

E-book

Quatro requisitos para uma filial zero trust

© 2024 Zscaler, Inc. Todos os direitos reservados.

Ao implementar uma abordagem zero trust nas filiais, as empresas podem não apenas fortalecer suas redes contra ameaças, mas também simplificar a conectividade para usuários, dispositivos e aplicativos em diversos locais.

No atual cenário empresarial dinâmico, muitas empresas enfrentam desafios para garantir a segurança de seus usuários, dispositivos e aplicativos. No passado, quando os aplicativos eram hospedados em data centers e os usuários se conectavam principalmente de escritórios, os requisitos de conectividade eram relativamente simples. As arquiteturas tradicionais baseadas em redes em estrela e firewalls foram eficazes para atender a essas necessidades. No entanto, à medida que o ambiente de trabalho moderno evoluiu, estas abordagens tradicionais agora têm dificuldade para fornecer proteção adequada contra ameaças e uma experiência de usuário ideal.

Hoje, os usuários não se conectam mais exclusivamente dos escritórios, mas de uma infinidade de locais, incluindo suas casas, cafeterias, aeroportos e mais. Além disso, a proliferação da Internet das Coisas (IoT) complica ainda mais o panorama da segurança empresarial, uma vez que dispositivos de IoT/TO dispositivos representam um risco adicional à segurança.

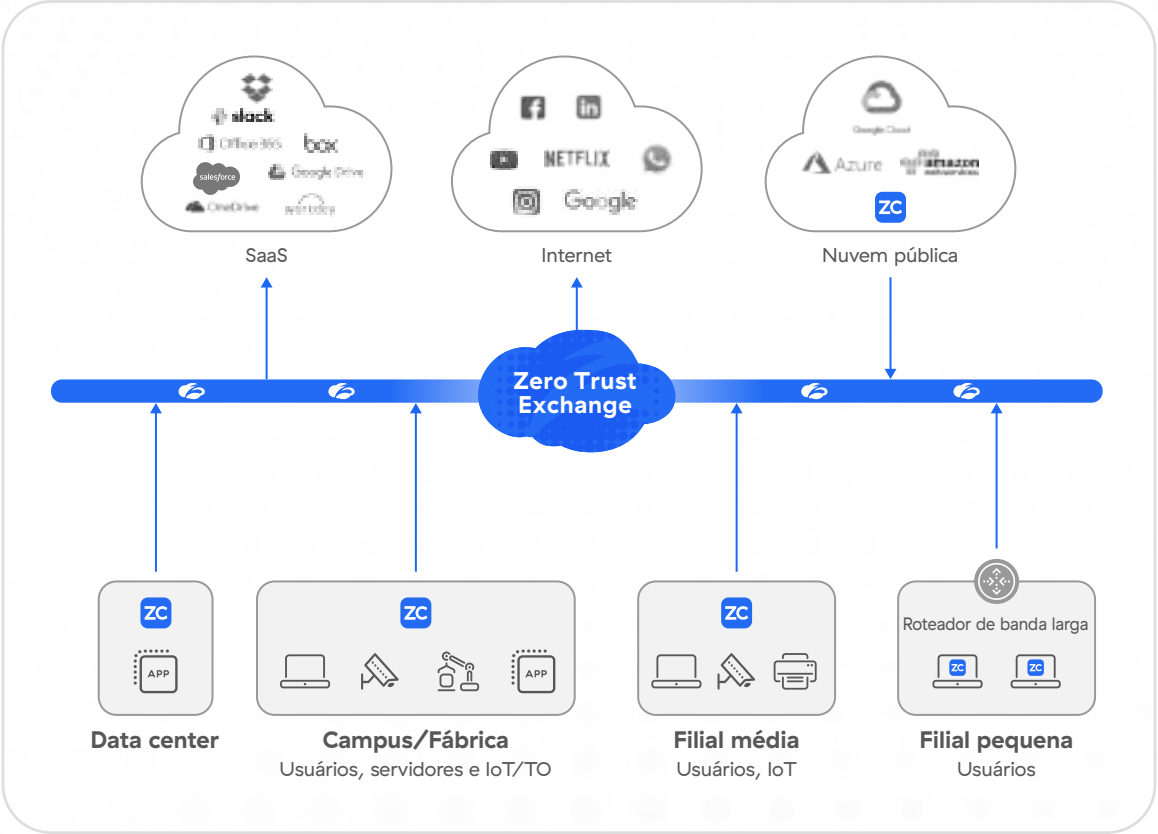

Figura 1: a filial zero trust oferece uma abordagem zero trust para a conectividade de rede

© 2024 Zscaler, Inc. Todos os direitos reservados.

