Zscaler Internet Access

Proteção baseada em IA em todos os lugares, para todos os usuários, aplicativos e locais

FOLHA DE DADOS

O Zscaler Internet Access™ define acesso seguro e rápido à internet e SaaS com a plataforma zero trust mais abrangente e confiável do setor.

A segurança de rede legada tornou-se ineficaz em um mundo que prioriza a nuvem e os dispositivos móveis

As arquiteturas em estrela legadas eram eficazes quando os usuários estavam localizados principalmente na sede ou em uma filial, os aplicativos residiam somente no data center corporativo e sua superfície de ataque era limitada ao que sua organização sancionava. Hoje, vivemos em um mundo drasticamente diferente, com um cenário de ameaças em que ransomware, ameaças criptografadas, ataques à cadeia de suprimentos e outras ameaças avançadas rompem as defesas de rede legadas. É hora de encontrar uma solução de segurança nativa da nuvem que reduza holisticamente os riscos e a complexidade, ao mesmo tempo que oferece flexibilidade para ajudar a impulsionar as iniciativas de negócios.

Zscaler Internet Access

Proteger corporações modernas, que priorizam a nuvem e a mobilidade, requer uma abordagem fundamentalmente diferente, baseada em zero trust. O Zscaler Internet Access, parte da Zscaler Zero Trust Exchange™, é a plataforma de Security Service Edge (SSE) mais implantada no mundo, baseada em uma década de liderança em Secure Web Gateway.

Disponibilizado como uma plataforma SaaS de segurança na nuvem dimensionável e resiliente, o ZIA elimina as soluções de segurança de rede legadas para impedir ataques avançados e prevenir a perda de dados com uma abordagem zero trust completa, que oferece:

A melhor e mais consistente segurança da categoria para a força de trabalho híbrida atual: ao fazer a transição para a segurança na nuvem, todos os seus usuários, aplicativos, dispositivos e locais recebem proteção garantida e sempre ativa com base na identidade e no contexto. Sua política de segurança está onde seus usuários estão.

Acesso ultrarrápido com zero infraestrutura: a arquitetura direta para a nuvem garante uma experiência de usuário rápida e sem interrupções. Isso elimina o retorno do tráfego, melhora o desempenho e a experiência dos usuários e simplifica a administração da rede, sem a necessidade de uma infraestrutura física.

Proteção baseada em IA da maior nuvem de segurança do mundo: inspeção em linha de todo o tráfego da internet e SaaS, incluindo descriptografia de SSL, com um conjunto de serviços de segurança na nuvem baseados em IA para impedir ransomware, phishing, malware de dia zero e ataques avançados baseados em inteligência de ameaças de 500 trilhões de sinais diários.

Gerenciamento simplificado: usar uma solução de segurança nativa da nuvem com IA, menos hardware para gerenciar, automação para otimizar fluxos de trabalho e criação de políticas focadas nos negócios libera tempo valioso para sua equipe se concentrar em objetivos estratégicos.

Serviços de segurança e proteção de dados integrados e baseados em IA

O Zscaler Internet Access inclui um conjunto completo de serviços de segurança e proteção de dados baseados em IA para ajudá-lo a impedir ataques e evitar a perda de dados. Por ser uma solução SaaS completamente distribuída em nuvem, é possível adicionar novos recursos sem a necessidade de adquirir hardware adicional ou passar por longos ciclos de implantação. Os módulos que fazem parte do Zscaler Internet Access são:

