FICHA TÉCNICA

# Zero Trust Cloud

**Proteja o tráfego de cargas de trabalho para a internet e entre cargas de trabalho com o poder da Zscaler Zero Trust Exchange™.**

A transformação digital está promovendo a criação e o uso de cargas de trabalho em uma ampla gama de ambientes de infraestrutura local, de nuvem privada e de nuvem pública. Sua empresa opera com essas cargas de trabalho, portanto, prevenir ataques cibernéticos e perdas de dados é essencial.

As arquiteturas de soluções legadas são inadequadas: elas fornecem proteção inconsistente contra ameaças e de dados, aumentam a superfície de ataque, deixam as portas abertas para a movimentação lateral e aumentam a complexidade e o custo operacionais.

A Zscaler Zero Trust Cloud simplifica radicalmente a segurança de cargas de trabalho híbridas. Com o poder da plataforma Zero Trust Exchange, ela protege o tráfego de saída de cargas de trabalho para a internet e entre cargas de trabalho na nuvem pública e em data centers locais para suas cargas de trabalho e servidores críticos.

A Zero Trust Cloud fornece proteção consistente contra ameaças e dados, elimina a superfície de ataque, interrompe a movimentação lateral, reduz a complexidade e diminui os custos operacionais.

> “Com a Zscaler Workload Communications, podemos padronizar facilmente as políticas de segurança tanto para usuários quanto para aplicativos, independentemente de onde estejam localizados.”
>
> **Rui Cabeço,** líder global de conectividade de saída, Siemens

## Desafios com cargas de trabalho legadas e segurança do servidor

Muitas empresas dependem de arquiteturas legadas para proteger suas cargas de trabalho na nuvem. A maioria delas faz uma combinação do seguinte:

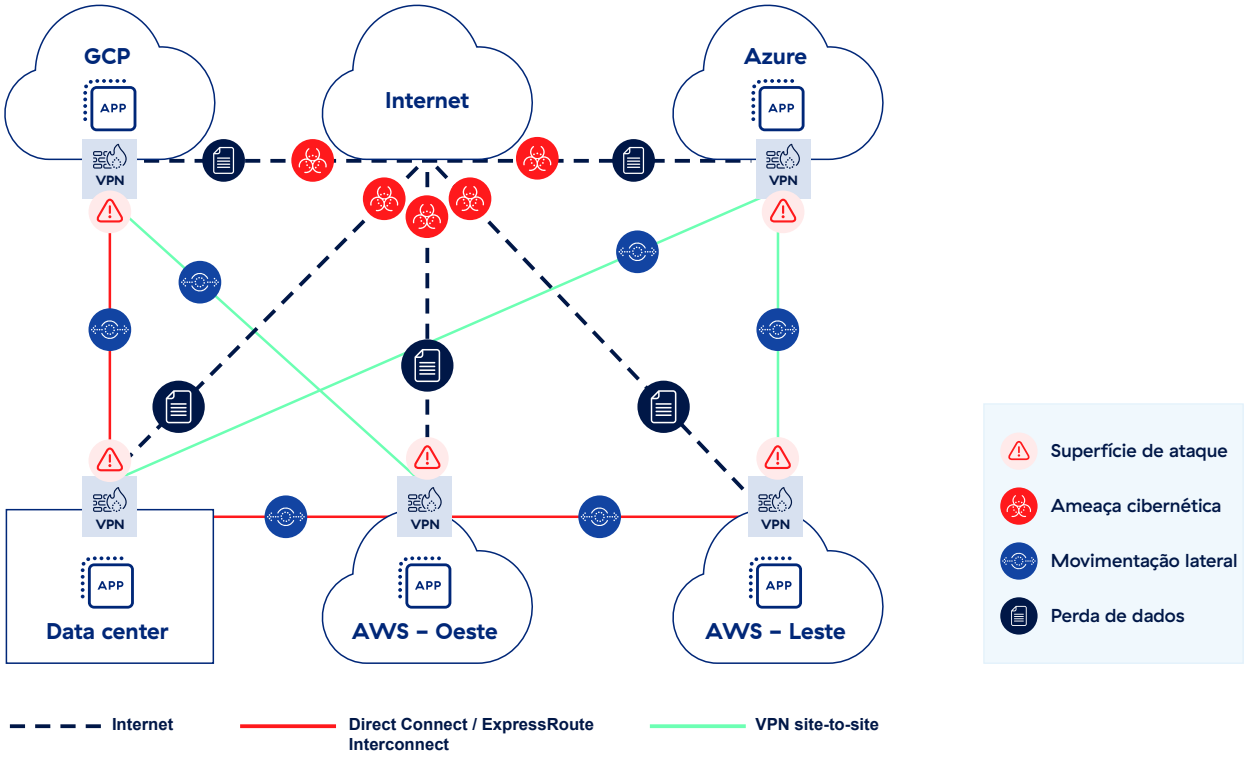
**Configurar soluções de segurança nativas oferecidas por provedores de serviços de nuvem pública**