O cenário dinâmico está conduzindo as organizações em direção a uma abordagem zero trust em relação à segurança. Os princípios do zero trust (nunca confiar, sempre verificar e impor acesso de privilégio mínimo) permitiram que muitas empresas frustrassem ataques cibernéticos sofisticados. Com o zero trust, os usuários têm acesso apenas aos aplicativos de que precisam, ao contrário das VPNs que colocam os usuários na rede e fornecem acesso irrestrito. Ao aplicar princípios de zero trust à conectividade de rede, as organizações podem proteger-se melhor contra ameaças, especialmente aquelas originadas nos locais. A implementação da abordagem zero trust na filial garante conectividade segura e operações simplificadas, superando complexidades de roteamento ou uma experiência de usuário degradada, ao mesmo tempo que elimina a superfície de ataque e evita a movimentação lateral de ameaças.

Uma arquitetura de filial zero trust garante maior segurança para todos os locais, incluindo filiais, fábricas, quiosques e data centers. Aqui estão quatro requisitos principais para garantir uma filial zero trust:

Garanta princípios de zero trust para sua rede 1

Proteja dispositivos de IoT/TO em suas filiais 2

Garanta rotas diretas para a nuvem para o tráfego de SaaS/ internet 3

Garanta uma experiência de usuário consistente para funcionários presenciais e remotos 4

© 2024 Zscaler, Inc. Todos os direitos reservados.

A SD-WAN tradicional não zero trust

Os dispositivos de SD-WAN tradicionais simplesmente estendem a rede corporativa até filiais remotas, expandindo a superfície de ataque corporativa. Eles oferecem proteção insuficiente contra a movimentação lateral de ameaças, permitindo que dispositivos comprometidos em locais remotos se comuniquem facilmente com aplicativos essenciais aos negócios no data center ou na nuvem pública. As empresas enfrentam maior risco de ameaças laterais e ataques baseados na internet devido ao uso de dispositivos de SD-WAN legados. Uma colcha de retalhos de dispositivos de segurança, ferramentas e políticas não padronizadas leva a um aumento do risco de segurança devido a falhas conhecidas e desconhecidas na cobertura de segurança. Portanto, ao projetar a conectividade segura das filiais, torna-se imperativo focar na implementação do zero trust para reduzir a superfície de ataque e evitar a movimentação lateral de ameaças.

Um relatório de 2023 sobre os riscos da VPN da Cybersecurity Insiders que entrevistou 382 profissionais de TI e especialistas em segurança cibernética descobriu que as VPNs representam riscos de segurança, com 88% das organizações expressando uma preocupação leve a extrema de que as VPNs possam colocar em risco a segurança de sua organização.

