O caminho para a substituição da VPN:

Explore quando e como as empresas estão substituindo VPNs desatualizadas

Conectividade segura, ágil e pronta para o futuro

74% das organizações reduzirão o hardware substituindo a VPN pelo ZTNA

As VPNs estão enfrentando crescentes vulnerabilidades e as organizações estão lutando com três desafios principais:

44%
dos funcionários em tempo integral são usuários híbridos ou remotos.

27%
dos usuários que acessam recursos internos são terceiros.

50%
dos funcionários acessam recursos internos a partir de dispositivos não gerenciados

Fonte: Pesquisa personalizada do Enterprise Strategy Group encomendada pela Cloudflare, "Considerations for Implementing Zero Trust for the Workforce", julho de 2024.

Embora as vulnerabilidades na VPN sejam bem conhecidas, há uma complacência persistente em mudar para uma alternativa Zero Trust. No entanto, com o risco de segurança aumentando e a experiência do usuário final mais afetada do que nunca, é hora de alinhar internamente e formar um plano para a substituição da VPN.

Introdução

As VPNs estão operando muito além de sua capacidade original e representam tanto um risco de segurança quanto um aumento de ineficiências para empresas, desde pequenas e médias até grandes corporações. Com a mudança de hábitos de trabalho e a proliferação de aplicativos e dispositivos, os funcionários agora estão trabalhando muito além dos tradicionais perímetros de rede. Esta é uma dor de cabeça contínua para aqueles que trabalham nas equipes de segurança e conectividade, onde as funções de conectividade podem abranger responsabilidades de TI, rede e infraestrutura.

As VPNs dificultam que as equipes de segurança cumpram os mandatos da arquitetura moderna e previnam, respondam e remedeiem adequadamente os ataques cibernéticos. E para os responsáveis por TI, redes e infraestrutura, as VPNs limitam a agilidade e a produtividade dos negócios, aumentando a complexidade na integração de novos funcionários e contribuindo para uma experiência do usuário ruim.

A substituição da VPN está na agenda dos líderes cibernéticos e a transição para um serviço de acesso à rede Zero Trust (ZTNA) é um excelente primeiro passo para capacitar as equipes de segurança e rede para fortalecer sua postura de segurança, reduzir os tickets de TI e melhorar a produtividade da equipe.

No entanto, a complacência prevalece no mercado bem como um movimento mais lento para mudar. Isso geralmente ocorre devido à falta de clareza sobre por onde começar a reduzir a dependência da VPN e em que ordem. Mas com as preocupações de segurança e a contínua experiência ruim do usuário final, é fundamental quebrar esse ciclo e priorizar o começar agora.

Este guia fornece aos líderes de TI e segurança exemplos de considerações sobre por onde começar, etapas claras para ajudar na transição para o ZTNA, além de dar exemplos de como outras organizações fizeram essa mudança essencial.

Conteúdo

Custos do atraso

A substituição da VPN geralmente fica na categoria "algum dia". No entanto, alguns cálculos simples podem ajudar a quantificar os verdadeiros custos de adiar o inevitável e dar o pontapé inicial no movimento em direção à mudança.

Para começar, essa calculadora é útil para entender o retorno do investimento na modernização de várias partes de sua pilha de segurança. Como alternativa, abaixo estão algumas ideias de custos envolvidos, que você pode usar e aplicar à sua empresa específica.

Risco de violações de segurança

Em fevereiro de 2024, a Agência de segurança cibernética e de infraestrutura (CISA), em conjunto com agências no Reino Unido, Canadá, Austrália e Nova Zelândia, emitiu um comunicado conjunto sobre agentes de ameaças que exploram vulnerabilidades na Ivanti. O conselho deles foi limitar as conexões de internet de saída dos dispositivos SSL VPN para restringir o acesso ao serviço necessário e limitar as conexões SSL VPN a contas sem privilégios.[1]

Ao escrever na publicação comercial SecurityInfoWatch.com, um dos principais especialistas disse que este é um alerta para todas as organizações ao redor do mundo para reavaliarem suas políticas de acesso remoto seguro.[2]

Além dos custos óbvios das violações de dados e dos danos à reputação, há também os seguros cibernéticos, que não apenas estão se tornando mais caros, mas também mais difíceis de obter.

