de acesso à rede zero trust (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

92% dos entrevistados compartilham a preocupação de que falhas não corrigidas em VPNs levem diretamente a incidentes de ransomware, o que destaca a dificuldade de manter as VPNs atualizadas continuamente e em tempo hábil

— Relatório de riscos da VPN de 2025 da Zscaler ThreatLabz

*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

©2025 Zscaler, Inc. Todos os direitos reservados.

Principais casos de uso

Acesso remoto seguro (substituto de VPN)
VPNs baseadas em nuvem ou em dispositivos físicos deixam você exposto a ataques cibernéticos. Elas são repletas de vulnerabilidades e exploradas com frequência por invasores. Seu design centrado na rede redireciona o tráfego, expande a superfície de ataque e permite a movimentação lateral, colocando os usuários diretamente na rede, o que leva a ataques de ransomware. As VPNs são inseguras, lentas e difíceis de gerenciar.

O ZPA soluciona 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 através da 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 proporciona 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 em 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 os custos, a complexidade e a sobrecarga de gerenciamento. O ZPA oferece 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), sem a necessidade de implantar infraestrutura adicional, como App Connectors.

Acesso seguro a aplicativos para usuários locais e remotos.
No ambiente de trabalho moderno, os usuários trabalham em casa, em outros locais remotos, em filiais e na sede, o que desafia os 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. É fundamental atender aos padrões de conformidade e regulamentação para garantir 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 de usuário para terceiros e via dispositivos pessoais
O acesso tradicional de terceiros dependia de soluções caras, complexas e de risco, como VDI, RDP, SSH ou VNC, que colocavam os usuários diretamente na rede e expunham os sistemas internos a dispositivos não confiáveis.

As funcionalidades de acesso sem cliente do ZPA facilitam o acesso de terceiros, reduzem os custos e minimizam os riscos. Terceiros, como prestadores de serviço, fornecedores e parceiros, podem usar qualquer navegador web em seus próprios dispositivos para se conectar a sites da intranet, sistemas internos e equipamentos, sem a necessidade de instalar um cliente. Ele mantém usuários terceirizados e dispositivos não gerenciados isolados da sua rede e aplicativos, garantindo que os dados sigilosos estejam protegidos contra uso não autorizado da área de transferência, impressão, upload e download. A integração do ZPA com o navegador Google Chrome Enterprise aprimorará a segurança para dispositivos não gerenciados/pessoais ao verificar o navegador Chrome Enterprise e incorporar informações adicionais de postura nas verificações de política do ZPA. Com o acesso sem cliente, a TI pode oferecer uma experiência melhor e mais segura para os usuários sem incorrer nos custos de gerenciamento de VDI legada. 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
Funcionários e fornecedores terceirizados precisam acessar recursos de OT/TI com frequência para maximizar

©2025 Zscaler, Inc. Todos os direitos reservados.

o tempo de atividade da produção e evitar interrupções causadas por falhas de equipamentos e processos. O ZPA oferece acesso rápido, seguro e confiável a ambientes de OT/TI a partir de locais externos, do chão de fábrica ou de qualquer outro lugar. O ZPA para OT/TI fornece acesso remoto totalmente isolado e sem cliente a sistemas internos de destino via RDP, SSH e VNC, sem exigir que os usuários instalem um cliente em seus dispositivos usando servidores de salto e VPNs legadas.

Alternativa à VDI

As equipes de TI e segurança não têm controle sobre dispositivos não gerenciados, o que gera riscos para os negócios. Para oferecer suporte ao acesso a aplicativos em dispositivos não gerenciados, as organizações tradicionalmente utilizam uma infraestrutura de desktop virtual (VDI). A VDI coloca os usuários diretamente na rede, expondo os aplicativos internos a terminais não gerenciados. Além disso, a VDI tem alto custo, é complexa de gerenciar e não é expansível. Com a transformação digital, os aplicativos modernos são geralmente baseados na web ou em navegadores, e transmitir uma área de trabalho inteira via VDI não proporciona uma boa experiência ao 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 acesso via navegador do ZPA 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 tem isolamento do navegador integrado, 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.

