E-BOOK

Como obter segurança consistente para cargas de trabalho em multinuvem

Índice

Introdução

As empresas estão migrando aplicativos e cargas de trabalho para a nuvem pública em um ritmo sem precedentes, por todos os motivos certos.

A transformação da nuvem traz uma ampla gama de benefícios, como economia de custos, maior eficiência operacional e outros. A migração para a nuvem é uma parte fundamental da transformação digital, que permite que uma organização se torne mais ágil; atenda melhor às necessidades de clientes, vendedores, fornecedores e parceiros terceirizados; e melhore a experiência do cliente.

À medida que um número crescente de organizações em todos os setores busca estratégias na nuvem para permanecerem competitivas com seus pares, a nuvem pública se tornou o novo data center empresarial. Ao mesmo tempo, ambientes híbridos e multinuvem se tornaram a norma. A IDC Research previu recentemente que, até o final de 2025, a maioria das empresas aproveitará a nuvem pública para plataformas de IA generativas, ferramentas de desenvolvimento e infraestrutura, com o uso da nuvem superando o de sistemas locais.[1]

Os três principais fornecedores de nuvem detêm 67% da participação de mercado

31% aws

25% Microsoft Azure

11% Google Cloud

A Gartner prevê que 51% dos gastos de TI em software de aplicativos, infraestrutura e serviços de processos organizacionais serão transferidos para a nuvem pública até 2025, ultrapassando os gastos em TI tradicional.[4]

Embora a transformação da nuvem tenha um enorme impulso, com as receitas combinadas dos provedores de nuvem pública previstas para exceder US$ 800 bilhões até o final de 2024,[2] o mercado é dominado por apenas três players:[3]

- Amazon Web Services (AWS), com 31% de participação de mercado
- Microsoft Azure, com 25% de participação de mercado
- Google Cloud, com 11% de participação de mercado

Esses provedores de nuvem pública oferecem aos seus clientes novas oportunidades de aproveitar maior velocidade, agilidade e elasticidade no que diz respeito ao uso de recursos de processamento. Tudo isso possibilita que os desenvolvedores criem novos ambientes em poucos segundos. E todos oferecem centenas de serviços diferentes, tanto autogerenciados quanto gerenciados por provedores.

No entanto, esses fatores também estão contribuindo para o surgimento de novos riscos de segurança, especialmente para organizações que continuam a depender de arquiteturas de segurança legadas para proteger seus ambientes de nuvem modernos. A incompatibilidade fundamental, entre as abordagens tradicionais para proteger cargas de trabalho locais e o que é necessário nos ambientes de nuvem atuais, geralmente torna a proteção de cargas de trabalho na nuvem cara, complexa e difícil.

1. IDC Research, IDC FutureScape: previsões mundiais da nuvem para 2024, 2023.
2. IDC Research, Rastreador semestral mundial de serviços de nuvem pública.
3. Statista, Mercado de infraestrutura na nuvem, 2024.
4. Gartner, Gartner diz que mais da metade dos gastos com TI empresarial em segmentos-chave de mercado serão transferidos para a nuvem até 2025.

Desafios de segurança de cargas de trabalho na nuvem

Organizações que migram cargas de trabalho para a nuvem sem modernizar sua abordagem de segurança enfrentam uma série de desafios comuns.

A aplicação de políticas inconsistentes ou ineficazes deixa as cargas de trabalho expostas a ameaças e ataques cibernéticos.

Depender de abordagens legadas para proteger e conectar cargas de trabalho na nuvem é inevitavelmente complexo e caro. As arquiteturas de segurança cibernética baseadas em firewalls e redes privadas virtuais (VPNs) simplesmente não foram projetadas para os ecossistemas de computação na nuvem atuais.

Cargas de trabalho expostas podem ser facilmente comprometidas. Os cibercriminosos podem manter organizações reféns com ataques de ransomware devastadores. Recuperar-se deles pode ser custoso e demorado.

As cargas de trabalho na nuvem exigem ampla comunicação com outras cargas de trabalho e com a internet. As abordagens de segurança legadas não são uma boa opção para essa conectividade sempre ativa.