- **Cloud Secure Web Gateway (SWG):** ofereça uma experiência web segura e rápida que elimina ransomware, malware e outros ataques avançados com análise em tempo real baseada em IA e filtragem de URL.
- **Agente de segurança de acesso à nuvem (CASB):** aplicativos em nuvem seguros com um CASB integrado para proteger dados, impedir ameaças e garantir a conformidade em seus ambientes de SaaS e IaaS.
- **Prevenção contra perda de dados (DLP) na nuvem:** proteja os dados em trânsito com a inspeção integrada completa e medidas avançadas, como correspondência exata de dados (EDM), reconhecimento óptico de caracteres (OCR) e aprendizado de máquina.
- **Zscaler Firewall e IPS na nuvem:** estenda a proteção líder do setor para todas as portas e protocolos e substitua os firewalls de borda e de filiais com uma plataforma nativa da nuvem.
- **Zscaler Sandbox:** bloqueie malwares nunca antes vistos e evasivos em protocolos de transferência de arquivos e da web com quarentena orientada por IA, compartilhando proteção consistente e global entre todos os usuários em tempo real.
- **Zero Trust Browser com tecnologia de IA:** Torne os ataques baseados na web obsoletos e evite a perda de dados criando um espaço livre virtual entre usuários, web e SaaS.

BENEFÍCIOS:

- **Evite ameaças cibernéticas e perda de dados com IA:** proteja sua organização contra ameaças avançadas com um conjunto de serviços de proteção de dados e ameaças cibernéticas baseados em IA, aprimorados por atualizações em tempo real provenientes de 500 trilhões de sinais diários de ameaças da maior nuvem de segurança do mundo.
- **Obtenha uma experiência de usuário sem igual:** obtenha a experiência de internet e SaaS mais rápida do mundo (até 40% mais rápida do que arquiteturas de segurança legadas) para acelerar a produtividade e aumentar a agilidade dos negócios.
- **Reduza custos e complexidade:** obtenha 139% de ROI com a Zscaler, substituindo 90% dos seus dispositivos caros, complexos e lentos por uma plataforma zero trust totalmente nativa da nuvem.
- **Proteja suas equipes híbridas:** Capacite funcionários, clientes e terceiros a acessar com segurança aplicativos web e serviços na nuvem de qualquer lugar, em qualquer dispositivo, com uma ótima experiência digital.
- **Unifique os esforços de SecOps e NetOps:** gere resultados de segurança mais rápidos e colaborativos com ferramentas compartilhadas, como insights de tráfego em tempo real, integrações orientadas por API e RBAC granular.
- **Obtenha soberania total de dados e conteúdo:** aplique conformidade para acesso seguro e localizado sem comprometer o desempenho usando Egress NAT, conteúdo geolocalizado e registro de dados no país.
- **Proteja a IA no seu ambiente:** habilite o uso seguro do Microsoft Copilot e outros aplicativos de IA.
- **Proteja ambientes de desenvolvedores em escala:** automatize a inspeção de SSL/TLS em mais de 30 ferramentas para desenvolvedores e faça sandbox de códigos e arquivos grandes ou desconhecidos com vereditos instantâneos de IA; tudo isso sem desacelerar a inovação.

©2025 Zscaler, Inc. Todos os direitos reservados.

- **Monitoramento de experiência digital:** reduza a sobrecarga operacional da TI e melhore o tempo de solução de chamados através de uma visão unificada das métricas de desempenho do aplicativo, caminho de nuvem e terminal para análise e solução de problemas.

- **Conectividade zero trust para filiais:** reduza os riscos e a complexidade com conectividade de filiais e data center não roteável para usuários, servidores e dispositivos de IoT/OT.

- **Segurança de DNS:** otimize a segurança e o desempenho do DNS para todos os usuários, dispositivos e aplicativos, em todas as portas e protocolos, em qualquer lugar do mundo.

Zscaler Internet Access para usuários e cargas de trabalho

Elimine o risco de cargas de trabalho na nuvem acessarem qualquer destino de internet ou SaaS com o Zscaler Internet Access. Ao remover a necessidade das cargas de trabalho acessarem a internet através de ferramentas legadas e centradas na rede como VPNs, firewalls (incluindo firewalls virtuais) ou WAN, é possível prevenir o comprometimento e impedir a movimentação lateral sem exigir uma diversidade de ferramentas de segurança. Ao aplicar o conjunto completo de recursos de segurança e proteção de dados do ZIA às cargas de trabalho, é possível unificar a segurança zero trust para seus usuários e cargas de trabalho em uma plataforma única e integrada.

