E-BOOK

Como as SD-WANs tradicionais permitem ataques de ransomware; e como impedi-los

Introdução

À medida que os desafios de segurança continuam a aumentar, as arquiteturas de rede não evoluíram para acompanhar o ritmo. De acordo com o Relatório de ransomware de 2024 da Zscaler ThreatLabz, vimos pagamentos de resgate maiores do que nunca e um aumento de 58% ano a ano no número de empresas extorquidas. O ransomware se espalha rapidamente pelas organizações por um motivo simples: as redes legadas confiam implicitamente em tudo conectado a elas, permitindo que o ransomware se mova livremente de dispositivos infectados em filiais remotas para aplicativos essenciais.

No passado, as organizações dependiam de um modelo de segurança de "castelo e fosso", em que todo o tráfego dentro da rede era considerado seguro por padrão, e os controles de segurança eram aplicados apenas no perímetro. À medida que se tornaram mais distribuídas e centradas na nuvem, as organizações simplesmente estenderam suas redes privadas para filiais e nuvens usando redes de longa distância definidas por software (SD-WAN) e VPNs site a site. Isso criou grandes redes planas confiáveis, onde os invasores podem se mover lateralmente, apesar da infinidade de firewalls implantados em todos os lugares.

Enquanto isso, as redes incluem um número cada vez maior de dispositivos de IoT. Estima-se que 55,7 bilhões desses dispositivos estarão conectados a redes corporativas até 2025, gerando 80 bilhões de zettabytes de dados a cada ano.[1] Essa expansão da borda cria uma superfície de ataque cada vez maior, tornando as organizações mais vulneráveis. Todas essas tendências tornam as abordagens de segurança baseadas em perímetro cada vez mais insustentáveis. Como resultado, ano após ano, o número (e o custo) de violações de dados continuam a aumentar e a atividade de ransomware continua a aumentar.

Para proteger sua infraestrutura contra essas ameaças crescentes, organizações de todos os setores estão cada vez mais recorrendo a uma abordagem zero trust para a segurança cibernética.

Aumento de 17,8% nos ataques de ransomware de 2023 a 2024.[2]

US$ 75 milhões: pagamento recorde por ataque de ransomware reportado em 2024.[2]

Aumento de 104% no número de vítimas de violação de dados de 2023 a 2024.[3]

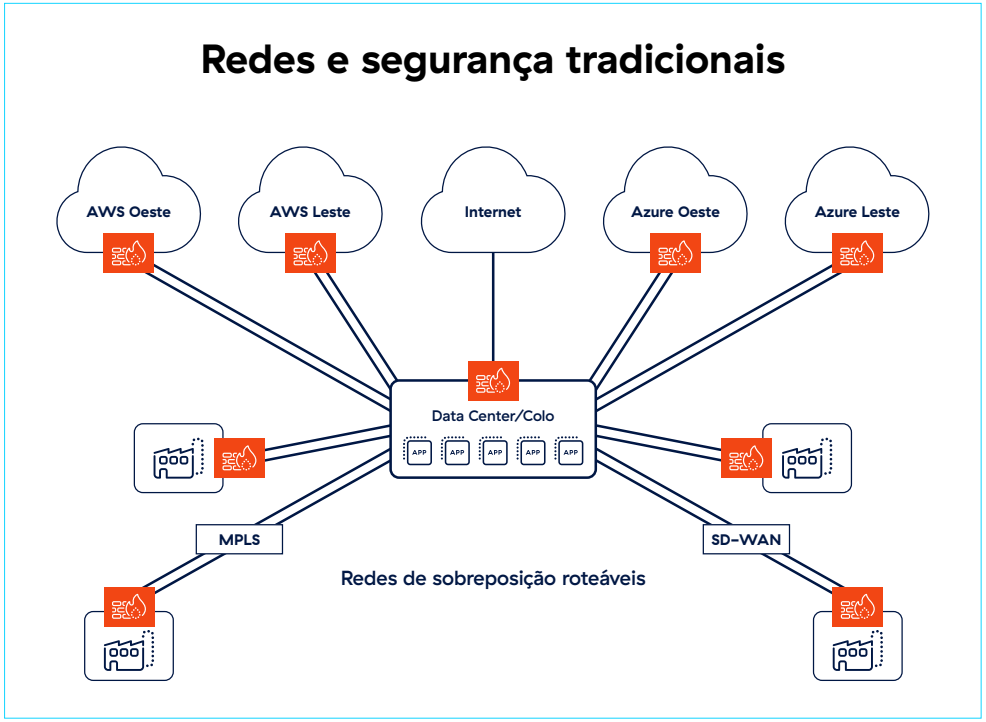
O custo médio global de uma violação de dados atingiu um recorde histórico de **US$ 4,88 milhões** em 2024.[4]