44%

sofreu uma violação de dados baseada na nuvem em 2024.[5]

49%

relatam que a complexidade da nuvem é um desafio significativo de conformidade e segurança.[6]

69%

experimentaram gastos excessivos em seu orçamento com a nuvem em 2023.[7]

5. Thales Group, Estudo de segurança na nuvem de 2024.
6. Ibid.
7. Gartner, Gastos com a nuvem em 2024: a TI equilibra os custos com a inovação da GenAI.

Os aplicativos atuais estão migrando. O zero trust deve ir com eles.

À medida que o trabalho remoto e híbrido se tornam comuns, organizações de todos os setores estão adotando o zero trust para proteger seus usuários. Em uma abordagem zero trust, a confiança nunca é concedida implicitamente. Em vez disso, presume-se que toda solicitação de acesso é hostil ou está comprometida, e a solicitação de acesso ao aplicativo é concedida se e somente se:

- Sua identidade e contexto (o "quem, o quê e onde" da solicitação) podem ser verificados
- Os riscos associados a essa solicitação podem ser avaliados em profundidade
- As políticas podem ser aplicadas por sessão

Com um número crescente de aplicativos e cargas de trabalho migrando para a nuvem, é essencial que as organizações estendam o mesmo grau de proteção que seus usuários desfrutam atualmente quando se trata de acesso de aplicativos a todos os seus ativos e serviços na nuvem. Isso significa estender a segurança baseada em zero trust para cada uma das suas cargas de trabalho na nuvem.

Quando as organizações migram seus aplicativos monolíticos legados para a nuvem, elas geralmente optam por refatorá-los usando uma abordagem de microsserviços. Isso possibilita aproveitar funcionalidades exclusivas da nuvem, como bancos de dados especializados, funções sem servidor e arquiteturas orientadas a eventos. Isso traz maior eficiência e pode reduzir custos, mas também cria um ambiente dinâmico e altamente automatizado. Nesse ambiente, as comunicações são constantemente trocadas entre cargas de trabalho.

As cargas de trabalho na nuvem devem frequentemente:

- Conectar-se à internet
- Comunicar-se com outras cargas de trabalho

O grande número de comunicações que devem ser enviadas entre cargas de trabalho é muito maior nesse tipo de ambiente do que no data center legado.

O que é uma carga de trabalho?

Uma carga de trabalho é o bloco de construção de um aplicativo na nuvem moderno. Em ambientes locais legados, a maioria das cargas de trabalho eram componentes dentro de grandes aplicativos monolíticos. Esse não é o caso nos ambientes nativos da nuvem atuais, onde os aplicativos normalmente consistem em muitos componentes modulares ou microsserviços. Cada serviço executa uma tarefa específica e se comunica com outros serviços para executar a lógica da organização.

Exemplos de cargas de trabalho incluem:

- Contêineres
- Máquinas virtuais (VMs)
- Fazendas de infraestrutura de desktop virtual (VDI)
- Funções sem servidor

A segurança de rede legada não funciona para a empresa nativa da nuvem

Muitas organizações embarcaram em sua jornada de transformação para a nuvem sem mudar sua estratégia de segurança para acompanhar o ritmo. Mas as arquiteturas de segurança de rede legadas foram criadas para o data center local, não para a nuvem. Quando as organizações tentam migrar para a nuvem, a arquitetura resultante é altamente complexa e ineficaz.