Ao emparelhar o ZIA com o Zscaler Private Access, você pode estender a proteção aos seus aplicativos e cargas de trabalho privados, estejam eles na nuvem pública ou em um data center privado.

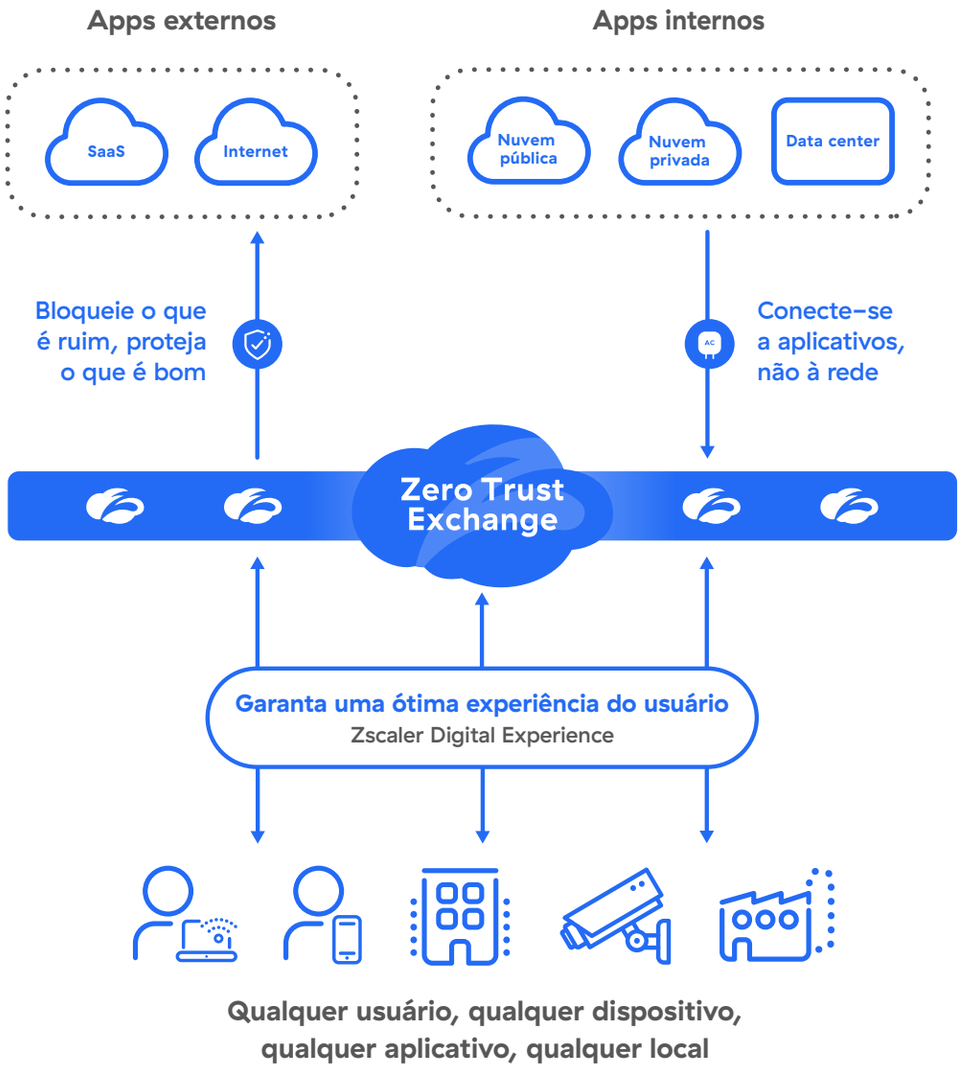


Figura 1: Zero Trust Exchange

*Gartner Magic Quadrant para Security Service Edge, 15 de abril de 2024, Charlie Winckless, et al.