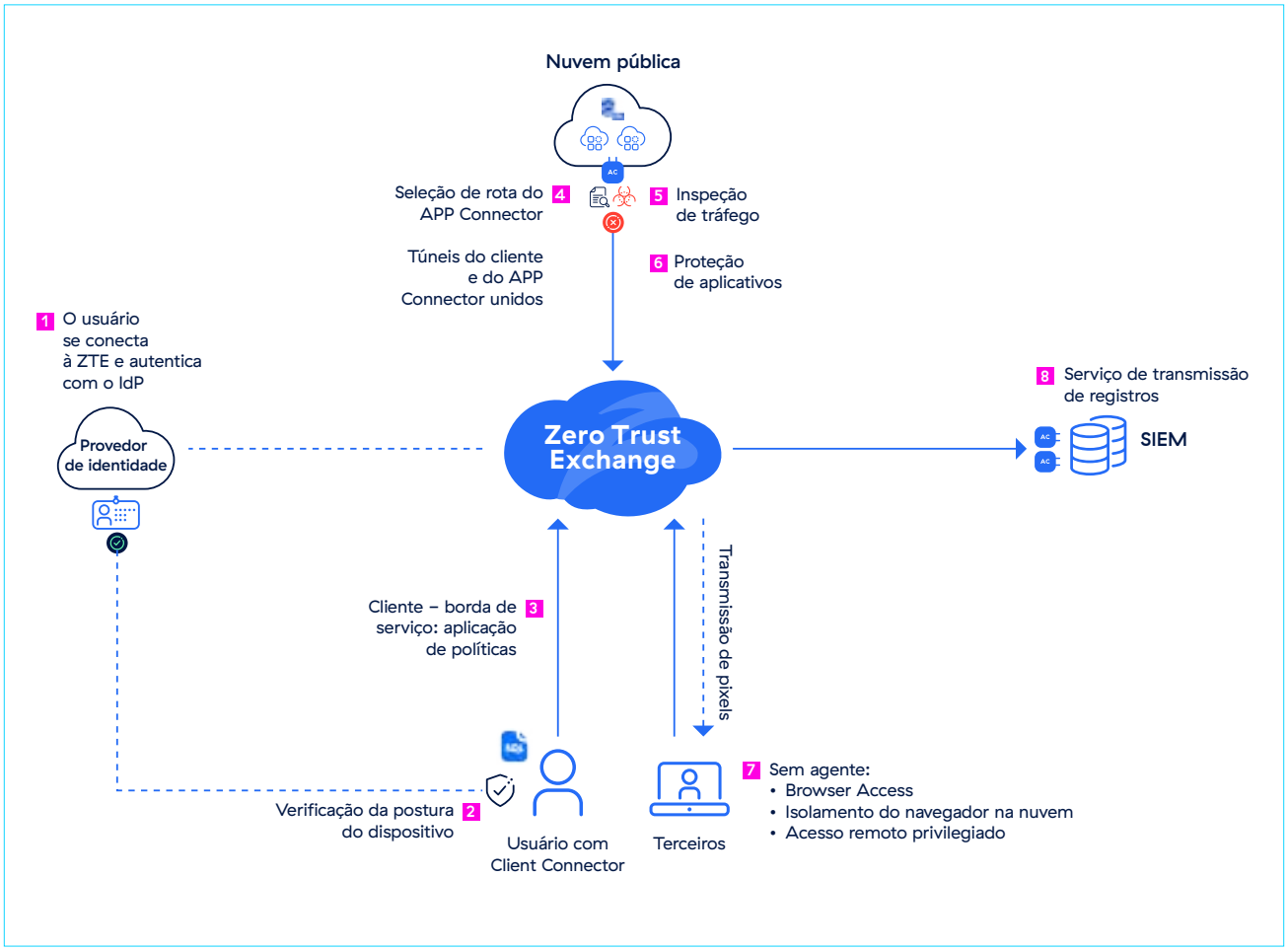
Microssegmentação (segmentação de usuário para aplicativo)

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

A segmentação autônoma de usuários para aplicativos da Zscaler oferece segmentação precisa de usuários para aplicativos e uma solução robusta para implantar facilmente políticas consistentes em grande escala, eliminando a movimentação lateral de ameaças. Ela automatiza todo o ciclo de segmentação, analisando cada aplicativo desde a fase de descoberta, segmentando mais rapidamente com recomendações baseadas em IA e fortalecendo sua posição com insights em tempo real.