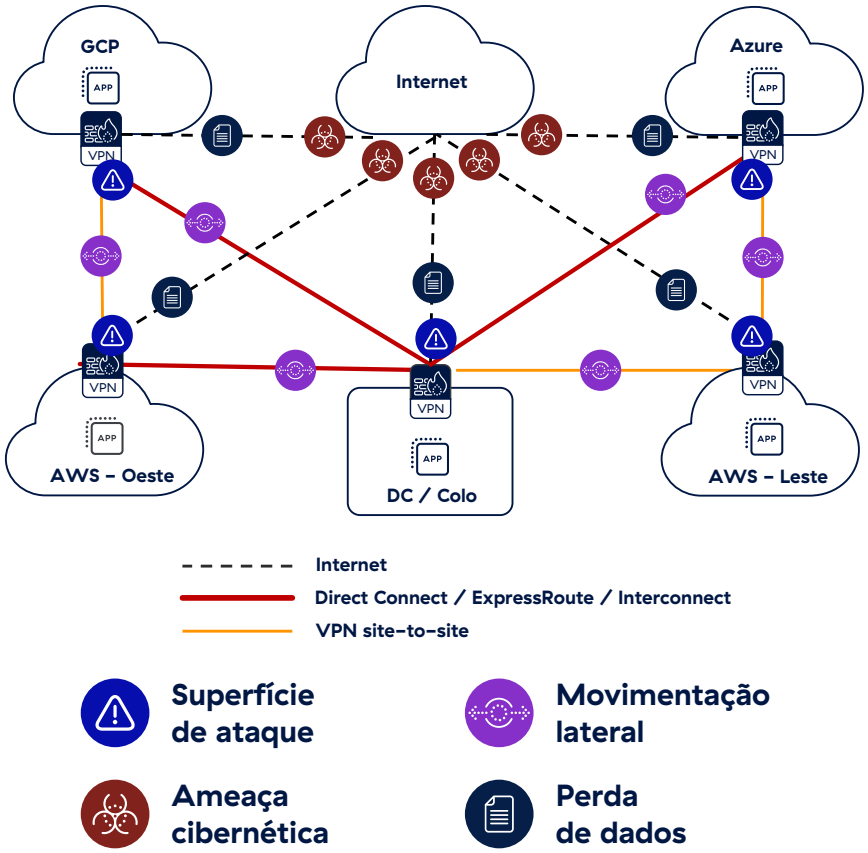
As cargas de trabalho na nuvem devem se comunicar com segurança entre si e com a internet. A abordagem legada para atingir isso envolve a construção de redes roteáveis entre infraestruturas de nuvem usando firewalls e VPNs, essencialmente estendendo a rede de longa distância da organização (WAN) para a nuvem.

Nesse modelo, as organizações devem instalar firewalls virtuais de nova geração (vNGFWs) em todos os lugares onde suas cargas de trabalho residem. Em um mundo onde ambientes híbridos e multinuvem são onipresentes, isso cria redes full mesh, nas quais cada nó se conecta diretamente a todos os outros. Essa arquitetura é extremamente complexa e desafiadora de gerenciar.

Se as organizações quiserem implementar recursos de segurança adicionais, como prevenção contra perda de dados (DLP) ou inspeção de TLS/SSL, elas precisarão utilizar dispositivos de segurança virtuais adicionais, criando ainda mais complexidade.

Mesmo dentro do ambiente de um único provedor de serviços na nuvem, as organizações precisarão configurar e gerenciar vários vNGFWs adicionais para proteger o tráfego norte–sul e leste–oeste entre cargas de trabalho na nuvem.

As comunicações de cargas de trabalho multiplicam a complexidade e os desafios de segurança



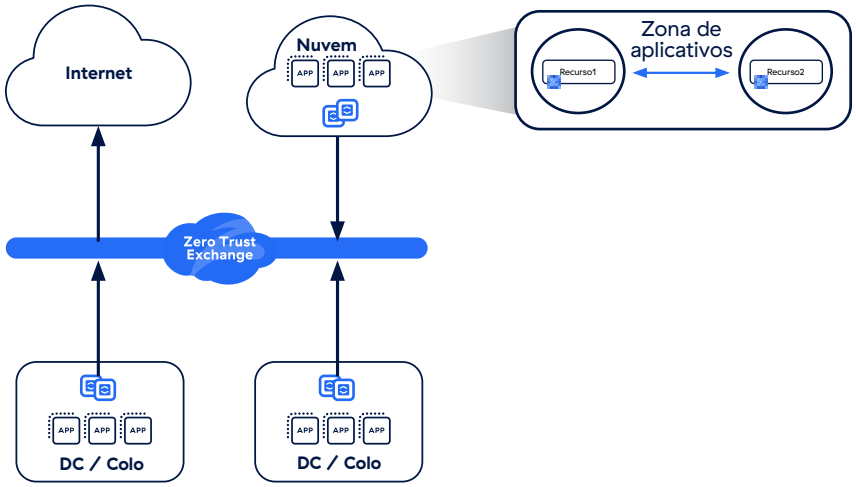
Defesa cibernética inadequada para os ecossistemas de processamento atuais

Contar com abordagens legadas para proteger e conectar cargas de trabalho na nuvem leva a:

