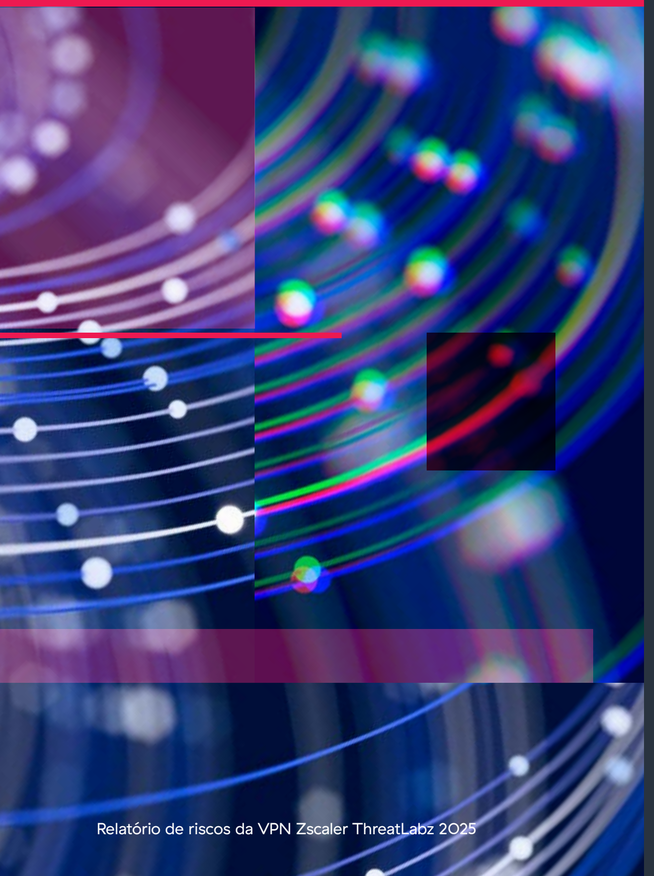
Cybersecurity INSIDERS

Zscaler Relatório de riscos da VPN de 2025 da ThreatLabz

Índice



Resumo executivo 3

Principais descobertas 4

Riscos da VPN: por que 81% das organizações estão migrando para o zero trust até 2026 5

Preocupações com a segurança de VPN 6

- A obsolescência das VPNs: riscos de segurança e frustrações dos usuários 6
- Ransomware e VPNs: uma tempestade perfeita de riscos 7
- VPNs e movimentação lateral: aumentando o raio de ação das violações 8

CVEs de VPN de 2020 a 2025: uma onda crescente de vulnerabilidades de alta gravidade 9

- Principais tendências: tipos de impacto das CVEs 10
- Principais tendências: vulnerabilidades críticas da VPN 11

Preocupações com a segurança de VPN (cont.) 13

- Os desafios da implementação de segmentação 13
- As VPNs aumentam os riscos de cibersegurança de fusões e aquisições 14
- Acesso de terceiros à VPN: uma porta de entrada para invasores 15

Desafios e falhas das medidas de proteção legadas 16

- As ferramentas tradicionais deixam os aplicativos privados expostos 16
- Implantação de NAC em ambientes de VPN: uma proteção limitada 17

Problemas de gerenciamento e de experiência de usuário da VPN 18

- O problema de desempenho da VPN: frustrando usuários e sobrecarregando a TI 18
- Gerenciamento de VPN: sobrecarregando equipes de TI e expondo vulnerabilidades 19
- O pesado fardo do gerenciamento de VPN 20
- Controles de acesso à VPN excessivamente amplos: uma falha crítica de segurança 21
- Substituição da VPN: uma mudança em direção ao acesso seguro 22

Adoção do zero trust 23

- O zero trust substitui a VPN em grande escala 23
- Prioridades do zero trust: o trabalho remoto promove a adoção 24
- Principais vantagens de substituir as VPNs por zero trust 25

Previsões de riscos da VPN para 2025 26

Práticas recomendadas de acesso seguro 28

- Reduza os riscos da VPN e fortaleça a segurança zero trust 28

Como a Zscaler transforma o acesso seguro 30

- Principais benefícios do Zscaler Private Access (ZPA) 31

Metodologia e dados demográficos 33

Sobre 34

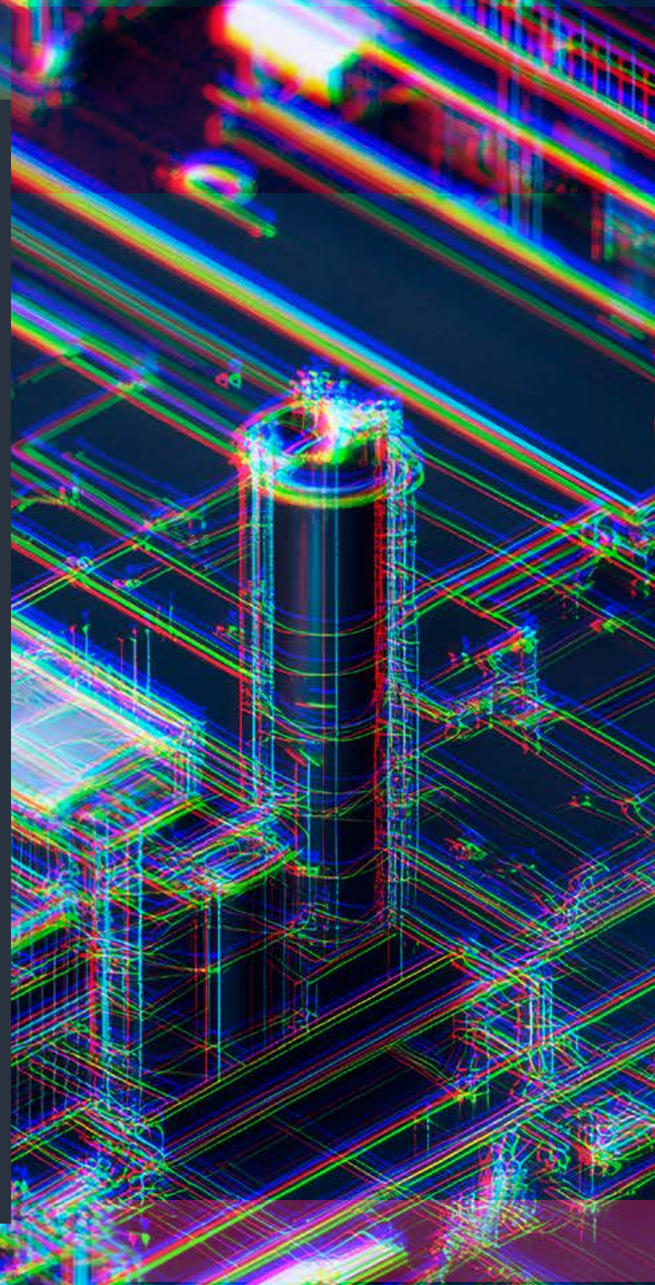
Resumo executivo

O Relatório de riscos da VPN de 2025 da Zscaler ThreatLabz oferece uma análise incisiva dos riscos em evolução associados às redes privadas virtuais (VPNs) e destaca a mudança urgente para arquiteturas zero trust, à medida que as organizações se esforçam para atender às demandas de segurança preparadas para o futuro. Antes anunciadas como a espinha dorsal do acesso remoto, as VPNs têm se tornado cada vez mais pontos focais para ameaças cibernéticas, passando de ferramentas essenciais a riscos significativos de segurança para organizações em todo o mundo. Este relatório, que reúne insights de mais de 600 profissionais de TI e segurança, revela uma mudança crucial no cenário da cibersegurança: **mais da metade das organizações pesquisadas sofreram ataques devido a vulnerabilidades de VPN somente no ano passado,** destacando a extrema necessidade de uma nova abordagem nos ambientes de trabalho cada vez mais híbridos de hoje.

Em 2025, a insatisfação com as VPNs tradicionais catalisou uma mudança, com as empresas reconhecendo, em sua maioria, que corrigir essas vulnerabilidades é uma corrida que não podem mais vencer. Essa percepção está promovendo a adoção generalizada de modelos zero trust, que prometem controle de acesso granular e reduzem significativamente os riscos de segurança. Notavelmente, **81% das organizações estão se preparando para implementar estratégias zero trust até 2026, com 65% planejando eliminar completamente as VPNs no mesmo período.** Além disso, frustrações operacionais, como conexões lentas, desconexões frequentes e processos de autenticação complexos, só aumentaram a urgência, promovendo um aumento na demanda por soluções zero trust que garantam acesso contínuo e seguro.

Todas essas mudanças acontecem dentro do contexto de um cenário de ameaças habilitado por IA. De fato, o aumento de ataques cibernéticos baseados em IA impactará a segurança da VPN de maneiras sem precedentes. Os invasores usarão cada vez mais a IA para reconhecimento automatizado de vulnerabilidades de VPN, facilmente verificadas pela internet pública. Técnicas como pulverização inteligente de senhas e desenvolvimento rápido de exploits permitirão que criminosos comprometam credenciais de VPN em maior escala. Mais abaixo na cadeia de ataque, técnicas de evasão baseadas em IA tornarão ainda mais difícil detectar intrusões baseadas em VPN antes que danos significativos ocorram. À medida que essas ameaças impulsionadas pela IA crescem, os riscos de VPN só aumentam, levando as empresas a adotar medidas de segurança proativas e acelerando a mudança já pronunciada em direção a soluções zero trust.

Reconhecendo essas mudanças, o relatório da ThreatLabz não apenas registra o declínio das VPNs, passando de ferramentas indispensáveis para problemáticas, mas também fornece insights práticos para empresas que navegam nesse cenário transformador.



Principais_ descobertas

1. A obsolescência das VPNs acelera:

Um número significativo de 65% das empresas deverá substituir seus serviços de VPN no próximo ano, o que representa um aumento de 23% em relação a 2024. Essa tendência é motivada principalmente pela incapacidade das VPNs de atender às demandas de segurança e conformidade das empresas modernas, destacando seu papel em agravar os riscos em vez de mitigá-los.

2. Aumento de ataques cibernéticos via exploits de VPN e preocupações com ransomware:

No ano passado, houve um aumento preocupante em incidentes cibernéticos vinculados a vulnerabilidades de VPN, com 56% das organizações relatando tais violações, um aumento alarmante em relação aos números anteriores. Enquanto isso, 92% dos entrevistados estão preocupados que vulnerabilidades de VPN não corrigidas levem diretamente a ataques de ransomware. Essas descobertas reforçam a tendência de que, com dificuldade para manter o ritmo acelerado de correção de vulnerabilidades, as empresas precisam de uma revisão robusta de segurança para preencher essas brechas críticas de segurança e mitigar os riscos sempre presentes de exploração da VPN.

3. A insatisfação do usuários final influencia o redirecionamento de segurança:

As frustrações dos usuários com as ineficiências da VPN, que vão desde velocidades lentas até autenticação complicada, complexa ou interrompida, estão influenciando cada vez mais as estratégias organizacionais. Esse descontentamento do usuário final está impulsionando o avanço em direção a arquiteturas zero trust que oferecem acesso ininterrupto e seguro, sem os aborrecimentos tradicionais associados às VPNs.

4. A mudança da VPN para o zero trust: do conceito à implementação:

Refletindo uma grande mudança estratégica, 81% das organizações estão ativamente agindo para implementar estruturas zero trust no próximo ano. Isso marca uma transição fundamental da visão do zero trust como um ideal teórico para reconhecê-lo como uma necessidade prática para substituir VPNs e, ao mesmo tempo, melhorar a segurança em ambientes de TI dinâmicos e distribuídos.

Riscos da VPN: por que 81% das organizações estão migrando para o zero trust até 2026_

As VPNs foram projetadas para fornecer acesso remoto, mas os tempos mudaram; e os invasores também. Hoje, as VPNs frequentemente servem como pontos de entrada para ataques de ransomware, roubo de credenciais e espionagem cibernética devido a vulnerabilidades difíceis de corrigir rapidamente; modelos de confiança implícita que fornecem acesso completo à rede; e permissões de acesso generalizadas. No geral, as vulnerabilidades de segurança são o maior desafio que as empresas enfrentam com as VPNs (de acordo com 54% dos entrevistados), ressaltando o fato de que os invasores rotineiramente exploram falhas não corrigidas ou contornam proteções para se infiltrar nas redes.

Os riscos tornam-se ainda mais pronunciados com o acesso de terceiros à VPN. Um número expressivo de 93% dos entrevistados expressa preocupação com vulnerabilidades de backdoor introduzidas por conexões externas de VPN, à medida que invasores exploram cada vez mais credenciais de terceiros para invadir redes sem serem detectados. Não se trata apenas do acesso inicial; as VPNs também tornam as violações mais destrutivas. Ao contrário das soluções zero trust, que aplicam políticas granulares para impedir a movimentação dentro das redes, as VPNs oferecem amplo acesso, permitindo que invasores se movam lateralmente e aumentem privilégios. No geral, 71% dos entrevistados identificam a movimentação lateral como uma das principais preocupações, reconhecendo como ela amplifica o escopo e o impacto de uma violação.

Esses desafios, somados a preocupações cotidianas como desempenho lento, autenticação complexa e desconexões frequentes, deixam claro por que as empresas estão abandonando as VPNs em favor de modelos zero trust. O Relatório de riscos da VPN de 2025, baseado em insights de 632 profissionais de TI e cibersegurança, tem como objetivo esclarecer o estado do uso da VPN em 2025 para entender melhor os riscos e desafios, além de oferecer às empresas orientações de práticas recomendadas para melhorar sua postura de segurança cibernética e sua abordagem de acesso remoto seguro.

As descobertas deste relatório oferecem aos líderes de TI e segurança insights baseados em dados sobre os motivos para aposentar VPNs obsoletas e adotar uma arquitetura zero trust moderna e disponibilizada na nuvem. A mudança da confiança implícita para a verificação contínua não é mais opcional: é essencial para proteger as empresas distribuídas de hoje, reduzir a complexidade da TI e garantir uma experiência perfeita ao usuário.

Preocupações com a segurança_ de VPN

A obsolescência das VPNs: riscos de segurança e frustrações dos usuários

As organizações que continuam a depender de VPNs para acesso remoto se veem cada vez mais expostas a falhas de segurança, ineficiências operacionais e crescente insatisfação do usuário final, reforçando o sentimento crescente de que as VPNs pertencem a uma era passada de segurança de acesso.

O principal desafio (riscos de segurança e conformidade, citados por 54% dos entrevistados) reforça a vulnerabilidade crítica das VPNs diante de ataques de ransomware, escalada de privilégios e ataques de movimentação lateral. Os invasores veem as VPNs como elos fracos, propícios à exploração, enquanto as organizações se esforçam para corrigir esses sistemas desatualizados com rapidez suficiente para acompanhar as ameaças avançadas.

A frustração dos usuários chegou ao ponto de ebulição: 51% dos entrevistados identificam o baixo desempenho das VPNs, incluindo elementos como conectividade lenta, quedas e protocolos de autenticação complicados, como um obstáculo à produtividade. As VPNs continuam sendo um fardo operacional, com 41% dos entrevistados citando dificuldades de gerenciamento e 37% sinalizando altos custos para manutenção contínua.

Esses números ilustram o quanto as VPNs se tornaram consumidoras de recursos, esgotando os orçamentos de TI e forçando as equipes a gastar tempo desnecessário em tarefas repetitivas de solução de problemas.

Adeus, abordagens legadas. Olá, zero trust.

Uma violação recente serve como um lembrete claro das vulnerabilidades da VPN. Em janeiro de 2025, um grupo chinês de espionagem cibernética explorou com sucesso uma vulnerabilidade de dia zero na Pulse Secure VPN da Ivanti, concedendo acesso não autorizado em redes corporativas. Este ataque, um dos vários direcionados à tecnologia de VPN nos últimos meses, destaca por que as organizações não podem mais depender de modelos de acesso legados para defender suas infraestruturas.