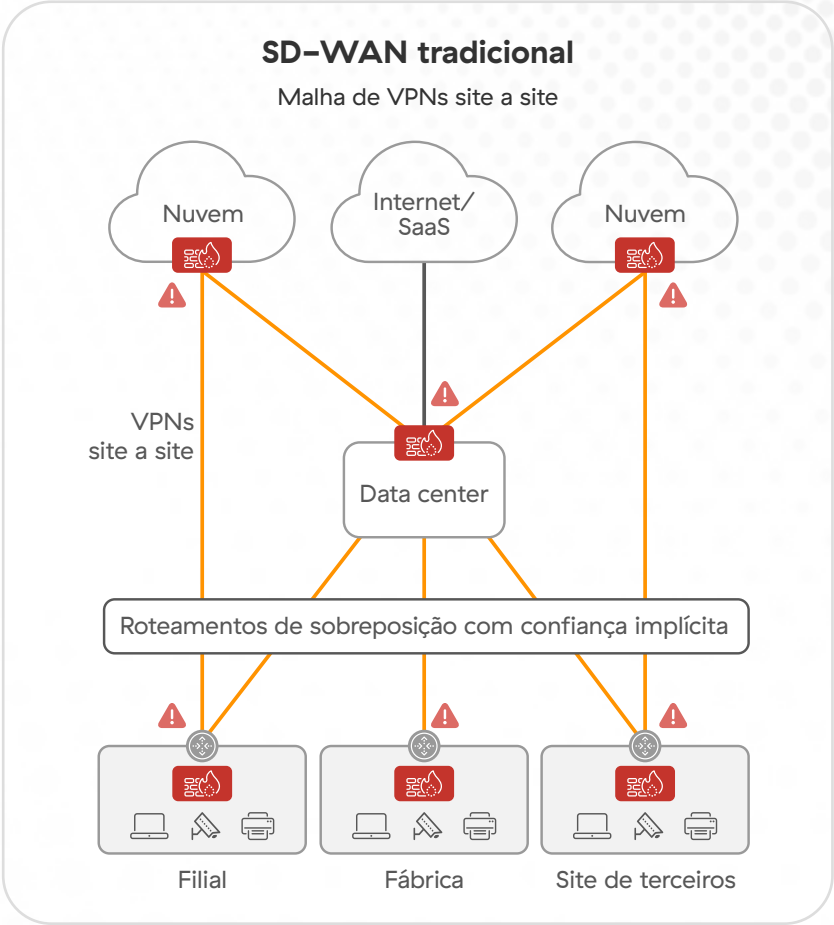

Figura 2: as SD-WANs tradicionais expandem a superfície de ataque e não protegem contra a movimentação lateral de ameaças.

© 2024 Zscaler, Inc. Todos os direitos reservados.



Além disso, 45% das organizações confirmaram que sofreram pelo menos um ataque que explorou vulnerabilidades da VPN nos últimos 12 meses: uma em cada três tornou-se vítima de ataques de ransomware relacionados à VPN. A ameaça crescente dos ataques cibernéticos que exploram vulnerabilidades relacionadas à VPN destaca a necessidade urgente de abordar a segurança das arquiteturas atuais.

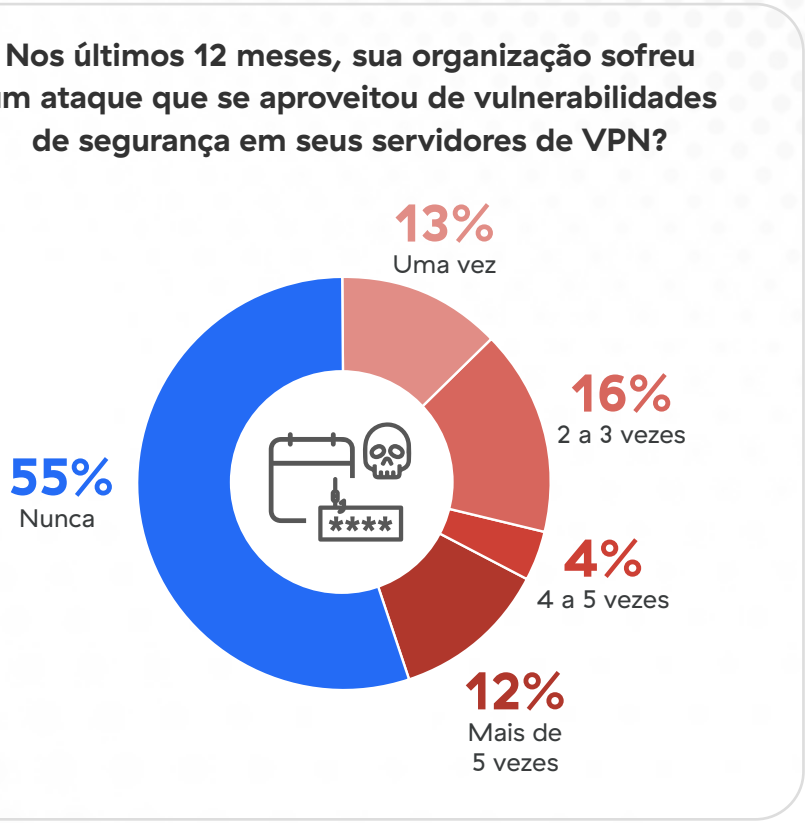

Figura 3: as organizações estão enfrentando um aumento nos ataques cibernéticos devido a vulnerabilidades em servidores de VPN.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Não é possível implementar zero trust com firewalls e VPNs