**Implantação de ferramentas de terceiros (firewall, inspeção de TLS/SSL, DLP, etc.) para camadas extras de proteção**

**Retorno do tráfego para a infraestrutura de segurança de rede local para inspeção e proteção**

O uso desses métodos apresenta vários desafios, incluindo:

- **Aumento da superfície de ataque e oportunidade de movimentação lateral.** Soluções como firewalls estendem a rede para cargas de trabalho e servidores, amplificando os riscos de movimentação lateral. Cada firewall voltado para a internet também aumenta a superfície de ataque. Isso pode abranger a internet para diferentes nuvens e ambientes locais. Além disso, uma colcha de retalhos de dispositivos virtuais, ferramentas operacionais e políticas não padronizadas introduz brechas conhecidas e desconhecidas na cobertura de segurança, aumentando o risco de segurança.
- **Brechas de visibilidade de TLS.** A inspeção de TLS pode usar recursos de computação significativos e apresentar desafios como degradação de desempenho quando habilitada. Gerenciar certificados distribuídos ou aplicar exclusões a cargas de trabalho fixadas cria desafios operacionais. Além disso, ela geralmente leva ao aumento dos custos de infraestrutura de segurança cibernética para dar conta da demanda.
- **Maior complexidade e baixo desempenho.** As soluções de rede e segurança legadas não foram criadas com cargas de trabalho na nuvem em mente, então produtos específicos como firewalls virtuais, proxies e gateways de NAT devem ser incorporados. Algumas soluções podem usar VMs separadas para cada função de segurança, resultando na inspeção sequencial no estilo de uma linha de montagem, o que aumenta a latência. Isso cria complexidades operacionais significativas quando aplicado em ambientes multinuvem.
- **Altos custos.** O uso de produtos específicos de segurança de rede legados (por exemplo, firewalls, IPS, roteadores), o provisionamento excessivo da infraestrutura de segurança de rede para compensar a falta de capacidade de dimensionamento e o uso crescente de serviços nativos da nuvem contribuem para o aumento das despesas de capital e operacionais.
- **Falta de registro comum.** Alguns mandatos legais e regulatórios podem exigir que as organizações armazenem registros por períodos prolongados. Acessar esses registros de diferentes ambientes de nuvem e armazená-los em uma infraestrutura de SIEM central pode ser complexo e caro.




## Estenda a arquitetura zero trust para nuvens públicas e data centers locais

A Zero Trust Cloud elimina a superfície de ataque da rede conectando cargas de trabalho e servidores à internet e aplicativos privados com uma arquitetura zero trust. Isso simplifica drasticamente a conectividade ao reduzir a dependência da sua organização em soluções legadas, como firewalls, ao mesmo tempo em que permite o encaminhamento flexível e facilita o gerenciamento de políticas com a estrutura de políticas comprovada do Zscaler Internet Access™ (ZIA) e do Zscaler Private Access™ (ZPA).

Tudo isso é possível graças à plataforma Zero Trust Exchange, que opera em hiperescala e pode lidar com qualquer aumento nas cargas de trabalho ou no tráfego do servidor, com dimensionamento elástico e horizontal. Com a Zero Trust Cloud, todo o tráfego de cargas de trabalho e de saída do servidor é encaminhado para a Zero Trust Exchange, onde as políticas de segurança podem ser aplicadas para inspeção completa de TLS/SSL e controle de acesso.

O tráfego de saída é então encaminhado para o destino pretendido, seja a internet, aplicativos SaaS ou outras cargas de trabalho e servidores hospedados em outras nuvens públicas ou data centers.