Com esses desafios, vários fornecedores de VPNs legadas começaram a rotular máquinas virtuais disponibilizadas na nuvem como soluções zero trust. No entanto, os serviços de VPN hospedados na nuvem permanecem fundamentalmente os mesmos de uma perspectiva arquitetônica:

Eliminar dependências de VPN não é mais uma atualização opcional: é uma necessidade imediata. As organizações precisam fazer a transição para verdadeiras estruturas zero trust que ofereçam acesso de privilégio mínimo, orientado por identidade e segmentação granular. Essas arquiteturas disponibilizadas na nuvem ajudam a reduzir superfícies de ataque laterais, melhorar a experiência dos usuários e diminuir a complexidade da TI, uma tríade de benefícios que as VPNs simplesmente não conseguem igualar.

Quais você considera os maiores desafios com suas soluções de VPN?

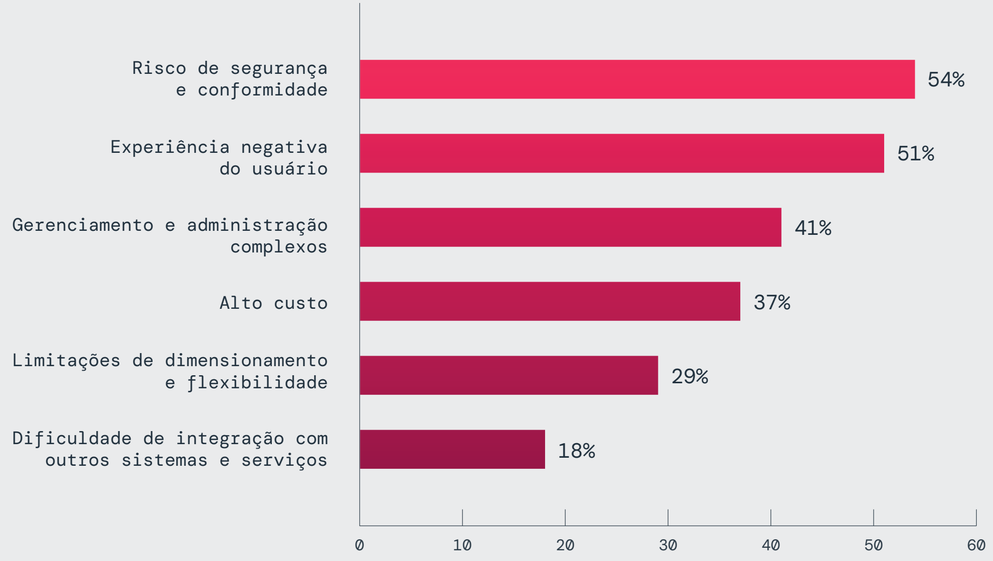


Figura 1: os maiores desafios com soluções de VPN.

são serviços conectados à internet com um endereço IP público que pode ser violado. Um exemplo: o setor testemunhou recentemente picos massivos na atividade de varredura que tem como alvo mais de vinte mil endereços IP de VPN públicos hospedados por um dos maiores fornecedores de segurança. Historicamente, esse tipo de atividade indica alguma probabilidade de que invasores possam estar se preparando para explorar vulnerabilidades ainda não divulgadas nos ativos de VPN visados. Em outras palavras: se você está acessível, é violável. E é por isso que, de uma perspectiva arquitetônica, a tecnologia de VPN baseada na nuvem nunca poderá atingir os verdadeiros princípios do zero trust, não importa a marca.

Ransomware e VPNs: uma tempestade perfeita de riscos

Os grupos de ransomware continuam a explorar vulnerabilidades em VPNs com uma precisão devastadora, aproveitando falhas de dia zero e fraquezas conhecidas antes que as organizações possam implantar correções de segurança. As VPNs se tornaram um “alvo fácil” para os invasores devido à sua ampla adoção e dependência de modelos de confiança de rede desatualizados.

No geral, 92% dos entrevistados expressaram altos níveis de preocupação com ransomwares direcionados a vulnerabilidades de VPN não corrigidas, destacando a necessidade crítica de mecanismos de proteção mais robustos. Esses dados ressaltam por que as VPNs agora são vistas como um problema, em vez de ferramentas confiáveis para mitigar riscos cibernéticos modernos.

Exemplos reais continuam a validar esses medos. Em janeiro de 2023, diversas organizações de saúde dos EUA foram vítimas de um ataque de ransomware causado por uma vulnerabilidade não corrigida do Citrix NetScaler (CVE-2023-4966). Essa exploração permitiu que invasores se infiltrassem em sistemas, interrompessem operações hospitalares, bloqueassem registros de pacientes e forçassem as instalações a redirecionar atendimentos de emergência críticos, tudo porque a vulnerabilidade não havia sido corrigida a tempo. Esse incidente ressalta o risco generalizado representado por VPNs sem correções. Os criminosos verificam com frequência os sistemas expostos, garantindo que possam se aproveitar das vulnerabilidades antes que as organizações apliquem correções, deixando as organizações em risco de comprometimento, interrupção operacional e perda financeira.

As organizações devem abandonar a rotina interminável de aplicação de correções e adotar estratégias defensivas proativas, adaptadas às ameaças em evolução. Estruturas zero trust priorizam o controle de acesso orientado por identidade e a verificação contínua, garantindo uma grande redução no risco de ransomware, mesmo quando as vulnerabilidades permanecem sem correção. Sistemas de detecção automatizados e políticas dinâmicas também contêm potenciais violações, impedindo que invasores se movam lateralmente ou aumentem privilégios.

Qual é o seu nível de preocupação em ser alvo de ransomware devido a vulnerabilidades não corrigidas?

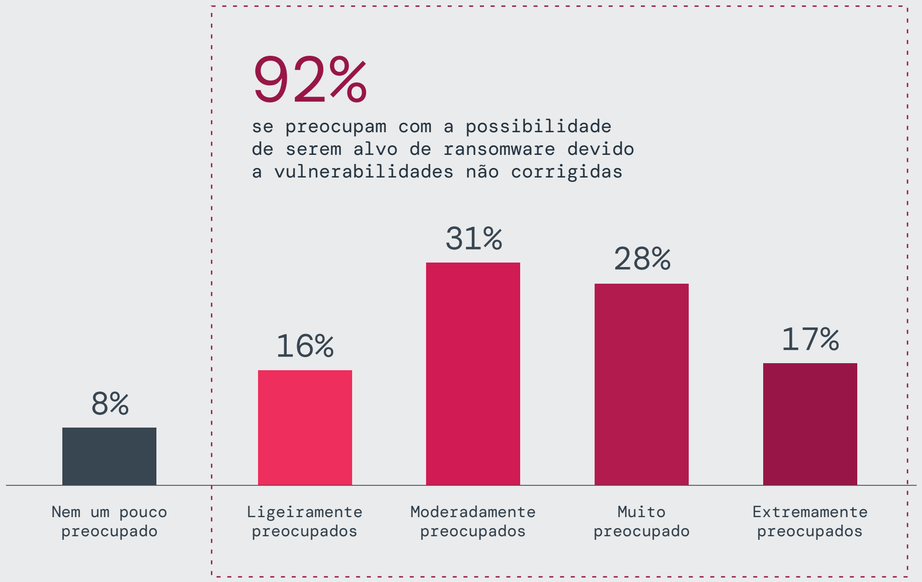


Figura 2: preocupações com ataques de ransomware.

VPNs e movimentação lateral: aumentando o raio de ação das violações

Além de permitir o comprometimento inicial por meio de ataques de ransomware e outras ameaças, as VPNs facilitam a movimentação lateral, uma técnica de ataque perigosa. Os invasores exploram o amplo acesso fornecido pelas VPNs para aumentar privilégios e se infiltrar mais profundamente nas redes visadas, geralmente com consequências devastadoras.

Um total de 71% dos entrevistados expressaram algum nível de preocupação com esse risco, com 32% expressando altos níveis de preocupação. Esses sentimentos são justificados, pois as VPNs geralmente concedem amplo acesso à rede, permitindo que invasores se movam sem serem detectados, aumentem privilégios e exfiltrem dados sigilosos uma vez dentro.

Em setembro de 2024, invasores exploraram diversas vulnerabilidades de dia zero no Cloud Service Appliance (CSA) da Ivanti, principalmente as vulnerabilidades CVE-2024-8963 e CVE-2024-8190, para violar diversas organizações, conforme confirmado pela Agência de Segurança Cibernética e de Infraestrutura (CISA) e pelo FBI. Os invasores contornaram controles administrativos, executaram comandos arbitrários, coletaram credenciais e implantaram web shells, permitindo a movimentação lateral entre as redes. Apesar de incidentes de segurança anteriores envolvendo VPNs da Ivanti, essas novas explorações demonstram que aplicar correções ou reestruturar soluções de VPN legadas ainda não consegue resolver as falhas de segurança fundamentais inerentes aos modelos de acesso remoto baseados em rede.

Qual é o seu nível de preocupação com a possibilidade de invasores se moverem lateralmente pela sua rede se uma VPN for comprometida?

89% estão preocupados com a movimentação lateral de invasores

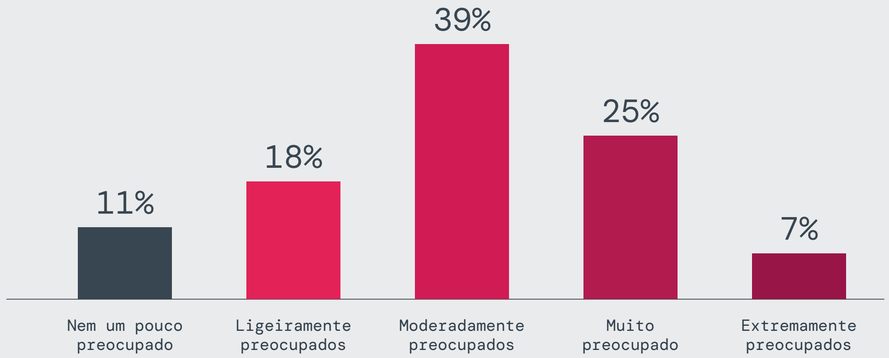


Figura 3: preocupações empresariais de que invasores se moverão lateralmente pela rede se uma VPN for comprometida.

Para mitigar esses riscos, as organizações devem fazer a transição do acesso baseado em VPN para o acesso à rede zero trust (ZTNA) com segmentação rigorosa. Ao contrário das VPNs, que concedem aos usuários amplo acesso à rede, o ZTNA fornece acesso em nível de aplicativo com base na identidade e no contexto, garantindo que os usuários possam acessar apenas os recursos específicos de que precisam. Essa abordagem impede a movimentação lateral mesmo que os invasores obtenham acesso inicial, reduzindo drasticamente a superfície de ataque e o raio de ação potencial das violações. Além disso, a implementação de rede e microssegmentação fortalece a segurança ao isolar sistemas críticos e impedir a comunicação não autorizada entre ativos comprometidos e seguros.

CVEs de VPN de 2020 a 2025: uma onda crescente de vulnerabilidades de alta gravidade

Nenhum software está imune a vulnerabilidades de segurança, e nem se deve esperar que esteja. No entanto, no caso da tecnologia de VPN, as vulnerabilidades, especialmente as ameaças de dia zero, podem ser particularmente prejudiciais, pois os criminosos podem facilmente sondar a infraestrutura de VPN afetada e explorá-la antes que qualquer correção seja lançada ou aplicada. A comunicação de CVEs é um ponto positivo, pois esse esforço de toda a comunidade ajuda fornecedores e clientes a seguir as práticas recomendadas e aprimorar sua higiene cibernética por meio de correções e divulgação. A forma como essas CVEs são descobertas e as informações que elas contêm refletem as mudanças no cenário de ameaças em evolução.

A Zscaler ThreatLabz analisou 411 vulnerabilidades e exposições comuns (CVEs) de VPN de 2020 a 2025, conforme relatado pelo programa de CVE da MITRE. As descobertas indicam um aumento gradual nas vulnerabilidades de VPN na primeira metade desta década. Essas CVEs abrangem uma ampla gama de falhas de VPN, desde a exploração de interfaces de gerenciamento baseadas na web, passando por vulnerabilidades de injeção de comando e validação de entrada, até falhas criptográficas e ataques de DoS e DDoS. Há várias vulnerabilidades recentes em VPNs, muitas das quais levaram a violações de segurança graves e altamente visíveis.

Muitas dessas CVEs são críticas. Em 2024, por exemplo, 60% das 83 vulnerabilidades de VPN relatadas pelo NIST indicaram uma pontuação de CVSS alta ou crítica. Enquanto isso, vulnerabilidades de execução remota de código (RCE), que permitem que invasores executem comandos arbitrários e potencialmente levem ao comprometimento do sistema, foram as CVEs de VPN mais comuns. Em outras palavras, longe de serem inócuas, a maioria das CVEs de VPN no ano passado deixou seus usuários extremamente vulneráveis a exploits que os invasores executam com relativa facilidade. Além disso, muitas dessas CVEs foram exploits de dia zero. Embora as CVEs em 2025 ainda sejam baixas no início do ano, vulnerabilidades importantes já foram divulgadas, como dois exploits de dia zero, CVE-2025-0282 e CVE-2025-0283.

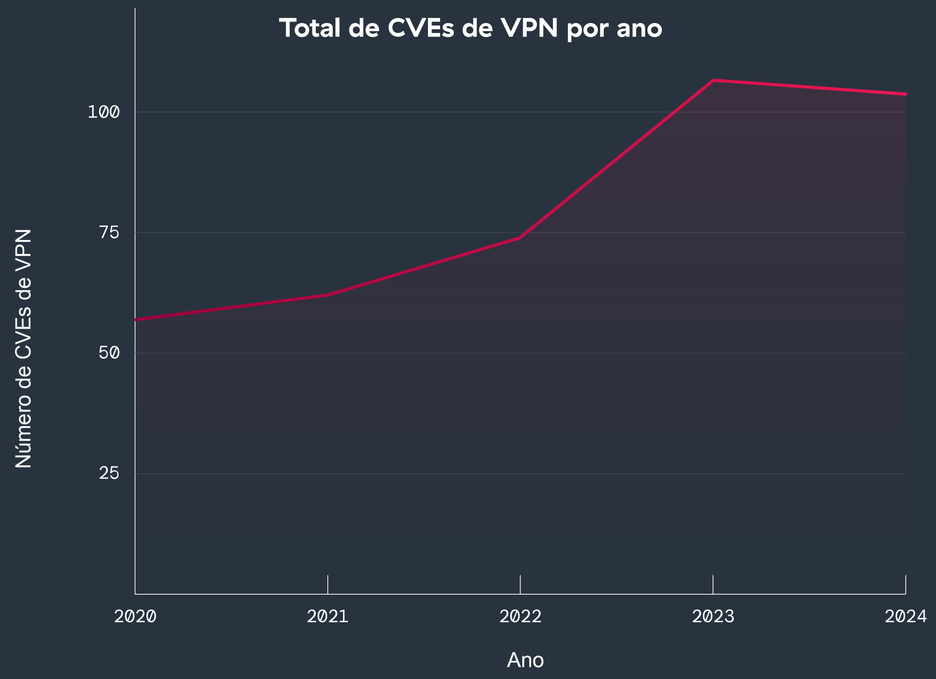


Figura 4: total de CVEs de VPN para cada ano, de 2020 a 2024.

1. A RCE continua sendo a principal ameaça

- **Observação:** as vulnerabilidades de RCE lideram a lista em todos os quatro anos, com 32 somente em 2024. A RCE é responsável por 149 CVEs, incluindo dados de 2025, tornando-se o tipo de vulnerabilidade mais frequente e crítico.
- **Implicação:** as vulnerabilidades de RCE permitem que invasores executem comandos arbitrários em dispositivos de VPN, o que pode levar ao comprometimento total do sistema. As empresas devem priorizar a aplicação de correções e a proteção de sistemas vulneráveis a tais exploits.

2. A escalada de privilégios está crescendo constantemente ao longo do tempo

- **Observação:** há um aumento constante nas CVEs de escalada de privilégios (66.7%), atingindo o pico em 2024 com 20 vulnerabilidades.
- **Implicação:** os invasores exploram cada vez mais falhas de VPN para aumentar privilégios e obter controle administrativo sobre os sistemas. As empresas devem garantir configurações seguras do sistema e restringir rigorosamente os privilégios de acesso.