- **Uma superfície de ataque expandida.** Cada vNGFW tem um local de rede identificável e, portanto, pode ser descoberto por invasores. Quanto mais firewalls forem implantados, maior será a superfície de ataque.
- **Comprometimento das cargas de trabalho.** Uma vez que os criminosos descobrem um ponto de entrada no ambiente e ganham uma posição ali, eles conseguem comprometer as cargas de trabalho.
- **Movimentação lateral de ameaças.** Como todas as cargas de trabalho são conectadas por meio de uma rede mesh, uma vez que uma única carga de trabalho é comprometida, os criminosos podem se mover lateralmente pela rede para comprometer outras.
- **Nenhuma proteção para dados sigilosos.** Conforme eles se movem pela rede, os invasores poderão encontrar e exfiltrar dados sigilosos, como informações financeiras de clientes e segredos comerciais.

O que é necessário: uma nova abordagem para proteger cargas de trabalho na nuvem

Proteger os ecossistemas de computação empresarial atuais, com sua profunda dependência de infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS) de vários provedores e fornecedores de serviços na nuvem, requer uma abordagem diferente, que coloque as políticas de segurança da organização no centro do design da rede. Isso significa oferecer acesso seguro e de privilégio mínimo com base na conectividade direta entre cargas de trabalho e de cargas de trabalho para a internet. Essa abordagem também simplifica a criação e a manutenção de uma arquitetura zero trust em todas as suas cargas de trabalho na nuvem.



Com essa nova e moderna abordagem:

- **A superfície de ataque é eliminada.** Diferentemente de soluções legadas, as cargas de trabalho são efetivamente invisíveis para os criminosos, essencialmente eliminando toda a superfície de ataque.
- **As cargas de trabalho estão protegidas.** A inspeção completa de conteúdo em linha, juntamente com recursos de DLP, fornece segurança robusta para dados e cargas de trabalho.
- **A movimentação lateral de ameaças é evitada.** Fornecer conectividade direta sem conexão a uma rede torna a movimentação lateral impossível.
- **Os dados são protegidos.** Adicionar a inspeção de TLS/SSL em escala para recursos de DLP possibilita fornecer proteção de dados abrangente em escala.
- **A complexidade e o custo são reduzidos.** Centralizar o gerenciamento da configuração de nuvem com a segurança, e habilitar a conectividade direta, torna possível reduzir a complexidade e os custos.

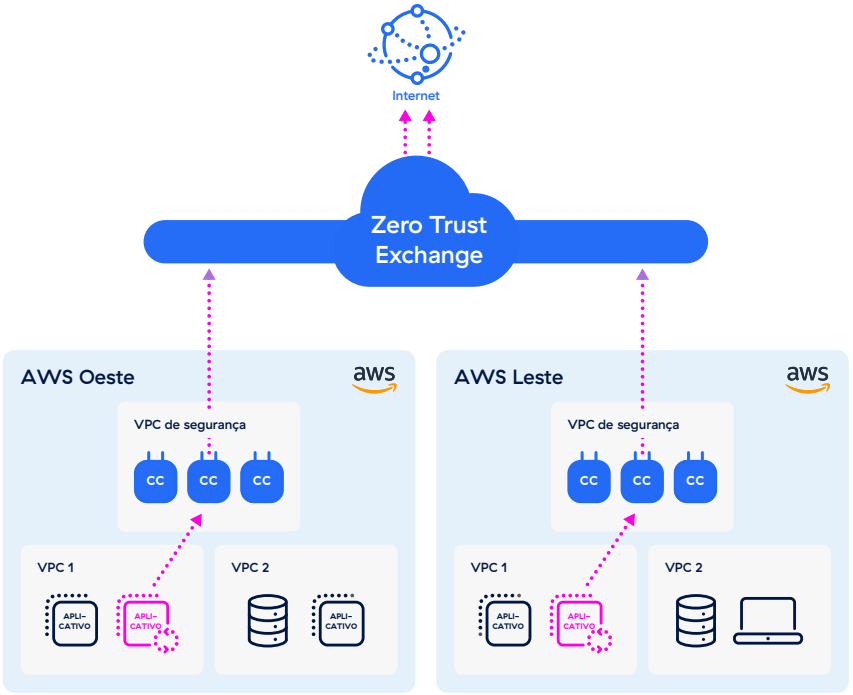
Simplifique e proteja as comunicações de cargas de trabalho para a internet

Como cada carga de trabalho na nuvem depende de comunicação quase constante pela internet pública, uma solução zero trust para cargas de trabalho na nuvem deve ser capaz de proteger toda a conectividade de saída. Dentro de uma arquitetura simples direta para a nuvem, a solução deve fornecer acesso seguro à internet para todas as cargas de trabalho, independentemente de estarem localizadas em uma nuvem pública ou no data center corporativo.