Tradicionalmente, as empresas implementavam VPNs site a site para garantir a conectividade a aplicativos críticos hospedados no data center. No entanto, à medida que esses aplicativos migram para a nuvem, a arquitetura de VPN site a site convencional torna-se menos viável, uma vez que o tráfego ainda é transferido para o data center, resultando em uma experiência de usuário degradada e em problemas de desempenho. Isso também introduz complexidade operacional, pois os túneis da VPN exigem gerenciamento e configuração do site individualmente. Consequentemente, as equipes de TI corporativas desejam fazer a transição de uma rede em estrela para uma arquitetura direta para a nuvem que envia o tráfego dos aplicativos para um provedor de segurança na nuvem, melhorando o desempenho dos aplicativos.

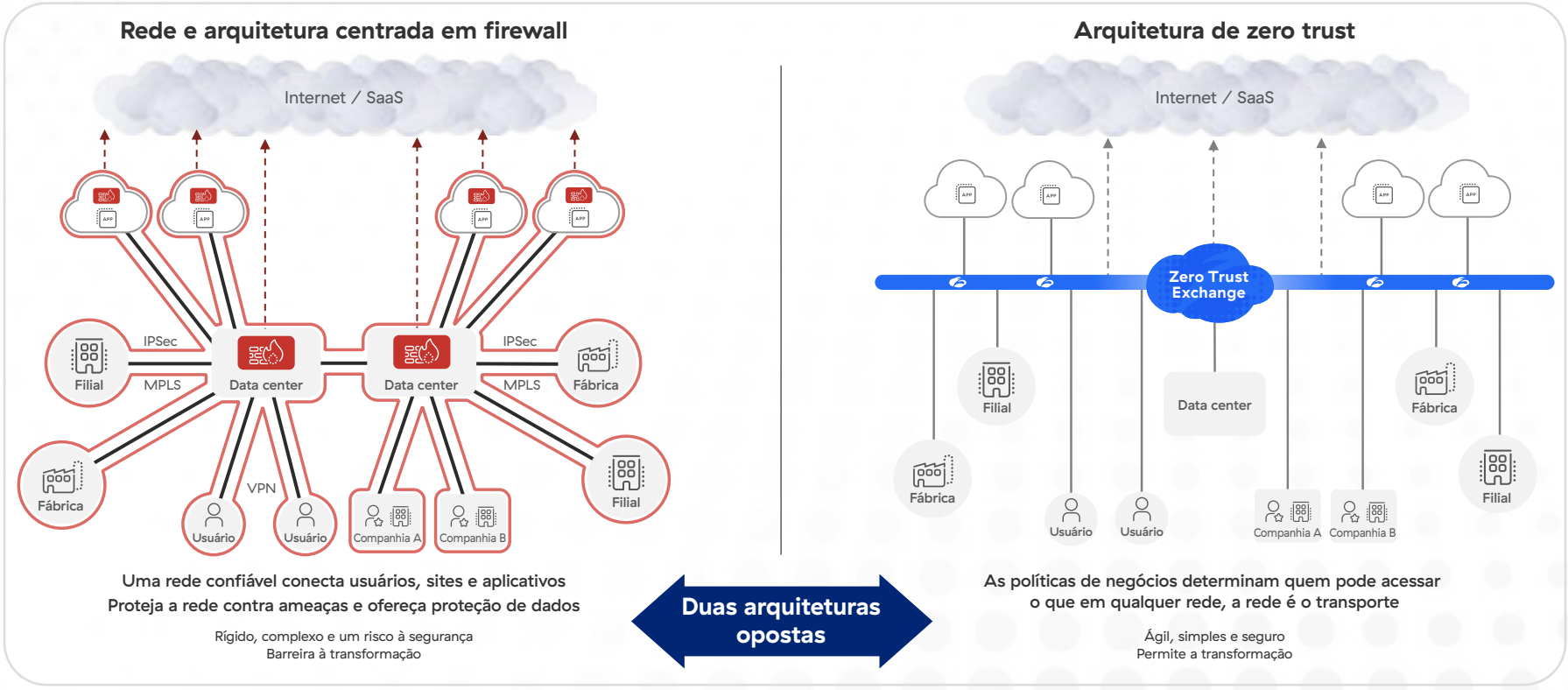

Figura 4: as organizações estão enfrentando um aumento nos ataques cibernéticos devido a vulnerabilidades em servidores de VPN.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Quatro requisitos essenciais para garantir uma filial zero trust