Com a Zero Trust Cloud, você pode:

### Obter proteção contra ameaças e de dados consistente e abrangente

Aplique políticas comuns em todos os ambientes

- Evite ataques de dia zero com inspeção de TLS em escala de nuvem e proteção contra ameaças
- Impeça vazamentos de dados com inspeção de DNS e proteção de dados em linha
- Limitar o número de destinos que as cargas de trabalho e os servidores podem acessar com controles rígidos

### Eliminar a superfície de ataque e a movimentação lateral

Conectcar aplicativos, não redes, e tornar-se indetectável

- Aplicar acesso de privilégio mínimo para segmentar cargas de trabalho usando IP, FQDN, VPC, VNet ou tags
- Conectar cargas de trabalho usando a Zero Trust Exchange, eliminando a superfície de ataque da rede
- Oferecer suporte de nuvem para nuvem, de nuvem para data center, de região para região

### Reduzir os custos e a complexidade operacional

Usar uma plataforma disponibilizada na nuvem para proteger todas as cargas de trabalho

- Proteger cargas de trabalho em todos os principais provedores de serviços na nuvem, incluindo AWS, Azure e GCP, usando uma plataforma unificada
- Automatize implantações de segurança por meio de interfaces programáveis usando modelos de infraestrutura como código (IaC)
- Utilize integrações do provedor de serviços de nuvem pública, como o Gateway Load Balancer da AWS, tags definidas pelo usuário da AWS e dimensionamento automático da AWS

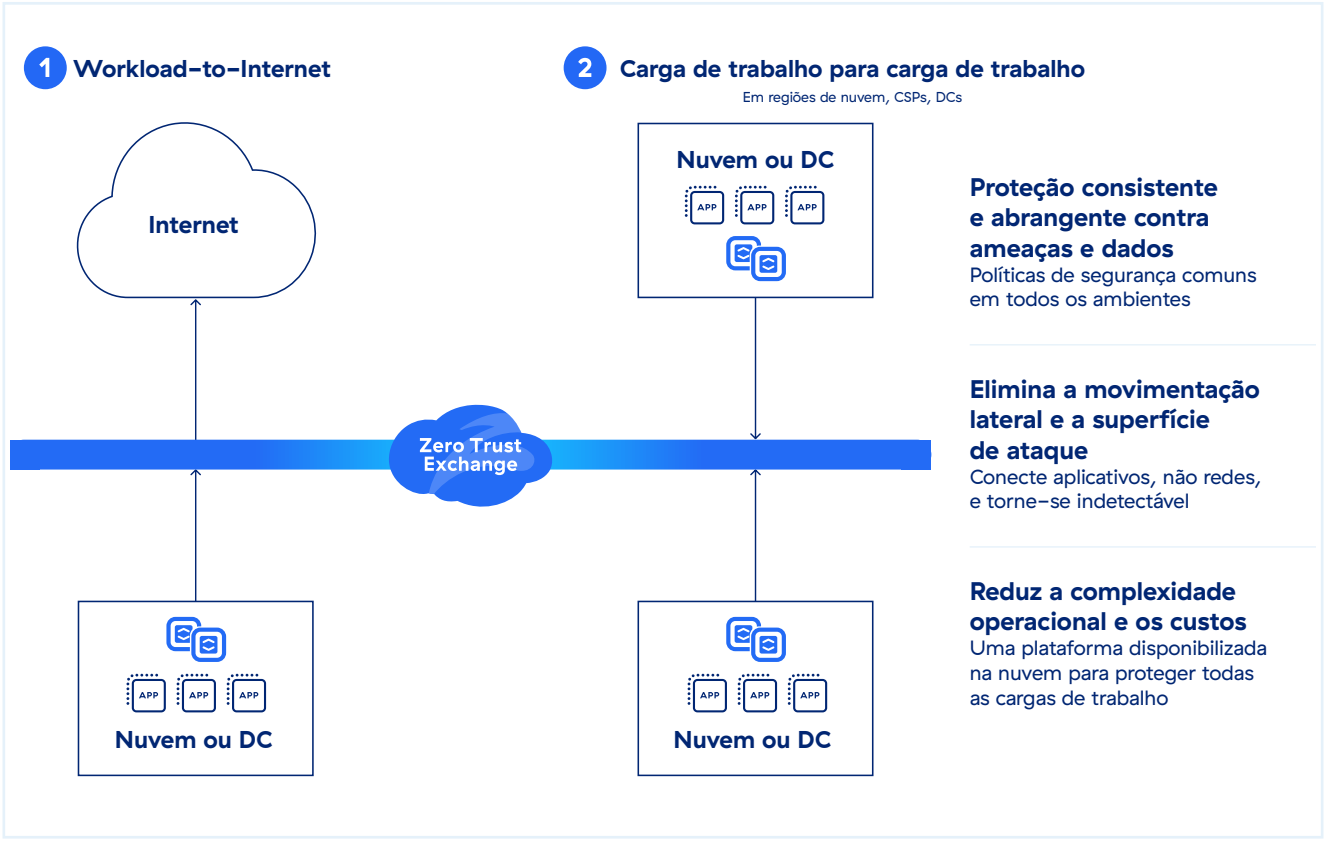



FIGURA Zscaler Zero Trust para cargas de trabalho

## Características da Zero Trust Cloud

A Zero Trust Cloud foi desenvolvida na Zero Trust Exchange, que conecta com segurança usuários, dispositivos e aplicativos usando políticas de negócios em qualquer rede e nuvem, em larga escala.