3. As vulnerabilidades de negação de serviço (DoS) mostram um aumento acentuado de 200%

- **Observação:** as CVEs relacionadas a DoS triplicaram de 9 em 2020 para 27 em 2024, tornando-se o segundo tipo de maior impacto nos últimos anos; 85 CVEs ao todo, incluindo dados de 2025 até o momento.
- **Implicação:** os ataques de DoS estão evoluindo em sofisticação, tornando os sistemas de VPN alvos preferenciais para interrupções operacionais. As empresas devem adotar a limitação de taxa e o modelamento de tráfego para mitigar esses riscos.

4. O vazamento de informações sigilosas é mais raro, mas ainda crítico

- **Observação:** embora relativamente menos comuns, com 41 CVEs no total, as vulnerabilidades de vazamento de informações sigilosas expõem credenciais críticas, chaves de criptografia e dados de usuários.
- **Implicação:** esse tipo de impacto é particularmente prejudicial à confidencialidade e à conformidade. As empresas devem implementar criptografia robusta, práticas de desenvolvimento de software seguras e monitoramento de tráfego para detectar e prevenir vazamentos de dados.

5. Crescimento constante nas vulnerabilidades de contorno de autenticação

- **Observação:** os incidentes de contorno de autenticação têm sido relativamente baixos, mas consistentes, crescendo de 4 em 2020 para um pico de 6 em 2023 e para 4 vulnerabilidades em 2024, totalizando 30 CVEs ao longo do tempo.
- **Implicação:** os invasores estão mirando em vulnerabilidades na autenticação multifator (MFA) e na lógica de login para se passar por usuários. As empresas devem fortalecer as configurações de MFA e monitorar comportamentos anormais de login.

Principais tendências: tipos de impacto das CVEs

Para entender o dano potencial dessas vulnerabilidades caso fossem exploradas, a ThreatLabz avaliou CVEs de VPN em cinco categorias de ataque: execução remota de código (RCE), escalada de privilégios, vazamento de informações, negação de serviço (DoS) e desvio de autenticação. Observe que algumas categorias são agrupamentos abrangentes para tipos de ataques separados, mas intimamente relacionados: por exemplo, o desvio de autenticação inclui ataques que podem ignorar a autenticação de segundo fator ou multifator (MFA), enquanto outros ignoram medidas básicas de autenticação. Em geral, qualquer vulnerabilidade de RCE será um item de alta prioridade a ser corrigido por qualquer organização.

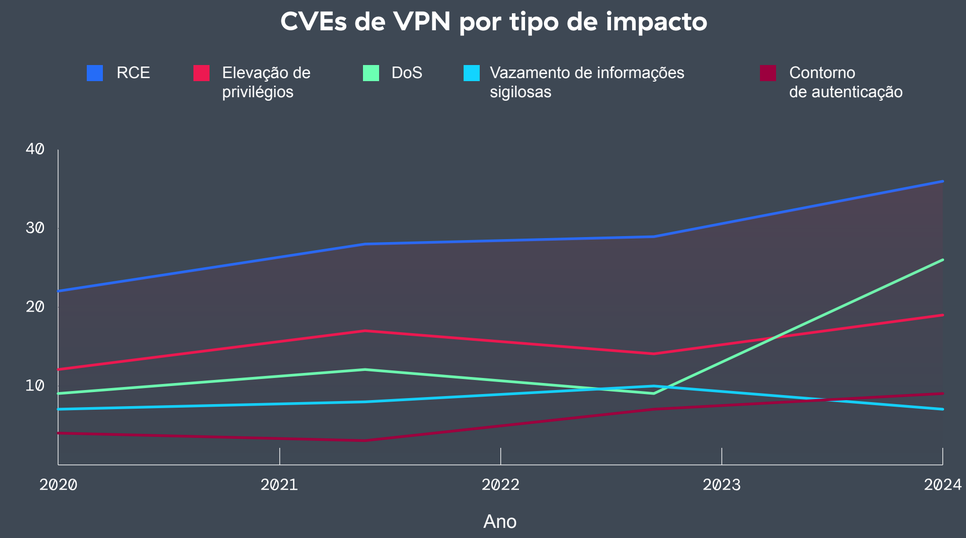


Figura 5: o tipo de impacto das CVEs de VPN de 2020 a 2024, abrangendo RCE, escalada de privilégios, vazamento de informações sigilosas de negação de serviço e desvio de autenticação.

Principais tendências: vulnerabilidades críticas da VPN

Além dos tipos de impacto, a ThreatLabz também analisou a gravidade das CVEs de VPN a cada ano. **No geral, a ThreatLabz constatou que as CVEs com pontuações de CVSS ALTA ou CRÍTICA aumentaram 38,9% entre 2020 e 2024.** De fato, 66,3% de todas as CVEs em 2024 foram classificadas como ALTA ou CRÍTICA, indicando um potencial impacto severo para as organizações quando tais CVEs são exploradas antes de serem corrigidas. Além disso, a ThreatLabz analisou tendências críticas em diferentes tipos de vulnerabilidades representadas nos dados de CVEs que as empresas devem compreender para melhor se defender contra as ameaças de VPN em evolução.

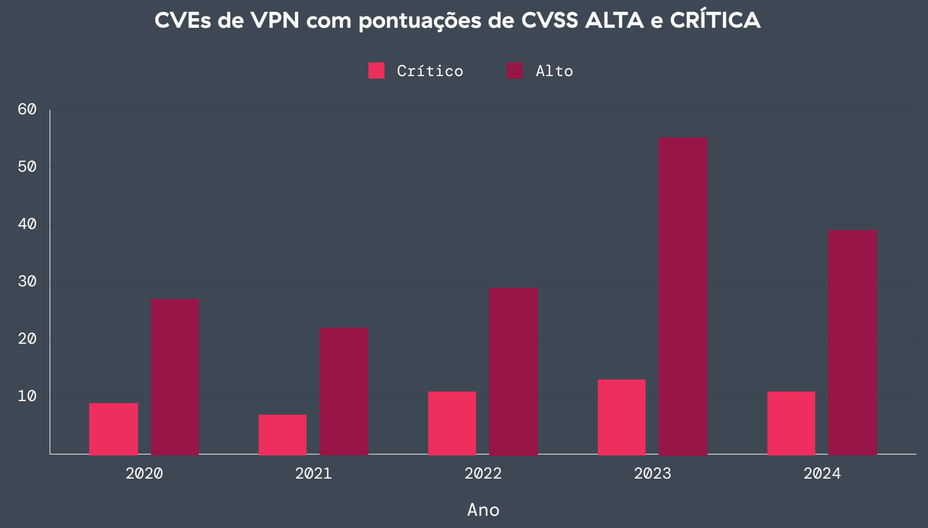


Figura 6: o volume de CVEs de VPN com pontuações de CVSS ALTA e CRÍTICA de 2020 a 2024.

1. Aumento da exploração de interfaces de gestão baseadas na web

- **Tendência:** as vulnerabilidades de injeção de comando e validação de entrada têm aumentado consistentemente, indicando o foco crescente dos invasores em portais administrativos e de gerenciamento, tanto da perspectiva do administrador quanto do usuário final. Como essas interfaces são inerentemente expostas à internet por meio de sua arquitetura, elas estão propensas à exploração por criminosos.
- **Escalada:** embora essas vulnerabilidades estivessem presentes em 2020–2021, elas se intensificaram significativamente a partir de 2022, sugerindo que os invasores veem essas interfaces de gerenciamento como alvos atraentes e acessíveis, especialmente devido a práticas inadequadas de codificação de segurança.

2. Autenticação generalizada e desvios de MFA

- **Tendência:** os ataques direcionados especificamente a métodos de autenticação, incluindo desvios de MFA, sequestro de sessão e gerenciamento inadequado de sessão, aumentaram constantemente.
- **Escalada:** os anos anteriores (2020—2021) viram principalmente desvios de autenticação mais simples, enquanto de 2023 a 2025, eles evoluíram para ataques mais avançados, automatizados e persistentes direcionados explicitamente às fraquezas da MFA, indicando a intenção dos invasores de minar medidas de segurança mais robustas.

3. Aumento de explorações de escalada de privilégios locais

- **Tendência:** vulnerabilidades de escalada de privilégios locais se tornaram mais prevalentes e cada vez mais graves.
- **Escalada:** o que começou como pequenos descuidos de configuração em 2020–2021 se intensificou em 2024–2025 em métodos mais sofisticados de escalada de privilégios, como sequestro de DLL, dando aos invasores acesso mais profundo ao nível do sistema.

4. Sofisticação crescente dos ataques de DoS e DDoS

- **Tendência:** os ataques de DoS evoluíram do esgotamento básico de recursos (2020—2021) para técnicas sofisticadas de amplificação de DDoS (2024—2025).
- **Escalada:** os invasores migraram de simples interrupções baseadas em pacotes malformados para ataques amplificados mais avançados, refletindo uma escalada estratégica para maximizar a interrupção operacional.

5. Falhas criptográficas persistentes e intensificadas

- **Tendência:** problemas relacionados à implementação criptográfica, como validação inadequada de certificados, vazamento de chaves e verificação de TLS insuficiente, aumentaram consideravelmente.
- **Escalada:** a partir de 2022, houve um pico perceptível nas vulnerabilidades criptográficas, atingindo o ápice em 2024–2025, com falhas de alta gravidade. Esse aumento demonstra o interesse estratégico dos adversários em explorar vulnerabilidades relacionadas à criptografia para minar a confidencialidade das VPNs.

Preocupações com a segurança de VPN (cont.)

Os desafios da implementação de segmentação

Considerando os riscos de movimentação lateral, muitas organizações tentam limitar a propagação de ataques por meio da segmentação. Embora a segmentação seja um mecanismo de defesa essencial para reduzir a superfície de ataque, sua implementação costuma ser desafiadora.

A pesquisa destaca esses desafios, com 51% das organizações prevendo ou enfrentando complexidade de configuração. Além disso, 39% relatam falta de experiência e recursos, enquanto 24% enfrentam gargalos de desempenho, indicando que as arquiteturas de rede legadas estão mal equipadas para dar suporte aos controles de acesso granulares necessários para os ambientes de TI atuais.

Os desafios de segmentação desempenharam um papel notável no ataque de ransomware ao MGM Resorts em 2023, onde os invasores obtiveram acesso inicial por meio de engenharia social, mas conseguiram se mover lateralmente devido à segmentação insuficiente. A violação interrompeu as operações do hotel, caixas eletrônicos e sistemas de jogos de cassino, custando à empresa cerca de US$ 100 milhões em danos. Esse caso destaca como a segmentação deficiente permite que invasores percorram sistemas críticos, amplificando o impacto de uma intrusão inicial.

Para enfrentar esses desafios, as organizações devem implementar modelos de segmentação baseados na nuvem e orientados por identidade que simplifiquem a aplicação de políticas e reduzam a sobrecarga manual. Ao contrário da segmentação de rede tradicional, que depende de regras complexas de firewall e configurações de VLAN, uma abordagem zero trust permite a segmentação dinâmica com base na identidade do usuário, postura do dispositivo e avaliações de risco em tempo real. Isso garante que somente usuários autorizados possam acessar aplicativos específicos, mantendo a rede segura como um todo.

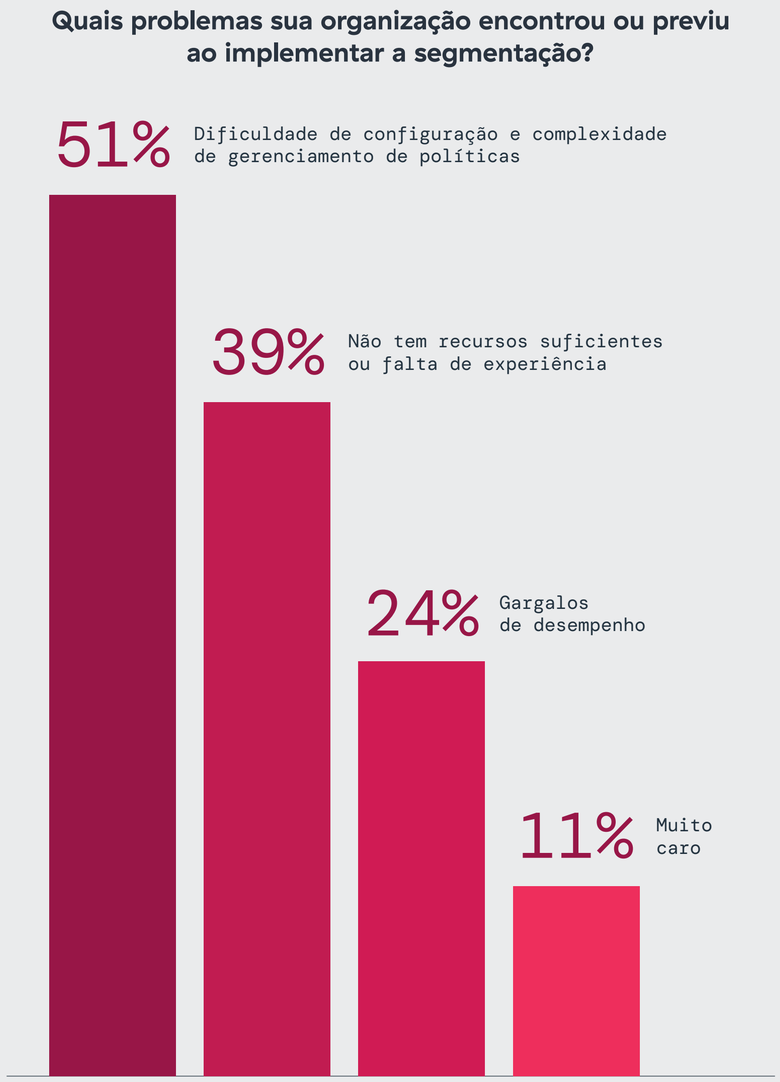


Figura 7: os principais desafios que as empresas enfrentam ao implementar a segmentação.

As VPNs aumentam os riscos de cibersegurança de fusões e aquisições

Além dos desafios de segurança do dia a dia, as principais transições de TI, como fusões e aquisições (M&A), representam riscos adicionais e expandem as superfícies de ataque. Essas transições geralmente envolvem a fusão de redes, aplicativos e identidades diferentes, o que pode levar a vulnerabilidades herdadas, configurações incorretas e controles de segurança fracos.

Quase dois terços (64%) dos entrevistados expressaram preocupação com as ameaças cibernéticas após fusões e aquisições, reconhecendo as brechas de segurança que surgem durante as integrações de TI.

Um exemplo recente é a violação de dados da Capita em 2023, onde invasores exploraram vulnerabilidades de segurança após uma aquisição corporativa, obtendo acesso não autorizado a dados sigilosos. O incidente foi resultado de políticas de segurança desalinhadas entre as entidades da fusão, permitindo que criminosos se movessem lateralmente pela rede recém-integrada. Essa violação destaca como controles de segurança inconsistentes, acesso de VPN legada e ambientes não segmentados criam condições ideais para ataques cibernéticos durante atividades de fusões e aquisições.

Para mitigar esses riscos durante fusões e aquisições, as organizações devem priorizar a devida diligência em cibersegurança, aplicar o acesso de privilégio mínimo e implementar a segmentação. Ao contrário dos modelos de acesso baseados em VPN, o zero trust impede que ambientes de TI mesclados herdem permissões de acesso amplas, reduzindo efetivamente o risco de movimentação lateral e escalada de privilégios. Ao substituir VPNs e defesas baseadas em perímetro por controles de acesso orientados por identidade que validam cada solicitação, as organizações podem proteger ambientes de TI legados e recém-integrados.

Você se preocupa com a vulnerabilidade a ataques cibernéticos após uma fusão ou aquisição?