Nos últimos anos, o custo do seguro cibernético disparou. E embora isso tenha começado a se estabilizar, a lista de exclusões está aumentando.[3]

A seguradora Munich Re sinalizou em um relatório recente que "seguradoras e modeladores de risco continuam a explorar os limites e possibilidades da segurabilidade".[4]

"Em um cenário de ameaças extremamente dinâmico, onde estressores geopolíticos e tecnológicos estão estabelecendo novas prioridades, enfrentar os desafios de segurabilidade e gerenciar o risco de acumulação é fundamental para a sustentabilidade e funcionalidade no longo prazo de um mercado ainda em maturação", afirma o relatório.

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
2. https://www.securityinfowatch.com/cybersecurity/article/55019571/vpns-no-more-new-cisa-advisory-signals-need-for-secure-remote-access-amid-china-sponsored-attacks
3. https://professional.ft.com/en-gb/blog/cyber-insurance-rate-hikes-slow-but-exclusions-expand/
4. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Experiência do usuário e integração ruins

Uma tecnologia ineficiente pode contribuir para a demissão das pessoas. No relatório Workfront's 7th Annual State of Work, 49% dos trabalhadores americanos disseram que deixariam o emprego devido a frustrações com a tecnologia[5].

E com a Gallup[6] estimando que o custo de substituição de um funcionário pode variar de metade a duas vezes o salário anual do funcionário, vale a pena pensar se a experiência do usuário de VPN ruim pode estar afetando a satisfação da equipe.

Isto é particularmente verdadeiro para funcionários cujas funções incluem lidar com informações confidenciais acessadas remotamente, como contadores, onde as pesquisas mostram que a experiência do usuário e a integração adequada de sistemas são algumas das maiores frustrações[7]. Ou aqueles que precisam acessar sistemas diferentes o tempo todo, como desenvolvedores de software. Se o acesso for lento ou ineficiente, isso pode ter um impacto mensurável na produtividade.

Eficiências de negócios e outros custos da empresa

Por outro lado, mudar para uma arquitetura Zero Trust pode gerar eficiências de negócios. Por exemplo, a integração manual pode criar trabalho adicional e aumentar o tempo que leva para que novos funcionários e prestadores de serviços se tornem produtivos, enquanto esperam que o hardware seja enviado manualmente e conectado a aplicativos e programas manualmente. Na verdade, uma empresa relatou uma **redução de 60% no tempo de integração após implementar uma ferramenta ZTNA.**[8]

Outros custos da empresa que podem ser reduzidos incluem o aumento da largura de banda devido aos custos de backhaul e o aumento do hardware.

5. https://www.zdnet.com/article/nearly-half-of-workers-will-quit-their-job-if-their-workplace-technology-is-not-up-to-scratch/
6. https://www.gallup.com/workplace/247391/fixable-problem-costs-businesses-trillion.aspx
7. https://www.icaew.com/technical/technology/technology-and-the-profession/mastering-mid-tier-technology/icaews-mid-tier-research-highlights-shifts-in-technology-adoption
8. https://www.cloudflare.com/case-studies/eteacher-group/

Custos estratégicos do atraso

Grande parte da estratégia empresarial, como por exemplo a atividade de fusões e aquisições (M&A), é afetada por redes e sistemas.

Por exemplo, um relatório da Deloitte[9] estimou que cerca de 60% das organizações consideram a postura de segurança cibernética em seu processo de due diligence como um fator crítico durante qualquer M&A.

"A tecnologia também desempenha um papel importante, não apenas permitindo a integração, mas também impulsionando o novo modelo operacional de negócios. Ela gera toda uma gama de ataques cibernéticos e uma postura de segurança cibernética inadequada pode retardar o processo de aquisição da empresa e, em alguns casos, também impedir o negócio", diz a Deloitte.

E, em um relatório recente do Enterprise Strategy Group, *Considerations for Implementing Zero Trust for the Workforce*, 78% dos líderes seniores de TI entrevistados concordaram que a atividade de fusões e aquisições está gerando a necessidade de acelerar a integração de TI em vários provedores de identidade e redes.[10]

Os custos estratégicos também podem incluir atrasos na implementação de novos aplicativos e até mesmo a perda de certificações de conformidade.

