Relatório de riscos da VPN Zscaler ThreatLabz 2024

Cybersecurity
INSIDERS

Explore as principais tendências de segurança, riscos e experiência do usuário da VPN, à medida que a adoção do zero trust atinge um momento crítico.

Índice

03 Visão geral

04 Principais conclusões

05 Preocupações de segurança com VPN

- 05 Ataques de VPN em ascensão
- 06 Principais vulnerabilidades de VPN no ano passado
- 07 Navegando pelas preocupações de segurança da VPN
- 08 Cenários principais para acesso seguro

09 Gerenciamento, desempenho e experiência do usuário de VPN

- 09 Desafios no gerenciamento da VPN
- 10 Desafios comuns dos usuários de VPN
- 11 Explorações de vulnerabilidades da VPN
- 12 Riscos de VPN de terceiros

13 Problemas de segurança com infraestrutura de VPN

- 13 Excesso de confiança na segurança de VPN
- 14 Vetores de ataques de ransomware
- 15 Preocupações com ransomware
- 16 Movimentação lateral em ataques de VPN
- 17 Preocupações de segurança da VPN após fusões e aquisições

18 Adoção empresarial do zero trust

- 18 Progresso na adoção do zero trust
- 19 Não há segurança zero trust na VPN
- 19 Como avançar da VPN para o acesso à rede zero trust
- 20 Por que o zero trust é mais seguro do que a VPN
- 21 Principais diferenças e vantagens

22 Previsões sobre VPN para 2024 e para os próximos anos

23 Como a Zscaler oferece a substituição da VPN e a transformação zero trust

- 24 Rede zero trust
- 24 Proteção contra ameaças cibernéticas
- 24 Proteção de dados

25 Práticas recomendadas para combater riscos da VPN

26 Metodologia e dados demográficos

Visão geral

O atual ambiente de trabalho distribuído e centrado na nuvem desencadeou uma mudança nos métodos de acesso das tradicionais redes privadas virtuais (VPNs) para estruturas de segurança mais robustas, como o zero trust. Tradicionalmente, as VPNs forneciam recursos essenciais de acesso remoto para conectar usuários ou escritórios inteiros. No entanto, a crescente sofisticação das ameaças cibernéticas, juntamente com a expansão das equipes de trabalho remotas e das tecnologias de nuvem, expuseram vulnerabilidades significativas nas VPNs. Devido à sua arquitetura legada, as VPNs concedem um acesso à rede excessivamente amplo assim que as credenciais são verificadas, aumentando significativamente o risco de ataques cibernéticos se essas credenciais forem comprometidas.

Explorações de alto perfil recentes de dispositivos de VPN destacaram vulnerabilidades críticas (nomeadamente: CVE-2023-46805, CVE-2024-21887 e CVE-2024-21893) que afetam setores essenciais, incluindo a defesa dos EUA. Essas vulnerabilidades permitem que invasores ignorem a autenticação, executem comandos com privilégios elevados e mantenham a persistência após a redefinição do dispositivo. Em resposta, a Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) emitiu uma diretriz de emergência às agências federais para desconectar imediatamente os dispositivos de VPN afetados devido a riscos substanciais de segurança.

Através da Ordem Executiva 14028, o governo dos EUA exige agora a adoção de arquiteturas zero trust para melhorar a segurança cibernética, afastando-se das VPNs tradicionais. Essa diretiva, parte de uma estratégia abrangente para fortalecer a segurança cibernética nacional, instrui as agências federais a implementarem o zero trust, que verifica cada solicitação de acesso, independentemente da origem. O Gabinete de Gestão e Orçamento (OMB) apoia essa iniciativa com uma Estratégia Federal de Zero Trust detalhada, destacando a mudança da confiança implícita baseada em VPN dentro dos perímetros da rede para a verificação contínua de toda e qualquer solicitação de acesso. Essas diretivas e recomendações refletem um consenso dentro da comunidade de segurança cibernética de que o zero trust proporciona uma defesa mais robusta contra ameaças cibernéticas complexas e em evolução, uma necessidade destacada pelas recentes vulnerabilidades e explorações relacionadas às VPNs tradicionais.

Como resultado, as organizações estão adotando rapidamente modelos de zero trust, que não confiam inerentemente em nenhum usuário ou dispositivo dentro ou fora do perímetro da rede e exigem verificação granular para cada solicitação de acesso. Esse modelo é particularmente eficaz na prevenção contra movimentação lateral dentro das redes, uma exploração que os invasores utilizam frequentemente para aprofundar sua intrusão após obterem acesso inicial.

Com base em uma pesquisa com 647 profissionais de TI e especialistas em segurança cibernética, este relatório explora os desafios multifacetados de segurança e experiência do usuário das VPNs para revelar a complexidade da gestão de acesso atual, as vulnerabilidades a vários ataques cibernéticos e o seu potencial para prejudicar a postura de segurança como um todo das organizações. O relatório também descreve modelos de segurança mais avançados, especialmente o zero trust, que se estabeleceu firmemente como uma estrutura robusta e pronta para o futuro para proteger e acelerar a transformação digital.

Agradecemos à Zscaler por contribuir para esta pesquisa de riscos da VPN. Sua experiência em soluções de zero trust e acesso seguro enriqueceu significativamente nossas descobertas. Estamos confiantes de que as informações contidas neste relatório serão um recurso essencial para profissionais de TI e segurança cibernética em sua jornada rumo à segurança zero trust.

Obrigado, Holger Schulze, fundador, Cybersecurity Insiders

“Durante o ano passado, inúmeras vulnerabilidades críticas da VPN serviram como pontos de entrada bem-sucedidos para ataques a grandes empresas e entidades federais. Considerando esses resultados repetidos, é crucial que as empresas antecipem que os criminosos explorarão cada vez mais esses ativos herdados e expostos à internet, físicos e virtuais, que lhes permitem facilmente navegar lateralmente pelas redes planas tradicionais. É essencial fazer a transição para a arquitetura zero trust, que reduz significativamente a superfície de ataque ao eliminar tecnologias legadas como VPNs e firewalls, impor controles de segurança consistentes com inspeção de TLS e limitar o raio de ataque com segmentação e deception, evitando violações prejudiciais.”

— DEEPEN DESAI, DIRETOR DE SEGURANÇA, ZSCALER

Principais descobertas

Os ataques de VPN estão aumentando.

56% das organizações sofreram um ou mais ataques cibernéticos relacionados à VPN no último ano (acima dos 45% do ano anterior) destacando a crescente frequência e sofisticação dos ataques direcionados a VPNs.

As VPNs não são páreo para ransomware, malware e DDoS.

Os entrevistados identificaram ataques de ransomware (42%), malware (35%) e DDoS (30%) como as principais ameaças que exploram vulnerabilidades da VPN, destacando a amplitude dos riscos que as organizações enfrentam devido às fraquezas inerentes às arquiteturas de VPN tradicionais.

A grande maioria está mudando para o zero trust.

78% das organizações planejam implementar estratégias de zero trust nos próximos 12 meses. Enquanto isso, 62% das empresas concordam que as VPNs são antizero trust.

O risco de movimentação lateral não pode ser ignorado.

53% das empresas violadas através de vulnerabilidades de VPN afirmam que os criminosos se moveram lateralmente, demonstrando falhas de contenção no ponto inicial do comprometimento que destacam os riscos das redes tradicionais e planas.

A maioria tem dúvidas sobre a segurança da VPN.

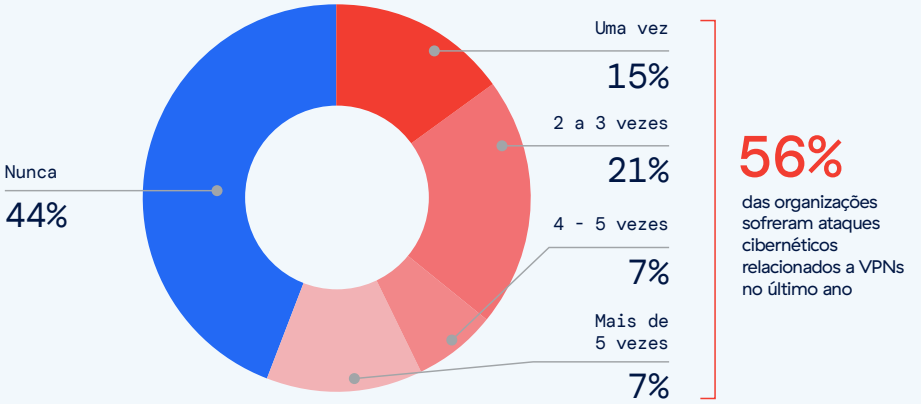
91% dos entrevistados expressaram preocupação com o comprometimento das VPNs em seu ambiente de segurança de TI, com violações recentes ilustrando os riscos de manter infraestruturas de VPN desatualizadas ou sem correção.

Preocupações de segurança com a VPN

Ataques de VPN em ascensão

A frequência e a gravidade dos ataques que exploram as vulnerabilidades das VPNs destacam a ineficácia das medidas convencionais de cibersegurança e ressaltam os riscos persistentes representados pela exposição da rede. Nossa pesquisa revela que 56% das organizações sofreram ataques cibernéticos no último ano que aproveitaram vulnerabilidades da VPN, um aumento significativo em relação aos 45% do ano anterior. De forma alarmante, 41% das organizações relataram ter sofrido dois ou mais ataques relacionados a VPN, indicando graves falhas de segurança.

Nos últimos 12 meses, sua organização sofreu um ataque que se aproveitou de vulnerabilidades de segurança em seus servidores de VPN?



As tendências recentes confirmam que os ataques às VPNs estão tornando-se não apenas mais frequentes, mas também mais sofisticados. Por exemplo, mais casos de ransomware que exploram falhas da VPN, especialmente após vulnerabilidades divulgadas publicamente, destacam as fraquezas críticas inerentes às VPNs tradicionais. Essas vulnerabilidades proporcionam aos invasores pontos de entrada fáceis para se infiltrarem nas redes e facilitam a movimentação lateral, levando a violações substanciais de dados e interrupções operacionais.