©2025 Zscaler, Inc. Todos os direitos reservados.

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.

©2025 Zscaler, Inc. Todos os direitos reservados.

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

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 usuário para aplicativo	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 autônoma de usuários para aplicativos	Automatize todo o ciclo de segmentação, visualizando cada aplicativo desde a fase de descoberta, segmentando mais rapidamente com recomendações baseadas em IA e fortalecendo sua posição com insights em tempo real. Com base em modelos de aprendizado de máquina continuamente treinados com milhões de sinais de clientes e seus padrões exclusivos de acesso a aplicativos, a segmentação autônoma de usuários para aplicativos pode ajudar você a eliminar a movimentação lateral de ameaças, acelerar sua jornada de ZTNA, além de simplificar e dimensionar as operações de zero trust.
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.
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.
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 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.
Acesso seguro a aplicativos S2C legados	Ofereça acesso seguro a aplicativos legados conectados à rede, como VoIP, impressoras Follow Me e outros aplicativos de servidor para cliente.
Acesso a aplicativos B2B	Ofereça acesso seguro bidirecional a aplicativos e cargas de trabalho hospedados na rede (extranet) do seu parceiro de negócios

©2025 Zscaler, Inc. Todos os direitos reservados.

Acesso baseado em cliente e sem cliente	Escolha o método de proteção ideal para o seu ambiente híbrido. O acesso baseado em 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 oferece a prestadores de serviços terceirizados e usuários de dispostivos pessoais acesso fácil a aplicativos a partir de qualquer dispositivo e navegador web.
ZTNA no escritório	Aplique o ZTNA para usuários internos usando bordas de serviço privadas do ZPA, garantindo acesso rápido e contínuo aos aplicativos. Nosso ZTNA universal garante acesso e políticas consistentes para os usuários, independentemente de local e aplicativo.
Continuidade de negócios e recuperação de desastres	Garanta o acesso ininterrupto a aplicativos essenciais, mesmo durante um evento imprevisível, com uma solução de continuidade de negócios hospedada pelo cliente ou totalmente gerenciada.

Benefícios

Minimize a superfície de ataque
Eliminar VPNs vulneráveis e tornar os aplicativos invisíveis para a internet torna impossível para usuários não autorizados encontrá–los e atacá–los. O ZPA cria um segmento individual entre um usuário autorizado e um aplicativo privado específico, removendo toda a conectividade de entrada e permitindo apenas conexões internas 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 princípio do privilégio mínimo garante que o acesso aos aplicativos seja concedido individualmente, de um usuário autorizado para aplicativos específicos, em vez de oferecer acesso total à rede. Portanto, a movimentação lateral entre aplicativos ou pela rede é impossível. Como o ZPA não se baseia em endereços IP, elimina–se a necessidade de configurar e gerenciar uma segmentação de rede complexa, listas de controle de acesso (ACLs), políticas de firewall ou traduções de endereços de rede (NATs).

Evite usuários comprometidos, ameaças internas e ataques avançados
Os recursos integrados de inspeção inline e DLP minimizam o risco de usuários comprometidos e ataques ativos. O ZPA interrompe automaticamente ataques web com cobertura completa para as técnicas mais prevalentes, incluindo OWASP Top 10, e suporte completo a assinaturas personalizadas 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, mantendo dados sigilosos fora de dispositivos não gerenciados por meio do isolamento integrado do navegador em nuvem.