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.

Gartner®

A Zscaler foi nomeada uma das líderes no Gartner® Magic Quadrant™ de 2024 para Security Service Edge.

VER MAIS

©2025 Zscaler, Inc. Todos os direitos reservados.

Casos de uso

PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS E RANSOMWARE

Migre da segurança de rede legada para a arquitetura zero trust revolucionária da Zscaler, que previne comprometimentos, elimina a superfície de ataque, impede a movimentação lateral e mantém os dados seguros.

Saiba mais

PROTEJA EQUIPES HÍBRIDAS

Permita que funcionários, parceiros, clientes e fornecedores acessem com segurança aplicativos web e serviços na nuvem de qualquer lugar e em qualquer dispositivo, e garanta uma excelente experiência digital.

Saiba mais

PROTEÇÃO DE DADOS

Impeça a perda de dados dos usuários, aplicativos SaaS e infraestruturas de nuvem pública causada por exposição acidental, roubo de dados ou ransomware de dupla extorsão.

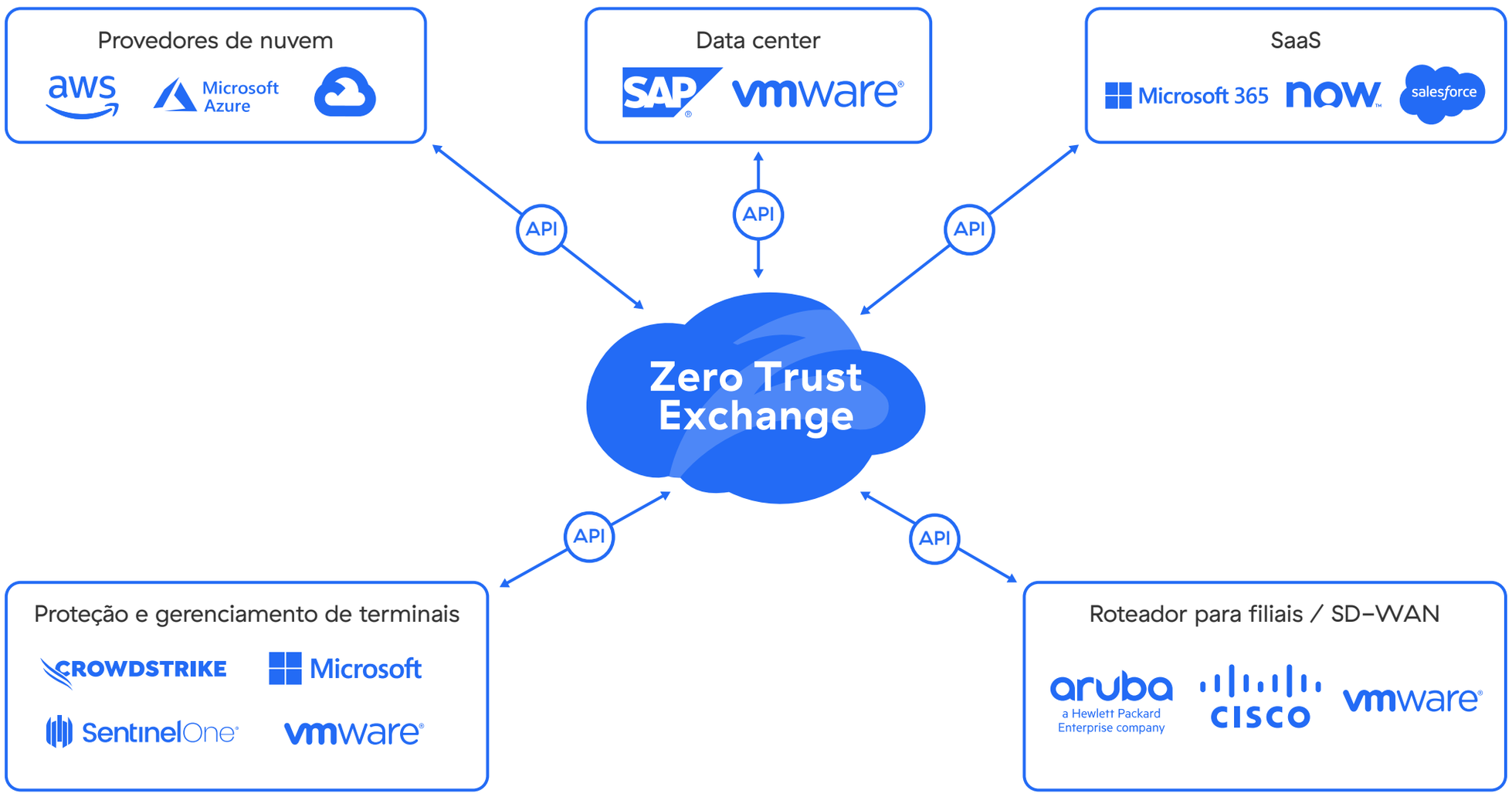
Saiba mais

MODERNIZAÇÃO DA INFRAESTRUTURA

Substitua redes caras e complexas por um acesso rápido, seguro e direto à nuvem, que não necessita de firewalls de borda ou em filiais.

Saiba mais

Ecossistema Zero Trust Exchange da Zscaler



©2025 Zscaler, Inc. Todos os direitos reservados.

TABELA 1: CARACTERÍSTICAS E RECURSOS DO ZSCALER INTERNET ACCESS	
CARACTERÍSTICAS	**DETALHES**
RECURSOS	
Filtragem de URL	Permitir, bloquear, alertar ou isolar o acesso do usuário a determinadas categorias ou destinos da web para impedir ameaças baseadas na web e garantir a conformidade com políticas organizacionais.
Inspeção SSL	Obtenha inspeção ilimitada do tráfego em TLS/SSL para identificar ameaças e perda de dados ocultas no tráfego criptografado. Especifique quais categorias da web ou aplicativos inspecionar com base em requisitos de privacidade ou regulamentares. Integre a inspeção com a ferramenta de desenvolvedor para proteger os fluxos de trabalho de desenvolvimento.
Segurança DNS	Identifique e encaminhe conexões de comando e controle suspeitas para os mecanismos de detecção de ameaças da Zscaler para obter uma inspeção completa do conteúdo.
IP dedicado	Forneça acesso a aplicativos que usam lista de permissões de IP com endereços IP dedicados à sua organização. Também permite uma transição fácil da arquitetura legada para o zero trust.