Os principais recursos necessários para proteger as comunicações de cargas de trabalho para a internet incluem:

- Inspeção completa de TLS/SSL baseada em proxy
- Superfície de ataque zero
- Permitir acesso apenas a locais aprovados
- Proteção avançada contra malware para bloquear ameaças de dia zero

Por exemplo, vamos imaginar que sua organização tenha aplicativos localizados na AWS West e na AWS East, e ambos precisam de uma atualização. A solicitação precisará ser encaminhada para uma plataforma central onde as políticas são aplicadas e gerenciadas. Uma solução ideal será capaz de aplicar políticas de zero trust e conectar origens e destinos com segurança.



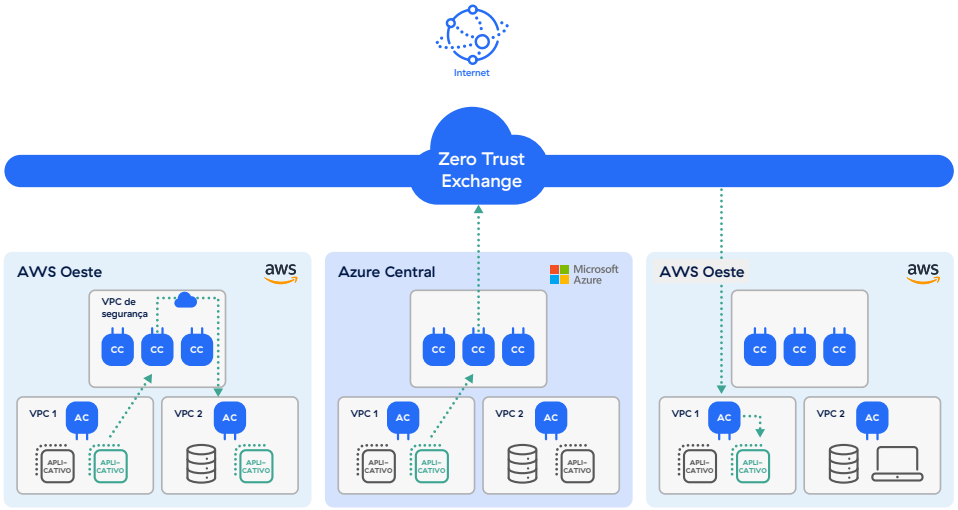
Simplifique e proteja as comunicações entre cargas de trabalho

Aplicar zero trust para cargas de trabalho na nuvem também requer conectividade segura entre cargas de trabalho. É essencial que as cargas de trabalho possam se comunicar, tanto entre várias nuvens quanto dentro de uma única nuvem privada virtual (VPC). Essas comunicações devem fluir pela plataforma de zero trust central, onde as políticas de segurança são aplicadas e onde a identidade e o contexto são usados para verificar a confiança antes de permitir a conexão.

Em particular, deve haver um mecanismo para facilitar as comunicações entre as cargas de trabalho. Para conectividade de VPC para VPC, o tráfego pode ser roteado de uma VPC para uma borda de serviço privada, de onde uma conexão seria então intermediada para o aplicativo de destino (localizado em uma VPC diferente). Para conectividade de nuvem para nuvem, o tráfego poderia ser encaminhado para uma plataforma de zero trust central, onde uma conexão seria intermediada para um aplicativo de destino localizado em uma nuvem diferente.

