

Zscaler Internet Access

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

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

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

As arquiteturas de rede em estrela legadas eram eficazes quando os usuários estavam a maior parte do tempo nas empresas e suas filiais, os aplicativos eram hospedados apenas no data center corporativo e a superfície de ataque estava limitada ao que sua organização sancionava. Hoje, vivemos em um mundo extremamente diferente, com um cenário de ameaças no qual ransomware, ameaças criptografadas, ataques à cadeia de suprimentos e outras ameaças avançadas invadem as defesas de rede legadas. Chegou a hora de encontrar uma solução nativa da nuvem que reduza o risco e a complexidade por completo e que, ao mesmo tempo, forneça flexibilidade para ajudar a avançar com as iniciativas comerciais.

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.

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.
- **Modernize sua arquitetura de segurança:** obtenha um ROI de 139% com a Zscaler ao substituir 90% do hardware caro, complexo e lento por uma plataforma zero trust totalmente nativa da nuvem.

Disponibilizado como uma plataforma SaaS dimensionável da maior nuvem de segurança do mundo, ele 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 imediato com zero infraestrutura:

a arquitetura cloud garante uma experiência de usuário rápida e integrada. Isso elimina o backhauling, melhora o desempenho e a experiência do usuário e simplifica a administração da rede — sem necessidade de 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 descryptografia 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: utilizar uma solução de segurança nativa da nuvem baseada em IA, sem hardware para gerenciar e contendo fluxos de trabalho diretos e criação de políticas focadas nos negócios libera o tempo valioso da sua equipe para que ela concentre-se em objetivos estratégicos.

*Gartner Magic Quadrant para Security Service Edge, 10 de abril de 2023, 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 fatos. 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.

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.

Gartner®

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

[Ver mais →](#)

- **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:** impeça ataques de malware nunca antes vistos e elusivos em protocolos de transferência de arquivos e da web através da quarentena baseada em IA, compartilhando uma proteção consistente e global entre todos os usuários em tempo real.
- **Isolamento do navegador na nuvem baseado em IA:** torne os ataques baseados na web obsoletos e previna a perda de dados criando um espaço livre virtual entre usuários, web e SaaS.
- **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/TO.
- **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 acessando 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 unir o ZIA com o [Zscaler Private Access](#), é possível estender a proteção para seus aplicativos e cargas de trabalho privados, estejam eles em uma nuvem pública ou em um data center particular.

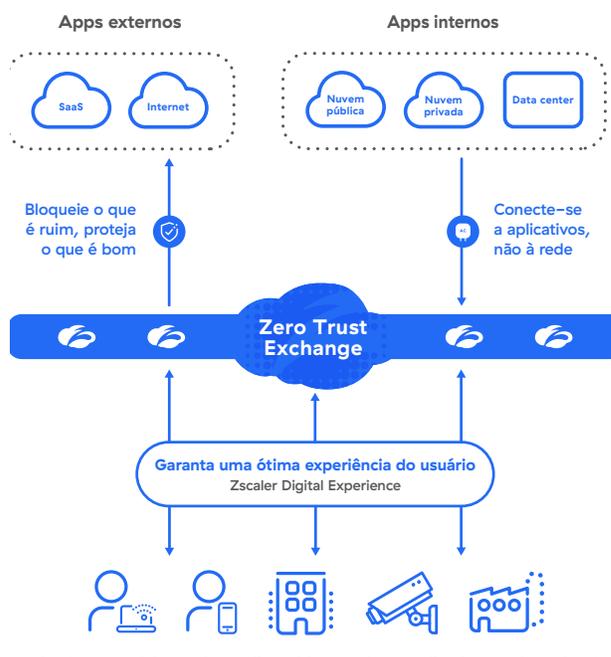


Figura 1: Zero Trust Exchange

Casos de uso



Proteção contra ameaças cibernéticas e ransomware

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

[Saiba mais →](#)



Proteja equipes híbridas

Capacite funcionários, parceiros, clientes e fornecedores a acessar com segurança aplicativos web e serviços de nuvem em qualquer lugar, de qualquer dispositivo, e garanta uma excelente experiência digital.