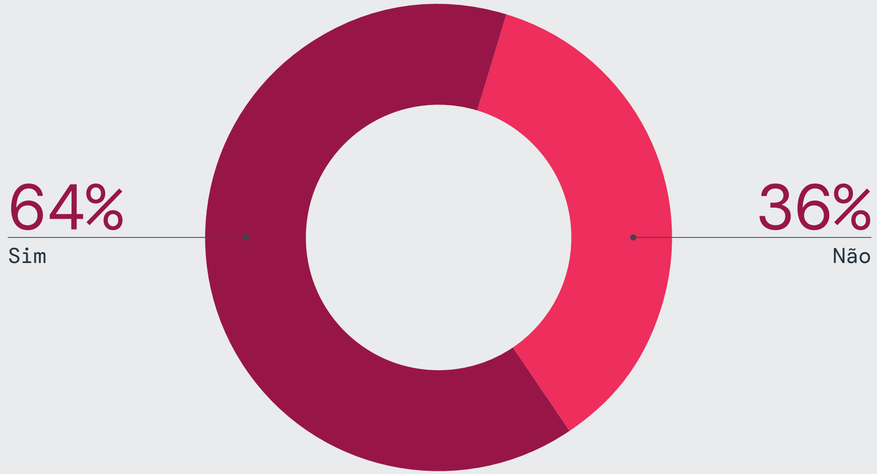


Figura 8: empresas estão preocupadas com ataques cibernéticos após fusões e aquisições

Acesso de terceiros à VPN: uma porta de entrada para invasores

O acesso de terceiros emergiu como um dos pontos de entrada mais vulneráveis para invasores. As VPNs tradicionais, por natureza, dependem de amplo acesso à rede depois que a autenticação é concluída, estendendo esse privilégio a fornecedores e parceiros externos. Essa prática cria pontos cegos que os invasores desejam explorar. Os invasores podem explorar credenciais roubadas ou fracas, configurações incorretas e vulnerabilidades não corrigidas para sequestrar essas conexões confiáveis. Com 93% dos entrevistados expressando preocupações críticas sobre vulnerabilidades de backdoor, o acesso de terceiros representa uma bomba-relógio para organizações que dependem de modelos de acesso estáticos e baseados em confiança.

Essa preocupação é bem fundamentada. Em agosto de 2024, o Enterprise Financial Group (EFG) sofreu uma violação de dados significativa que expôs informações pessoais de quase 20.000 clientes. A violação foi rastreada até vulnerabilidades em uma VPN de terceiros usada pelo EFG, que os invasores exploraram para se infiltrar na rede e acessar dados sigilosos. Esse incidente ressalta como VPNs de terceiros criam brechas de segurança que invasores podem explorar como pontos de entrada em redes corporativas.

As organizações devem começar auditando o acesso à VPN de terceiros e aplicando controles de políticas mais rigorosos, como acesso por tempo limitado, inspeção de tráfego de ponta a ponta (do dispositivo para o aplicativo) e autenticação adaptativa. A transição para um modelo zero trust permitirá a aplicação de acesso específico ao aplicativo, garantindo que parceiros externos tenham apenas o acesso mínimo necessário. Além disso, o monitoramento contínuo e as políticas baseadas em risco podem mitigar significativamente as vulnerabilidades de terceiros.

Qual é o seu nível de preocupação com terceiros servindo como uma possível backdoor para invasores em sua rede por meio do seu acesso de VPN?

93% estão preocupadas com terceiros servindo como possíveis backdoors para suas redes por meio do acesso via VPN

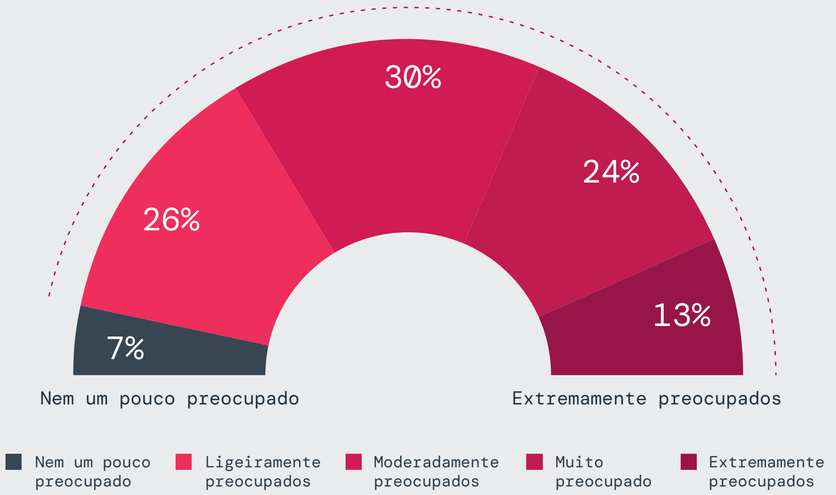


Figura 9: preocupações empresariais sobre o acesso à VPN de terceiros facilitando ataques cibernéticos.

Desafios e falhas das medidas de proteção legadas

As ferramentas tradicionais deixam os aplicativos privados expostos

Proteger aplicativos privados contra ameaças cada vez mais sofisticadas baseadas na web, como ransomware, roubo de credenciais e abuso de API tornou-se uma prioridade crítica para as empresas modernas. Mesmo assim, muitas organizações continuam a depender de ferramentas legadas, mal equipadas para combater o cenário de ameaças atual.

De acordo com a pesquisa, firewalls (84%), firewalls de aplicativos web (WAFs, 58%), e VPNs (43%) ainda dominam as defesas de ataques na web das organizações. No entanto, os invasores estão cada vez mais ignorando essas ferramentas, aproveitando dispositivos sem correções, configurações inadequadas e fraquezas inerentes aos modelos de segurança baseados em perímetro, mostrando que essas defesas legadas não atendem mais às demandas dos cenários de ameaças modernos.

Violações recentes destacam as deficiências dessas defesas baseadas em perímetro. Em agosto de 2024, hackers chineses (um grupo apelidado de Salt Typhoon) infiltraram grandes empresas de telecomunicações dos EUA, incluindo AT&T e Verizon, explorando vulnerabilidades em dispositivos de rede e roteadores sem correções. Esse ataque comprometeu metadados sigilosos de mais de 1 milhão de usuários, demonstrando como adversários sofisticados podem burlar medidas de segurança tradicionais, como firewalls e VPNs.

A única solução viável para proteger aplicativos privados de forma eficaz é ir além das defesas de perímetro obsoletas e adotar modelos de acesso zero trust. As arquiteturas zero trust eliminam a dependência de segurança baseada em rede, permitindo que os usuários se conectem diretamente aos aplicativos sob políticas rigorosamente aplicadas de acesso granular e de privilégio mínimo. Ao contrário de firewalls e VPNs, as arquiteturas zero trust permitem que os usuários se conectem diretamente aos aplicativos com acesso granular e de privilégio mínimo. Essa abordagem bloqueia tentativas de acesso não autorizado e previne movimentação lateral, sequestro de sessão e roubo de credenciais, táticas comumente usadas por invasores para burlar as defesas de perímetro tradicionais.

Quais produtos você usa para proteger seus aplicativos privados contra ataques baseados na web?

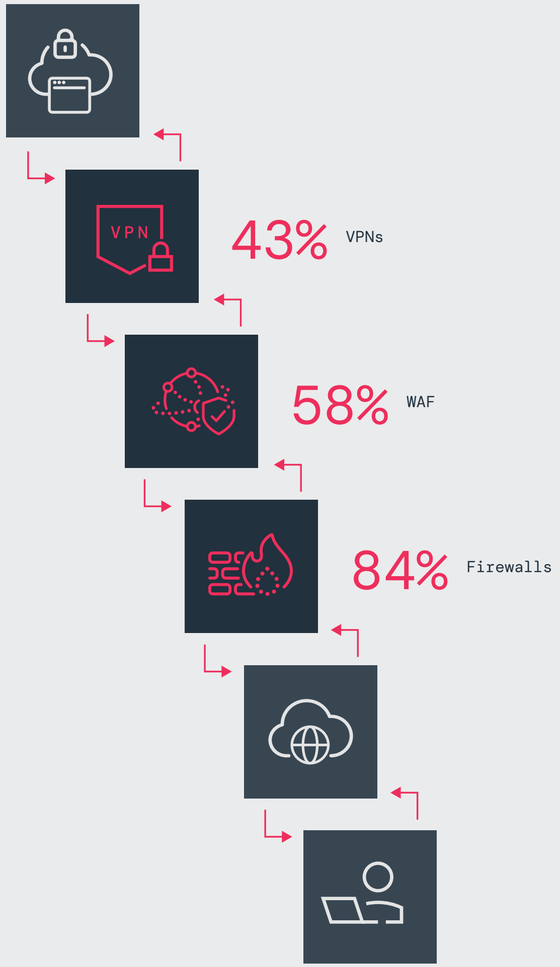


Figura 10: produtos de segurança em uso por empresas para defender aplicativos privados contra ameaças baseadas na web.

Implantação de NAC em ambientes de VPN: uma proteção limitada

Um número notável de 54% das organizações pesquisadas relatam usar NAC para proteger o acesso da VPN a recursos privados. No entanto, essas implantações ainda não conseguiram evitar as violações e explorações comumente associadas às vulnerabilidades da VPN, destacando a incapacidade do NAC de abordar os riscos sistêmicos dos modelos de confiança baseados em rede.

As soluções de NAC aplicam verificações de postura do dispositivo, autenticação e segmentação de rede. No entanto, elas não abordam os principais problemas de segurança da VPN, como permissões de acesso amplas, riscos de movimentação lateral e dependência de confiança implícita.

Violações recentes demonstram que, mesmo com o NAC implementado, as vulnerabilidades de VPN continuam sendo uma fraqueza crítica. Em novembro de 2023, o Departamento de Energia dos EUA confirmou um grande incidente de segurança envolvendo credenciais de VPN comprometidas, o que permitiu que invasores ignorassem os controles de acesso e se infiltrassem em sistemas internos sigilosos. Isso destaca como os invasores podem explorar as fraquezas da VPN diretamente, seja por meio de credenciais roubadas, vulnerabilidades não corrigidas ou sequestro de sessão, tornando o NAC uma defesa incompleta se o modelo de confiança subjacente permanecer inalterado.

Você está usando um NAC (controle de acesso à rede) entre sua VPN e os recursos privados?

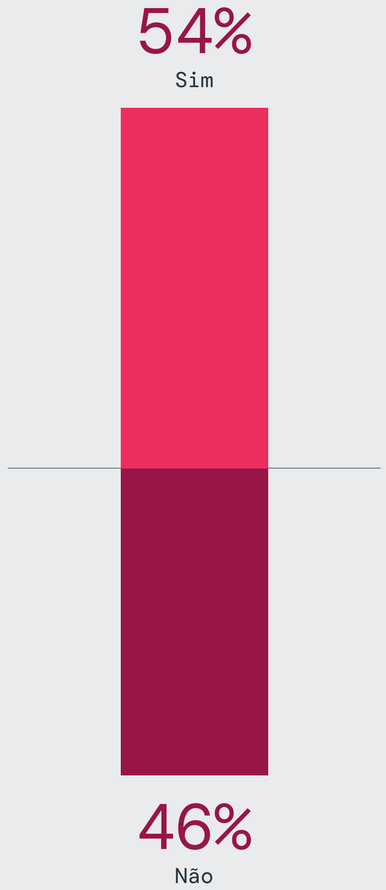


Figura 11: proporção de empresas que usam NAC entre VPNs e recursos privados.

Para superar as limitações das arquiteturas de NAC e VPN legadas, as organizações devem adotar um modelo de segurança zero trust. O zero trust elimina a ampla confiança da rede ao permitir que os usuários se conectem diretamente a aplicativos específicos sob políticas continuamente validadas vinculadas à identidade, postura do dispositivo e contexto. O zero trust não apenas bloqueia acessos não autorizados, mas também impede a movimentação lateral, frustrando invasores antes que eles possam aumentar privilégios ou exfiltrar dados.

Problemas de gerenciamento_e de experiência de usuário da VPN

O problema de desempenho da VPN: frustrando usuários e sobrecarregando a TI

As VPNs não são apenas um risco de segurança; elas também são uma grande fonte de insatisfação dos usuários. Os usuários finais expressam cada vez mais frustrações com problemas de desempenho da VPN, o que cria obstáculos para a produtividade e aumenta a pressão sobre as equipes de TI.

Velocidades de conexão lentas são a reclamação mais comum (23%), ressaltando a reputação das VPNs quanto à latência, congestionamento e baixo desempenho ao acessar aplicativos na nuvem a partir de casa. Os desafios de autenticação também continuam sendo um problema significativo, com 20% dos entrevistados citando processos de login complexos e 17% tendo dificuldades para acessar aplicativos devido a erros de autenticação.

Esses desafios de desempenho interrompem as operações comerciais diárias, reduzem a produtividade e transformam o suporte técnico de TI em um gargalo, enquanto as equipes lutam com frequentes solicitações de solução de problemas; um problema que só piora à medida que os ambientes de trabalho remoto e híbrido aumentam em complexidade.

A substituição de VPNs por acesso à rede zero trust (ZTNA) não apenas elimina o congestionamento de largura de banda, mas também melhora muito a experiência do usuário final, oferecendo conexões diretas, seguras e sem latência aos aplicativos. Ao contrário das VPNs, que roteiam todo o tráfego por meio de um gateway central e criam gargalos de desempenho, o ZTNA oferece acesso direto e seguro aos aplicativos sem degradação do desempenho. Ao adotar controles de acesso orientados por identidade, verificação contínua e segurança disponibilizada na nuvem, as organizações podem não apenas eliminar frustrações comuns com a VPN, mas também aumentar a produtividade das equipes de trabalho e reduzir a carga da TI relacionada à solução de problemas e suporte a estruturas de VPN inflexíveis.

Qual é a queixa mais comum relatada por seus usuários ao acessar aplicativos via VPN?

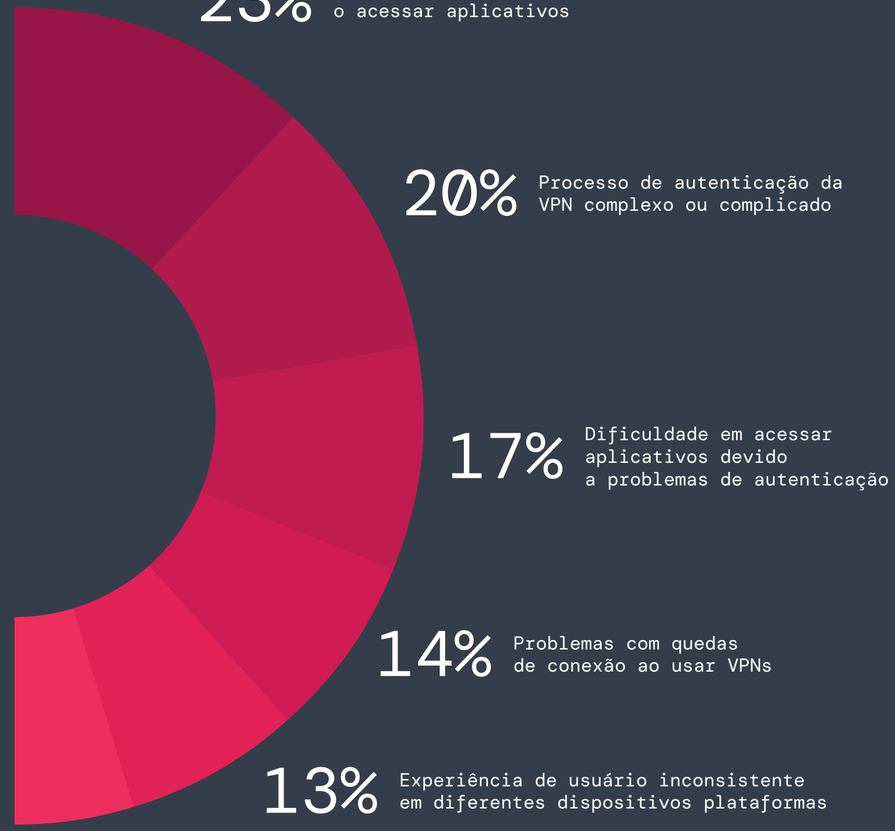


Figura 12: as reclamações mais comuns entre usuários de VPN.