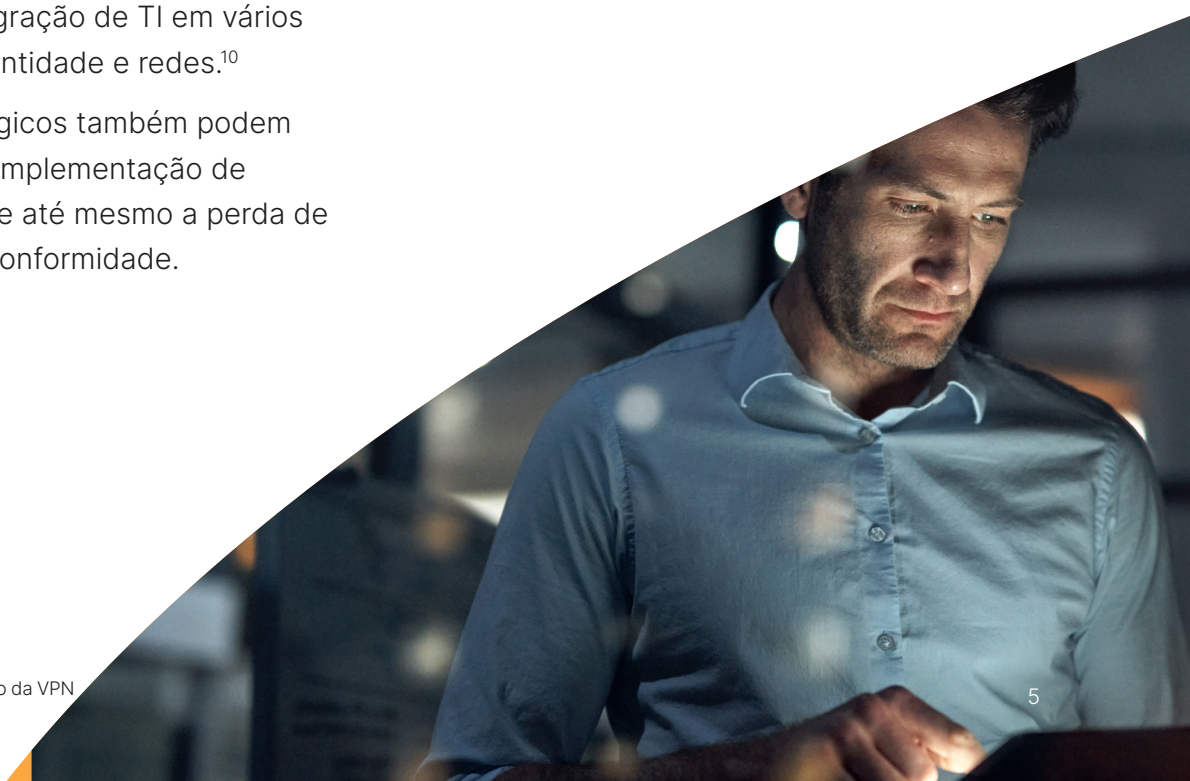
Custos pessoais do atraso

Uma violação cibernética pode refletir negativamente na reputação de todos os envolvidos, desde os diretores de uma empresa até os profissionais de segurança responsáveis pela prevenção de ataques. Pesquisadores da Universidade de Oxford estudaram os impactos de um ataque cibernético, incluindo o psicológico e o na reputação, identificando áreas como a saída de funcionários e relacionamentos prejudicados com os clientes .[11]

Não apenas isso, mas em muitas jurisdições ao redor do mundo, os diretores podem e estão sendo responsabilizados pessoalmente[12].

Além disso, uma VPN ineficiente apenas aumenta as cargas de trabalho da equipe de TI, tanto em termos de ineficiências do usuário quanto de aumento de tickets de TI.

9. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-for-mergers-and-acquisitions-noexp.pdf
10. https://cfl.re/esg-zero-trust-workforce-ebook-2024
11. https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks
12. https://www.whitecase.com/insight-alert/director-liability-cyber-breaches-transatlantic-warning-signs, https://www.allens.com.au/insights-news/insights/2022/04/cyber-risks-resilience-and-responsibilities/



Garantir o alinhamento interno

A substituição da VPN é um projeto multifuncional, portanto, garantir o alinhamento interno é essencial para uma implementação bem-sucedida e oportuna.