Controle de arquivos	Bloqueie ou autorize o download/upload de arquivos para aplicativos com base em aplicativos, usuários ou grupos de usuários.
Traga seu próprio IP	Mantenha a consistência e o controle sobre sua identidade de rede e garanta aos aplicativos de terceiros ou à infraestrutura dependente que o tráfego se origina somente da sua organização.
Controle de largura de banda	Aplique políticas de largura de banda para dar preferência aos aplicativos críticos da empresa em detrimento do tráfego recreativo.
Registros baseados no país	Armazene e gerencie registros dentro das fronteiras de um país específico para atender à conformidade com os requisitos de soberania de dados que exigem que os dados relacionados aos cidadãos sejam processados de acordo com as leis locais.
Proteção avançada contra ameaças	Impeça ataques cibernéticos avançados como malware, ransomware, ataques à cadeia de suprimentos, phishing e muito mais com nossa proteção avançada proprietária contra ameaças. Defina políticas granulares com base na tolerância ao risco de sua organização.
Proteção de dados integrada (dados em trânsito)	Utilize os recursos de proxy de encaminhamento e inspeção SSL para controlar o fluxo de informações sigilosas a destinos perigosos da web e aplicativos de nuvem em tempo real, impedindo que ameaças internas e externas acessem os dados. A proteção avançada integrada é disponibilizada independentemente do aplicativo ser sancionado ou não gerenciado, sem a necessidade de logs de dispositivo de rede.
Proteção de dados fora de banda (dados em repouso)	Utilize integrações de API para verificar aplicativos SaaS, plataformas de nuvem e seus conteúdos, identificando dados sensíveis em repouso e automaticamente remediando a situação através da revogação de compartilhamentos perigosos ou externos, por exemplo.
Prevenção contra intrusões	Obtenha proteção completa contra ameaças de botnets, ameaças avançadas e de dia zero, além de informações contextuais sobre o usuário, aplicativo e ameaça. O IPS na nuvem e na web trabalha perfeitamente em firewall, sandbox, DLP e CASB. Implante assinaturas de ameaças personalizadas usando o Cloud Custom IPS para detectar e interromper ataques direcionados.