Ofereça uma experiência de usuário excepcional
A conectividade consistentemente rápida, que não exige login e logout em clientes de VPN, proporciona aos usuários remotos uma experiência de acesso mais segura e eficiente. Fornecedores, prestadores de serviços e parceiros terceirizados se beneficiam do acesso descomplicado a partir de qualquer dispositivo e navegador web, sem a necessidade de instalar um cliente. Os usuários se cadastram com suas credenciais de SSO existentes (Azure AD, Okta, Ping, etc.). Além disso, os administradores podem manter a produtividade dos usuários, detectando e solucionando proativamente problemas de desempenho causados por dificuldades de acesso a aplicativos privados, interrupções no caminho da rede ou congestionamento da rede.

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

©2025 Zscaler, Inc. Todos os direitos reservados.

Zscaler Private Access (ZPA): várias opções para começar

	Plataforma Zscaler Essentials (ZS-ESS-PLATFORM)	Plataforma sem clientes do ZPA (ZPA-CLIENTLESS-PLATFORM)	Plataforma Zscaler Private Access (ZS-ZPA-PLATFORM)	Plataforma Zscaler (ZS-PLATFORM)
Serviços da plataforma Private Access				
Controle de acesso granular por usuário, grupo e portas	✓ 1 usuário por 20 usuários inscritos (mín.: 500 usuários inscritos)	✓	✓	✓
Serviço de transmissão de registros				
Monitoramento contínuo da integridade de todos os aplicativos				
Ancoragem de IP de origem: encaminhe seletivamente o tráfego de aplicativos para os servidores de destino apropriados				
App Connector: VM leve que permite conexões internas com a Zscaler ZTE	Quantos forem necessários, até o máximo do sistema	Quantos forem necessários, até o máximo do sistema	Quantos forem necessários, até o máximo do sistema	Quantos forem necessários, até o máximo do sistema
Borda de serviço privado do ZPA: ZTNA para usuários remotos e no escritório	–	–		
ZPA para aplicativos legados (VOIP, S2C, etc.)	–	–	Complemento de bordas de serviço de VPN (mínimo: 50 usuários)	Complemento de bordas de serviço de VPN (mínimo: 50 usuários)
Nuvem de continuidade de negócios do ZPA	–	–	Complemento (mínimo: 500 usuários)	Complemento (mínimo: 500 usuários)
Segmentação de usuário para aplicativo	10 segmentos de aplicativos	20 segmentos de aplicativos	20 segmentos de aplicativos	20 segmentos de aplicativos
Segmentação e insights autônomos de usuário para aplicativo	–	–	**Complemento**	**Complemento**
Acesso de terceiros			Complemento (mínimo: 500 usuários)	Complemento (mínimo: 500 usuários)
Acesso baseado em navegador para dispositivos não gerenciados	–	✓	✓ Licenças adicionais para usuários convidados podem ser adquiridas com a ZPA-CLIENTLESS-PLATFORM	✓ Licenças adicionais para usuários convidados podem ser adquiridas com a ZPA-CLIENTLESS-PLATFORM
Portal de usuário: portal web único para usuários acessarem aplicativos autorizados e consoles privilegiados				
Acesso remoto privilegiado Standard: PRA sem cliente para sistemas de OT (até 10) (RDP/SSH/VNC)				
Isolamento do navegador para aplicativos privados e SaaS		**Complemento**	**Complemento**	**Complemento**
Monitoramento da experiência digital	–	–	✓	✓
ZDX Standard: visibilidade da telemetria de usuários, conectividade e aplicativos				
Proteja aplicativos e dados privados	**Complemento**			
Proteção de dados para aplicativos privados, resposta a incidentes e classificação de dados		–	**Complemento**	✓
Zscaler Deception: iscas integradas para detectar usuários comprometidos		–	✓ (mínimo: 500 usuários)	✓ (mínimo: 500 usuários)
AppProtection para proteger aplicativos privados contra OWASP Top 10 e inspeção de tráfego web		**Complemento**	**Complemento**	**Complemento**

©2025 Zscaler, Inc. Todos os direitos reservados.