Os projetos de substituição de VPN podem ser iniciados por equipes de segurança e de TI/rede/infraestrutura dependendo das necessidades de cada empresa. O importante é que essas equipes trabalhem em conjunto para alinhar a propriedade e a implementação. Um bom ponto de partida é entender todos os grupos que provavelmente estarão envolvidos em uma colaboração e fazer o alinhamento entre as várias dinâmicas de negócios que afetam sua necessidade de promover mudanças.

O patrocínio executivo também pode desempenhar um papel fundamental para ajudar a alinhar as equipes, se necessário.

Um workshop gratuito sobre arquitetura de quadro branco com a equipe de especialistas em segurança da Cloudflare também pode ajudar. Você pode reservar um aqui.

Desafios da segurança legada

Como as VPNs estão limitadas ao perímetro corporativo, é mais difícil prevenir, responder e corrigir incidentes de segurança devido à falta de visibilidade e à incapacidade de restringir o movimento lateral e as permissões de acesso.

Isso resulta em soluções alternativas que são ineficientes para gerenciar e políticas excessivamente restritivas para atender aos mandatos de segurança. E se a conformidade falhar, isso pode levar a multas, incapacidade de fechar negócios e responsabilidade pessoal.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Desafios da conectividade legada

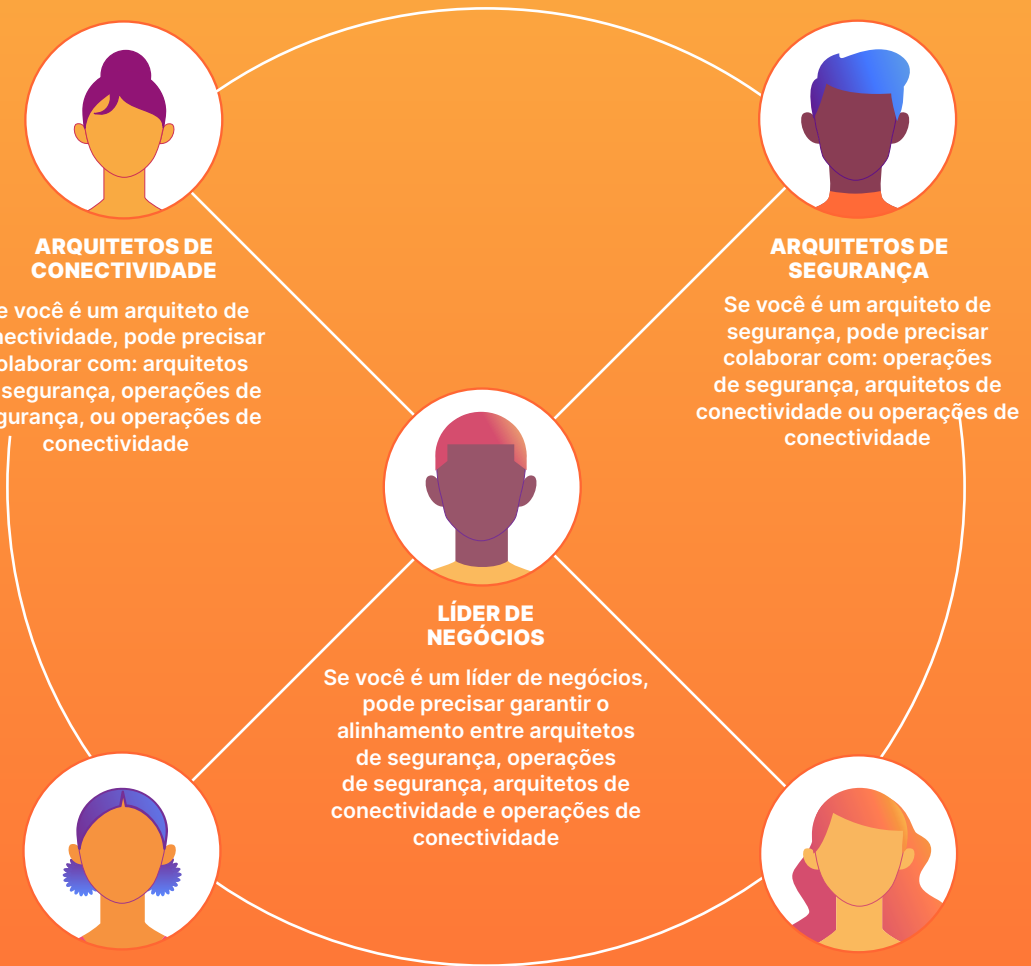
Enquanto isso, para as funções de conectividade (que podem abranger responsabilidades de TI, rede e infraestrutura), uma VPN afeta operações de negócios, colocando limites na agilidade da empresa, especialmente em tempos de crescimento.