Os principais recursos necessários para proteger as comunicações entre cargas de trabalho incluem:

- Proteção da conectividade multinuvem e multirregional
- Proteção da conectividade entre VPC/VNET
- Eliminação da superfície de ataque de rede com acesso à rede zero trust (ZTNA)
- Bloqueio da movimentação lateral de ameaças



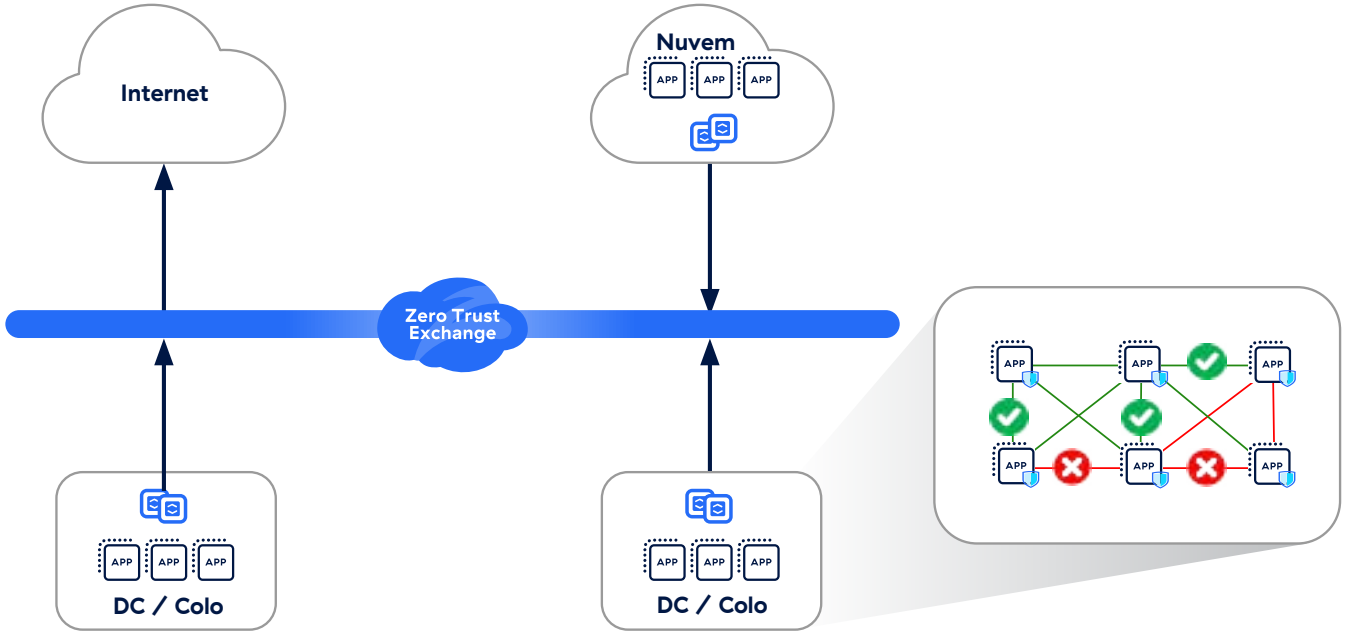
Obtenha facilmente microssegmentação granular

Um componente essencial da segurança zero trust, a microssegmentação impede a movimentação lateral de ameaças ao dividir grupos de aplicativos ou cargas de trabalho em pequenos segmentos com base nos requisitos de comunicação de aplicativos individuais. As cargas de trabalho têm permissão para se comunicar dentro de seus próprios segmentos, mas não podem trocar comunicações não autorizadas com cargas de trabalho fora deles.

A microssegmentação possibilita aplicar políticas zero trust em um nível granular em toda a rede interna da organização, não apenas em seu perímetro, estendendo proteções consistentes para cargas de trabalho locais e também para aquelas executadas na nuvem.

Os principais recursos necessários para a microssegmentação de cargas de trabalho incluem:

- Descoberta de recursos em tempo real com tecnologia de IA
- Segmentação baseada em host e não baseada em host
- Capacidade de segmentar cargas de trabalho dentro e entre VPCs/VNETs



Uma solução de zero trust para cargas de trabalho na nuvem deve ter várias características principais:

N.º 1: a capacidade de realizar inspeção de TLS/SSL em escala

Muitas das ameaças mais perigosas da atualidade estão escondidas à vista de todos no tráfego criptografado. Para detectá-las, você precisa de uma plataforma abrangente que possa executar inspeção completa de TLS/SSL em escala, sem as limitações de desempenho impostas por aplicativos legados.