Principais vulnerabilidades de VPN no ano passado

Em meio à recente série de CVEs de alta gravidade que impactam produtos de VPN, não é surpresa que as empresas estejam relatando mais ataques que exploram esses tipos de vulnerabilidades. É claro que nenhum fornecedor ou tecnologia específica pode estar imune a vulnerabilidades de software. No caso da VPN, o desafio para as empresas é que cada CVE pode representar um único ponto de falha de segurança para a empresa: uma base que permite aos invasores comprometer um ativo de VPN, estabelecer persistência, mover-se lateralmente pela rede e roubar dados. À medida que os CVEs de VPN continuam a ser divulgados nesse ritmo, eles serão um risco persistente para as empresas que usam VPNs para conectividade remota.

Uma série de CVEs recentes destaca uma falha de arquitetura

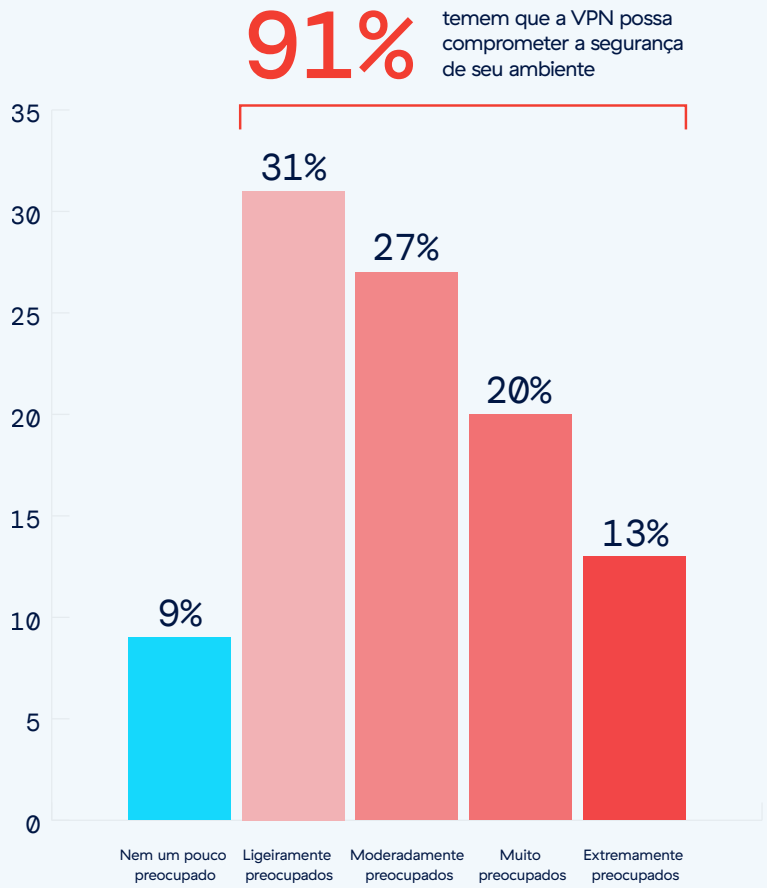
Navegando pelas preocupações de segurança da VPN

Os resultados da pesquisa refletem preocupações profundas sobre o comprometimento dos ambientes de segurança pelas VPNs, refletindo as tendências atuais e aumentando as vulnerabilidades nas tecnologias de VPN. A esmagadora maioria dos entrevistados (91%, contra 88% em 2023) expressam preocupação com o fato de as VPNs comprometerem sua segurança de TI, ressaltando a maior conscientização sobre os riscos relacionados às VPNs entre as organizações.

Essa preocupação é justificada pelas recentes explorações direcionadas às VPNs da Ivanti, em que os invasores aproveitaram vulnerabilidades graves para se infiltrarem nas redes e exfiltrarem dados sigilosos. Esses incidentes, envolvendo vulnerabilidades como CVE-2024-21888 e CVE-2024-21893, destacam os riscos de manter e proteger infraestruturas de VPN desatualizadas ou sem correção. Além disso, a arquitetura inerente das VPNs apresenta riscos de segurança significativos no atual cenário digital sem perímetro. À medida que as empresas adotam cada vez mais serviços na nuvem e os modelos de trabalho remoto evoluem, as VPNs enfrentam novos desafios de segurança, incluindo o gerenciamento de direitos de acesso amplos e a proteção de uma superfície de ataque em expansão.

Essas vulnerabilidades e limitações arquitetônicas ressaltam uma mudança fundamental nas perceções em relação à segurança da VPN, alinhando-se com tendências mais amplas de segurança cibernética que defendem estruturas mais dinâmicas e resilientes, como o zero trust.

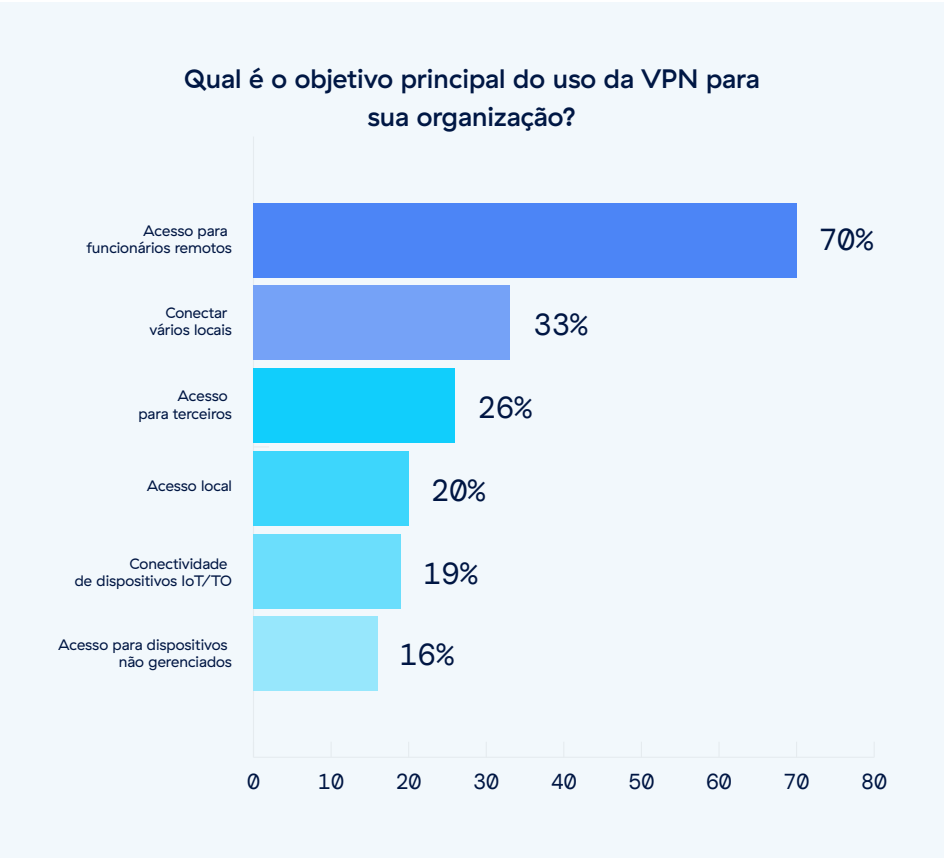
As organizações voltadas para o futuro fazem a transição para arquiteturas zero trust para obter um controle mais granular e reduzir significativamente a superfície de ataque, nunca conferindo confiança implícita, seja dentro ou fora de um perímetro de rede. A adoção de tal estratégia aborda as vulnerabilidades imediatas das VPNs tradicionais e alinha-se com uma abordagem proativa de segurança cibernética, essencial para a adaptação ao cenário de ameaças em evolução.



Principais cenários para acesso seguro

Compreender por que as organizações usam VPNs é essencial, pois destaca como elas priorizam o acesso seguro em vários cenários de negócios. Isso também revela quais casos de uso de redes estão mais expostos a riscos de segurança, indicando áreas que exigem estratégias de segurança de acesso mais robustas e inovadoras.

Significativos 70% das organizações utilizam VPNs principalmente para proteger o acesso de funcionários remotos. Esse uso generalizado torna o acesso remoto um alvo principal para ataques cibernéticos. Depois disso, 33% usam VPNs para conectar vários sites, apresentando riscos substanciais, pois essas conexões podem servir como vetores para ataques cibernéticos se não forem devidamente protegidas. Em seguida, 26% das organizações observaram o acesso de terceiros, o que complica ainda mais a segurança devido às diferentes posturas de segurança das diferentes partes interessadas externas e à falta de controle sobre as políticas de segurança. Além disso, 20% das organizações utilizam VPNs para acesso local e 19% as utilizam para conectividade de dispositivos de IoT/OT.



As VPNs não fornecem mais segurança adequada para casos de uso de acesso crítico no atual cenário de ameaças cibernéticas em evolução, porque operam em modelos de confiança desatualizados que concedem amplo acesso à rede mediante a simples autenticação do usuário. Esse amplo acesso expõe as organizações a riscos significativos, permitindo que possíveis invasores explorem um único ponto de entrada para navegar e extrair dados sigilosos através da rede.