1 Garanta princípios de zero trust para sua rede

As VPNs site a site estendem sua rede corporativa para filiais, data centers, regiões de nuvem e terceiros. As redes tradicionais expandem sua superfície de ataque para entidades além do seu controle direto e permitem fluxos de tráfego implicitamente, permitindo a movimentação lateral de ameaças. Ao contrário da segmentação de rede tradicional, que divide a rede em zonas e é complexa de gerenciar, a segmentação de usuário para aplicativo e de dispositivo para aplicativo fornece acesso granular e contextual somente quando autorizado. Uma rede baseada em princípios de zero trust elimina os riscos inerentes às redes planas tradicionais e ajuda a evitar a complexidade de camadas em firewalls para controles de segurança, experiência e problemas de desempenho. Isso também introduz complexidade operacional, pois os túneis de VPN exigem gerenciamento e configuração do site individualmente. Consequentemente, as equipes de TI corporativas desejam fazer a transição de uma rede em estrela para uma arquitetura direta para a nuvem que envia o tráfego de aplicativos para um provedor de segurança na nuvem, melhorando o desempenho dos aplicativos.

2 Proteja dispositivos de IoT/TO em suas filiais ou locais de filiais

Os dispositivos de IoT/TO estão se proliferando em quase todas as organizações com o surgimento de dispositivos “inteligentes”, como impressoras, TVs, câmeras, leitores de cartões e sensores. Esses dispositivos executam uma infinidade de sistemas operacionais com diversos riscos de segurança, e o gerenciamento de correções continua sendo um desafio. Muitos líderes de TI não têm visibilidade sobre esse dispositivos, muito menos um inventário detalhado; no entanto, esses dispositivos geralmente têm acesso irrestrito aos aplicativos essenciais em seus data centers e serviços na nuvem. Com os ataques baseados em malware de IoT aumentando em 400%[1], isso representa um vetor de ameaça significativo para sua organização. As organizações devem proteger os dispositivos de IoT/TO em filiais ou fábricas para proteger suas operações comerciais.

Os ataques de malware baseados em IoT e TO aumentaram 400% desde 2022, representando um vetor de ameaça significativo.

© 2024 Zscaler, Inc. Todos os direitos reservados.

3 Garanta rotas diretas para a nuvem para tráfego de SaaS e Internet

A arquitetura direta para a nuvem conecta rapidamente qualquer usuário ou dispositivo de IoT/TO a qualquer aplicativo, onde quer que o usuário ou dispositivo de IoT/TO esteja no mundo. A implementação de rotas diretas para a nuvem para tráfego de SaaS e internet é crucial para otimizar o desempenho da rede e garantir conectividade contínua. As arquiteturas de rede em estrela, que fazem retorno do tráfego para um data center por meio de links MPLS caros, degradam o desempenho dos aplicativos e prejudicam a produtividade dos negócios. Quando os aplicativos eram hospedados no data center, fazia sentido fazer o retorno do tráfego dos aplicativos para um hub regional. No entanto, com a migração dos aplicativos para a nuvem, enviar o tráfego de usuários ou dispositivos de IoT/TO diretamente para o seu destino faz mais sentido. Uma arquitetura direta para a nuvem permite que tráfego de aplicativos SaaS e da internet sigam as rotas mais eficientes e diretas até seus destinos. Isso traz muitos benefícios, incluindo economia de custos, experiência aprimorada do usuário e simplificação da rede.

Atualmente, os líderes empresariais desejam uma experiência semelhante à de um café para seus usuários e equipes de TI, que torne a conexão com aplicativos corporativos o mais simples possível e, ao mesmo tempo, proporcione desempenho superior dos aplicativos.

4 Garanta experiências de usuário consistentes para funcionários presenciais e remotos

Muitos funcionários trabalham remotamente ou dividem seu tempo entre trabalhar em casa e no escritório. Essa mudança na dinâmica de trabalho trouxe à luz um desafio significativo. Ou seja, os usuários frequentemente expressam insatisfação com a qualidade da conectividade no escritório em comparação com o seu ambiente de trabalho doméstico. Essa situação introduz um novo conjunto de preocupações que as equipes de TI devem abordar. As tecnologias de VPN que fazem retorno do tráfego para um data center resultam em uma experiência de usuário ruim e inconsistente, o que impacta negativamente os negócios e diminui a produtividade.