Gerenciamento de VPN: sobrecarregando equipes de TI e expondo vulnerabilidades

As VPNs estão sobrecarregando as equipes de TI com vulnerabilidades de segurança persistentes, demandas de manutenção pesadas em termos de recursos e modelos de acesso desatualizados que não atendem mais às necessidades dos ambientes empresariais atuais focados na nuvem. A principal preocupação entre essas equipes (52%) são falhas de segurança que levarão a incidentes de segurança, ressaltando os riscos contínuos relacionados ao roubo de credenciais, exploits de software sem correção e invasores que aproveitam o acesso via VPN para movimentação lateral sem controles. Esses riscos ressaltam por que as VPNs são cada vez mais vistas como soluções de acesso com alto risco de vulnerabilidade.

As VPNs se tornaram um dreno financeiro e operacional para as equipes de TI, com 41% dos entrevistados destacando custos exorbitantes de recursos vinculados à sua manutenção. O ciclo implacável de aplicação de correções, solução de problemas e monitoramento de logs é necessário para proteger uma infraestrutura desatualizada, mas deixa as equipes sobrecarregadas e incapazes de se concentrar em atividades de maior valor.

A incapacidade das VPNs de aplicar controles de acesso granulares é outra fraqueza crítica, citada por 35% dos entrevistados. Em vez de conceder acesso preciso e baseado em identidade a aplicativos específicos, as VPNs geralmente fornecem conectividade de rede ampla e irrestrita, aumentando drasticamente o potencial de ameaças internas e movimentação lateral de invasores. Além disso, 26% citam a sobrecarga operacional do gerenciamento de concentradores de VPN e outros dispositivos, ilustrando a complexidade de manter dispositivos de hardware, túneis de rede e gateways de acesso para sustentar a conectividade remota. Essas complexidades são especialmente insustentáveis em uma era em que ambientes de trabalho remotos e nativos da nuvem exigem soluções mais ágeis e dimensionáveis.

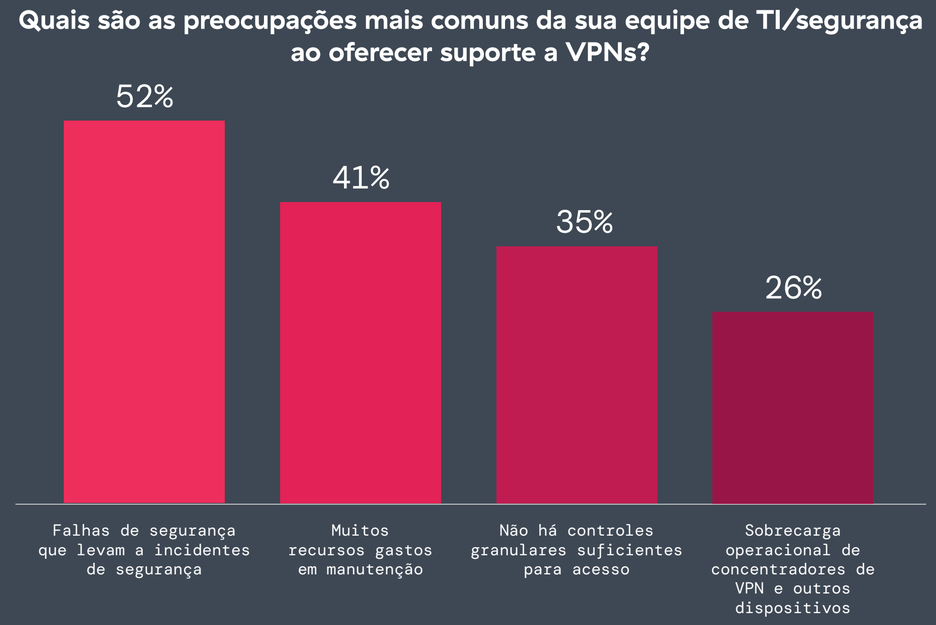


Figura 13: as principais preocupações das equipes de TI e segurança ao dar suporte a VPNs.

Para enfrentar esses desafios, as organizações devem fazer a transição do acesso de VPN baseado em rede para um modelo zero trust disponibilizado na nuvem, que elimina a confiança implícita, reduz as superfícies de ataque e otimiza as operações de TI. A adoção do zero trust reduz a sobrecarga operacional relacionada à VPN, simplifica o gerenciamento de acesso e minimiza os riscos de segurança em escala. As equipes de TI ficam livres do fardo das constantes tarefas de manutenção, o que permite que elas se concentrem em iniciativas de segurança proativas e, ao mesmo tempo, ofereçam experiências de usuário mais rápidas e integradas.

O pesado fardo do gerenciamento de VPN

O gerenciamento da infraestrutura de VPN continua sobrecarregando as equipes de TI, com as principais preocupações centradas na confiabilidade, no desempenho e na sobrecarga de manutenção. Solucionar problemas de conectividade e estabilidade da VPN continua sendo o principal desafio, citado por 54% dos entrevistados. As equipes de TI enfrentam dificuldades constantes para manter o tempo de atividade consistente da VPN, com falhas de conexão criando interrupções generalizadas que degradam a produtividade, comprometem a segurança e frustram os funcionários.

Equilibrar o desempenho da VPN e a experiência de usuário continua sendo um desafio significativo (50%), já que as VPNs geralmente introduzem latência, desconexões e velocidades inconsistentes, especialmente em ambientes que priorizam a nuvem. Além disso, 47% dos profissionais de TI destacam as demandas frequentes de correções e os custos de recursos como um grande obstáculo, ressaltando os desafios operacionais de mitigar vulnerabilidades persistentes e manter sistemas desatualizados.

Esses desafios desempenharam um papel em diversas violações de alto perfil. De dezembro de 2023 até o início de 2024, diversas agências governamentais foram alvos de um ataque relacionado à VPN. Atrasos na correção de uma vulnerabilidade amplamente conhecida permitiram que cibercriminosos explorassem softwares VPN desatualizadas, obtendo acesso não autorizado à rede. Esse caso destaca a inadequação de ciclos de aplicação de correções reativos, mesmo entre organizações com equipes de TI dedicadas, e demonstra como defesas de VPN incompletas expõem setores críticos a ameaças em evolução.

Com a infraestrutura de VPN consumindo recursos de TI significativos para solução de problemas de conectividade, aplicação de correções de segurança e otimização de desempenho, as organizações devem reavaliar a viabilidade a longo prazo do acesso baseado em VPN. Ao substituir concentradores de VPN e dispositivos de rede, como firewalls e NACs, por uma arquitetura nativa da nuvem, as equipes de TI podem eliminar gargalos de infraestrutura, reduzir ciclos de aplicação de correções e eliminar a necessidade de solução de problemas manuais de falhas de conexão.

O acesso de privilégio mínimo e orientado por políticas garante que os usuários se conectem apenas a aplicativos autorizados, sem o fardo de gerenciar regras complexas de firewall ou políticas de segmentação de rede. Ao fazer a transição para um modelo zero trust disponibilizado na nuvem, as empresas poderão eliminar gargalos relacionados à VPN, garantindo ao mesmo tempo acesso contínuo e orientado por políticas aos aplicativos, sem o fardo de gerenciar infraestrutura de rede, correções de software ou esforços complexos de dimensionamento.

Quais são as três principais preocupações no gerenciamento da sua infraestrutura de VPN?

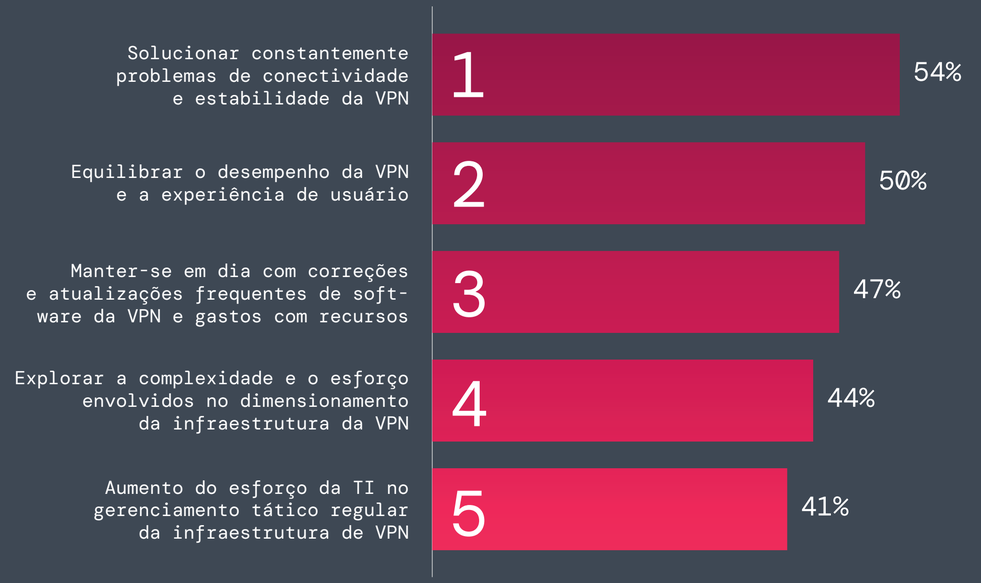


Figura 14: as principais preocupações entre as equipes de TI no gerenciamento da infraestrutura de VPN.

Controles de acesso à VPN excessivamente amplos: uma falha crítica de segurança

A principal causa de muitos riscos de segurança da VPN está na forma como as VPNs definem o acesso. Em vez de fornecer acesso preciso e específico ao aplicativo, muitas organizações ainda concedem amplo acesso à rede e contam com modelos de confiança implícita, deixando sistemas críticos expostos.

Os resultados da pesquisa revelam que 52% das organizações ainda dependem de modelos de acesso desatualizados, como regras de firewall de rede estática (28%) ou acesso aberto para usuários autenticados (24%). Esses controles desatualizados facilitam a passagem de invasores pelas redes sem serem detectados, aumentam privilégios e exfiltram dados críticos quando o acesso é obtido.

Incidentes recentes ressaltam os perigos de um acesso tão amplo. No início de 2024, a Global Affairs Canada (GAC) sofreu uma violação de segurança significativa devido a uma VPN comprometida usada por funcionários para acessar a sede em Ottawa. Os invasores exploraram vulnerabilidades na VPN, obtendo acesso não autorizado à rede e potencialmente expondo informações sigilosas. O evento demonstrou como o acesso irrestrito e privilegiado à rede fornece uma estrutura ideal para movimentação lateral e infiltração mais profunda.

Para mitigar esses riscos, as organizações devem eliminar a confiança implícita e aplicar controles de acesso granulares e baseados em identidade. A mudança de modelos de acesso amplos baseados em rede para segmentação direta no nível do aplicativo garante que um determinado usuário possa acessar somente os recursos específicos necessários para sua função, reduzindo significativamente as superfícies de ataque e impedindo a movimentação lateral.

Como você define o acesso dos usuários da VPN aos aplicativos?

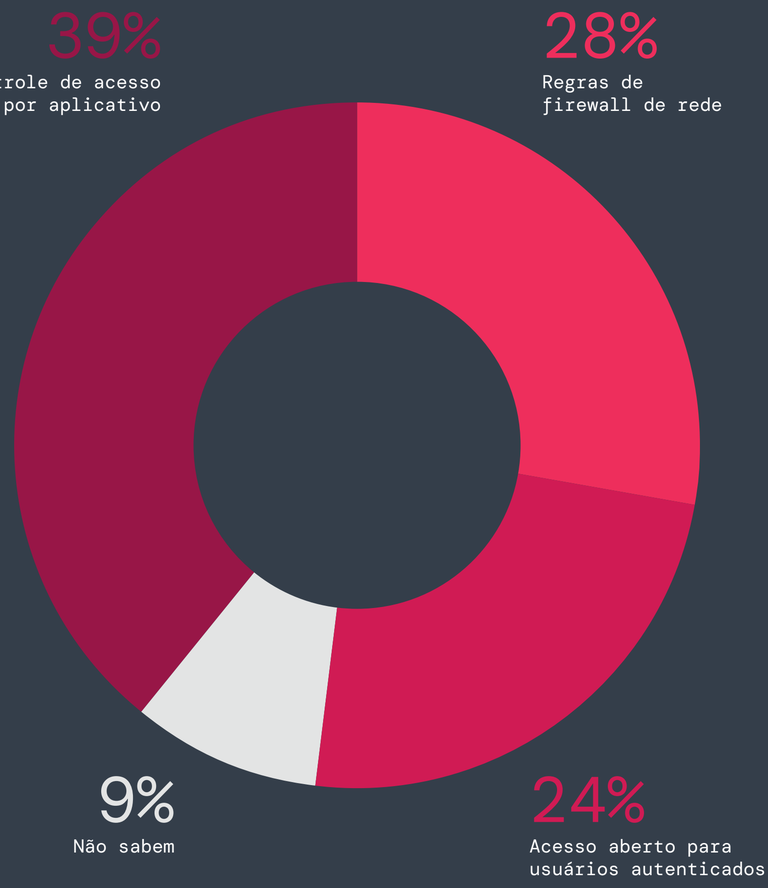


Figura 15: as maneiras como as empresas definem o acesso dos usuários de VPN aos aplicativos.

Substituição da VPN: uma mudança em direção ao acesso seguro

As crescentes vulnerabilidades de segurança, os desafios da experiência de usuário e a alta sobrecarga de manutenção das VPNs estão levando as organizações a acelerar sua transição para tecnologias modernas de acesso seguro, como o ZTNA. Essa mudança sinaliza a crescente percepção de que as VPNs não são mais capazes de atender às demandas modernas de segurança ou operacionais.

A pesquisa confirma isso, com 65% dos entrevistados dizendo que suas organizações estão substituindo ou planejando substituir suas VPNs no próximo ano.

À medida que as organizações estão cada vez mais abandonando as VPNs, elas devem priorizar a adoção de modelos de segurança disponibilizados na nuvem que apliquem acesso granular no nível do aplicativo em vez de ampla conectividade de rede. O ZTNA elimina os riscos relacionados à VPN garantindo que os usuários possam acessar apenas os recursos de que precisam, com base na identidade e na postura de segurança, sem nunca colocá-los na rede corporativa. Essa abordagem aumenta a segurança, reduz a complexidade operacional e melhora a experiência dos usuários, tornando a substituição da VPN uma etapa urgente e necessária para empresas modernas.

Quais são seus planos para substituir seu serviço de VPN atual?