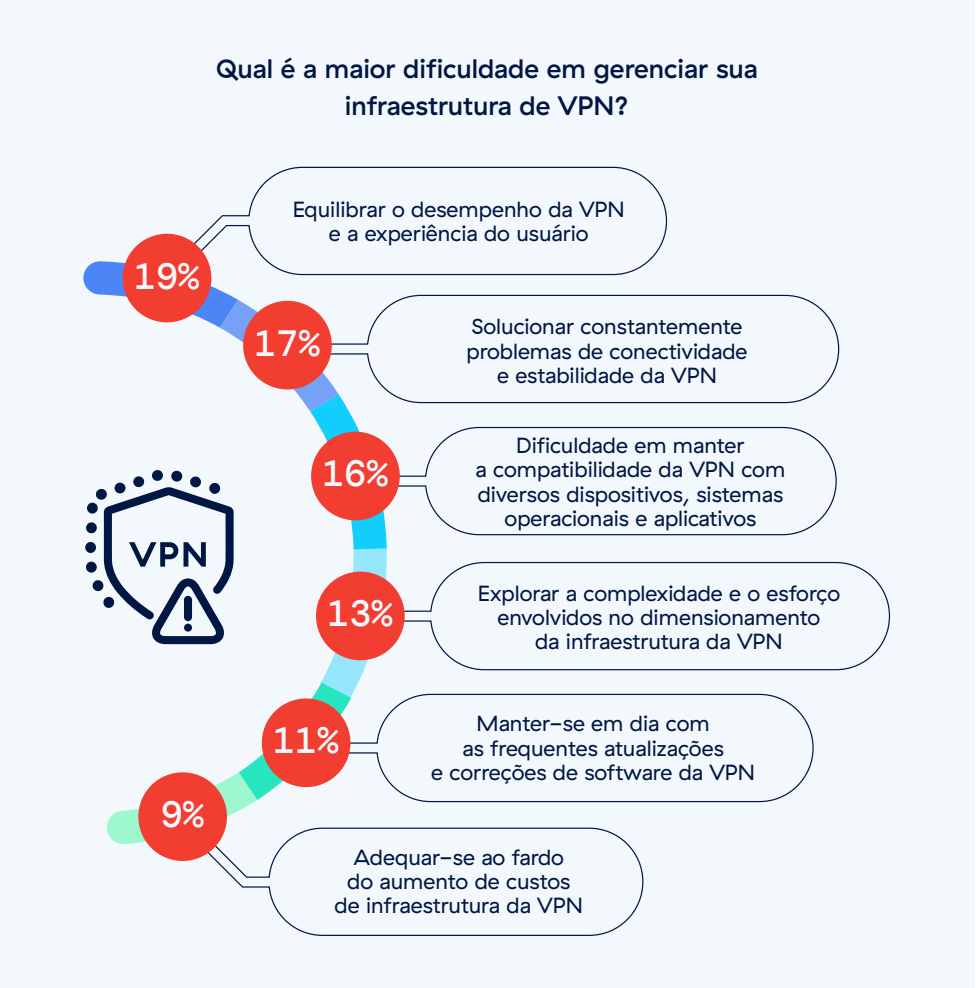
Gerenciamento, desempenho e experiência do usuário de VPN

Desafios no gerenciamento da VPN

Além dos riscos de segurança inerentes, o gerenciamento de infraestruturas de VPN apresenta desafios significativos para as equipes de TI, à medida que os requisitos para soluções de acesso robustas se intensificam em ambientes de trabalho dispersos e centrados na nuvem. O principal desafio de gerenciamento para profissionais de TI é o equilíbrio entre o desempenho da VPN e a experiência do usuário (19%). Essa questão é crucial porque tem impacto direto na produtividade: se a VPN tornar a rede mais lenta ou se revelar demasiado complicada de utilizar, pode levar a uma menor satisfação dos funcionários e a processos de negócio lentos e ineficientes.

A próxima preocupação mais comum, citada por 17% dos entrevistados, é a solução constante de problemas de conectividade e estabilidade da VPN. Esses problemas não apenas tomam o tempo da equipe de TI, mas também causam interrupções frustrantes para os usuários. Outros desafios notáveis incluem a falta de compatibilidade das VPNs com uma ampla gama de dispositivos, sistemas operacionais e aplicativos, que cerca de 16% dos profissionais de TI consideram oneroso. Além disso, 13% dos entrevistados têm dificuldade com a complexidade e a natureza trabalhosa do dimensionamento da infraestrutura de VPN, uma questão crítica à medida que as organizações crescem e as suas necessidades aumentam em meio a uma grave escassez de profissionais qualificados em segurança cibernética.

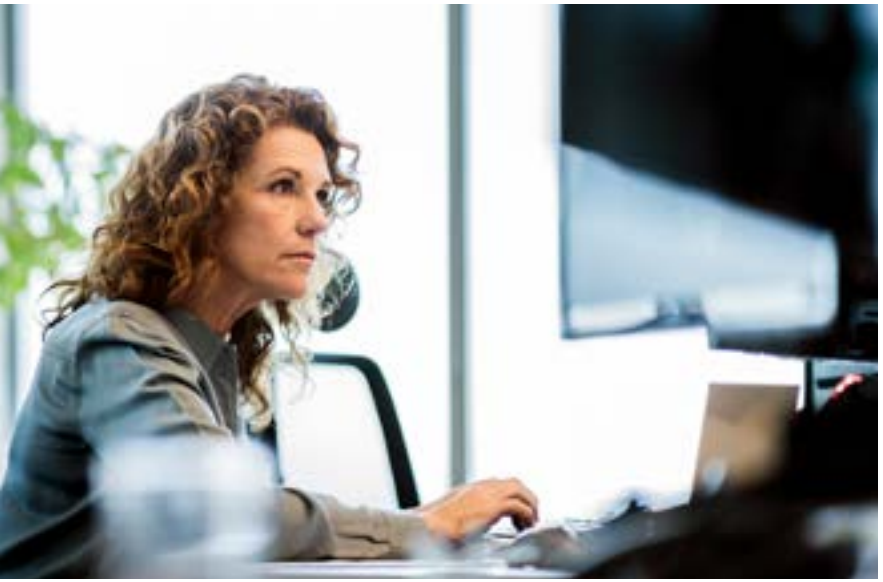
Esses insights ressaltam a necessidade de as organizações explorarem alternativas mais ágeis, fáceis de usar e com menos uso intensivo de recursos, como modelos de acesso à rede zero trust (ZTNA). O ZTNA oferece controle mais granular, capacidade de dimensionamento aprimorada e reduz a sobrecarga de gerenciamento, tornando-o uma escolha superior à VPN tradicional no cenário dinâmico de segurança cibernética atual.



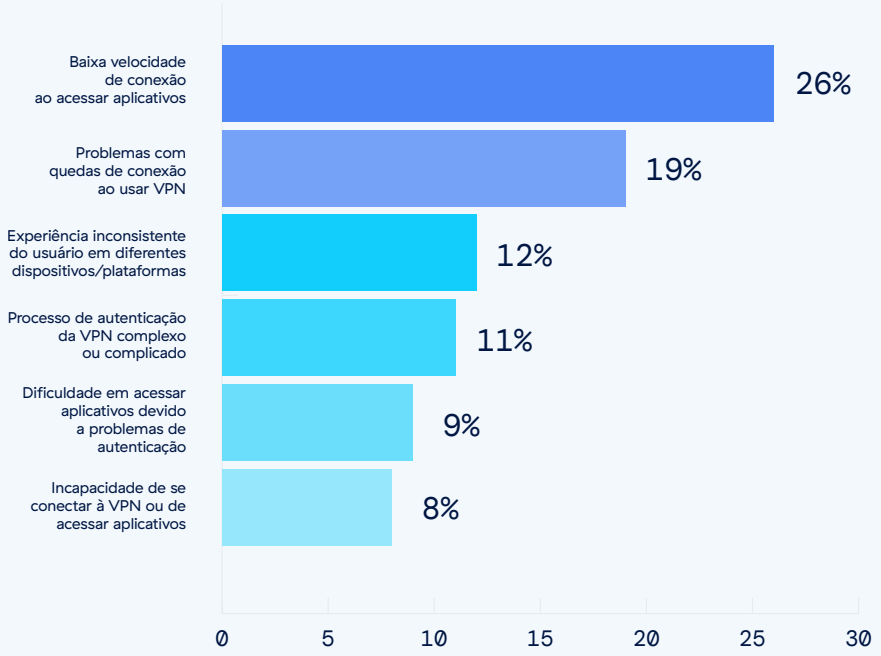
Desafios comuns dos usuários de VPN

A reclamação mais frequente dos usuários sobre o uso da VPN, conforme observado por 26% dos entrevistados, é a velocidade lenta da conexão. Isso destaca um problema crítico de produtividade e satisfação do usuário, uma vez que velocidades lentas podem reduzir significativamente a eficiência de tarefas rotineiras e o acesso a recursos baseados na nuvem, especialmente em ambientes de trabalho domésticos.

Quedas de conexão da VPN representam o segundo problema mais comum, citado por 19% dos entrevistados. Esse problema pode prejudicar tarefas e comunicações contínuas, afetando significativamente a experiência do usuário e a continuidade operacional. Experiências de usuário inconsistentes em diferentes dispositivos e plataformas, relatadas por 12% dos usuários, apontam para a necessidade de um desempenho de acesso mais uniforme.



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



Para abordar essas questões, as organizações devem considerar a adoção de soluções de acesso à rede que ofereçam mais estabilidade e consistência para diversas plataformas. A implementação de uma arquitetura zero trust pode ser particularmente eficaz, pois aumenta a segurança sem introduzir gargalos de desempenho. As redes zero trust garantem que problemas de conexão não comprometam a segurança e que o controle de acesso seja rigoroso e adaptável a diferentes ambientes de usuários.

Na sua opinião, quais tipos de ataques cibernéticos são mais propensos a explorar as vulnerabilidades de VPN da sua organização?

Para combater essas vulnerabilidades, as organizações devem adotar medidas de segurança proativas, como um modelo zero trust. O zero trust aplica controles de acesso rigorosos e verificação contínua de todas as conexões de rede, independentemente de sua origem. Essa estratégia mitiga com eficácia os riscos representados por uma vasta gama de ataques que exploram as fraquezas da VPN, limitando a movimentação lateral e reforçando controles de acesso robustos.

Explorações de vulnerabilidades da VPN

A variedade de ataques cibernéticos que exploram os pontos fracos da VPN destaca a amplitude dos riscos que as organizações enfrentam. A pesquisa revela que 42% dos entrevistados identificam os ataques de ransomware como os mais propensos a explorar vulnerabilidades da VPN, destacando o impacto significativo e as ocorrências frequentes. Isso é seguido por infecções por malware, relatadas por 35% dos entrevistados, e ataques de DDoS, observados por 30%, que comprometem a disponibilidade, bem como a confidencialidade e integridade dos sistemas.