**Arquitetura de proxy zero trust:** nossa arquitetura de proxy multiusuário desenvolvida especificamente para conectar origens e destinos com segurança, ao mesmo tempo em que fornece visibilidade total do tráfego de saída.

**Descriptografia de TLS em escala de nuvem:** a inspeção de alto desempenho é feita por uma arquitetura Single-Scan, Multi-Action criada para trabalhar em larga escala.

**Segmentação granular de aplicativo para aplicativo:** acesso zero trust e de privilégio mínimo para todas as cargas de trabalho e servidores, proporcionando aplicação e gerenciamento simplificados de políticas de negócios.

**Inspeção bidirecional de ameaças:** a proteção contra ameaças com tecnologia de IA, alimentada por 500 trilhões de sinais diários e 320 bilhões de transações diárias, oferece proteção contra ransomware sempre ativa e hermética, prevenção de ameaças de dia zero e prevenção de malware desconhecido.

**Proteção de dados em linha:** inspeção de DLP dimensionável e de alto desempenho em todos os canais e locais.

**Plataforma comum, pronta para várias nuvens:** uma plataforma unificada fornece gerenciamento de políticas, monitoramento de tráfego e rastreamento de registros. As políticas padronizadas são aplicadas na AWS, Azure, GCP e data centers locais.

## Recursos da Zero Trust Cloud

| PLATAFORMA ZSCALER ZERO TRUST CLOUD | |
|---|---|
| **CARACTERÍSTICAS** | **DETALHES** |
| **Nuvem Pública e Cobertura no local** | Oferece suporte à proteção de cargas de trabalho na AWS, Microsoft Azure, Google Cloud Platform, regiões da Microsoft Azure China e AWS GovCloud com suporte adicional para servidores de data centers locais. Certificação FedRamp para AWS GovCloud. |
| **Inspeção de TLS/SSL** | Obtenha inspeção ilimitada de tráfego por TLS/SSL para identificar ameaças e perda de dados ocultos no tráfego criptografado. Especifique quais categorias da web ou aplicativos inspecionar com base em requisitos de privacidade ou regulamentares. |
| **Transmissão de registros** | Consolide logs de todas as cargas de trabalho e servidores, globalmente, em um repositório central determinado pela sua organização, com o Zscaler Nanolog Streaming Service. Os administradores podem visualizar e extrair dados de transações por cargas de trabalho na nuvem em tempo real. |
| **Infraestrutura como código** | A Zscaler fornece modelos e provedores da Terraform que automatizam o provisionamento e a implantação de políticas de segurança e máquinas virtuais de Cloud Connector. |
| **Suporte de conectividade** | Utiliza IPsec, GRE ou Cloud Connectors para direcionar o tráfego de saída das cargas de trabalho para a Zero Trust Exchange. IPsec e GRE protegerão o tráfego das cargas de trabalho para a internet. Os Cloud Connectors são usados para proteger o tráfego de internet e de cargas de trabalho. |

| ZSCALER INTERNET ACCESS PARA CARGAS DE TRABALHO À INTERNET | |
|---|---|
| **CARACTERÍSTICAS** | **DETALHES** |
| **Comunicações de cargas de trabalho para a internet ou cibernética** | Evite ameaças cibernéticas e perda de dados em comunicações de cargas de trabalho para a internet. Inclui inspeção de SSL, IPS, filtragem de URL e proteção de dados para todas as comunicações. |
| **Filtragem de URL** | Permita, bloqueie, alerte ou isole o acesso de cargas de trabalho a determinadas categorias ou destinos da web para impedir ameaças baseadas na web e garantir a conformidade com políticas organizacionais. |
| **Ameaça avançada ou cibernética** | Impeça ataques cibernéticos avançados como malware, ransomware, ataques à cadeia de suprimentos, entre outros, com nossa proteção avançada proprietária contra ameaças. Defina políticas granulares com base na tolerância ao risco de sua organização. |
| **Análise de malware** | Detecte, previna e isole ameaças desconhecidas ocultas em cargas maliciosas integradas através da IA/ML para impedir ataques de paciente zero. |
| **Prevenção contra intrusões** | Obtenha proteção completa contra botnets, ameaças avançadas e de dia zero, juntamente com informações contextuais sobre as cargas de trabalho. O IPS na nuvem e na web funciona perfeitamente em firewalls, sandboxes e DLP. |
| **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. |
| **Filtragem DNS** | Controle e bloqueie solicitações DNS de destinos conhecidos e maliciosos. |
| **Controle de arquivos** | Bloqueie ou permitia o download/upload para aplicativos com base na identidade da carga de trabalho ou aplicativo. |
| **Controle de largura de banda** | Aplique políticas de largura de banda para priorizar aplicativos essenciais da empresa em detrimento do tráfego recreativo. |
| **Política de acesso e segurança dinâmica e baseada em risco** | Adapte automaticamente a política de segurança e acesso às cargas de trabalho, servidores, destinos de internet e risco de conteúdo. |
| **Ameaça correlacionada Insights** | Diminua o tempo de investigação e resposta com alertas contextualizados e correlacionados, com informações sobre pontuação da ameaça, ativo afetado, gravidade e muito mais. |
| **Filtragem de conteúdo e regras com estado** | Filtre por política em 6 classes, 101 categorias e 29 supercategorias. Aproveite a classificação dinâmica de conteúdo para URLs desconhecidos e a pesquisa segura. Aplique políticas granulares por endereço IP, grupos e identidades hospedadas. |