[Saiba mais →](#)



Proteção de dados

Impedindo a perda de dados dos usuários, aplicativos SaaS e infraestruturas de nuvens públicas, seja por consequência de 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 na nuvem, que remove a necessidade de firewalls de borda e de filiais.

[Saiba mais →](#)

Ecosistema Zero Trust Exchange da Zscaler

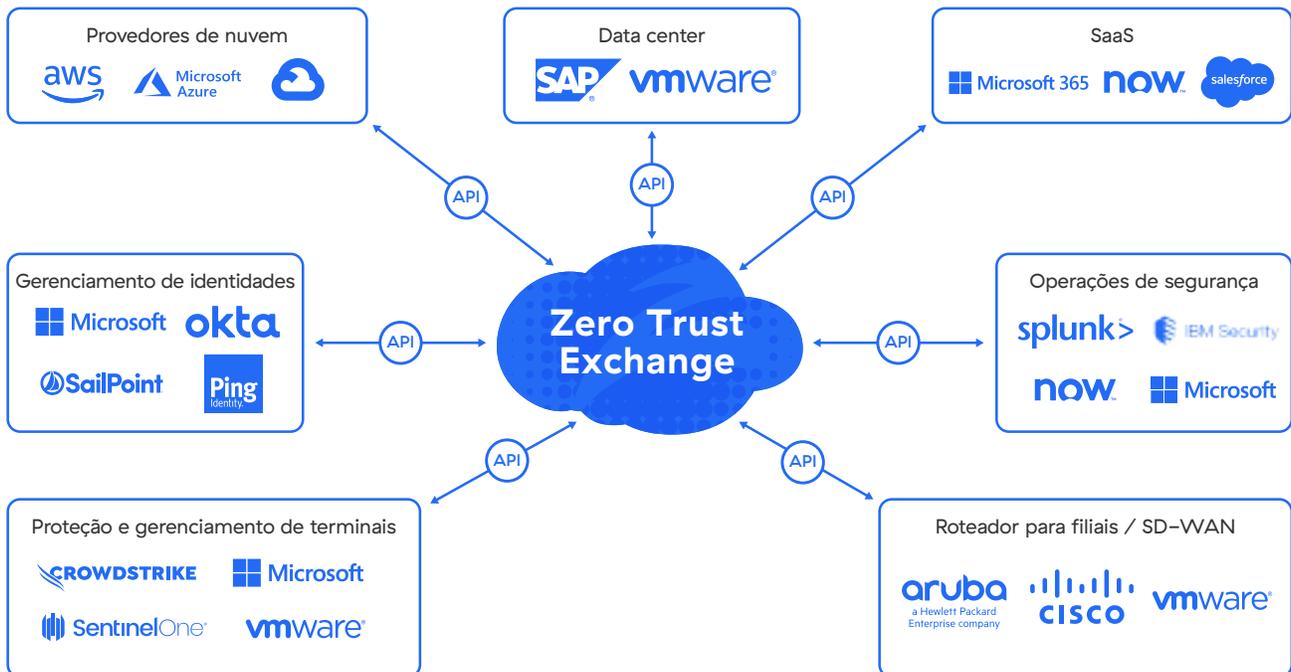


Figura 2: ecossistema de parceiros do Zscaler Internet Access

TABELA 1: CARACTERÍSTICAS E RECURSOS DO ZSCALER INTERNET ACCESS

CARACTERÍSTICAS	DETALHES
Recursos	
Filtragem de URL	Permita, bloqueie, alerte ou isole 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 de tráfego TLS/SSL ilimitada para identificar ameaças e perdas de dados ocultas no tráfego criptografado. Especifique quais categorias da web ou aplicativos inspecionar com base em requisitos regulamentares ou de privacidade.
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.
Controle de arquivos	Bloqueie ou autorize o download/upload de arquivos para aplicativos com base em aplicativos, usuários ou grupos de usuários.
Controle de largura de banda	Aplique políticas de largura de banda para dar preferência aos aplicativos críticos da empresa em detrimento do tráfego recreativo.
Proteção avançada contra ameaças	Impeça ataques cibernéticos avançados, como malware, ransomware, ataques à cadeia de suprimentos, phishing e muito mais com nossa exclusiva proteção avançada 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.
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.
Isolamento da 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	Obtenha 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	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 carga de trabalho para a internet. Inclui inspeção 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

CARACTERÍSTICAS	DETALHES
Recursos da plataforma	
Opções flexíveis de conectividade	<ul style="list-style-type: none"> • Zscaler Client Connector (ZCC): encaminhe o tráfego para a Zero Trust Exchange através de um agente leve e compatível com Windows, macOS, iOS, iPadOS, Android e Linux. • Tunelamentos GRE ou IPsec: use tunelamentos GRE e/ou IPsec para enviar tráfego de dispositivos sem ZCC para a Zero Trust Exchange. • Isolamento do navegador: conecte perfeitamente qualquer dispositivo BYOD ou sem gerenciamento com o Cloud Browser Isolation integrado. • Encadeamento de proxy: a Zscaler aceita o encaminhamento do tráfego de um servidor proxy para outro, embora isso não seja 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 casos de uso exclusivos, estão disponíveis serviços de borda privados e virtuais.
Privacidade e retenção de dados	<p>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.</p> <p>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.</p>
Principais certificações de conformidade	<p>Certificações incluídas:</p> <ul style="list-style-type: none"> • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C <p>Veja a lista completa de nossas certificações de conformidade aqui.</p>
Compatibilidade granular com APIs	<p>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).</p> <p>Saiba mais</p>