65%

das organizações têm um plano em vigor para substituir seus serviços de VPN existentes

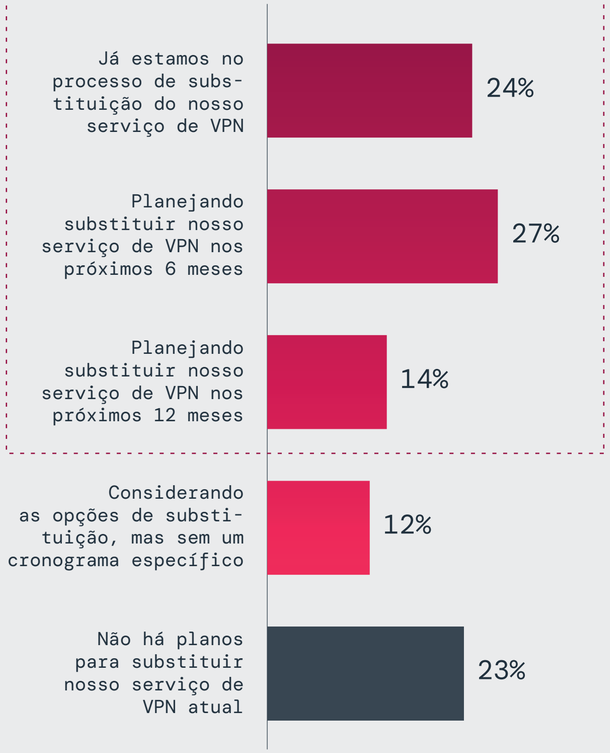
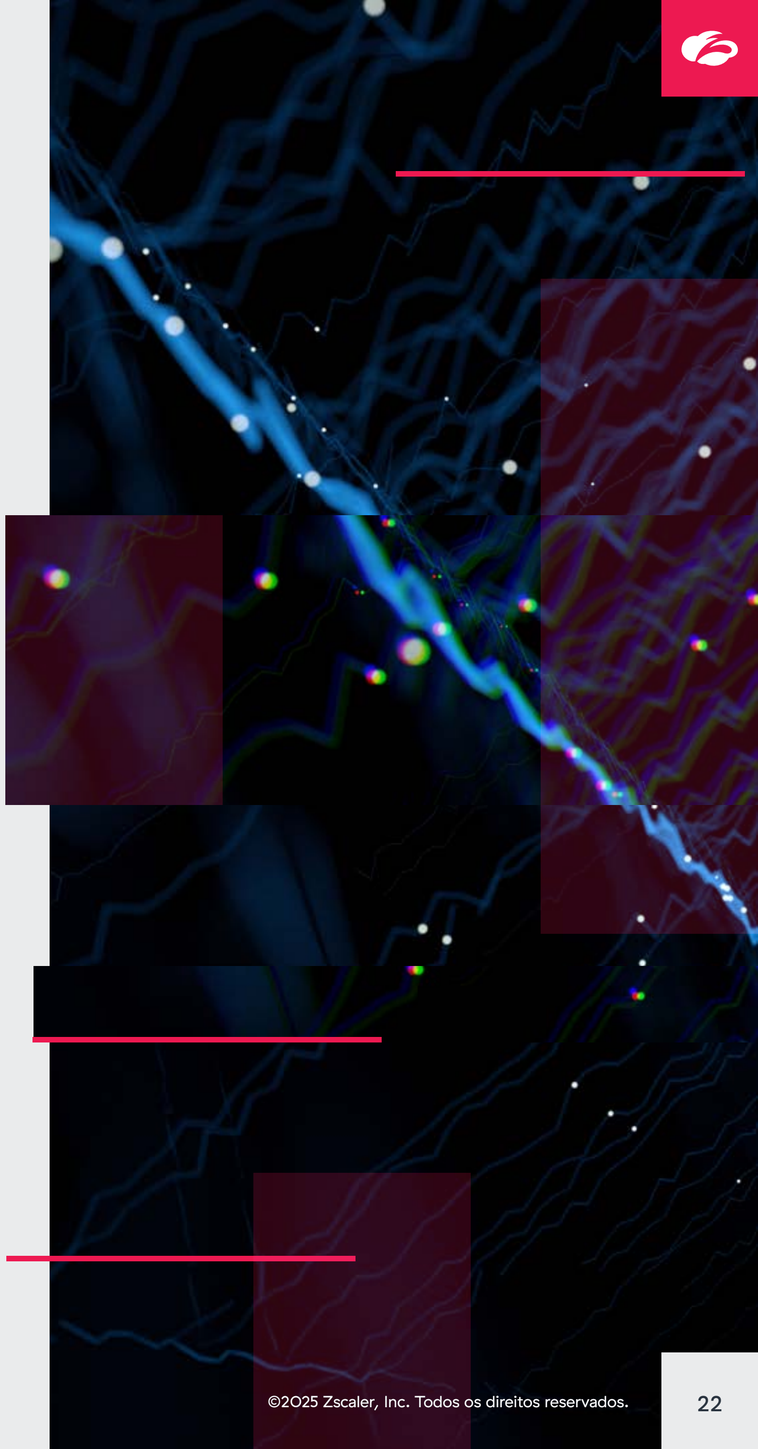


Figura 16: planos empresariais para substituir serviços de VPN existentes.



Adoção_ do zero trust

O zero trust substitui a VPN em grande escala

À medida que a tendência de substituição da VPN se acelera, a grande maioria das organizações está recorrendo a arquiteturas zero trust para oferecer controles de acesso granulares, reduzir suas superfícies de ataque e melhorar a produtividade dos usuários. Os resultados da pesquisa ressaltam a dinâmica crescente dessa mudança de paradigma: 81% dos entrevistados indicam ter planos de o adotar zero trust este ano. Entre eles, 35% já estão implementando soluções de zero trust, 24% preveem implementações dentro de seis meses e 22% têm estratégias de implantação programadas para o ano seguinte, mostrando o zero trust como a estratégia líder do setor para substituir tecnologias de acesso legadas, como VPNs.

A adoção bem-sucedida do zero trust exige alinhamento entre as equipes de segurança e as operações comerciais. As organizações devem realizar avaliações de risco para identificar seus pontos de acesso mais vulneráveis, seja acesso remoto, integrações de terceiros ou aplicativos críticos, e priorizar a implantação do zero trust adequadamente. Aproveitar a automação para aplicação de políticas pode acelerar a transição e, ao mesmo tempo, reduzir a sobrecarga administrativa.

Quais são os seus planos para adotar uma estratégia zero trust na sua organização?

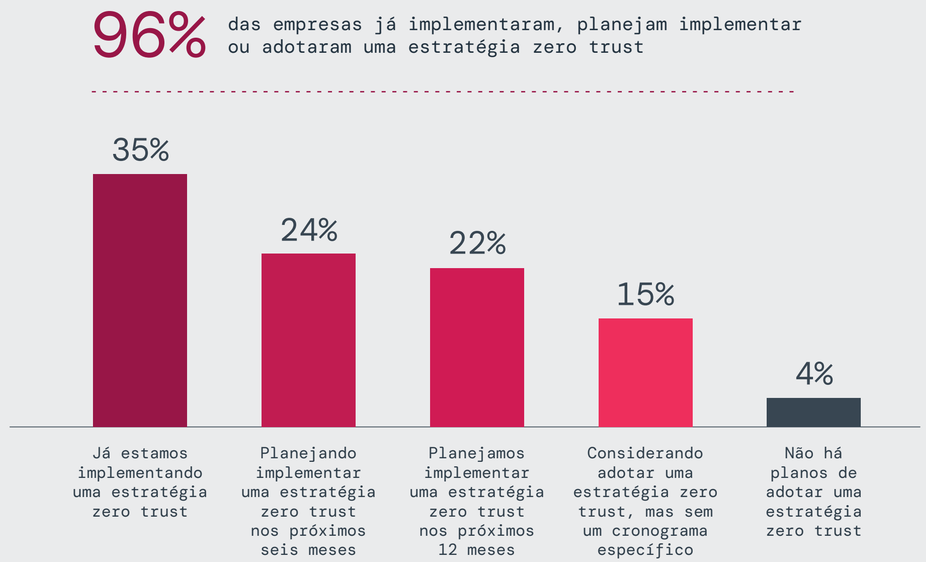


Figura 17: planos empresariais para implementar uma estratégia zero trust.

Prioridades do zero trust: o trabalho remoto promove a adoção

O abandono das VPNs tradicionais ressalta uma transformação importante: as organizações estão recorrendo a arquiteturas zero trust para abordar falhas de segurança, otimizar as operações de TI e atender às demandas de equipes de trabalho remotas descentralizadas. Essa mudança estratégica destaca o zero trust como a solução moderna para mitigar os riscos de VPN e simplificar o gerenciamento de segurança.

Os resultados da pesquisa indicam que proteger equipes de trabalho remotas é a principal motivação para essa mudança, com 37% das organizações se concentrando no trabalho remoto e 28% na segurança das equipes de trabalho híbridas. Essa mudança reflete uma tendência mais ampla em direção a modelos de segurança que oferecem acesso direto e específico a aplicativos, reduzindo assim as complexidades associadas ao gerenciamento de vários produtos específicos inerentes às configurações de VPN legadas.

Implementar uma estrutura zero trust não apenas fortalece a segurança, mas também alivia a sobrecarga operacional de gerenciar inúmeras soluções de segurança. Ao unificar as políticas e os controles de segurança em um sistema coeso, as organizações podem reduzir a sobrecarga administrativa e otimizar as operações. Por exemplo, uma plataforma zero trust que executa várias ações de políticas em uma única verificação pode eliminar a necessidade de encadear várias soluções, simplificando a experiência de usuário e mantendo uma segurança robusta.

Para proteger efetivamente equipes de trabalho remotas e híbridas com uma arquitetura zero trust, as organizações devem se concentrar na integração de medidas de segurança que minimizem a complexidade. A implementação de uma plataforma zero trust unificada pode consolidar várias funções de segurança, reduzindo a necessidade de utilizar vários produtos específicos e simplificando o gerenciamento. Essa abordagem melhora a segurança e a eficiência operacional, permitindo que as equipes de TI se concentrem em iniciativas estratégicas em vez de gerenciar uma gama complexa de ferramentas de segurança.

Qual é o principal caso de uso para implantar uma solução zero trust?

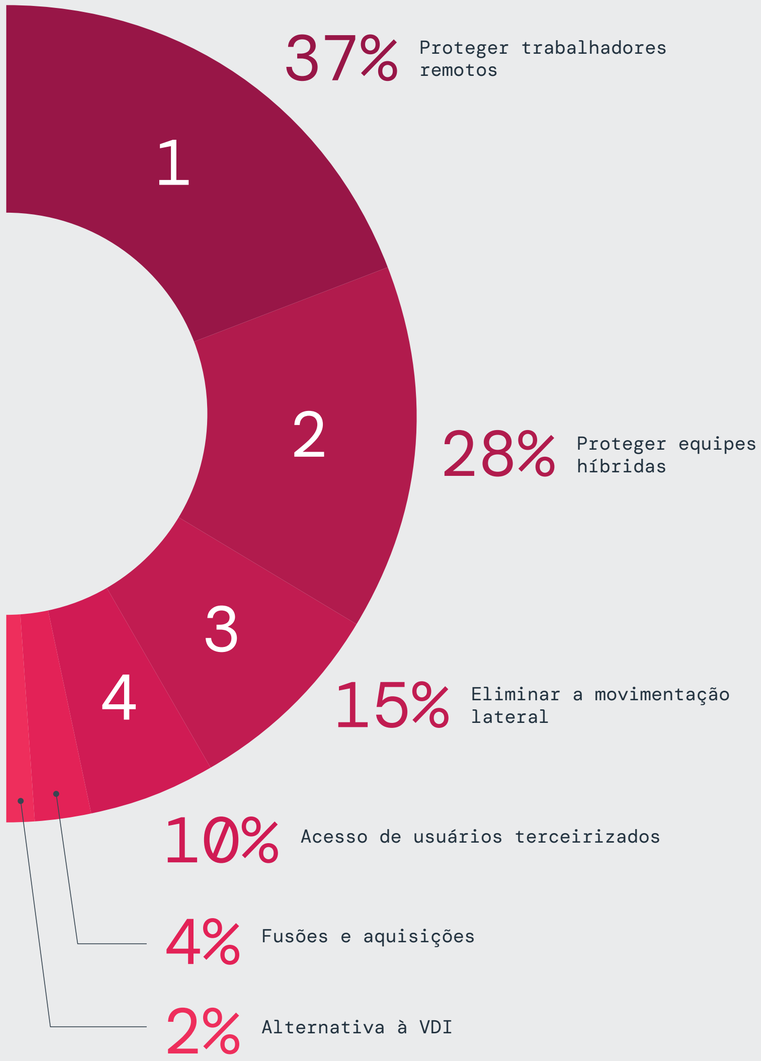


Figura 18: principais casos de uso de soluções de zero trust por parte das empresas.

Principais vantagens de substituir as VPNs por zero trust

A adoção de soluções de zero trust está transformando a segurança empresarial, oferecendo benefícios de longo alcance que vão além do acesso seguro, principalmente na simplificação do gerenciamento, na melhoria do desempenho e da capacidade de dimensionamento, na redução drástica da superfície de ataque e na melhoria da eficiência dos recursos. As organizações que substituem modelos de VPN por zero trust não estão apenas atualizando ferramentas; elas estão preparando toda a sua estratégia de acesso remoto para o futuro.

A grande maioria dos entrevistados (76%) vê a segurança e a conformidade aprimoradas como uma vantagem primária, reforçando como o zero trust substitui o acesso implícito à rede e reduz a exposição a ataques de ransomware, roubo de credenciais e riscos de movimentação lateral.

Além disso, 64% relatam ganhos em simplicidade de gerenciamento, capacidade de dimensionamento e experiência do usuário como uma vantagem primária, já que o zero trust elimina os encargos operacionais do gerenciamento de concentradores de VPN, aplicação constante de correções e solução de problemas de acesso.

Quase metade (45%) dos entrevistados citam a substituição da VPN por uma solução de zero trust como um passo crítico em direção a uma arquitetura zero trust completa. Enquanto isso, 34% destacam a capacidade de dimensionamento e a flexibilidade superiores que tornam o zero trust uma solução mais eficaz para proteger equipes de trabalho remotas e híbridas. Outros benefícios se somam ao perfil de valor do zero trust: melhor experiência do usuário final (32%), integrações perfeitas entre sistemas de TI e segurança (28%) e redução de custos operacionais por meio da economia de recursos (18%). Coletivamente, essas vantagens ilustram por que as organizações estão rapidamente abandonando VPNs legadas em favor do zero trust.

O ManpowerGroup, líder global em soluções de equipes de trabalho, oferece um estudo de caso convincente sobre como proteger o acesso com zero trust. Diante da tarefa de oferecer suporte a uma vasta mão de obra remota, a organização substituiu com sucesso sua infraestrutura de VPN legada por uma solução zero trust da Zscaler. Notavelmente, em apenas 18 dias, o ManpowerGroup ampliou o acesso seguro a aplicativos para mais de 30.000 usuários, alcançando continuidade ininterrupta dos negócios e reduzindo drasticamente os incidentes de suporte técnico em 97%. Essa implantação destaca a capacidade de uma arquitetura zero trust de expandir rapidamente, simplificar operações e gerar resultados mensuráveis para produtividade e segurança.

Se você substituiu uma solução de VPN por uma solução de zero trust, quais você considera as principais vantagens em comparação à solução de VPN anterior?

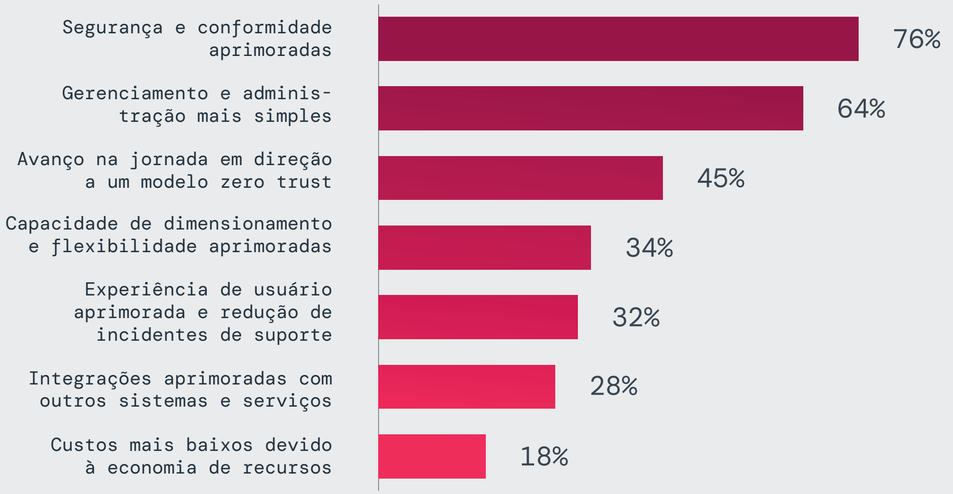


Figura 19: as empresas compartilham as principais vantagens de uma solução zero trust, em comparação com uma solução de VPN anterior.

A adoção do zero trust deve começar com mudanças táticas que eliminem o acesso à rede orientado por VPN em favor de conexões diretas em nível de aplicativo para combater riscos de movimentação lateral. As organizações podem priorizar a substituição do acesso legado para casos de uso críticos, como a proteção de conexões de usuários remotos e de terceiros, antes de ampliar os recursos de zero trust para todo o seu ecossistema de TI. Automatizar as políticas de acesso (usando um único conjunto de políticas) e integrar a segurança baseada em identidade simplificará ainda mais o gerenciamento do zero trust, oferecendo capacidade de dimensionamento entre sistemas distribuídos. Essas estruturas inteligentes capacitam as equipes de TI a manter o controle da segurança em tempo real sem sacrificar a agilidade ou a eficiência.