©2025 Zscaler, Inc. Todos os direitos reservados.

Política de acesso e segurança dinâmica e baseada em risco	Adapte automaticamente a política de segurança e acesso de acordo com o usuário, dispositivo, aplicativo e risco do conteúdo.
Captura de tráfego	Captura de pacotes direta: capture facilmente o tráfego descriptografado por meio de critérios específicos nos mecanismos de políticas da Zscaler, oferecendo suporte a análises forenses de segurança eficientes sem a necessidade de dispositivos adicionais.
Análise de malware	Detecte, previna e isole ameaças desconhecidas ocultas em cargas maliciosas integradas através da IA/ML para impedir ataques de paciente zero.
Filtragem DNS	Controle e bloqueie solicitações DNS de destinos conhecidos e maliciosos.
Zero Trust Browser (isolamento web)	Torne as ameaças baseadas na web obsoletas ao oferecer conteúdo ativo como um fluxo benigno de pixels ao navegador do usuário final.
Informações sobre ameaças correlacionadas	Diminua o tempo de investigação e resposta com alertas contextualizados e correlacionados, com informações sobre pontuação da ameaça, ativo afetado, gravidade e muito mais.
Isolamento de aplicativos	Permita o acesso seguro de dispositivos sem agentes e não gerenciados a SaaS, nuvem e aplicativos privados, com controle granular sobre ações de usuário como copiar/colar, fazer upload/download e impressão para impedir a perda de dados sigilosos.
Monitoramento da experiência digital (ZDX)	Obtenha uma visão unificada das métricas de desempenho de aplicativos, rotas na nuvem e terminais para análise e solução de problemas.
Conectividade de filial Zero Trust	Modernize a conectividade de filiais com a Zero Trust Exchange, eliminando a superfície de ataque e evitando a movimentação lateral.
Proteção de comunicação da carga de trabalho para a internet	Evite o comprometimento e impeça a movimentação lateral de comunicações de cargas de trabalho para a internet. Inclui inspeção de SSL, IPS, filtragem de URL e proteção de dados para todas as comunicações.
Visibilidade de dispositivos IoT	Obtenha uma visão completa de todos os dispositivos de IoT, servidores e dispositivos de usuários não gerenciados em sua empresa, com descoberta automatizada, monitoramento contínuo e classificação de IA/ML com recursos de rotulagem automática líderes do setor
Controle de acesso baseado em função (RBAC)	Permissões dimensionadas corretamente para controlar o que os administradores podem editar e visualizar relatórios de políticas e análises na plataforma da Zscaler, para evitar conflitos e melhorar a governança.

©2025 Zscaler, Inc. Todos os direitos reservados.