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.
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	<p>Compatibilidade com:</p> <ul style="list-style-type: none"> • iOS 9 ou posterior • Android 5 ou posterior • Windows 7 e posterior • Mac OS X 10.10 e posterior • CentOS 8 • Ubuntu 20.04 <p>Saiba mais</p>
Branch Connector	<p>Compatibilidade com:</p> <ul style="list-style-type: none"> • VMware vCenter ou vSphere Hypervisor • CentOS • RedHat

Zscaler Internet Access Editions

	Recursos	Essenciais	Empresa	Transformação	Ilimitado
Serviços da plataforma		Filtragem de conteúdo, AV integrado, inspeção de SSL, Nanolog Streaming	(+) Certificado SSL privado	(+) Cloud NSS, recuperação de registros NSS, acesso ao DC estendido, túnel IPSec, alertas contextuais, ZIA Virtual Private Service Edge (8)	(+) Ancoragem de IP de origem, ambiente de teste, categorização de prioridade, ZIA Virtual Private Service Edge (32), proteção de servidor e IoT (1 GB/10 usuários)
Proteção contra ameaças	Proteção avançada contra ameaças (incluindo detecção de phishing e C2 baseada em IA) Proteção contra ameaças conhecidas e desconhecidas (URL, AV, Botnet/C2, Phishing)	ticado	ticado	ticado	ticado
	Cloud Sandbox Prevenção contra ataques de dia zero analisando arquivos suspeitos com a quarentena baseada em IA	Complemento	Complemento	ticado	ticado
	Isolamento — proteção contra ameaças cibernéticas Proteção contra ataque de dia zero de conteúdo suspeito da web. Isolamento baseado em risco com tecnologia de IA	Complemento	Complemento	Isolamento para proteção cibernética: Std (100 MB/ usuário/mês)	Isolamento para proteção cibernética: Std (1,5 GB/ usuário/mês)
	Informações sobre ameaças correlacionadas Acelere as investigações e o tempo de resposta com inteligência contextual contra ameaças	-	ticado	ticado	ticado
	Políticas dinâmicas e baseadas em risco Adapta e recomenda automaticamente políticas de segurança com base em vários fatores de risco	-	-	ticado	ticado
	Engano integrado Aumente sua postura de segurança zero trust atraindo, detectando e interceptando proativamente invasores ativos	-	-	Standard ¹	Standard ¹
	Transformação da rede	Resolução e filtragem de DNS Resolver de DNS confiável para resolução de DNS geocêntrica e ideal	Até 64 regras	Até 64 regras	ticado
	Detecção de túnel DNS Detecte e evite ataques baseados em DNS e exfiltração de dados por meio de túneis DNS	-	-	ticado	ticado
	Controle de largura de banda Controle de tráfego e priorização de largura de banda, limitação de taxa para tráfego da web		ticado	ticado	ticado
	Firewall de nuvem Proteção para o trabalho de qualquer lugar para todos os usuários e tráfego (web e não-web) com inspeção de SSL infinita	Rede, serviços de aplicativos, locais, FQDNs até 10 regras	Rede, serviços de aplicativos, locais, FQDNs até 10 regras	(+) usuários que trabalham de qualquer lugar, locais, inspeção profunda de pacotes de aplicativos	(+) usuários que trabalham de qualquer lugar, locais, inspeção profunda de pacotes de aplicativos
	Proteção para tráfego não autenticado Proteja redes com segurança de nível de operadora totalmente automatizada e com limitações	0,5 GB/usuário/mês	1 GB/usuário/mês	1,5 GB/usuário/mês	2 GB/usuário/mês