Procure uma solução que possa oferecer:

- **Capacidade ilimitada** para inspecionar todo o tráfego em TLS/SSL dos seus usuários sem preocupações de desempenho
- **Capacidade de dimensionamento elástica** com base nas demandas de tráfego
- **Gerenciamento de certificados simplificado**
- **Controle de políticas granulares** que simplifica a conformidade ao excluir o tráfego criptografado de usuários para categorias de sites como saúde ou bancos

N.º 2: recursos robustos de proteção de dados

Uma abordagem de defesa em profundidade para proteção de dados inclui a capacidade de aplicar políticas de prevenção contra perda de dados (DLP) em escala sem afetar o desempenho. Isso fornece uma camada extra de proteção. Caso uma carga de trabalho na nuvem seja comprometida, ainda haverá um mecanismo para aplicar políticas e impedir a exfiltração de dados.

Procure uma solução que possa oferecer:

- **Um painel simplificado** onde as políticas de DLP possam ser configuradas e gerenciadas
- **Técnicas avançadas de gerenciamento de dados,** como correspondência exata de dados (EDM) e reconhecimento óptico de caracteres (OCR)
- **Inspeção confiável de conteúdo em linha em larga escala**

N.º 3: recursos avançados de proteção contra ameaças

Para bloquear as ameaças mais perigosas e sofisticadas da atualidade, uma plataforma zero trust de segurança de cargas de trabalho na nuvem deve ser capaz de garantir que cada pacote, de cada carga de trabalho, possa ser totalmente inspecionado do início ao fim. Isso requer recursos integrados e sempre ativos de inspeção de TLS/SSL, assim como a capacidade de aplicar políticas granulares para todo o tráfego.

Além disso, os principais recursos a serem procurados incluem:

- **Tecnologias de deception integradas** usando chamarizes, iscas e honeypots para proteger seus ativos mais valiosos com alta fidelidade e baixas taxas de falsos positivos
- **Sandbox na nuvem** para colocar em quarentena e inspecionar ameaças potenciais em vez de permitir que elas passem
- **Proteção contra malware** que pode bloquear ransomware, spyware e malware conhecidos, bem como novas ameaças

N.º 4: segmentação abrangente baseada em host

A microssegmentação impede a movimentação lateral de ameaças para minimizar o raio de ação e os danos que um incidente cibernético pode causar. A microssegmentação baseada em host depende de agentes instalados em dispositivos de terminais para fornecer controle e visibilidade muito mais granulares, facilitando o gerenciamento da segmentação baseada em identidade. O uso de um agente permite a segmentação com base em políticas dinâmicas e compreensíveis para humanos, em vez de regras estáticas em nível de rede.

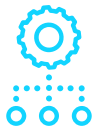
Em particular, procure uma solução que possa fornecer:

- **Descoberta de recursos em tempo real** aproveitando a IA para fornecer visibilidade granular em todos os dispositivos, serviços e ativos dentro do seu ecossistema empresarial
- **Recomendações de políticas zero trust** com base na análise de tráfego
- **Integração com uma plataforma zero trust,** para que você possa proteger e segmentar seu ambiente em apenas um lugar, sem a necessidade de implantar vários produtos específicos

Os principais casos de uso para proteger a conectividade de cargas de trabalho

Uma solução baseada em zero trust para conectividade de cargas de trabalho pode ajudar as organizações a resolver vários desafios importantes. Aqui estão quatro dos mais comuns:

Proteção do tráfego para a internet
Quando os aplicativos se comunicam com a internet ou aplicativos SaaS, o tráfego de saída precisa ser inspecionado em busca de ataques cibernéticos e vazamentos de dados. A Zscaler opera a maior plataforma de segurança na nuvem em linha do mundo, que fornece proteção avançada contra ameaças em escala de nuvem sem qualquer impacto de desempenho ou degradação de serviço.



Segmentação de cargas de trabalho
Com a solução de comunicações de cargas de trabalho certa, é possível adotar uma abordagem granular e metódica para a segmentação de cargas de trabalho. Isso simplifica a aplicação de políticas para controlar a conectividade para cargas de trabalho em VPCs, regiões e nuvens públicas e privadas.