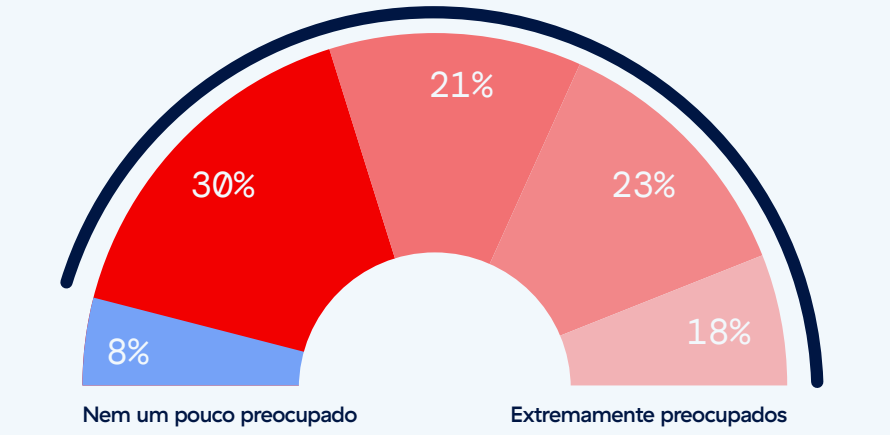
Risco de terceiros da VPN

A pesquisa ressalta uma preocupação significativa em relação ao acesso à VPN por terceiros como uma vulnerabilidade de segurança de rede. Notáveis 92% dos entrevistados expressam apreensão sobre esse risco, indicando um pequeno aumento em relação aos 90% de 2023. Esse reconhecimento crescente destaca a possibilidade do acesso de terceiros servir como ponto de entrada para ameaças cibernéticas.

Novos insights sobre vulnerabilidades e violações da VPN validaram ainda mais essas preocupações. As VPNs tradicionais normalmente fornecem ampla validação pós-credencial de acesso à rede, representando riscos se as medidas de segurança de fornecedores terceirizados forem comprometidas.

Qual é o seu grau de preocupação com terceiros servindo como possíveis backdoors para invasores entrarem na sua rede por meio do acesso via VPN?

92% se preocupam com terceiros servindo como possíveis backdoors para suas redes por meio do acesso via VPN



As organizações devem acelerar a transição das VPNs tradicionais para arquiteturas zero trust. Essa mudança envolve a implementação de sistemas que verificam rigorosamente as solicitações de acesso com base na identidade e no contexto, limitando o acesso de fornecedores terceirizados a recursos específicos essenciais para as suas tarefas.

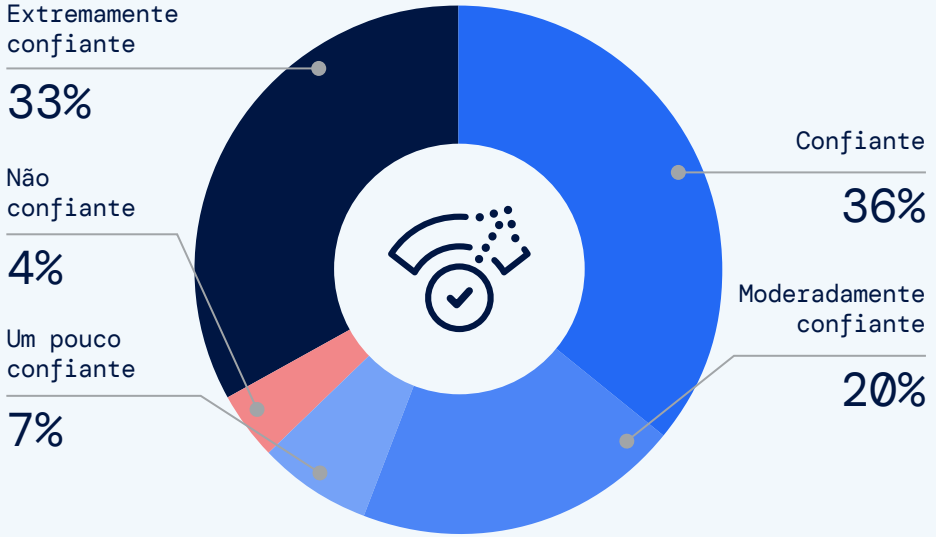
Problemas de segurança com a infraestrutura de VPN

Excesso de confiança na segurança de VPN

O recente aumento nas violações de VPN destaca uma desconexão entre a segurança percebida e o risco real. As recentes explorações de alta gravidade em produtos de VPN ressaltam que mesmo organizações bem preparadas podem estar subestimando as capacidades dos adversários cibernéticos que exploram vulnerabilidades inerentes à tecnologia de VPN. Significativos 69% dos entrevistados alegaram ter alta confiança na capacidade de sua organização de lidar com vulnerabilidades de VPN, o que pode não estar totalmente alinhado com o cenário de ameaças crescentes, onde agentes sofisticados exploram até mesmo pequenas fraquezas muito rapidamente. O excesso de confiança pode ser particularmente arriscado dada a complexidade e persistência das recentes explorações de VPN, como demonstrado por incidentes envolvendo grupos patrocinados por governos e gangues de criminosos cibernéticos que atacam sistemas não corrigidos por períodos prolongados.

As organizações devem recalibrar a sua postura de segurança, incorporando avaliações rigorosas de vulnerabilidade, atualizações frequentes e treinamento abrangente de sensibilização para a segurança. É aconselhável adotar uma abordagem de segurança em camadas que não dependa excessivamente das VPNs para proteção abrangente. Essa abordagem deve incluir monitorização avançada, deteção de anomalias e integração de princípios de zero trust.

Qual é o seu nível de confiança na capacidade da sua organização de detectar e mitigar vulnerabilidades de VPN que a expõem a ataques de segurança cibernética?

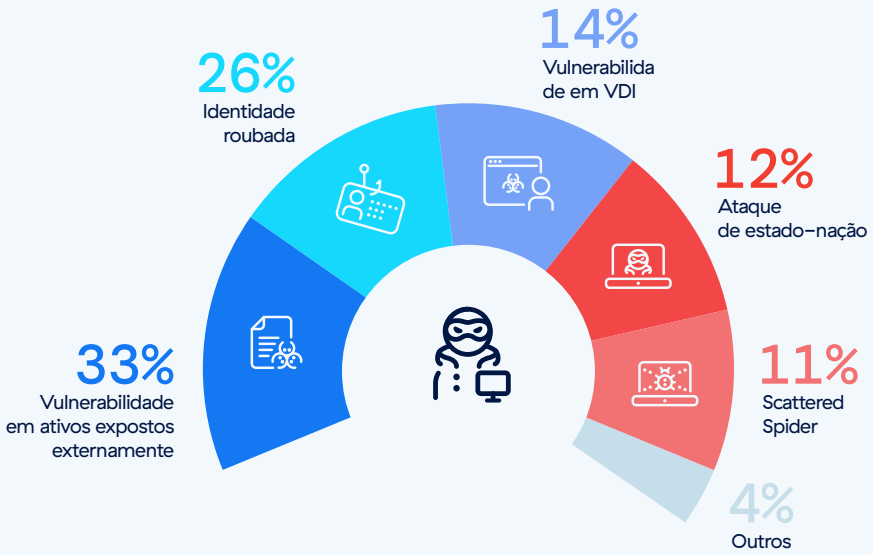


Vetores de ataque de ransomware

A pesquisa identifica claramente vulnerabilidades em ativos expostos externamente como o vetor de ataque potencial de ransomware mais preocupante, observado por 33% dos entrevistados. Isso aponta para um reconhecimento generalizado dos riscos associados aos serviços de rede ou aplicativos web expostos, que são muitas vezes o primeiro ponto de entrada para ataques de ransomware.

Identidades roubadas seguem de perto, com 26%, destacando o papel que as credenciais comprometidas desempenham ao permitir que invasores contornem medidas de segurança e obtenham acesso para entregar cargas de ransomware. As preocupações sobre vulnerabilidades em infraestruturas de desktops virtuais (VDI) e ataques de estados-nação, de 14% e 12%, respectivamente, destacam as diversas origens das ameaças de ransomware contra as quais as organizações devem se defender. O Scattered Spider (um grupo cibercriminoso que utiliza táticas sofisticadas de engenharia social, incluindo phishing, ataques de fadiga de autenticação multifatorial e troca de SIM), preocupa 11% dos participantes.

Qual é a sua maior preocupação como principal causa do ransomware?



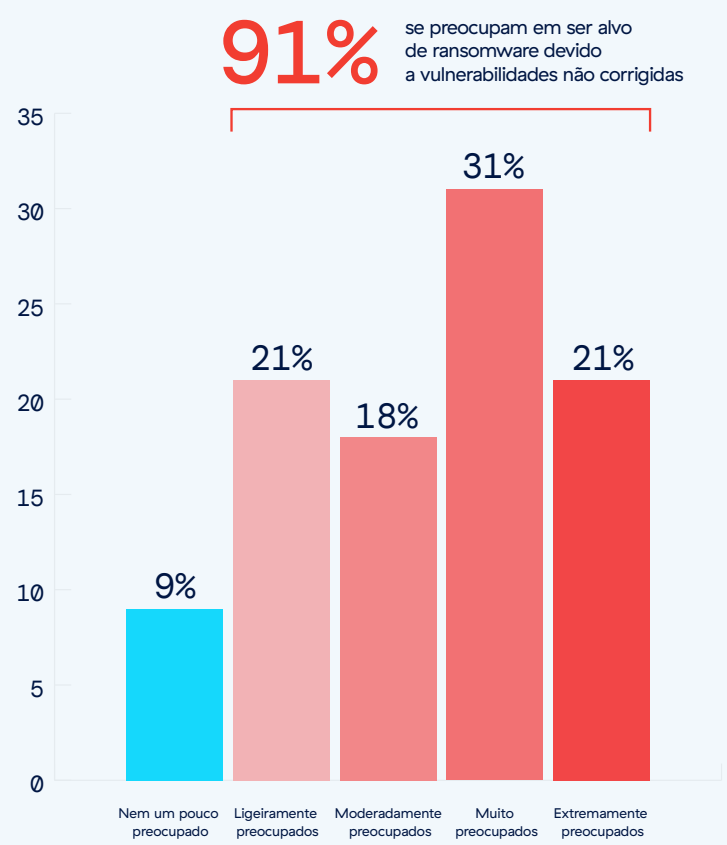
As organizações devem melhorar suas defesas e protocolos de gestão de identidade. A implementação de processos abrangentes de gerenciamento de vulnerabilidades e a adoção de um modelo de segurança zero trust podem reduzir efetivamente o risco de ataques de ransomware, negando o acesso aos recursos da rede e a propagação lateral.