1: IDC Research, Futuro dos ecossistemas industriais: dados e insights compartilhados, 2021.
2: Relatório de ransomware de 2024 da Zscaler ThreatLabz.
3: Identity Theft Resource Center, Análise de Violação de Dados do primeiro período de 2024.
4: IBM, Relatório sobre o custo de uma violação de dados de 2024.

O que é e o que não é SD-WAN tradicional?

A SD-WAN aproveita a automação para direcionar o tráfego de rede para o caminho mais eficiente em vários serviços e infraestruturas de transporte de rede. Protocolos de roteamento com reconhecimento de aplicativo melhoram o desempenho do aplicativo priorizando o tráfego entre aplicativos críticos.

As soluções tradicionais de SD-WAN simplesmente estendem a rede da organização para filiais e data centers. Projetada para simplificar a conectividade, a SD-WAN permite que dispositivos em qualquer lugar, incluindo filiais, fábricas e sites de terceiros, se comuniquem com aplicativos no data center ou na nuvem pública. Compostas por uma malha de dispositivos e VPNs site a site, essas arquiteturas oferecem pouca ou nenhuma proteção contra movimentação lateral de ameaças e ransomware.



Permite a movimentação lateral de ameaças e facilita ataques de ransomware

Expande a superfície de ataque para filiais, fábricas, nuvem

Aumenta o custo, a complexidade e os tempos de implantação

A SD-WAN foi projetada para melhorar a conectividade, tornando mais rápido e fácil para os usuários acessarem os recursos. Mas conectividade não é sinônimo de segurança. O zero trust exige que a identidade e a postura de segurança sejam verificadas antes que a conectividade seja permitida. A confiança implícita incorporada às redes legadas apenas as torna mais difíceis de proteger e facilita a rápida disseminação de ransomware.

Para alcançar o zero trust em uma SD-WAN tradicional, uma organização precisa adicionar dispositivos de segurança, ferramentas e pontos de aplicação de políticas adicionais. O resultado é uma colcha de retalhos de firewalls, VPNs em malha e outras ferramentas, como controle de acesso à rede (NAC), soluções de segurança de DNS, etc. Essa arquitetura é complexa e consome recursos excessivos de orçamento e pessoal para ser gerenciada.

> “Na verdade, quando a conectividade é alcançada por meio da confiança por padrão, ela está em desacordo com o modelo zero trust.”

O que é zero trust?

Zero trust é uma estratégia de segurança que afirma que nenhuma entidade (usuário, aplicativo, serviço ou dispositivo) deve ser considerada confiável por padrão. Seguindo o princípio do acesso de privilégio mínimo, antes de qualquer conexão ser autorizada, a confiança é estabelecida com base no contexto e na postura de segurança da entidade, e então reavaliada continuamente para cada nova conexão, mesmo que a entidade tenha sido autenticada anteriormente.