Em primeiro lugar, desperdiça tempo de várias maneiras, incluindo a integração de novas contratações usando processos manuais complexos, o gerenciamento de tickets e reclamações excessivos de usuários finais e a configuração de políticas de firewall complexas para tentar segmentar a rede.

Além disso, o tempo resultante de produtividade para novas contratações, perda de produtividade para usuários finais e janelas de manutenção estendidas afetam sua reputação e podem levar à frustração dos executivos de alto escalão.

Confira abaixo para obter mais detalhes.

Você pode precisar colaborar com:



ARQUITETOS DE CONECTIVIDADE

Se você é um arquiteto de conectividade, pode precisar colaborar com: arquitetos de segurança, operações de segurança, ou operações de conectividade

ARQUITETOS DE SEGURANÇA

Se você é um arquiteto de segurança, pode precisar colaborar com: operações de segurança, arquitetos de conectividade ou operações de conectividade

LÍDER DE NEGÓCIOS

Se você é um líder de negócios, pode precisar garantir o alinhamento entre arquitetos de segurança, operações de segurança, arquitetos de conectividade e operações de conectividade

OPERAÇÕES DE CONECTIVIDADE

Se você estiver em operações de conectividade, talvez precise colaborar com: arquitetos de segurança, operações de segurança ou arquitetos de conectividade

OPERAÇÕES DE SEGURANÇA

Se você estiver em operações de segurança, talvez precise colaborar com: arquitetos de segurança, arquitetos de conectividade ou operações de conectividade

	Por que as empresas precisam abandonar a VPN	Valor que a substituição da VPN irá agregar
 **Arquiteto de segurança**	Para os arquitetos de segurança, arquiteturas de segurança legadas fragmentadas significam maior complexidade, possíveis vulnerabilidades e mais dificuldade em atender aos requisitos de conformidade.	A migração para o ZTNA proporciona aos arquitetos de segurança um gerenciamento centralizado de todos os recursos mais importantes. Além de testes simplificados e compreensão da conectividade e acesso em todo o ambiente.
 **Operações de segurança**	As VPNs tradicionais expõem muito a rede, especialmente quando as credenciais do usuário são comprometidas. Elas também são menos escaláveis e eficientes. O crescente número de conexões dificulta a inspeção de tráfego para operações de segurança. Além disso, é difícil atualizar e corrigir redes domésticas e dispositivos de propriedade privada, criando possíveis lacunas de segurança.	A migração para o ZTNA permite que operações de segurança limite a exposição da rede e proteja dados confidenciais, mesmo se as credenciais do usuário forem comprometidas. Também fornece segurança consistente nas redes corporativas e domésticas, sem que seja necessário gerenciar dispositivos privados. Além disso, permite a capacidade de escalar de forma eficaz com cargas de trabalho hospedadas em nuvem e de lidar com a inspeção de tráfego de forma eficiente.
 **Arquiteto de conectividade**	O uso de VPNs cria inconsistências entre os sistemas de TI no escritório e os remotos. Os arquitetos de conectividade podem fazer malabarismos com várias configurações e redundâncias em sua VPN (ou até mesmo vários fornecedores de VPN) para acomodar diferentes departamentos, regiões e empresas subsidiárias. O hardware legado também causa dores de cabeça, principalmente quando não está alinhado à agilidade exigida pelas empresas modernas.	Abandonar as VPNs significa uma arquitetura escalável, flexível, moderna, ágil, confiável e resiliente. Essa mudança também traz mais segurança e conformidade e gera eficiências em custos e operações. Além disso, um serviço ZTNA é mais compatível e mais facilmente integrado às tecnologias existentes
 **Operações de conectividade**	Operações de conectividade, ao usar VPNs, muitas vezes faz malabarismos com vários agentes de dispositivos e vários provedores de proteção de identidade e endpoints, além de lidar com dispositivos privados não gerenciados. Eles precisam gerenciar VPNs configuradas manualmente que consomem muito tempo e geram tickets de usuários. Também são responsáveis por gerenciar gargalos de largura de banda e tráfego. Eles muitas vezes são culpados por problemas de desempenho e interrupções e são cada vez mais responsáveis por fornecer aplicativos para a força de trabalho.	Fazer a transição das VPNs significa menos ferramentas e integrações para operações de conectividade gerenciar. Além disso, alivia a carga de trabalho, pois permite automatizar os fluxos de trabalho o máximo possível e fazer com que os usuários finais façam o autoatendimento para suas solicitações de TI. Além disso, uma boa experiência do usuário final reflete bem neles, um serviço rápido e confiável que aumenta a produtividade, em vez de atrapalhar.