Preocupações com ransomware

Os resultados da pesquisa mostram que 52% dos entrevistados estão muito ou extremamente preocupados com a ameaça do ransomware devido a vulnerabilidades não corrigidas. Isso se justifica porque as vulnerabilidades não corrigidas continuam sendo o principal vetor de ataque do ransomware. Análises recentes mostram que uma parte substancial dos ataques de ransomware explora essas vulnerabilidades, com um impacto notavelmente grave em comparação com outros tipos de ataques cibernéticos.

Os grupos de ransomware estão se tornando mais sofisticados, e muitos agora usam táticas avançadas que podem explorar rapidamente vulnerabilidades recém-descobertas antes que as organizações possam corrigi-las. Esse rápido ciclo de exploração encurta enormemente a janela de resposta a vulnerabilidades críticas, destacando a necessidade urgente de adotar medidas de segurança avançadas que reduzam a superfície de ataque.

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



Movimentação lateral em ataques de VPN

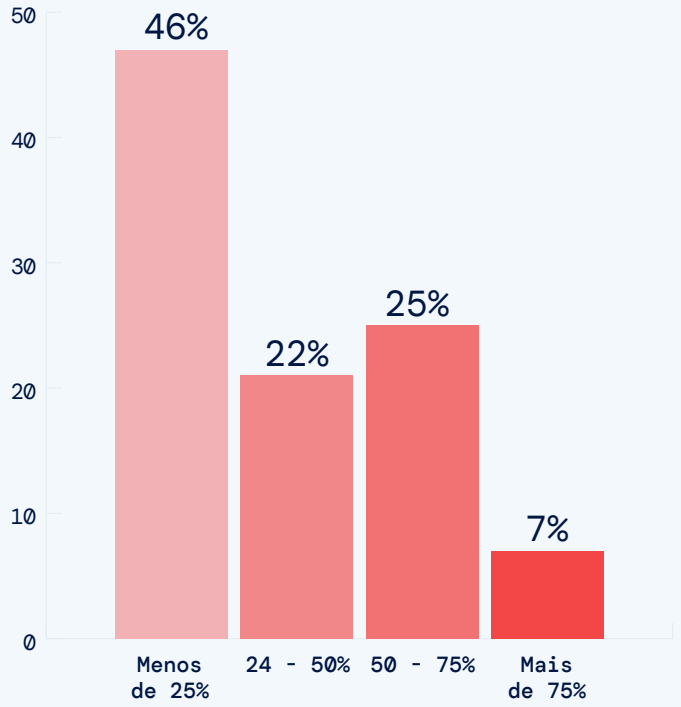
A maioria dos entrevistados (53%) relatam que mais de 25% dos ataques relacionados a VPNs envolveram movimentação lateral, demonstrando falhas significativas de contenção no ponto inicial do comprometimento. Quase um terço (32%) sofreram movimentações laterais em mais da metade dos ataques, indicando grandes desafios no controle da propagação de ameaças quando os adversários violam as defesas da rede.

A movimentação lateral é um risco significativo nas VPNs, pois os invasores podem obter amplo acesso à rede semelhante ao de um usuário autenticado. Isso permite que eles se movam furtivamente pela rede e ataquem áreas sigilosas.

Dessa forma, as VPNs podem agravar os riscos e expandir o âmbito de um ataque para além do seu ponto de entrada inicial. Resolver isso exige uma segmentação rigorosa, de preferência com o tráfego de usuário para aplicativo passando por uma arquitetura zero trust, além de monitoramento contínuo. Isso reduz substancialmente o raio de ação da movimentação lateral, oferecendo acesso granular a um conjunto menor de aplicativos para cada usuário individual, enquanto o restante fica invisível.

A crescente sofisticação dos ataques que exploram as vulnerabilidades das VPN ressalta a necessidade de uma mudança em direção a uma estrutura zero trust. Ao impor controles de acesso rigorosos e verificação contínua, o zero trust limita as movimentações laterais não autorizadas e aumenta a segurança em cenários digitais em expansão.

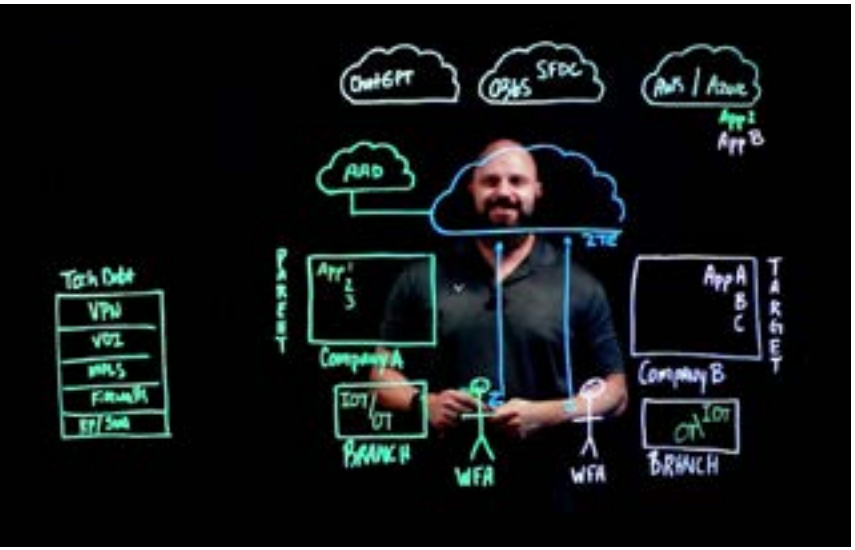
De todos os ataques que sua organização sofreu, que porcentagem envolveu ameaças que se espalharam lateralmente após obter acesso por meio da VPN?



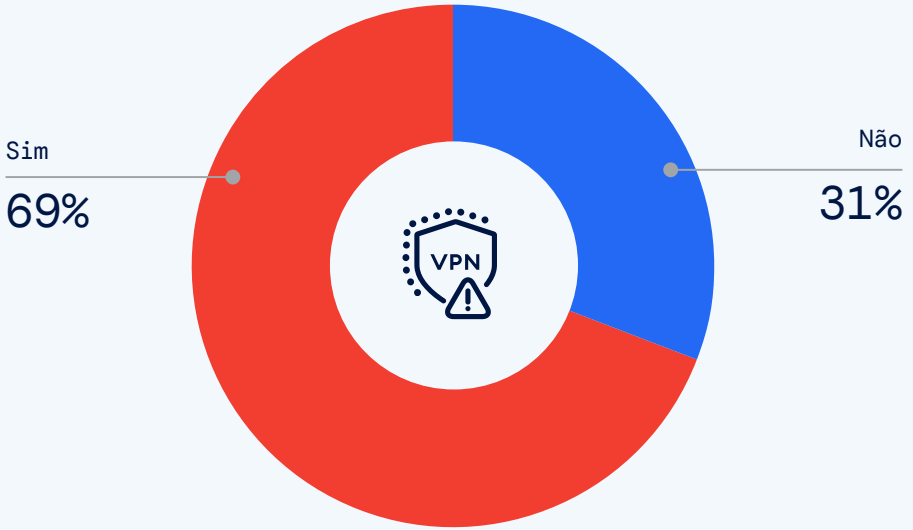
Preocupações de segurança da VPN Depois de fusões e aquisições

Preocupações em torno do impacto das fusões e aquisições (M&A) na infraestrutura de VPN existente destacam as vulnerabilidades potenciais que surgem das mudanças organizacionais e da integração de redes diferentes.

Substanciais 69% dos entrevistados expressam apreensão sobre ataques cibernéticos após fusões e aquisições, destacando a preocupação generalizada com os riscos de segurança associados a essas transformações corporativas. Esse sentimento reflete uma compreensão clara de que as atividades de fusões e aquisições podem desestabilizar as estruturas de segurança existentes, aumentando a exposição a ameaças cibernéticas.



Você teme se tornar vítima de um ataque após fusões e aquisições com sua infraestrutura atual?



Períodos de transição durante fusões e aquisições apresentam oportunidades únicas para as organizações eliminarem gradualmente tecnologias de VPN antiquadas e vulneráveis em favor de estruturas de zero trust. Especificamente, as arquiteturas zero trust melhoram a segurança, fornecendo segmentação abrangente do ambiente entre usuários e aplicativos, cargas de trabalho e cargas de trabalho, filiais e dispositivos, sejam dispositivos gerenciados, dispositivos não gerenciados, sistemas de IoT ou TO. Essa abordagem reforça significativamente a segurança durante e após uma transição por meio de verificação rigorosa de todos os usuários e dispositivos, segmentação abrangente e aplicação rigorosa de controles de acesso de privilégio mínimo.

Adoção empresarial de zero trust

Progresso na adoção do zero trust

A pesquisa reflete uma forte tendência para a adoção de estruturas de segurança zero trust, ressaltando o reconhecimento crescente da sua importância no reforço da segurança cibernética organizacional. Significativos 31% dos entrevistados já estão implementando o zero trust (contra 27% em 2023), indicando um esforço proativo crescente para proteger melhor os recursos da rede.

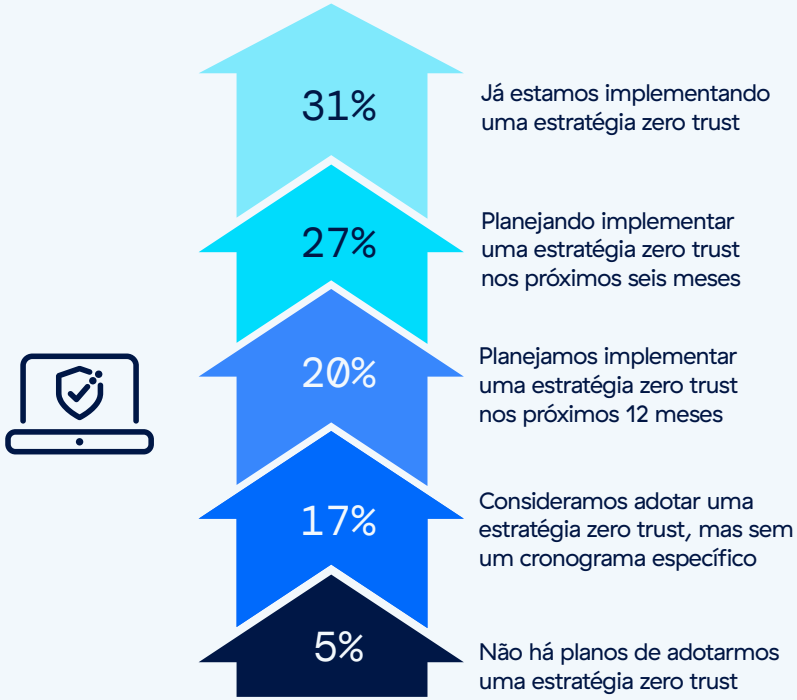
Além disso, 27% das organizações planejam implementar uma estratégia zero trust nos próximos seis meses (acima dos 18% em 2023), e outros 20% das organizações planejam fazer a mudança nos próximos 12 meses, demonstrando um compromisso generalizado com a transição para o zero trust em um futuro próximo. Isso confirma que mais de três quartos dos entrevistados (78%) reconhecem a urgência e os benefícios do zero trust.