Primeiros passos com zero trust

Começar com uma rede aberta e plana e adicionar pontos de aplicação e controles de segurança para implantar o zero trust é operacionalmente complexo e caro. Os projetos de segmentação de rede geralmente duram meses ou até anos, e os requisitos geralmente mudam antes que esses projetos sejam concluídos. E se você pudesse começar ao contrário? E se suas filiais pudessem ser como cafeterias, sem uma rede roteável conectando-as aos aplicativos da organização na nuvem?

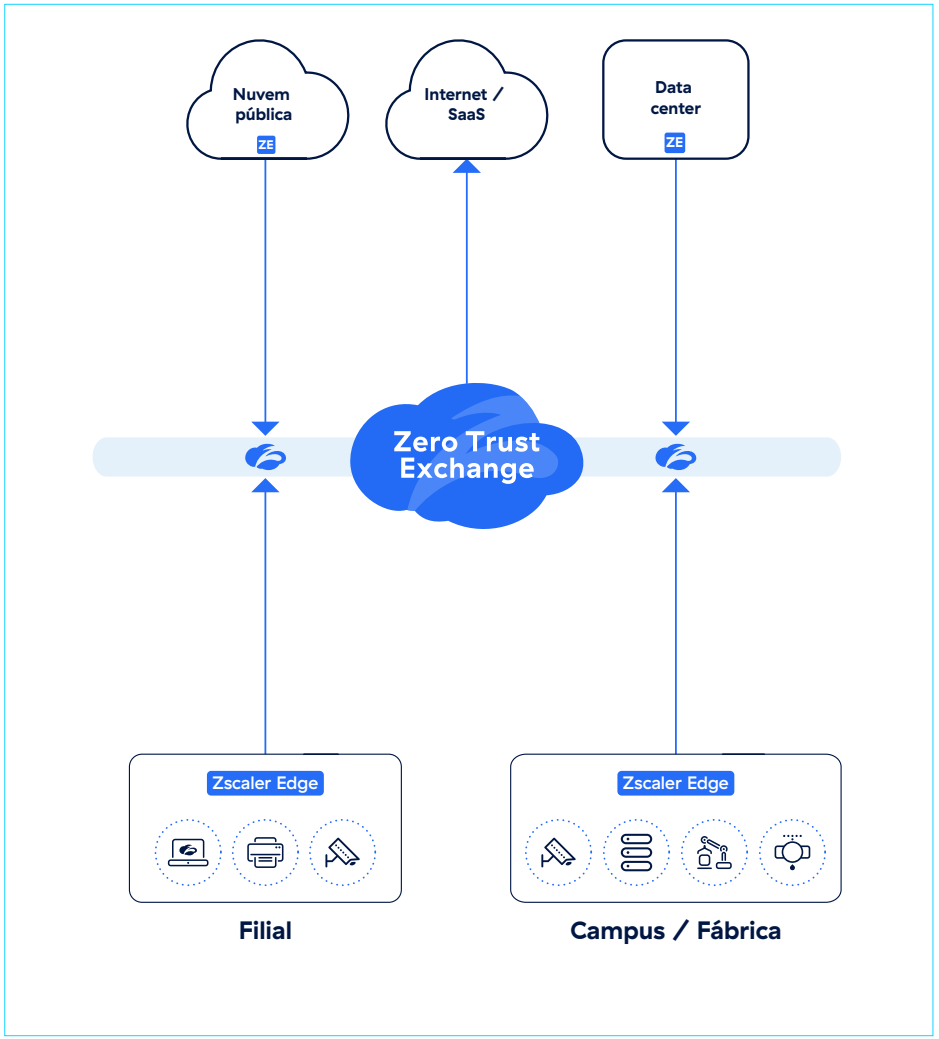
Ela conecta usuários e dispositivos a aplicativos com base em políticas, não na presença de rede, fornecendo segurança robusta e simplicidade operacional.

Essa é uma abordagem zero trust nativa que torna a movimentação lateral impossível, já que usuários e dispositivos (incluindo dispositivos de internet das coisas (IoT) e tecnologia operacional (OT)) nunca estão conectados diretamente aos aplicativos. Em vez disso, eles se comunicam por meio da plataforma Zscaler Zero Trust Exchange™, que facilita a proteção completa de dados e contra ameaças cibernéticas com controles de acesso robustos baseados em identidade e contexto.