Por onde começar

Depois que as equipes internas estiverem alinhadas, a próxima etapa é elaborar um plano claro de como abordar a implementação do ZTNA.

Um relatório recente do Enterprise Strategy Group encomendado pela Cloudflare, *Considerations for Implementing Zero Trust for the Workforce*,[13] entrevistou tomadores de decisão seniores de segurança de TI na América do Norte e na Europa.

Uma conclusão importante foi que a amplitude de usuários e aplicativos torna a migração para o ZTNA um processo que é melhor se for dividido em fases.

Para simplificar, a pesquisa dividiu a pesquisa em três fases: fase 1: lançamento inicial, fase 2: expansão e fase 3: avanço. Na prática, não há um número "certo" de fases ou maneiras de abordar a implantação do ZTNA, e algumas organizações podem nunca chegar a 100% de substituição, talvez devido ao nicho, a recursos legados ou preocupações gerais de gerenciamento de mudanças. O segredo é começar pequeno e criar impulso em direção à modernização em um ritmo adequado.

Lançamento inicial

No primeiro estágio, a organização identifica as principais prioridades e, em seguida, visa um conjunto limitado de casos de uso ou funcionalidades antes de uma implementação mais ampla.

As organizações devem tentar encontrar projetos que entreguem alto valor em relação ao tempo investido. Isso ajuda a criar impulso e manter o projeto avançando.

Expansão

Na fase 2, a organização lança disponibilidade para um conjunto mais amplo de funcionários, aumenta a cobertura em um conjunto mais amplo de aplicativos ou tira proveito de recursos ou capacidades adicionais.

Avanço

Na fase 3 e além, a organização implanta amplamente a iniciativa para a maioria dos funcionários e aplicativos, usando recursos avançados e garantindo que o projeto atenda aos objetivos gerais.

Se quiser ajudar a mapear seu próprio plano, você pode agendar um workshop gratuito sobre arquitetura de quadro branco com a equipe de especialistas em segurança da Cloudflare aqui.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Porcentagem média de usuários e aplicativos abordados durante o lançamento inicial

25%
Lançamento inicial

Grupos de usuários mais comuns
- Vendas
- TI
- Executivos de alto escalão

Tipos de aplicativo mais comuns
- ERP
- Comunicação e colaboração
- Armazenamento e compartilhamento de arquivos

Benefícios da implantação sem agente

Quase três quartos (71%) dos entrevistados disseram que suas ferramentas de ZTNA atuais apoiaram a implantação sem agente e 84% disseram que isso os ajudou a acelerar significativamente a adoção do Zero Trust por meio de implantação simplificada.

Os entrevistados também concordaram que o ZTNA sem agente abordou efetivamente os casos de uso, usuários e aplicativos que queriam abranger, o que significa que eles poderiam expandir a cobertura sem implantar ferramentas adicionais que usam agentes.

Benefícios percebidos com a implantação sem agente

Aprox. 84%

dos entrevistados

- **A implantação simplificada reduziu a carga administrativa e os possíveis pontos de falha**
- **Adoção de Zero Trust significativamente acelerada**
- **Escalabilidade mais fácil, eliminando instalações de agentes individuais em cada dispositivo**
- **Atende com eficácia aos nossos casos de uso e escala para o número desejado de usuários e aplicativos**

Como outros clientes adotaram o Zero Trust

Conforme mencionado, as equipes de segurança e conectividade têm seus próprios impulsionadores para querer substituir as VPNs, e o movimento em direção à substituição pode ser iniciado a partir de qualquer um deles e ampliado à medida que mais colaboradores aderem. Não há uma maneira definida de fazer isso, pois a propriedade do projeto varia de empresa para empresa.