No entanto, 17% dos entrevistados ainda consideram implementar uma estratégia zero trust sem um prazo específico (contra 23% em 2023), destacando alguma hesitação ou potenciais desafios no planejamento ou início da transição. Apenas uma pequena fração (5%) relatam não ter planos para adotar o zero trust (contra 8% em 2023), possivelmente por falta de recursos.

Uma análise por tamanho de empresa indica que as organizações maiores incluídas na nossa pesquisa, especialmente aquelas com mais de 20 mil funcionários, são mais propensas e ágeis a adotar estratégias zero trust, com 33% já as implementando. Em contraste, as pequenas empresas, com mil a 5 mil funcionários, apresentam uma taxa de adoção ligeiramente inferior, em 29%, sugerindo que a escala e a disponibilidade de recursos podem influenciar o ritmo e o âmbito da integração do zero trust.

As organizações que ainda estão em dúvida ou que planejam adotar o zero trust devem começar avaliando sua postura atual de segurança e arquitetura de rede para identificar necessidades específicas e possíveis desafios

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

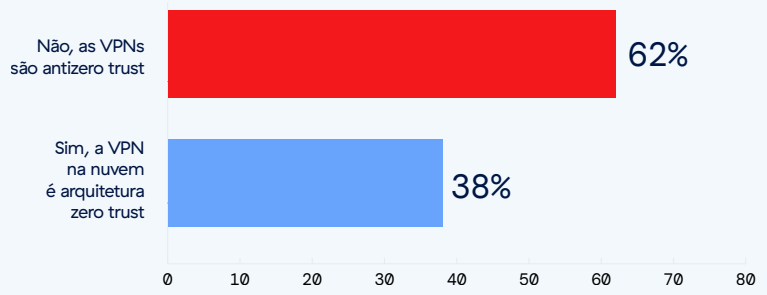


Não há segurança zero trust na VPN

Os resultados da pesquisa refletem uma divisão significativa nas crenças sobre a compatibilidade das VPNs com estruturas de segurança zero trust. A maioria (62%) acredita que as VPNs são fundamentalmente “antizero trust”, confirmando que as arquiteturas de VPN tradicionais não se alinham com os princípios do zero trust. Por outro lado, 38% dos entrevistados consideram as VPNs, especialmente as plataformas baseadas na nuvem, compatíveis com arquiteturas zero trust.

Embora essa perspectiva possa resultar de fornecedores de VPN alegando que suas soluções baseadas na nuvem estão alinhadas com os princípios do zero trust, é importante examinar essas afirmações de forma crítica. A simples hospedagem de um serviço de VPN na nuvem, por exemplo, não confere automaticamente atributos de zero trust. A segurança zero trust requer mais do que apenas um ambiente de hospedagem seguro; ela exige uma mudança fundamental das defesas baseadas em perímetro para um modelo onde a segurança seja dinâmica, granular e baseada no contexto.

Você acredita que pode obter segurança zero trust com VPNs?



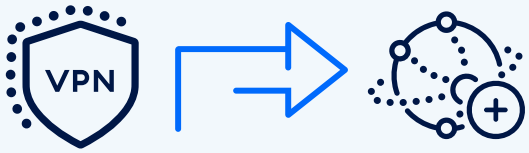
A verdadeira segurança zero trust envolve a validação contínua de todos os usuários e dispositivos, a aplicação do acesso de privilégio mínimo e a segmentação do tráfego para evitar a movimentação lateral, recursos que as VPNs tradicionais, mesmo as baseadas na nuvem, não oferecem. Portanto, as organizações devem confirmar se uma VPN alega ser “zero trust” realmente incorpora esses princípios fundamentais, em vez de confiar apenas em promessas de marketing.

Como avançar da VPN para o acesso à rede zero trust

Os resultados da pesquisa mostram que a maioria das organizações está fazendo uma mudança estratégica, com 53% dos entrevistados citando planos para substituir as soluções de VPN existentes por soluções de ZTNA em um futuro próximo. O ZTNA oferece uma abordagem mais flexível e segura, aplicando políticas baseadas no contexto do usuário, localização e segurança do dispositivo, sem presumir confiança com base na localização da rede. Isto contrasta com as VPNs tradicionais, que geralmente concedem amplo acesso a uma rede, criando vulnerabilidades de segurança.

Para 53% das organizações que estão migrando para o ZTNA, é crucial garantir uma transição tranquila, planejando avaliações de risco abrangentes, atualizando políticas de acesso e educando os usuários sobre os novos protocolos. Entretanto, os 47% que ainda não planejam mudar devem avaliar seus atuais desafios de segurança e considerar se o ZTNA poderia abordá-los de forma mais eficaz do que a VPN.

Você planeja substituir sua solução de VPN atual por uma solução de acesso à rede zero trust (ZTNA) em um futuro próximo?



53%

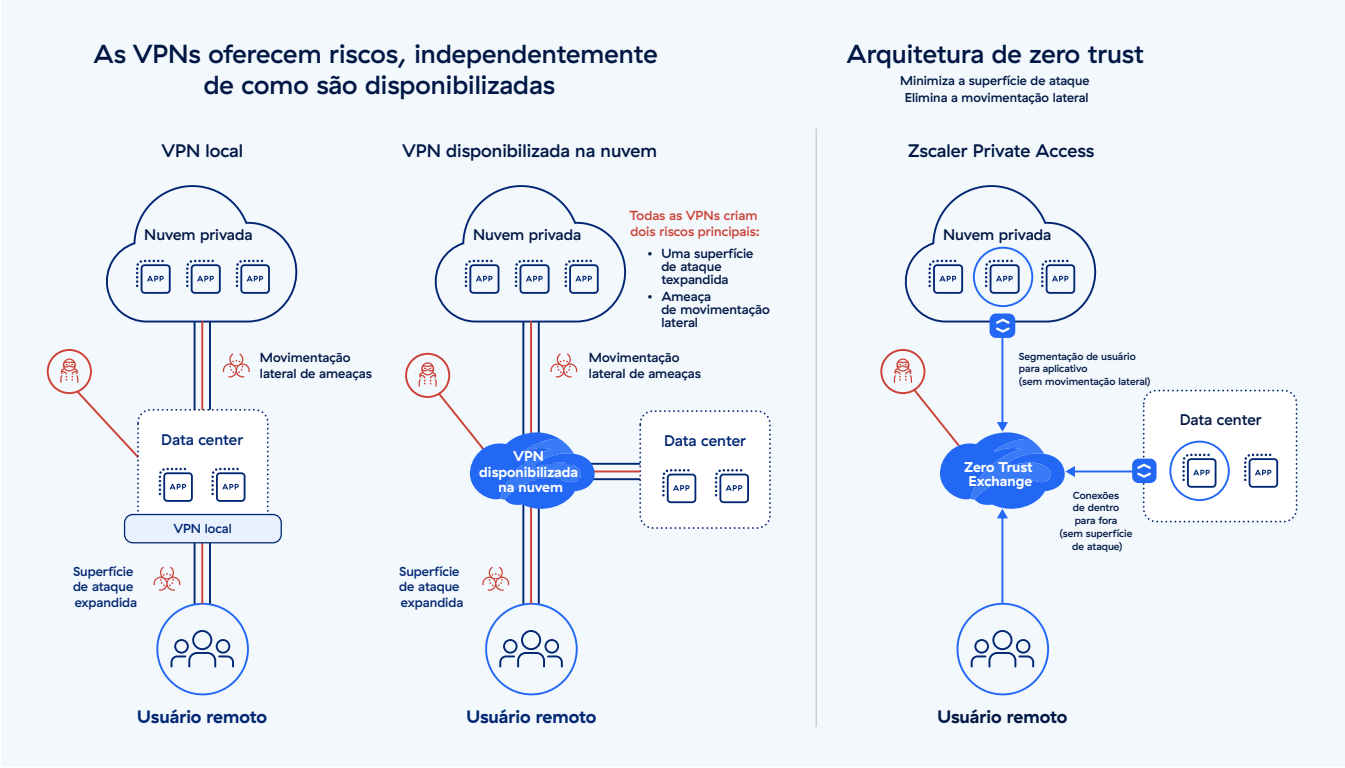
planejam substituir a VPN por uma solução de ZTNA em breve

Por que o zero trust é mais seguro que a VPN

Do ponto de vista arquitetônico, o zero trust e o ZTNA são mais seguros do que as VPNs tradicionais por vários motivos, principalmente devido a uma estrutura de segurança robusta que nunca confia inerentemente em nenhuma conexão específica. As arquiteturas tradicionais baseadas em VPN são suscetíveis a um único ponto de falha. Quando uma VPN ou um dispositivo é comprometido (como por meio de um novo CVE), os criminosos podem explorar a confiança inerente a uma rede plana para obter acesso a toda a rede, mover-se lateralmente, roubar dados e implantar ransomware. É por isso que os profissionais de segurança estão cada vez mais preocupados com os riscos de segurança da VPN.

As VPNs locais e fornecidas na nuvem apresentam vulnerabilidades de segurança semelhantes. Além disso, as VPNs introduzem complexidade, resultando em sobrecarga desnecessária e tarefas demoradas, como provisionamento de usuários, gerenciamento de tabelas de roteamento, solução de problemas de conectividade, aplicação de correções, monitoramento e otimização de desempenho.