> “Zero Trust SD-WAN é uma nova maneira de fornecer às filiais e data centers acesso rápido e confiável à internet, aplicativos privados e serviços na nuvem sem estender a rede corporativa para todos os lugares.”

Essa abordagem zero trust:

- **Melhora o desempenho de aplicativos.**
  As empresas podem substituir VPNs site a site complexas por uma arquitetura direta para nuvem simples que oferece desempenho rápido e consistente para dar suporte à produtividade.
- **Minimiza a superfície de ataque da internet.**
  Soluções de WAN legadas expõem as portas da VPN à internet pública, deixando a rede vulnerável a ataques. Com a SD-WAN zero trust, os aplicativos privados ficam atrás da Zero Trust Exchange, onde não podem ser descobertos ou atacados pela internet.
- **Impede a movimentação lateral de ameaças.**
  As VPNs site a site criam uma grande rede roteável onde uma infecção por malware pode ser transmitida de um único dispositivo para tudo na rede. Com a SD-WAN zero trust, as conexões são feitas diretamente para os aplicativos, não para a rede. Isso torna a movimentação lateral impossível.
- **Reduz custos e complexidade.**
  Essa abordagem elimina a necessidade de vários firewalls, VPNs, NAC e outras soluções em camadas. O resultado é uma arquitetura mais simples, menos dispendiosa e muito mais fácil de configurar e manter.



A Zscaler soluciona os desafios da SD-WAN tradicional

Ao usar a Zero Trust Exchange para conectar com segurança filiais, fábricas e data centers, a Zscaler garante acesso zero trust uniforme e consistente para todos os usuários, dispositivos de IoT/OT e aplicativos.

	SD-WAN Zero Trust	SD-WAN tradicional
Reduz a superfície de ataque e interrompe a movimentação lateral de ameaças	Sim	Não
Reduz a complexidade das regras de firewall e ACL	Sim	Não
Elimina o comprometimento entre segurança e desempenho	Sim	Não
Elimina a necessidade de usar firewalls na filial	Sim	Não

A SD-WAN zero trust da Zscaler é flexível o suficiente para oferecer suporte a diversas opções de implantação que não exigem uma substituição completa. Ela pode funcionar junto com a infraestrutura de SD-WAN da sua filial existente e criar sobreposições zero trust para a Zero Trust Exchange. Isso garantirá acesso seguro e de alto desempenho dos dispositivos de sua filial a aplicativos privados em outros locais e na nuvem, sem permitir a movimentação lateral de ameaças.

Se você estiver adotando uma nova abordagem para as necessidades de conectividade da sua organização, comece com uma arquitetura zero trust nativa que reduza a complexidade e elimine a necessidade de firewalls adicionais em todos os lugares. A SD-WAN zero trust da Zscaler pode gerenciar suas conexões de ISP e direcionar o tráfego de aplicativos de forma inteligente para oferecer aos seus usuários uma experiência segura em filiais, semelhante à de uma cafeteria, ao mesmo tempo em que mantém sua organização protegida contra ataques de ransomware.

Impeça ataques de ransomware com zero trust

O zero trust é essencial para enfrentar os desafios de segurança atuais e reduzir o risco de ataques de ransomware. Com a SD-WAN zero trust da Zscaler, sua organização pode proteger todas as comunicações e eliminar a possibilidade de movimentação lateral de ameaças sem o custo e a complexidade operacional das abordagens legadas. Além disso, experiências digitais excepcionais manterão clientes, funcionários e outros usuários finais produtivos e satisfeitos.

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes tenham mais agilidade, eficiência, resiliência e proteção. A 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 de segurança integrada na nuvem do mundo. Para saber mais, visite **www.zscaler.com.br**.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com.br