Para fornecer algumas ideias de como isso pode ser, aqui estão algumas histórias de clientes que destacam os principais catalisadores e o valor obtido com a substituição da VPN do ponto de vista de arquitetos e operações de segurança e arquitetos e operações de conectividade, embora haja, é claro, um cruzamento. Essas histórias de clientes analisam como as empresas migraram desses pontos de partida ao longo da transição e, em seguida, destacam os principais resultados para a organização.

ESTUDO DE CASO

Arquiteto de segurança

Conglomerado de mídia e publicidade que protege mais de 50 mil trabalhadores do conhecimento

A necessidade de resolver vulnerabilidades de segurança urgentes levou a uma mudança no longo prazo

Em 2022, um grande conglomerado de mídia e publicidade decidiu retirar suas operações da Rússia após a invasão da Ucrânia. Pouco tempo depois, a empresa começou a enfrentar tentativas de ataque aos seus sites públicos. As preocupações sobre essas ameaças, inclusive se tornar um alvo para agentes apoiados pelo estado, aumentaram a ponto de a empresa desconectar todos os ativos da web e vários aplicativos internos críticos em uma noite de domingo.

Solução

A Cloudflare, em colaboração com um importante parceiro de implementação, iniciou uma resposta rápida para mitigar ameaças direcionadas a sites externos. Como próximo passo, a empresa implementou o serviço acesso à rede Zero Trust (ZTNA) da Cloudflare para proteger alguns dos aplicativos baseados na web críticos que haviam sido interrompidos de forma mais severa para milhares de usuários.

Em 48 horas, a empresa conseguiu retomar operações comerciais críticas. E em poucos dias, a empresa implementou o ZTNA para vários milhares de funcionários adicionais.

Depois de restabelecer suas operações comerciais estáveis, a empresa começou a reconsiderar sua abordagem de longo prazo para proteger o acesso. A mudança da aplicação da política de acesso para uma rede em nuvem distribuída globalmente ofereceu uma oportunidade de oferecer uma experiência mais consistente aos funcionários, que trabalhavam em muitos países, tanto remotos quanto no escritório.

Nos meses seguintes, a empresa estendeu as políticas baseadas em identidade e em grupo para centenas de aplicativos e milhares de usuários. Em maio de 2022, quase 50 mil estavam usando a Cloudflare para se autenticar em seus aplicativos mais usados, reduzindo a maior parte do tráfego das VPNs existentes da empresa.

Resultados

A empresa estima que modernizar sua segurança com o Cloudflare Zero Trust em toda a organização pode reduzir os custos em mais de US$ 5 milhões anualmente, graças à economia de tempo na administração de TI, ganhos de produtividade para os usuários finais, menores gastos com VPN e outras ferramentas legadas e à menor probabilidade e redução dos possíveis impactos de uma violação de dados.

ESTUDO DE CASO

Operações de segurança

A EQT protege mais de 2 mil trabalhadores do conhecimento

EQT

A rápida escala da força de trabalho apresentou um desafio para a segurança

A empresa de investimentos com sede na Suécia, EQT, expandiu sua presença global e regional, ampliou rapidamente sua força de trabalho e concluiu uma grande migração para a nuvem. As mudanças combinadas aumentaram os riscos para a equipe central de TI e segurança responsável por proteger seus funcionários e investidores, bem como fornecer suporte à segurança para as empresas de seu portfólio.

Anteriormente, a EQT dependia de ferramentas tradicionais, como o Active Directory no local da Microsoft, para definir políticas de acesso para seus aplicativos no local. Para complicar as coisas, logo após sua migração para a nuvem, a EQT dependia de uma combinação de seus próprios proxies personalizados e VPN no local, que eram difíceis de manter e nem sempre seguros.

Ao mesmo tempo, a EQT estava se concentrando no desenvolvimento de seus próprios aplicativos internos para impulsionar o crescimento dos negócios e, por sua vez, na contratação de mais desenvolvedores que precisavam de acesso seguro e simplificado. A empresa tinha mais de vinte aplicativos web proprietários que eram usados todos os dias para trabalhos importantes por um número crescente de usuários.

Solução

Hoje, a EQT protege o acesso a todos os aplicativos auto-hospedados para todos os funcionários e prestadores de serviços empregando o serviço acesso à rede Zero Trust (ZTNA) da Cloudflare. Usando uma abordagem Zero Trust, a Cloudflare autentica uma solicitação para um aplicativo somente após verificar a identidade do usuário, neste caso, com base na integração com o provedor de identidade da EQT, o Okta.