Em uma arquitetura zero trust, nenhuma conexão é considerada confiável. Os usuários se conectam diretamente aos aplicativos, nunca à rede subjacente. Além disso, cada conexão é encerrada automaticamente, independentemente da origem, antes de ser verificada por sete camadas de controles de segurança zero trust. A arquitetura zero trust permite que as organizações segmentem de forma abrangente seus ambientes com acesso granular: de usuários para aplicativos, de cargas de trabalho para cargas de trabalho, entre filiais e entre dispositivos, incluindo dispositivos de IoT e TO.



Principais diferenças e vantagens

Superfície de ataque significativamente reduzida
Uma arquitetura zero trust oferece conectividade de dentro para fora que oculta ativos, aplicativos, servidores críticos e muito mais da internet pública, ao mesmo tempo que elimina a necessidade de ativos vulneráveis como VPNs e firewalls. Isso permite que as empresas forneçam conectividade híbrida para suas equipes de trabalho e, ao mesmo tempo, reduzam bastante a superfície de ataque. Por outro lado, as arquiteturas baseadas em VPNs e firewalls exigem que as empresas expandam a superfície de ataque para acomodar o aumento de conectividade.

Verificação contínua
Os modelos de zero trust aplicam a verificação contínua de credenciais e postura de segurança antes de conceder acesso aos recursos, tornando muito mais difícil para entidades não autorizadas obter e manter acesso a informações e sistemas sigilosos. Enquanto isso, com as VPNs, o usuário ou dispositivo geralmente tem amplo acesso aos recursos da rede assim que o acesso é concedido.

Acesso de privilégio mínimo
Os princípios do zero trust aplicam políticas de acesso de privilégio mínimo, garantindo que os usuários e dispositivos tenham acesso apenas aos recursos necessários para suas funções específicas. Isso minimiza o risco de ameaças internas e movimentações laterais dentro de uma rede, vulnerabilidades comuns em infraestruturas de VPN.

Acesso granular e segmentação
Ao dividir os recursos de rede em segmentos separados (entre usuários e aplicativos, entre cargas de trabalho, entre dispositivos) o zero trust isola possíveis violações em zonas menores, reduzindo significativamente o impacto de um ataque. Embora as organizações muitas vezes tentem segmentar seus ambientes de rede, trata-se de um processo operacionalmente complexo e caro que, na prática, muitas vezes permanece incompleto, requer centenas de regras de firewall distintas e expõe áreas de rede mais amplas a usuários autenticados.

Capacitação das atuais equipes de trabalho híbridas
O zero trust possibilita estender facilmente o acesso extremamente rápido a aplicativos privados entre usuários remotos, além da sede, filiais e parceiros terceirizados.

Experiência do usuário aprimorada e complexidade reduzida
O zero trust aprimora a experiência do usuário, eliminando a necessidade de todo o tráfego remoto ser roteado através de um ponto de rede central, um gargalo de desempenho comum com a VPN. Essa arquitetura é mais capaz de lidar com os requisitos de dimensionamento das redes modernas que incluem políticas de IoT e dispositivos pessoais. Além disso, o zero trust reduz a sobrecarga de gerenciamento, automatizando os controles de segurança e simplificando a aplicação de políticas de segurança em toda a rede.

Essas vantagens arquitetônicas fazem do zero trust uma alternativa atraente às VPNs tradicionais, especialmente no atual cenário de ameaças cada vez mais sofisticado e distribuído. Para as organizações que procuram reforçar as suas defesas de segurança cibernética, a adoção de uma abordagem zero trust proporciona uma infraestrutura de segurança mais robusta, flexível e dimensionável.

Previsões sobre VPN para 2024 e para os próximos anos

1 As vulnerabilidades e explorações graves das VPNs aumentarão

Dada a frequência, gravidade e escala das vulnerabilidades de VPN divulgadas no ano passado, as empresas devem esperar que essa tendência continue. Os criminosos e os pesquisadores de segurança estão cientes do risco elevado de vulnerabilidades de alta gravidade em produtos de VPN. Por sua vez, eles estão ativamente à procura de mais, o que torna provável que CVEs adicionais sejam encontrados nos próximos meses e anos.

2 Ataques de alto perfil causados por VPNs ganharão destaque

Intimamente relacionada à nossa primeira previsão, veremos mais organizações de grande porte divulgarem violações resultantes de vulnerabilidades de VPN exploradas. Em parte devido às novas diretrizes regulamentares da SEC, que exigem que as empresas públicas divulguem detalhes sobre violações com impacto material. Como vimos, os criminosos criam backdoors consistentemente em ambientes atacados quando ocorrem vulnerabilidades de VPN, apenas para explorá-los em datas posteriores, mesmo depois de essas vulnerabilidades terem sido corrigidas. À medida que o ano avança, mais desses itens começarão a ser divulgados em arquivos públicos da SEC e a chegar aos noticiários.

3 Um aumento nas ofertas de VPN com tecnologia de IA aumentará as preocupações de segurança e privacidade

Em meio aos avanços contínuos em IA, as soluções de VPN baseadas em IA inundarão o mercado. Contudo, as empresas devem avaliar esses produtos com cautela. Embora prometam um melhor desempenho, a integração da IA amplificará os riscos de segurança e aumentará as oportunidades para os invasores explorarem as vulnerabilidades da VPN. Além disso, surgirão preocupações com a privacidade decorrentes de análises extensivas de dados que aumentam o risco de exposição de informações sigilosas.

4 Os ataques de "password-spraying" em VPNs continuarão a crescer

Os invasores encontrarão cada vez mais maneiras de explorar práticas fracas de gerenciamento de senhas e perfis de conexão de VPN padrão não utilizados por meio de ataques de "password-spraying". Nesses ataques, os criminosos tentam usar a mesma senha em muitas contas de VPN até conseguirem fazer login, obtendo acesso não autorizado. Com inúmeras violações recentes de VPN de alto perfil aproveitando efetivamente essa técnica, as empresas devem esperar que ataques semelhantes persistam.

5 Os gastos empresariais passarão da VPN para a conectividade zero trust

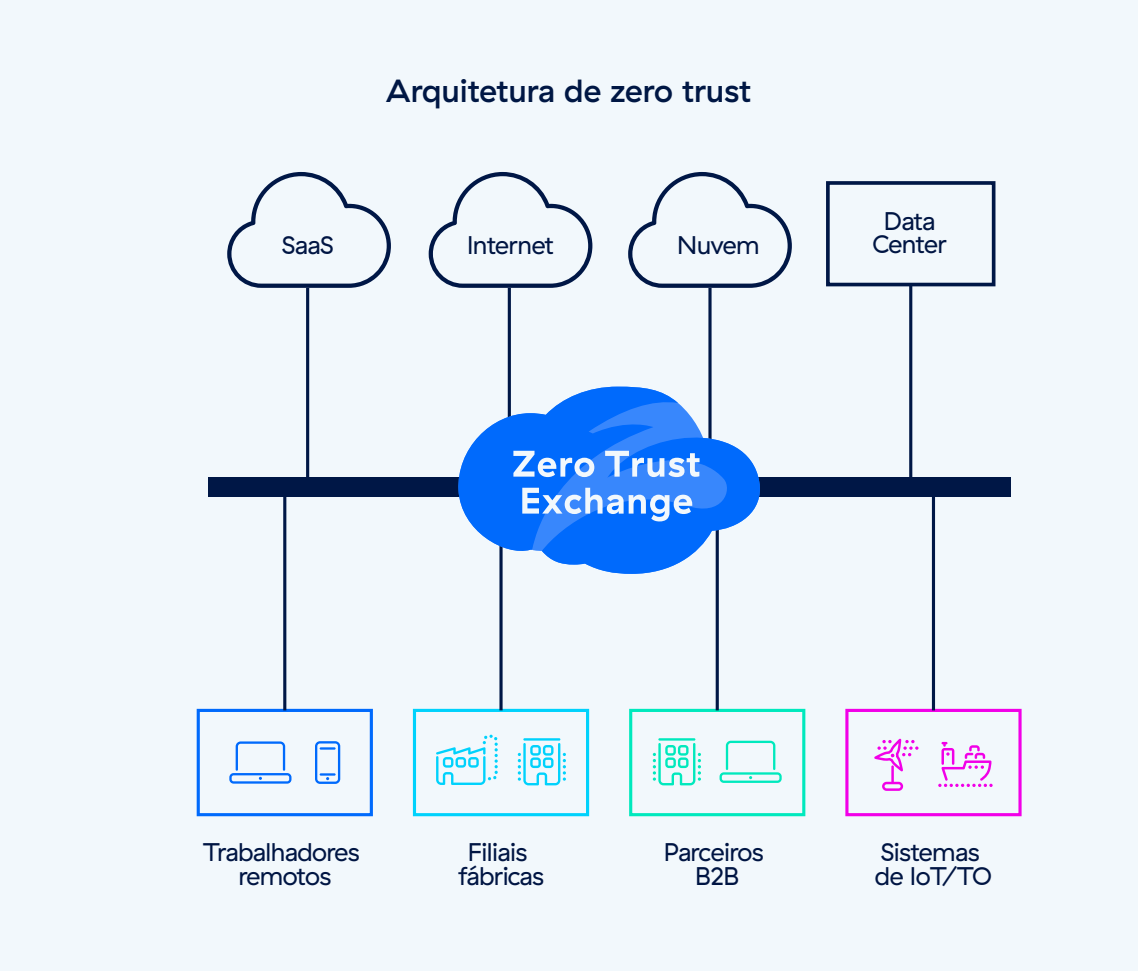
Embora a VPN ofereça há muito tempo conectividade remota para empresas, os desafios de segurança consistentes e crescentes da tecnologia dificultarão justificar gastos a longo prazo. À medida que as empresas consolidam um consenso em torno do zero trust como a arquitetura preferida para segurança e conectividade, os orçamentos empresariais continuarão a mudar para iniciativas de zero trust para proteger equipes de trabalho remotas.