CARACTERÍSTICAS	DETALHES
RECURSOS DA PLATAFORMA	
Opções de conectividade flexíveis	• Zscaler Client Connector (ZCC): encaminhe tráfego para a Zero Trust Exchange por meio de um agente leve compatível com Windows, macOS, iOS, iPadOS, Android e Linux. • Túneis de GRE ou IPsec: use túneis de GRE e/ou IPsec para enviar tráfego para a Zero Trust Exchange para dispositivos sem ZCC. • Isolamento do navegador: conecte facilmente qualquer dispositivo pessoal ou não gerenciado com o isolamento do Zero Trust Browser integrado. • Encadeamento de proxy: a Zscaler oferece encaminhamento do tráfego de um servidor proxy para outro, mas isso não é recomendado em ambientes de produção. • Arquivos PAC: envie tráfego para a Zero Trust Exchange com arquivos PAC para dispositivos sem ZCC.
Implantação disponibilizada na nuvem	Plataforma 100% nativa da nuvem disponibilizada como um serviço SaaS. Para planejamento de continuidade de negócios e outros casos de uso especiais, bordas de serviço privadas e virtuais estão disponíveis.
Privacidade e retenção de dados	Ao registrar dados, o conteúdo nunca é gravado no disco e não há controles granulares para determinar com precisão onde os registros são feitos. Utilize o controle de acesso baseado em funções (RBAC) para fornecer acesso somente leitura, anonimização/ofuscação de nome de usuário e direitos de acesso separados por departamento ou função, de acordo com as principais regulamentações de conformidade. Os dados são retidos por um período contínuo de seis meses ou menos, dependendo do produto. É possível adquirir armazenamento adicional que retém os dados pelo tempo que desejar.
Principais certificações de conformidade	Certificações incluídas: • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C Veja a lista completa de nossas certificações de conformidade aqui.
Compatibilidade granular com APIs	Mantemos integrações de API REST com vários fornecedores de identidade, rede e segurança. Por exemplo, é possível compartilhar logs entre a Zscaler e o seu SIEM baseado na nuvem ou local (como o Splunk). Saiba mais
Emparelhamento direto	O emparelhamento direto com os principais fornecedores de internet e SaaS e destinos de nuvem públicos garante o caminho de tráfego mais rápido possível.

©2025 Zscaler, Inc. Todos os direitos reservados.

CARACTERÍSTICAS	DETALHES
ACORDOS DE NÍVEL DE SERVIÇO (SLAS)	
Disponibilidade	99,999%, medido por transações perdidas
Latência do proxy	Menos de 100 ms, inclusive quando a verificação contra ameaças e DLP está ativada
Captura de vírus	100% dos vírus e malwares conhecidos
PLATAFORMAS E SISTEMAS COMPATÍVEIS	
Client Connector	Compatibilidade com: • iOS 9 ou posterior • Android 8 ou posterior • Windows 8 e posterior • Mac OS X 10.14 e posterior • CentOS 9 • Ubuntu 20.04 Saiba mais
Branch Connector	Compatibilidade com: • VMware vCenter ou vSphere Hypervisor • CentOS • RedHat

©2025 Zscaler, Inc. Todos os direitos reservados.

Zscaler Internet Access: várias opções para começar

	PLATAFORMA ESSENTIALS Comece sua jornada zero trust com acesso seguro e confiável à internet e acesso privado limitado, com outras inovações da Zscaler.	PLATAFORMA ZSCALER Desbloqueie a solução de SASE/SSE completa, incluindo acesso total à internet, acesso privado e proteção de dados.
SERVIÇOS DA PLATAFORMA		
Encaminhamento de tráfego: Client Connector, GRE, PAC, encadeamento de proxy, IPsec	✓	✓
Vários provedores de identidade (IdP), acesso à API, postura do dispositivo	✓	✓
Autenticação: SAML, LDAP seguro, Kerberos	✓	✓
Ambiente de teste ZS	–	–
Acesso aos DCs públicos da Zscaler	✓	✓
Acesso a DCs públicos da Zscaler de alto custo (Austrália, Nova Zelândia, Dubai (não regulamentado), América do Sul, África, Coreia do Sul, Taiwan e China continental)	–	✓
China Premium/Acesso regulamentado ao DC do Oriente Médio	–	–
ACESSO À INTERNET		
Filtragem de conteúdo	✓	✓
Controle de tipo de arquivo	✓	✓
Inspeção de TLS/SSL	✓	✓
Certificado SSL privado	✓	✓
Controle de largura de banda	✓	✓
Stream para SIEM local (serviço de streaming nanolog com gerenciamento ao vivo)	✓	✓
Nuvem NSS (para > 500 usuários)	✓	✓
Ancoragem de IP de origem	–	✓
ZIA Private Service Edge – dispositivo virtual	–	✓
Hardware: ZIA Private Service Edge – 3 instâncias, 5 instâncias	–	–