Atualmente, os líderes empresariais desejam uma experiência semelhante à de um café para seus usuários e equipes de TI, que torne a conexão com aplicativos corporativos o mais simples possível e, ao mesmo tempo, proporcione desempenho superior dos aplicativos. Eles desejam uma experiência onde os usuários corporativos possam acessar os aplicativos de que precisam com consistência uniforme de experiência entre a casa e o escritório e com a mesma facilidade de uso, o que é impossível ao se conectar a redes por meio de VPNs. Para permanecerem relevantes no mundo competitivo atual, as organizações devem garantir experiências de usuário consistentes para funcionários presenciais e remotos, a fim de aumentar a produtividade dos funcionários e estimular a criatividade.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Aplicação de princípios de zero trust à SASE

A Secure Access Service Edge (SASE) integra serviços de rede e segurança em uma solução unificada disponibilizada na nuvem, simplificando as operações, reduzindo a complexidade e permitindo que as organizações apliquem políticas consistentes em suas redes. A SASE combina rede zero trust com serviços essenciais de segurança fornecidos pela nuvem, como SWG, CASB, FWaaS e ZTNA. É crucial reconhecer que as soluções de SASE baseadas na SD-WAN tradicional oferecem proteção inadequada, aumentando a superfície de ataque corporativa e expondo aplicativos críticos a diversas ameaças da internet.

Além disso, a capacidade de segmentação da SD-WAN tradicional é fragmentada e pouco refinada, o que permite que as ameaças se espalhem facilmente para outros sistemas, com risco de derrubar sites ou redes inteiras.

O Enterprise Strategy Group (ESG) da TechTarget entrevistou 390 profis-sionais de TI e segurança cibernética em diversas organizações na América do Norte (EUA e Canadá) para compreender o estado da SASE. De acordo com esse estudo, os três principais casos de uso que levam as organizações à SASE são:

1. Alinhar políticas de rede e segurança
2. Reduzir ou eliminar a superfície de ataque da internet
3. Melhorar a segurança do usuário remoto

Todos os três casos de uso da SASE destacam a importância de fornecer conectividade segura para usuários, dispositivos e aplicativos para estabelecer uma estrutura SASE resiliente. As organizações que embarcam na implementação da SASE devem priorizar soluções que cumpram os princípios de zero trust. As SD-WANs tradicionasi conectam vários sites por meio de VPNs site a site ou roteamentos de sobreposição, estabelecendo uma confiança implícita que concede acesso irrestrito a recursos comerciais essenciais, mesmo para entidades comprometidas. Por outro lado, as SD-WANs baseadas em princípios de zero trust reduzem efetivamente a superfície de ataque e protegem contra a movimentação lateral de ameaças, ao mesmo tempo que facilitam a comunicação segura de usuário para aplicativo e de dispositivo para aplicativo.



Figura 5: ss organizações estão enfrentando um aumento nos ataques cibernéticos devido a vulnerabilidades em servidores de VPN.

© 2024 Zscaler, Inc. Todos os direitos reservados.

Conclusão

As tradicionais arquiteturas de rede das filiais dependem de confiança implícita, expandindo a superfície de ataque até a filial mais distante e permitindo que ameaças cibernéticas se movam lateralmente por toda a organização. Ao adotar uma abordagem zero trust nas filiais, as empresas podem fortalecer suas redes contra ameaças e simplificar a conectividade para os usuários, dispositivos de IoT/TO e aplicativos em diversos locais. Projetar uma rede de filiais com princípios de zero trust melhora a postura de segurança corporativa, eliminando a superfície de ataque e evitando a movimentação lateral de ameaças, ao mesmo tempo que supera as complexidades de roteamento. É importante que as organizações considerem cuidadosamente os quatro requisitos descritos aqui ao implementarem os princípios de zero trust em filiais para navegar com eficácia pelas demandas complexas e em constante mudança de segurança e conectividade de rede.

Referências:

1. zscaler.com.br/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. info.zscaler.com/2023-vpn-risk-report-br
3. zscaler.com.br/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

© 2024 Zscaler, Inc. Todos os direitos reservados.



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**.

©2024 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, ZDX™ 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