Como a Zscaler oferece a substituição da VPN e a transformação zero trust

Firewalls e VPNs tradicionais criam uma superfície de ataque massiva que permite que invasores vejam e explorem recursos expostos. Ao colocar os usuários na rede e permitir que acessem qualquer aplicativo hospedado, essas abordagens legadas proporcionam aos invasores acesso fácil a dados sigilosos. Elas tornam desafiador e demorado fornecer acesso ou compartilhar com segurança recursos com fornecedores, prestadores de serviços e agências terceirizados. Além disso, elas elevam os custos, aumentam a complexidade e são lentas demais para atender às equipes de trabalho remotas atuais.

A plataforma Zscaler Zero Trust Exchange™, a maior nuvem de segurança integrada do mundo, conecta com segurança usuários, cargas de trabalho, IoT/TO e parceiros B2B sem estender o acesso à rede.

O Zscaler Private Access™ (ZPA™), parte essencial da Zero Trust Exchange, fornece acesso direto a aplicativos privados ocultos atrás da Zero Trust Exchange, minimizando a superfície de ataque, oferecendo segmentação granular de 1:1 entre usuário e aplicativo, eliminando a movimentação lateral e fornecendo proteção de aplicativos privados e inspeção de tráfego em linha, ao mesmo tempo que interrompe ameaças de dia zero, elevando sua postura de segurança. Por ser um serviço nativo da nuvem, o ZPA pode ser implantado em poucas horas para substituir ferramentas de acesso remoto legadas como VPNs e VDIs.



Rede zero trust

O ZPA oferece acesso granular e segmentado com conectividade de dentro para fora para aplicativos e cargas de trabalho privados. Além disso, o ZPA inclui um conjunto abrangente de serviços de controle de acesso, incluindo segmentação de usuário para aplicativo baseada em IA, com recomendações automatizadas para políticas de acesso de usuário e segmentos de aplicativos, segmentação de carga de trabalho para carga de trabalho, acesso remoto privilegiado, borda de serviço privado, acesso por navegador e mais.

Proteção contra ameaças cibernéticas

O ZPA oferece recursos avançados de proteção cibernética para proteger sua organização. Isso inclui recursos de proteção de aplicativos que usam inspeção de segurança integrada para impedir os ataques de aplicativos mais comuns e vulnerabilidades de dia zero, bem como tecnologia de deception que atrai invasores com aplicativos iscas e facilita a detecção de ameaças sofisticadas.

Proteção de dados

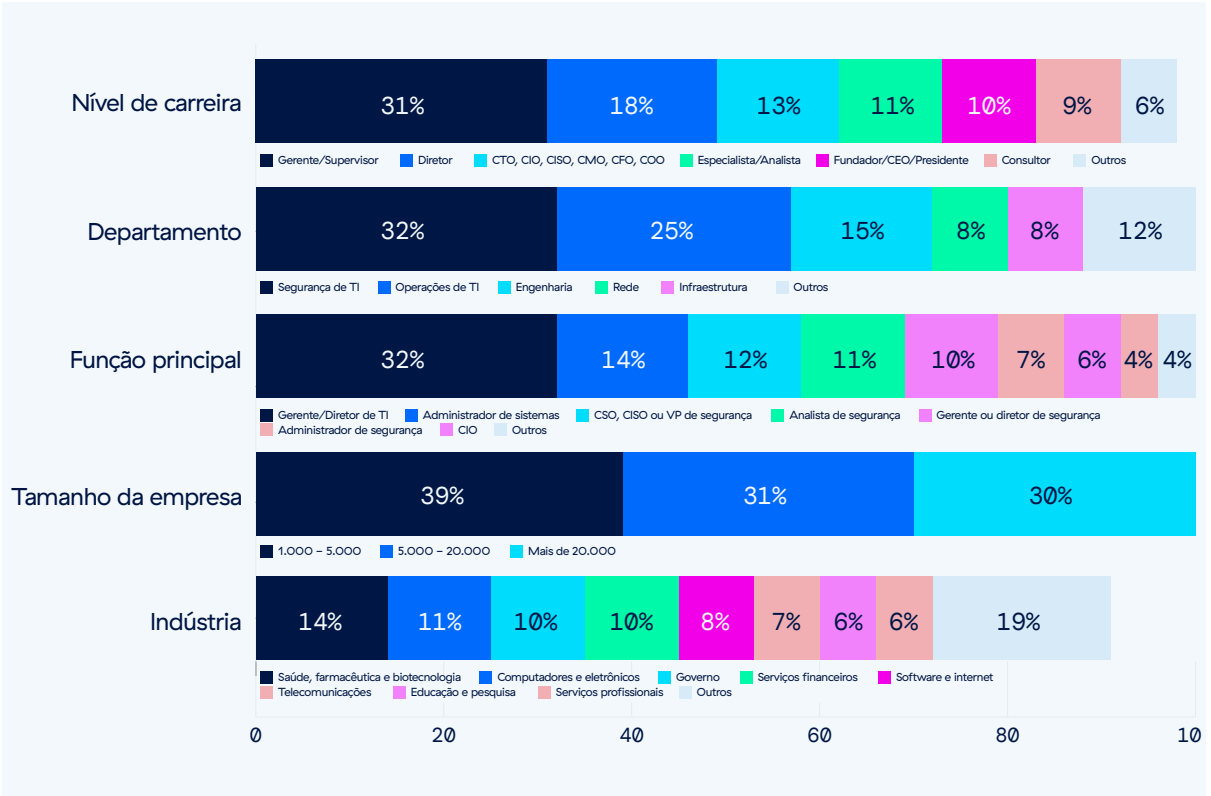
O ZPA fornece proteção holística de dados e interrompe a perda de dados em todos os canais com prevenção contra perda de dados (DLP) na web, DLP de terminais e isolamento de navegador que evita vazamento de dados para usuários vulneráveis e dispositivos pessoais.

Práticas recomentadas para combater riscos da VPN

- **Minimize a superfície de ataque:** forneça acesso direto aos aplicativos, garantindo que tanto os aplicativos quanto os usuários fiquem invisíveis para a internet, evitando efetivamente que invasores os descubram e os explorem para obter acesso inicial.
- **Evite o comprometimento inicial:** inspecione todo o tráfego de maneira integrada para interromper automaticamente explorações de dia zero, malware ou outras ameaças sofisticadas.
- **Bloqueie o acesso não autorizado:** use uma autenticação multifator (MFA) robusta, como senhas ou tokens de uso único, biometria ou credenciais FIDO2 para validar solicitações de acesso do usuário. Por outro lado, o MFA fraco geralmente usa abordagens com perguntas de redefinição de senha.
- **Aplique o acesso de privilégio mínimo:** restrinja as permissões para usuários, tráfego, sistemas e aplicativos com base na identidade e no contexto, garantindo que apenas usuários autorizados possam acessar recursos aprovados (fornecendo segurança adicional em casos de comprometimento da MFA ou roubo de credenciais).
- **Elimine a movimentação lateral:** conecte os usuários diretamente aos aplicativos, e não à rede, para limitar o raio de ação de um possível incidente e mitigar o risco de movimentação lateral da ameaça.
- **Desative usuários comprometidos e ameaças internas:** habilite a inspeção e o monitoramento integrados para detectar usuários comprometidos com acesso à sua rede, aplicativos privados e dados.
- **Impeça a perda de dados:** inspecione os dados em trânsito e em repouso para impedir o roubo ativo de dados durante um ataque.
- **Implante defesas ativas:** aproveite a tecnologia de deception com iscas e realize buscas diárias contra ameaças para inviabilizar e capturar ataques em tempo real.
- **Teste sua postura de segurança:** obtenha avaliações terceirizadas de risco com frequência e conduza atividades de "purple team" para identificar e reforçar as falhas em seu programa de segurança. Solicite que seus provedores de serviços e parceiros de tecnologia façam o mesmo e compartilhe os resultados desses relatórios com sua equipe de segurança.

Metodologia e dados demográficos

Este relatório é baseado nos resultados de uma abrangente pesquisa on-line feita com 647 profissionais de TI e segurança cibernética, conduzida em abril de 2024, para identificar as últimas tendências de adoção corporativa, desafios, falhas e preferências de soluções relacionadas ao risco das VPNs. Os entrevistados variam de executivos técnicos a profissionais de segurança de TI e representam uma seção equilibrada de organizações de vários tamanhos em diversos setores.



Sobre a Zscaler

A Zscaler 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 SASE é a maior plataforma integrada de segurança na nuvem do mundo. Para saber mais, visite www.zscaler.com.br.

Sobre o ThreatLabz

A ThreatLabz é o braço de pesquisa de segurança da Zscaler. Essa equipa de nível internacional é responsável por caçar novas ameaças e garantir que milhares de organizações que utilizam a plataforma global da Zscaler estejam sempre protegidas. Além da pesquisa de malware e análise comportamental, os membros da equipe estão envolvidos na pesquisa e desenvolvimento de novos módulos protótipos para proteção avançada contra ameaças na plataforma da Zscaler e realizam com frequência auditorias de segurança internas para garantir que os produtos e a infraestrutura da Zscaler atendam aos padrões de conformidade de segurança. A ThreatLabz frequentemente publica análises aprofundadas de ameaças novas e emergentes em seu portal research.zscaler.com.br.

Sobre a Cybersecurity Insiders

A Cybersecurity Insiders reúne mais de 600 mil profissionais de segurança de TI e fornecedores de tecnologia de nível internacional para auxiliar na solução inteligente de problemas e na colaboração para enfrentar os desafios de segurança cibernética mais críticos da atualidade.

Nossa abordagem busca criar e curar conteúdo exclusivo que eduque e informe os profissionais de segurança cibernética sobre as últimas tendências, soluções e práticas recomendadas de segurança cibernética. Abrangendo estudos de pesquisa abrangentes, análises imparciais de produtos, guias eletrônicos práticos, webinars envolventes e artigos educacionais, estamos comprometidos em oferecer recursos que forneçam respostas baseadas em evidências para os complexos desafios atuais de segurança cibernética.

Entre em contato conosco hoje mesmo para saber como a Cybersecurity Insiders pode ajudar você a se destacar em um mercado saturado e aumentar a demanda, a visibilidade da marca e a presença de liderança de ideias.

Envie-nos um e-mail para info@cybersecurity-insiders.com ou visite cybersecurity-insiders.com.

Experimente seu mundo, seguro.

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