| ZSCALER PRIVATE ACCESS PARA CARGAS DE TRABALHO A CARGAS DE TRABALHO | |
|---|---|
| **CARACTERÍSTICAS** | **DETALHES** |
| **Segmentação de carga de trabalho para carga de trabalho** | Conectividade e comunicação seguras entre cargas de trabalho em ambientes híbridos e multinuvem. |
| **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 potencial superfície de ataque. |
| **Alimentado por IA Segmentação de aplicativos** | 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. A segmentação baseada em ML pode ajudar você a minimizar sua superfície de ataque interna com modelos de ML treinados continuamente em milhões de sinais de clientes e seus padrões exclusivos de acesso a aplicativos. |
| **Proteção de aplicativos** | Proteja aplicativos e infraestrutura privados contra os ataques mais prevalentes com inspeção de segurança em linha e de alto desempenho de toda a carga de aplicativo que expõe ameaças. Identifique e bloqueie os riscos de segurança web conhecidos, como o OWASP Top 10, e as vulnerabilidades emergentes de dia zero que podem contornar os controles de segurança de rede tradicionais. |

| PROTEÇÃO DE DADOS | |
|---|---|
| **CARACTERÍSTICAS** | **DETALHES** |
| **Proteção de dados integrada (dados em trânsito)** | Para tráfego de carga de trabalho para internet e entre cargas de trabalho, use recursos de proxy de encaminhamento e inspeção de SSL para controlar o fluxo de informações sigilosas para destinos web de risco e aplicativos na nuvem em tempo real, interrompendo ameaças internas e externas aos dados. A proteção avançada integrada é disponibilizada independentemente do aplicativo ser permitido ou não gerenciado, sem a necessidade de logs de dispositivo de rede. |
| **Correspondência Exata de Dados (EDM)** | Identifique e proteja dados personalizados da empresa. |
| **Correspondência de documentos indexados (IDM)** | Identifique e proteja documentos e formulários personalizados. |
| **Reconhecimento óptico de caracteres (OCR)** | Encontre e evite a perda de dados em imagens e capturas de tela. |

(Os recursos listados não são coletivamente exaustivos. Recursos e características específicos podem estar disponíveis apenas com diferentes edições da Zscaler).

| EDIÇÕES DA ZSCALER ZERO TRUST CLOUD | |
|---|---|
| **NOME DA EDIÇÃO** | **RECURSOS** |
| **Zero Trust for Workloads Standard** | • Assinatura anual de 1 GB de tráfego mensal para Zero Trust for Workloads Standard:<br>• Inclui filtragem com estado e Cloud Connector |
| **Zero para cargas de trabalho Advanced** | • Tudo disponível na edição Workloads Standard<br>• Acesso à internet para cargas de trabalho: inspeção de SSL/TLS, proteção avançada contra ameaças, NSS em nuvem, ancoragem de IP de origem<br>• Acesso privado para cargas de trabalho: segmentos de aplicativo, sublocalização, registros e relatórios padrão LSS<br>• Proteção de dados para cargas de trabalho: web em linha (somente no modo monitor)<br>• Proteção cibernética para cargas de trabalho: firewall padrão, controle de DNS |
| **Zero Trust for Workloads Advanced Plus** | • Tudo disponível na edição Workloads Advanced<br>• Proteção de dados para cargas de trabalho: proteção de dados em linha e classificação avançada<br>• Proteção cibernética para cargas de trabalho: firewall avançado para cargas de trabalho, sandbox avançada para cargas de trabalho |

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