©2025 Zscaler, Inc. Todos os direitos reservados.

PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS		
Proteção contra ameaças cibernéticas Standard: proteção avançada contra ameaças, sandbox Standard, firewall zero Standard, Zero Trust Browser Standard	✓	✓
Antivírus e antispyware em linha	✓	✓
Sandbox Advanced	–	–
Firewall Zero Trust Advanced	–	–
Zero Trust Browser Advanced (1,5 GB de tráfego/ usuário/mês, medido entre todos os usuários do Zero Trust Browser)	–	–
Zero Trust Browser Unlimited (sem limites de uso de tráfego)	–	–
ACESSO PRIVADO (ZPA)		
Acesso seguro a apps privados (na nuvem, data centers): streaming de logs, ancoragem de IP de origem, múltiplos IdP, monitoramento de integridade)	1 usuário por 20 usuários inscritos (mín.: 500 usuários inscritos)	✓
Conectores de aplicativos	Quantos forem necessários (até o máximo do sistema)	Quantos forem necessários (até o máximo do sistema)
PROTEÇÃO DE DADOS		
Proteção de dados Standard: controle de aplicativos na nuvem, relatório de TI invisível, restrição de utilização, web em linha (modo monitor), API SaaS (1 aplicativo), segurança de GenAI	✓	✓
Web em linha e DLP de GenAI, todos os aplicativos (internet e acesso privado)	–	✓
GERENCIAMENTO DE RISCOS		
Gerenciamento de riscos Standard: Deception Standard	–	✓
ZERO TRUST PARA CARGAS DE TRABALHO		
Zero Trust para cargas de trabalho Standard: filtragem com estado, DNS, inspeção de TLS	1 GB de tráfego de carga de trabalho mensal por usuário inscrito	2 GB de tráfego de carga de trabalho mensal por usuário inscrito
EXPERIÊNCIA DIGITAL (ZDX)		
ZDX Standard: Pre-Set	✓	–
Padrão ZDX	–	✓
SUPORTE		
Suporte Standard	✓	✓
Suporte Plus	–	–

©2025 Zscaler, Inc. Todos os direitos reservados.

MODELO DE LICENCIAMENTO

Todas as edições do Zscaler Internet Access são precificadas por usuário. Para determinados produtos dentro da sua edição de plataforma, os preços podem variar além da contagem de usuários. Para mais informações sobre preços, fale com sua equipe de contas da Zscaler.

Faz parte da holística Zero Trust Exchange

A Zero Trust Exchange garante conexões rápidas e seguras e permite que seus funcionários trabalhem de qualquer lugar usando a internet como rede corporativa. Baseada no princípio zero trust de acesso de privilégio mínimo, a plataforma oferece segurança abrangente usando identidade baseada no contexto e aplicação de políticas.

O fantástico sobre a Zscaler é que ela fornece tudo o que precisamos em uma plataforma zero trust: inspeção de tráfego em SSL dimensionável, outras funcionalidades de prevenção de ameaças e proteção de dados.

NITIN NEGI
Gerente sênior de engenharia e operações de cibersegurança, Micron Technology

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A plataforma 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 160 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™ 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**

zscaler™

Zero Trust Everywhere