Previsões de riscos da VPN para_2025

Vulnerabilidades críticas de VPN continuarão a surgir

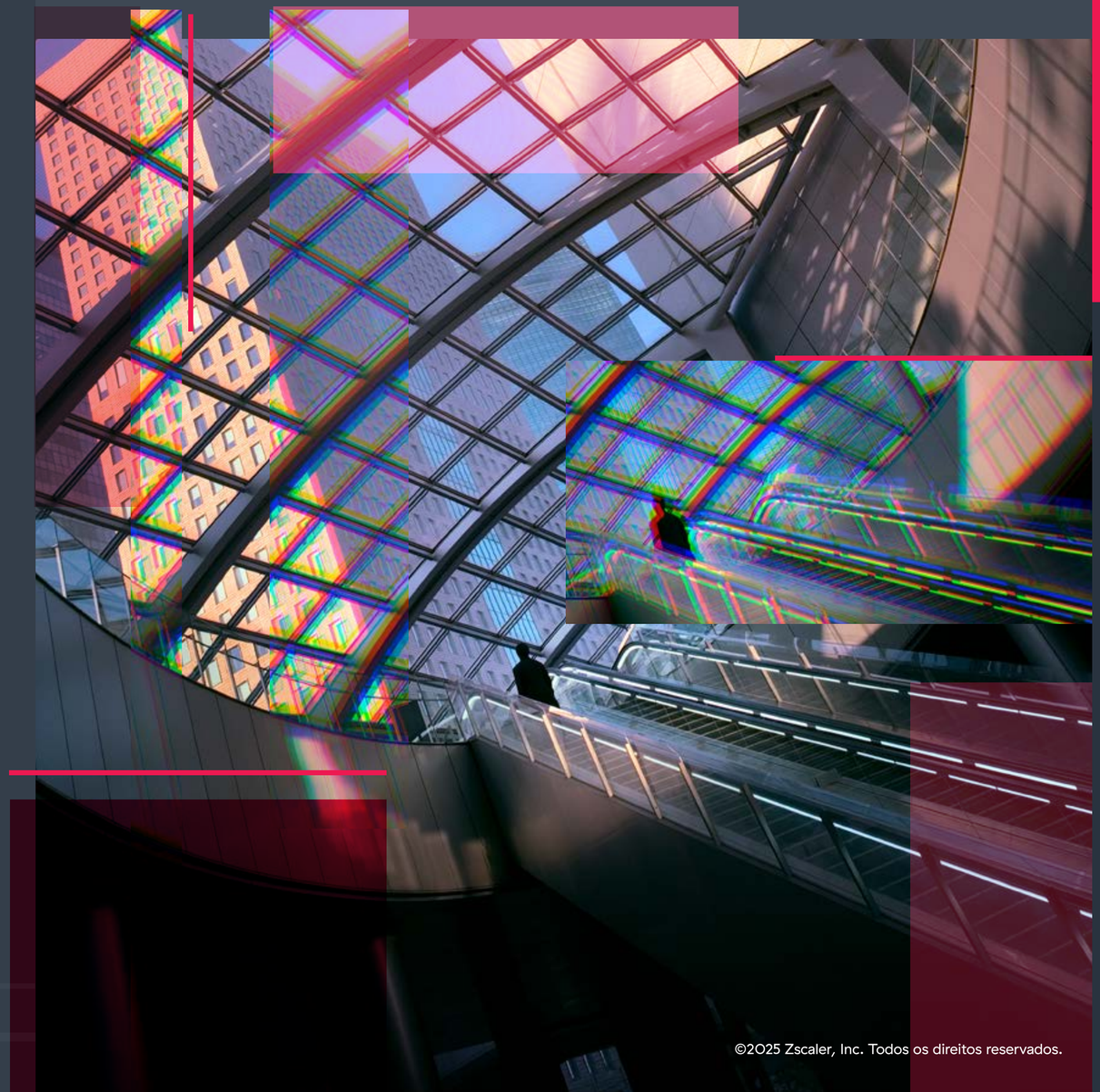
O número crescente de exploits de VPN nos últimos anos acelerará em 2025. As tecnologias de VPN são um alvo primário dos invasores porque expõem as empresas à internet, tornando as vulnerabilidades fáceis de verificar e explorar. À medida que as organizações lutam para corrigir falhas de VPN a tempo, os invasores continuarão a descobrir e a transformar novas vulnerabilidades de alta gravidade em armas, como visto na violação da Ivanti Pulse Secure em janeiro de 2025. Pesquisadores de segurança e criminosos cibernéticos estão investigando ativamente as infraestruturas de VPN, tornando inevitáveis as divulgações contínuas de CVEs críticas.

Os grupos de ransomware intensificarão exploits de VPN

Como 92% dos entrevistados expressaram preocupação com vulnerabilidades de VPN não corrigidas, os ataques de ransomware continuarão a explorar falhas de VPN conhecidas e de dia zero como o principal método de acesso inicial. Grupos de ransomware como serviço (RaaS) frequentemente verificam VPNs expostas com vulnerabilidades não corrigidas, permitindo que eles implantem ransomware antes que as equipes de TI possam responder. A campanha de ransomware de janeiro de 2025 direcionada a organizações de saúde dos EUA demonstra como as falhas de segurança de VPN oferecem aos invasores acesso direto a sistemas sigilosos. À medida que esses ataques se tornam mais automatizados, a necessidade de transição para a segurança zero trust se tornará ainda mais urgente.

A movimentação lateral via VPNs gerará ataques mais destrutivos

Os invasores exploram o amplo acesso fornecido pelas VPNs para se movimentar lateralmente, aumentar privilégios e exfiltrar dados, algumas das técnicas mais eficazes usadas por criminosos cibernéticos e agentes a serviço de governos. Com 71% das organizações preocupadas com esse risco, a segmentação de rede é frequentemente vista como uma solução, mas sua complexidade dificulta a implementação. Muitas organizações não têm pessoal qualificado para gerenciar a segmentação de forma eficaz, o que leva a projetos que levam meses para serem concluídos ou paralisam completamente. Para atenuar esses desafios, as empresas devem adotar a segmentação zero trust, que aplica acesso de privilégio mínimo aos aplicativos, eliminando rotas de movimentação lateral sem o ônus operacional da segmentação de rede tradicional.



O acesso à VPN por terceiros continuará sendo um vetor de ameaça importante

Como 93% dos entrevistados expressaram preocupação com vulnerabilidades de VPN de terceiros, os invasores continuarão mirando pontos de acesso externos fracos. Credenciais de terceiros roubadas e acessos à VPN mal configurados continuam entre os principais pontos de entrada dos criminosos cibernéticos. A violação do Enterprise Financial Group (EFG) de 2024 demonstrou como os invasores exploram conexões de VPN de terceiros para se infiltrar em ambientes corporativos. Muitas organizações não têm visibilidade das permissões de acesso de terceiros, dificultando a aplicação de políticas de segurança. Para mitigar esses riscos, as organizações devem fazer a transição para uma estrutura zero trust, aplicando acesso de privlégio mínimo e verificação contínua para todas as conexões externas.

As explorações de VPN baseadas em IA aumentarão

O aumento de ataques cibernéticos impulsionados por IA impactará a segurança das VPNs de maneiras sem precedentes. Os invasores utilizarão cada vez mais a IA para reconhecimento automatizado, pulverização inteligente de senhas e desenvolvimento rápido de exploits, permitindo-lhes comprometer credenciais de VPN em grande escala. Técnicas de evasão impulsionadas por IA tornarão ainda mais difícil a detecção de intrusões baseadas em VPNs antes que danos significativos ocorram. Enquanto isso, soluções de segurança de VPN impulsionadas por IA podem introduzir brechas de segurança imprevistas, levando a novos vetores de ataque que os cibercriminosos explorarão. À medida que as ameaças impulsionadas por IA aumentam, as organizações devem adotar medidas de segurança proativas, como verificação contínua de identidade e controles de acesso zero trust.

Grandes violações relacionadas à VPN serão manchetes

Após várias violações de alto perfil em 2024, as organizações enfrentarão maior pressão para divulgar incidentes cibernéticos relacionados à VPN. Com as novas regulamentações da SEC exigindo transparência sobre riscos de cibersegurança, as organizações que sofrem com exploits de VPN enfrentarão maior escrutínio regulatório, danos à reputação e possíveis penalidades financeiras. Como as VPNs continuam a servir como principal ponto de entrada para ataques, as organizações serão forçadas a reavaliar modelos de acesso legados, acelerando a migração em direção à segurança zero trust.

Os investimentos em zero trust aumentarão com o declínio das VPNs

Com 65% das organizações já substituindo ou planejando substituir suas VPNs dentro de um ano, o investimento em segurança zero trust está acelerando, remodelando fundamentalmente o cenário de acesso remoto. Os requisitos regulatórios e as exigências de seguro cibernético estão pressionando as organizações a irem além das VPNs, pois as soluções legadas não atendem às demandas de segurança, capacidade de dimensionamento e conformidade. A adoção do zero trust não apenas reduz o risco cibernético, mas também elimina os altos custos de manutenção de concentradores de VPN, dispositivos de rede e ciclos contínuos de aplicação de correções. Como resultado, as VPNs são cada vez mais vistas como obsoletas, o que leva a uma mudança em todo o setor em direção a modelos de segurança zero trust.

Essas previsões destacam um consenso crescente: organizações que adiarem a adoção do zero trust permanecerão altamente vulneráveis à medida que as explorações de VPN aumentarem. O futuro do acesso seguro depende da mitigação proativa de riscos, não de correções reativas, tornando agora o momento de ir além das VPNs.

Práticas recomendadas de acesso_seguro

Reduza os riscos da VPN e fortaleça a segurança zero trust

1. **Remova o acesso baseado em rede para minimizar a superfície de ataque.** Impeça que invasores explorem pontos de entrada de rede expostos, eliminando gradualmente VPNs e acesso baseado em rede em favor da conectividade direta e específica para cada aplicativo. Dados da pesquisa mostram que 54% das organizações citam os riscos de segurança como seu principal desafio com VPNs, reforçando a necessidade de remover dependências de VPN e modelos de segurança baseados em firewall que expõem as empresas a ataques.

2. **Impeça o comprometimento inicial com a prevenção de ameaças em linha.** Inspecione todo o tráfego criptografado e não criptografado em linha para bloquear exploits de dia zero, malware e payloads de ransomware antes que cheguem aos usuários. Como 92% das organizações se preocupam com ransomwares direcionados a vulnerabilidades de VPN, a inspeção de tráfego em tempo real e o bloqueio baseado em políticas são essenciais. Um modelo de segurança nativo da nuvem elimina a necessidade de firewalls locais e reduz a superfície de ataque.

3. **Fortaleça a autenticação e a segurança da identidade.** Implemente autenticação multifator (MFA) resistente a phishing, como credenciais FIDO2, biometria ou tokens de hardware para verificar o acesso do usuário. Evite métodos de autenticação legados, como MFA por SMS e notificações push, que os invasores frequentemente contornam. Integre a segurança orientada por identidade com a verificação contínua, em vez de depender de autenticação única.

4. **Aplique o acesso de privilégio mínimo e baseado em contexto com o ZTNA.** Substitua o amplo acesso da VPN pelo acesso à rede zero trust (ZTNA) para garantir que os usuários se conectem apenas a aplicativos autorizados, nunca à própria rede. Controles de acesso granulares e just-in-time (JIT) baseados em identidade, postura do dispositivo e análise de risco em tempo real garantem que os usuários acessem apenas o que precisam, quando precisam.

5. **Elimine a movimentação lateral com a segmentação zero trust.** Conecte os usuários diretamente aos aplicativos, e não à rede, para impedir que invasores se movam pelos sistemas caso obtenham acesso inicial. A segmentação zero trust e a microssegmentação com reconhecimento de identidade garantem que, mesmo que um usuário seja comprometido, um invasor não possa migrar para outros recursos ou aumentar privilégios. O ZTNA elimina os túneis de VPN, que são um importante facilitador da movimentação lateral.

6. **Proteja o acesso de terceiros e externo com controles baseados em identidade.** Aplique o acesso de privilégio mínimo para terceiros, fornecedores e prestadores de serviço, aplicando controles rigorosos de sessão, verificações de integridade do dispositivo e monitoramento contínuo. Substituir o acesso de terceiros baseado em VPN pelo ZTNA reduz significativamente a exposição ao risco de credenciais de fornecedores comprometidas, uma mudança bem-vinda para os 93% das organizações preocupadas com os riscos de VPNs de terceiros.

7. **Aprimore a proteção de dados com políticas zero trust integradas.** Implante controles integrados de prevenção contra perda de dados (DLP) e agentes de segurança de acesso à nuvem (CASB) para inspecionar, criptografar e impedir a movimentação não autorizada de dados em tempo real. Uma estrutura de segurança zero trust garante que todo o tráfego de usuário seja inspecionado e controlado, mesmo em aplicativos SaaS e ambientes de nuvem.

8. **Implemente segurança orientada por IA e monitoramento contínuo.** Utilize análises em tempo real, tecnologia de prevenção de fraudes e detecção comportamental automatizada com tecnologia de IA para interromper ameaças antes que elas se agravem. As soluções de ZTNA oferecem pontuação de risco em tempo real, impedindo que contas comprometidas acessem aplicativos sigilosos. A busca proativa diária por ameaças e os controles de acesso baseados em risco reduzem significativamente o impacto das violações.

9. **Avalie e adapte continuamente a postura de segurança.** Realize avaliações de risco automatizadas, testes de penetração e simulações de adversários para ajustar dinamicamente as políticas de segurança zero trust. Configurações incorretas de segurança e a falta de aplicação são fatores-chave para violações graves, tornando a aplicação automatizada e orientada por políticas essencial para reduzir erros humanos.

10. **Elimine a infraestrutura de VPN e automatize a aplicação de políticas de segurança.** Elimine a necessidade de concentradores de VPN, gerenciamento de regras de firewall e listas manuais de controle de acesso adotando um modelo zero trust disponibilizado na nuvem. O ZTNA oferece políticas de segurança dinâmicas que se adaptam em tempo real a mudanças de conformidade, atualizações regulatórias e ameaças cibernéticas em evolução, sem configuração manual ou dependências de hardware.

Ao implementar essas práticas recomendadas, as organizações podem eliminar os riscos de segurança das VPNs com uma estrutura de segurança zero trust resiliente, garantindo verificação contínua, acesso de privilégio mínimo e mitigação proativa de ameaças.