	Recursos	Essenciais	Empresa	Transformação	Ilimitado
Proteja os dados e evite a perda de dados	Cloud App Control + restrições de usuário Encontre e controle aplicativos de risco ou não sancionados (TI invisível)	ticado	ticado	ticado	ticado
	Isolamento — proteção de dados (SaaS) Evite a perda de dados de aplicativos SaaS para dispositivos pessoais ou terminais não gerenciados (sem cliente)	Complemento	Complemento	Complemento	Isolamento para proteção de dados (SaaS): Std. (100 MB/ usuário/mês)
	DLP, CASB, Inline Web Essentials, API SaaS (1 aplicativo) Evite a perda de dados sigilosos para a internet. Analise 1 aplicativo SaaS para compartilhamento de risco de dados sigilosos ou malware	-	Data Protection Std (DLP e CASB Essentials)	(+) Retroanálise de API de SaaS	ticado
	API SaaS, segurança da cadeia de suprimentos SaaS, dispositivos não gerenciados, classificação, gerenciamento de incidentes Benefícios da Standard Data Protection Plus: controle os riscos de dispositivos pessoais transmitindo dados como pixels, verifique vários aplicativos SaaS em busca de compartilhamentos de risco/malware, personalize a DLP com EDM, IDM, OCR e ferramentas para gerenciamento de incidentes e automação de fluxo de trabalho	Complemento	Complemento	Complemento	ticado
Monitoramento da experiência digital	Monitore as experiências digitais a partir da perspectiva do usuário final para otimizar o desempenho e corrigir rapidamente os problemas de aplicativos, redes e dispositivos.	-	Padrão	Padrão	Padrão
Premium Support Plus		Complemento	Complemento	Complemento	ticado

Modelo de licenciamento

Todas as edições do Zscaler Internet Access são cobradas por usuário. Para certos produtos da sua edição, o preço pode variar independentemente do número de usuários. Para obter mais informações sobre valores, fale com a equipe da sua conta 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.

“ Quando ataques de ransomware acontecem a outras empresas, milhares de sistemas no seu ambiente são prejudicados, além dos sérios impactos causados pela necessidade de pagar um resgate. Quando esse tipo de evento vira notícia, recebo ligações de executivos preocupados e posso ficar tranquilo em dizer que estamos protegidos.

Ken Athanasiou, VIP e CISO, AutoNation



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](https://twitter.com/zscaler).

©2024 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.