Migração para a nuvem
Esse é frequentemente um processo demorado e árduo para as organizações. Elas devem considerar muitos fatores, incluindo qual estratégia de migração seguir. Faz sentido simplificar a vida e mudar, ou os aplicativos devem ser refatorados ou reconstruídos? A solução certa de comunicações de cargas de trabalho pode tornar mais simples e fácil conectar aplicativos de nuvem recém-migrados com segurança.

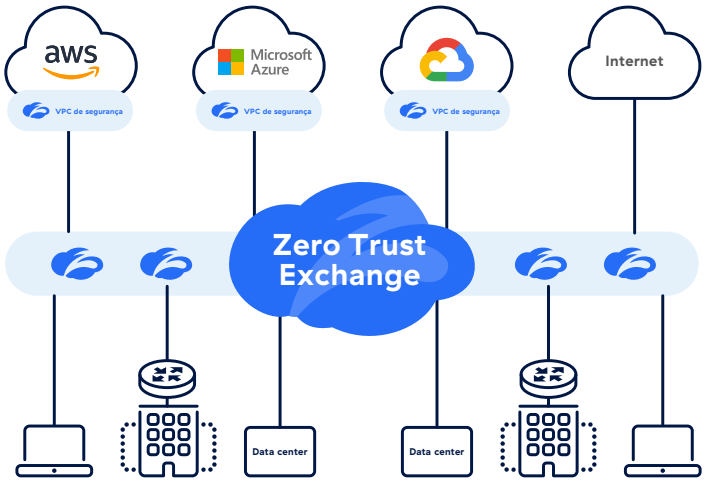
Fusões e aquisições (M&A)
Com uma solução de comunicação de cargas de trabalho moderna, baseada zero trust e nativa na nuvem, é possível fornecer acesso seguro a aplicativos entre redes, sem a necessidade de redesenhar e rearquitetar redes para conectá-los.

Zscaler Workload Communications é a resposta

Procurando uma solução completa que possa fazer tudo isso e muito mais? A Zscaler Zero Trust Exchange™ possibilitou reinventar completamente as comunicações de cargas de trabalho dentro de uma arquitetura simples, comprovada e direta para a nuvem.

Combinando o Zscaler Internet Access™ (ZIA) para comunicações entre cargas de trabalho e internet, o Zscaler Private Access™ (ZPA) para comunicações entre cargas de trabalho e recursos de microssegmentação zero trust de segmento individual, a Zscaler Workload Communications é uma abordagem abrangente para proteger a conectividade de cargas de trabalho na nuvem e no local. Ao mesmo tempo, ela é capaz de manter o desempenho para garantir que seus usuários tenham ótimas experiências e a capacidade de dimensionamento para acompanhar a evolução da sua presença na nuvem à medida que suas operações crescem.

A Zscaler Workload Communications fornece segurança na nuvem baseada em zero trust altamente eficaz que pode ser dimensionada de acordo com suas necessidades. Os recursos de dimensionamento automático elástico permitem que ela lide com aumentos de tráfego com facilidade. A Zero Trust Exchange já opera em hiperescala, com mais de 150 data centers ao redor do mundo. A Zscaler gerencia todas as atualizações automaticamente em seu nome, e a infraestrutura é nativamente integrada à infraestrutura de segurança dos provedores de nuvem pública, aproveitando funcionalidades como gateways de trânsito e balanceadores de carga.



Além disso, a Zscaler Workload Communications simplifica e centraliza o gerenciamento de políticas. Todas as políticas podem ser criadas e atualizadas em um único console central e fácil de usar. Elas são aplicadas dentro da Zero Trust Exchange, onde as políticas do ZIA ou ZPA podem ser aproveitadas para fornecer inspeção completa de conteúdo e controle baseado em identidade das comunicações de cargas de trabalho. De lá, as comunicações podem ser encaminhadas para qualquer destino, seja a internet ou outros aplicativos privados em ambientes de nuvem. As políticas podem ser prontamente aplicadas em escala sempre que você precisar implantar cargas de trabalho adicionais na nuvem.

Se você tiver interesse em saber mais sobre os benefícios de usar a Zscaler Workload Communications, entre em contato conosco hoje mesmo. Você também pode saber mais visitando a página web da Zscaler Zero Trust Cloud Connectivity.

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 SASE 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