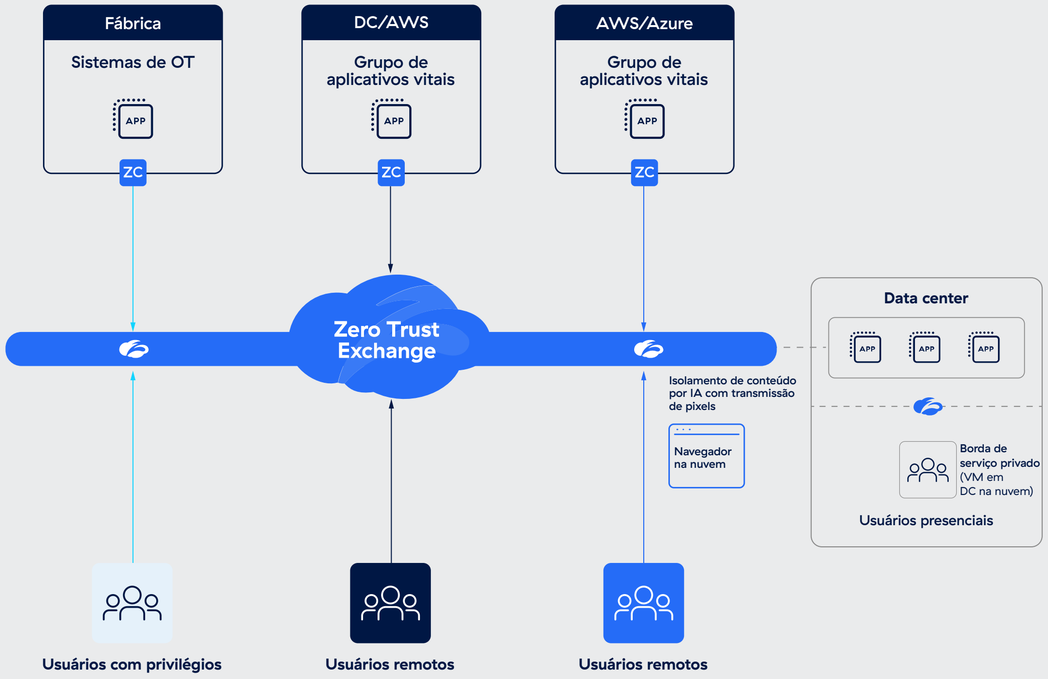
Como a Zscaler transforma o acesso_seguro

As VPNs e os firewalls tradicionais expandem significativamente a superfície de ataque de uma organização ao colocar os usuários diretamente na rede. Esse amplo acesso facilita aos invasores a exploração de vulnerabilidades, a entrada e a movimentação lateral no ambiente. À medida que as ameaças continuam a evoluir e o trabalho híbrido se torna a norma, confiar nessas tecnologias desatualizadas representa riscos críticos de segurança que exigem soluções mais seguras e adaptáveis.

O Zscaler Private Access™ (ZPA) oferece uma alternativa segura e dimensionável a soluções de acesso remoto legadas, como VPNs. Como uma solução nativa da nuvem, o ZPA oferece acesso zero trust para todos os usuários, oferecendo conectividade direta a aplicativos privados. Para minimizar a superfície de ataque, os aplicativos são protegidos pela plataforma Zscaler Zero Trust Exchange™. Essa abordagem elimina a movimentação lateral por meio da segmentação de usuário para aplicativo com tecnologia de IA e defende contra ameaças sofisticadas com inspeção de tráfego integrada, além de proteção de aplicativos e dados.

O ZPA pode ser implantado em poucas horas para substituir VPNs e ferramentas de acesso remoto legadas por uma plataforma zero trust holística e nativa da nuvem. Com a tecnologia da maior nuvem de segurança do mundo, o ZPA oferece conectividade rápida, confiável e de baixa latência para usuários em qualquer lugar do mundo. Sua arquitetura nativa da nuvem garante capacidade de dimensionamento elástica, atendendo perfeitamente às necessidades de equipes de trabalho distribuídas e híbridas em diversas regiões geográficas.

Com o ZPA, as empresas podem adotar modelos de equipes de trabalho híbridas e com foco na nuvem com confiança, sabendo que seus recursos estão protegidos, seus usuários estão produzindo e suas operações de TI estão preparadas para o futuro.



Principais benefícios do Zscaler Private Access (ZPA)

Minimize a superfície de ataque para proteger contra ataques de ransomware

As vulnerabilidades de VPN expõem organizações a usuários mal-intencionados, levando a ataques de ransomware e roubo de credenciais. O ZPA elimina esse risco ocultando todos os aplicativos por trás da Zero Trust Exchange e concedendo aos usuários acesso direto e zero trust somente aos aplicativos autorizados. Ao impedir que usuários não autorizados, incluindo fornecedores e prestadores de serviços terceirizados, descubram aplicativos e se movam lateralmente, o ZPA protege efetivamente contra ataques de ransomware. Ele oferece acesso remoto seguro para todos os aplicativos, incluindo aplicativos privados, aplicativos conectados à rede, como VoIP, e aplicativos de servidor para cliente. Além disso, o ZPA minimiza o impacto das interrupções por meio de uma solução abrangente de continuidade de negócios e ajuda as organizações a atender aos rigorosos requisitos de conformidade.

Elimine a movimentação lateral de ameaças

O ZPA aplica acesso de privilégio mínimo conectando usuários diretamente a aplicativos específicos, impedindo o acesso a outros aplicativos na rede. Ele fornece insights visuais sobre do usuário ao aplicativo e as políticas aplicadas, aprimorando a visibilidade e o controle. A segmentação com tecnologia de IA do ZPA gera automaticamente recomendações para segmentos e políticas de aplicativos, simplificando a implementação da segmentação e garantindo capacidade de dimensionamento e segurança robusta.

Obtenha visibilidade granular e análises.

O ZPA fornece visibilidade detalhada e em tempo real sobre o uso de aplicativos, o comportamento do usuário e os padrões de acesso. As equipes de TI podem usar esses dados para monitorar, auditar e identificar rapidamente possíveis ameaças, aprimorando a postura geral de segurança. Isso também pode ajudar a garantir a conformidade regulatória.

Forneça acesso sem cliente para mitigar vulnerabilidades de terceiros

O acesso sem cliente do ZPA simplifica o acesso de terceiros, permitindo que prestadores de serviço e parceiros se conectem com segurança a aplicativos por meio de qualquer navegador, sem a necessidade de um cliente. Ele isola dispositivos não gerenciados da rede corporativa, protege dados sigilosos e se integra ao navegador Google Chrome Enterprise para maior segurança de dispositivos pessoais. Essa abordagem moderna reduz custos, minimiza os riscos associados ao acesso de terceiros e elimina a dependência do gerenciamento da VDI legada.

Evite o comprometimento de aplicativos privados

O ZPA minimiza o risco de comprometimento de aplicativos privados e perda de dados realizando uma inspeção completa em linha do tráfego de aplicativos privados de ponta a ponta. Recursos robustos de prevenção contra perda de dados garantem que informações sigilosas permaneçam seguras, ao mesmo tempo em que bloqueiam acessos não autorizados. Ao ocultar aplicativos da internet pública e oferecer conexões seguras entre usuários e aplicativos com base em princípios de zero trust, o ZPA reduz a superfície de ataque, impede a movimentação lateral e protege contra violações, aumentando a segurança geral.

Simplifique o gerenciamento de políticas e acelere a implantação

O ZPA otimiza as operações de TI simplificando a implantação de acesso remoto, o gerenciamento de políticas e a segmentação de usuário para aplicativo. Tarefas que antes consumiam muito tempo, como integração de usuários, aplicação de correções e atualizações, agora podem ser concluídas em minutos, reduzindo significativamente o esforço da TI. Com gerenciamento centralizado e recomendações de políticas automatizadas, o ZPA permite que as equipes de TI melhorem a eficiência, minimizem a complexidade e se concentrem em iniciativas estratégicas em vez de operações do dia a dia.

Aplique controle de acesso baseado na postura do dispositivo

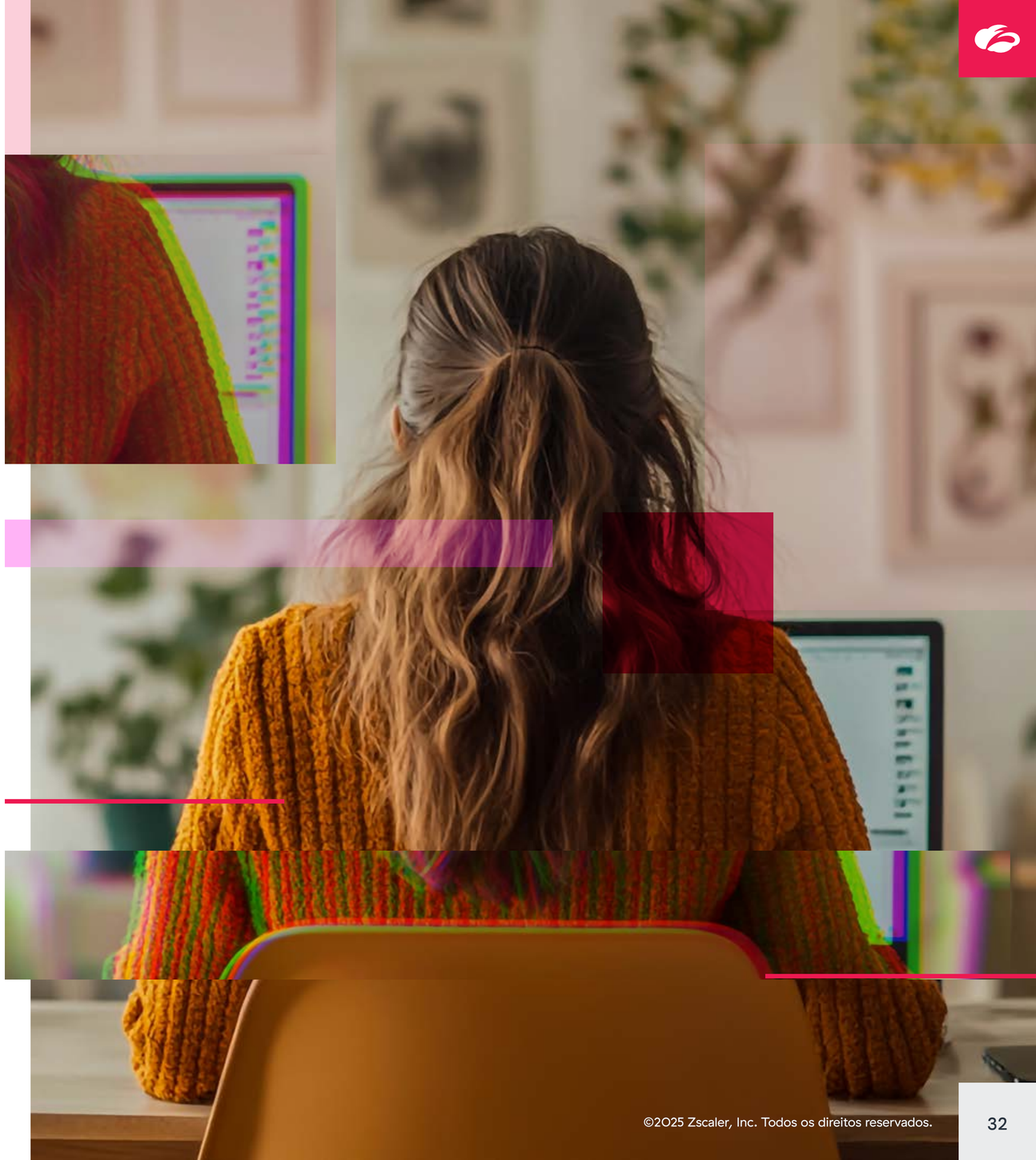
O ZPA se integra com ferramentas de avaliação de postura de terminais para verificar a postura de segurança dos dispositivos do usuário antes de conceder acesso. Isso garante que somente dispositivos compatíveis possam se conectar, reduzindo riscos de dispositivos não gerenciados ou comprometidos.

Forneça uma experiência superior aos usuários

O ZPA garante experiências ideais para o usuário ao fornecer conectividade rápida, contínua e segura para aplicativos essenciais aos negócios. Ao contrário das VPNs que fazem o retorno do tráfego por meio de um data center centralizado, o ZPA oferece conexões diretas do usuário ao aplicativo por meio da Zero Trust Exchange. Isso reduz drasticamente a latência e melhora o desempenho dos aplicativos, independentemente de os usuários estarem no local, remotamente ou em trânsito. Ao minimizar múltiplos logins e a dependência de software baseado em cliente, o ZPA simplifica o acesso e aumenta a produtividade. Além disso, os recursos de monitoramento proativo do ZPA otimizam a resolução de problemas, garantindo acesso ininterrupto e de alta qualidade para todos os usuários.

Reduza o custo total de propriedade

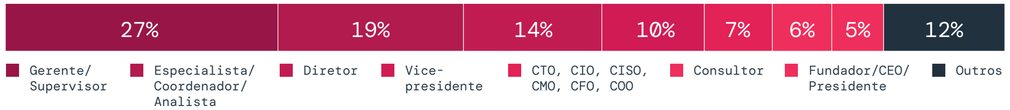
O ZPA reduz significativamente o custo total de propriedade ao eliminar a necessidade de vários produtos específicos, como VPNs, firewalls, NACs e concentradores de VPN. Construído em uma arquitetura zero trust nativa da nuvem, o ZPA elimina custos de infraestrutura relacionados a suporte de hardware, manutenção, reparos e atualizações. Seu gerenciamento simplificado e aplicação automatizada de políticas reduzem a sobrecarga operacional, permitindo que as equipes de TI economizem tempo e recursos, ao mesmo tempo em que melhoram a segurança e a capacidade de dimensionamento.



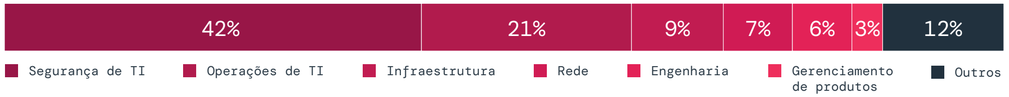
Metodologia_ e dados demográficos

Este relatório é baseado em uma pesquisa abrangente com 632 profissionais de TI e cibersegurança realizada no início de 2025, examinando riscos de segurança da VPN, tendências de acesso empresarial e a adoção de arquiteturas zero trust. Os entrevistados incluíram executivos, profissionais de segurança de TI e líderes de infraestrutura de rede de vários setores. As descobertas deste relatório fornecem uma perspectiva baseada em dados sobre o declínio das VPNs e a migração para o zero trust, oferecendo insights essenciais para organizações que modernizam suas estratégias de segurança de acesso.

Nível de carreira

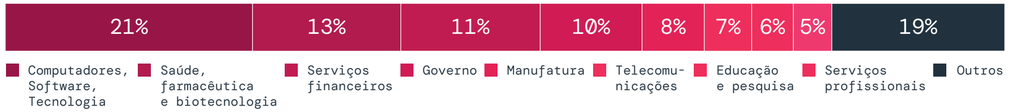


Departamento



Tamanho da empresa

Indústria



Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ciberataques e perda de dados ao conectar 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 na nuvem integrada do mundo. Para saber mais, visite **www.zscaler.com/br.**

Sobre a ThreatLabz

ThreatLabz é o braço de pesquisa de segurança da Zscaler. Essa equipe de classe mundial é responsável por perseguir novas ameaças e garantir que as milhares de organizações que usam a plataforma global Zscaler estejam sempre protegidas. Além da pesquisa de malware e análise comportamental, os membros da equipe estão envolvidos na pesquisa e no desenvolvimento de novos módulos para proteção avançada contra ameaças na plataforma Zscaler, e realizam regularmente auditorias internas de segurança para garantir que os produtos e a infraestrutura da Zscaler atendam aos padrões de conformidade de segurança. A ThreatLabz publica regularmente análises aprofundadas de ameaças novas e emergentes em seu portal, **research.zscaler.com**.

Sobre a Cybersecurity Insiders

CYBERSECURITY INSIDERS: SUA FONTE CONFIÁVEL DE INSIGHTS SOBRE CIBERSEGURANÇA BASEADOS EM DADOS

A Cybersecurity Insiders fornece insights baseados em evidências e validação de terceiros, capacitando líderes de cibersegurança a tomar decisões estratégicas e informadas. Com base em mais de uma década de pesquisa com uma rede global de mais de 600 mil profissionais de cibersegurança, oferecemos inteligência prática que ajuda os líderes a navegar pelas ameaças em evolução, avaliar novas tecnologias e moldar estratégias voltadas para o futuro com confiança.

Para fornecedores de cibersegurança, transformamos insights de pesquisa em resultados, construindo credibilidade, visibilidade e confiança por meio de formatos de alto impacto, como relatórios de mercado baseados em dados e webinars que estabelecem liderança inovadora, guias do CISO que apresentam as práticas recomendadas, análises de produtos que validam soluções, artigos de instruções que educam os compradores e reconhecimento de prêmios que elevam a reputação da marca.

Ao combinar esse conteúdo com distribuição integrada, ajudamos as marcas a ganhar confiança, ampliar o reconhecimento e impulsionar a demanda em um mercado de cibersegurança concorrido.

Saiba mais: cybersecurity-insiders.com

Holger Schulze
CEO e fundador
da Cybersecurity Insiders

zscaler™ | Zero Trust Everywhere

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. 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 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**