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 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
- **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
- **Proteja o acesso via navegador:** utilize o acesso baseado no navegador para terceiros com DLP integrada.
- **Elimine a movimentação lateral com a segmentação autônoma de usuários para aplicativos:** oferece segmentação precisa de usuários para aplicativos, visualiza o acesso e ajusta políticas usando aprendizado de máquina para minimizar as superfícies de ataque e prevenir 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

Zscaler é nomeada uma das líderes no Gartner® Magic Quadrant™ de 2025 para Security Service Edge**

Saiba mais

**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.

©2025 Zscaler, Inc. Todos os direitos reservados.

Componentes básicos

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

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

ZPA App Connector
App Connectors são máquinas virtuais leves que ficam à frente de aplicativos privados implantados no data center ou na nuvem pública, intermediando a conectividade de segurança entre um usuário autorizado e um aplicativo específico, por meio de uma conexão interna que não expõe os aplicativos à internet.

ZPA Network Connector
Network Connectors são máquinas virtuais leves implantadas na frente dos servidores de aplicativos no data center e que se conectam às bordas de serviço de VPN na nuvem da Zscaler por meio de um túnel de dentro para fora.

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

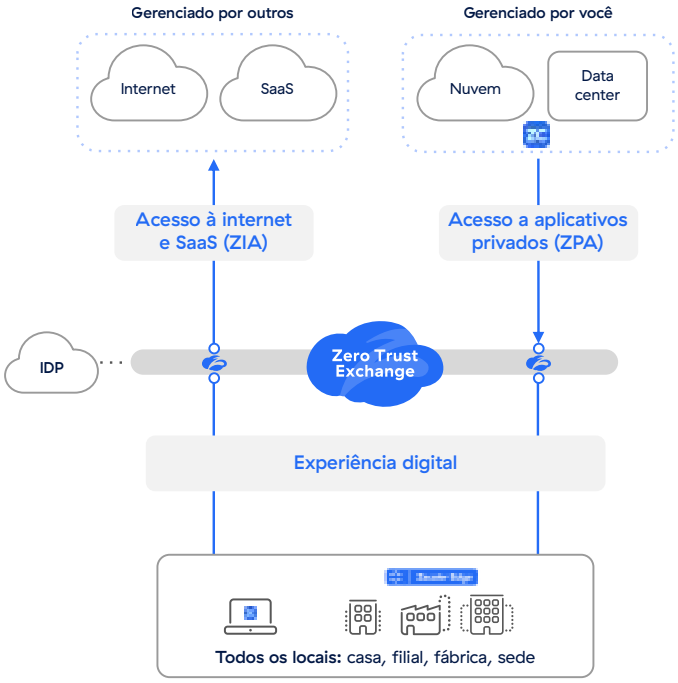
Controlador de nuvem privada do ZPA
Os controladores de nuvem privada são controladores baseados em instância para usuários, bordas de serviço privado do ZPA e App Connectors, que podem ser utilizados quando a nuvem da Zscaler não estiver disponível ou acessível.

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.

©2025 Zscaler, Inc. Todos os direitos reservados.

Zscaler protege equipes de trabalho: acesso seguro, rápido e confiável a aplicativos,
implantável em dias para aprimorar a proteção cibernética e a experiência de usuário



Proteção superior contra ameaças e de dados,
excelente experiência do usuário, redução de custos e complexidade

Especificações técnicas

Componente Zscaler	Plataformas e sistemas compatíveis	
Client Connector	iOS 17 ou posterior Android 9 ou posterior Windows 8 ou posterior	ChromeOS versão 137 ou posterior Linux MacOS 14 ou posterior
Acesso sem cliente	Navegadores web modernos: (compatíveis com HTML5), Chrome, Edge, Firefox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Borda de serviço privado	AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat	
Controlador de nuvem privada	AWS, Microsoft Azure, VMware, Red Hat	

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 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**.

©2025 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ e outras marcas registradas listadas em **zscaler.com/br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

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