A EQT também conseguiu automatizar a grande maioria dos processos de configuração de políticas por meio da integração da Cloudflare com o Terraform, a ferramenta de infraestrutura como código.

Resultados

A semana inteira, agora leva cinco minutos.

As equipes de segurança da EQT valorizam o poder de fortalecer a segurança com políticas de negação padrão e privilégios mínimos que são consistentes com as práticas recomendadas de Zero Trust, ao mesmo tempo em que simplificam a experiência para seus funcionários.

Antes da Cloudflare, alterar ou criar políticas de acesso a aplicativos podia levar até uma semana inteira, agora o processo leva cinco minutos.

Arquiteto de conectividade

A Canva conecta mais de 7 mil trabalhadores do conhecimento

Canva

A expansão exigia maior agilidade e simplificação

A plataforma de design gráfico da Canva é usada por milhões em todo o mundo. À medida que a empresa se expandia, contratava mais funcionários e terceirizava mais trabalho para desenvolvedores terceirizados, os administradores de TI se confrontaram com a necessidade de encontrar uma maneira melhor de autenticar usuários e rastrear o uso de aplicativo.

Solução

A Canva precisava de uma solução que lhe permitisse continuar a escalar globalmente e manter o alto desempenho sem sacrificar a segurança.

Para melhorar a segurança e a eficiência, a Canva adotou a Cloudflare, que fornece acesso seguro aos aplicativos internos. Após um piloto bem-sucedido com o CanvaWorld, uma plataforma interna de mídia social, a Canva expandiu o uso do ZTNA para testes internos e fluxo de trabalho de desenvolvimento de front-end.

Resultados

Eliminar as ineficiências causadas por senhas compartilhadas

Além de eliminar as ineficiências causadas por senhas compartilhadas, o Cloudflare Zero Trust melhorou bastante a segurança dos aplicativos internos da Canva e evitou que ela desenvolvesse seu próprio sistema de gerenciamento de identidade e acesso (IAM).

Isso também significou que a Canva não precisou criar funções de permissão de usuários nos aplicativos que o ZTNA protege. Por exemplo, a empresa queria conceder aos funcionários diferentes níveis de permissões no CanvaWorld, algo que o ZTNA permite.

O ZTNA também torna a integração e o desligamento de funcionários e prestadores de serviços mais fácil e seguro. Isso significa que, conforme as pessoas vão e vêm, a Canva pode simplesmente adicioná-las e removê-las. Não há necessidade de alterar uma senha comum, depois salvá-la em um arquivo e notificar a todos.

ESTUDO DE CASO

Operações de conectividade

A Delivery Hero conecta mais de 40 mil trabalhadores do conhecimento

Delivery Hero

A rápida expansão precisava de integração simplificada e menos problemas de conectividade

Entre 2016 e 2020, a plataforma de entrega Delivery Hero expandiu o alcance global e aumentou sua força de trabalho de cerca de 9 mil para cerca de 30 mil funcionários. A TI e a segurança da empresa lutavam para acompanhar a integração de novos usuários e empresas com diferentes pilhas de tecnologia. A mudança para o trabalho remoto em 2020 aumentou as demandas de segurança ainda mais, forçando a Delivery Hero a gerenciar uma superfície de ataque expandida.

A Delivery Hero dependia de uma solução de VPN, que era ineficiente para gerenciar e lenta para os usuários finais.

Solução

A Delivery Hero garantiu primeiro o acesso a aplicativos internos usando o Cloudflare One, uma plataforma de serviço de acesso seguro de borda (SASE) que inclui um serviço ZTNA para proteger o acesso remoto.

Eles se concentraram primeiro na aplicação de verificações baseadas em identidade para aplicativos web, um caso de uso inicial comum que não requer a implantação de nenhum software cliente de dispositivo.

Depois de proteger o acesso aos recursos internos com a Cloudflare, a Delivery Hero iniciou um processo semelhante para segurança em todos os seus recursos voltados para o público, que incluem sites, aplicativos de clientes para computadores e dispositivos móveis e portais administrativos voltados para o fornecedor.

Resultados

Escalar com mais eficiência simplificando o processo

Hoje, a Delivery Hero usa a Cloudflare para proteger o acesso de mais de 40 mil funcionários a todos os aplicativos em ambientes auto-hospedados, SaaS e não web. A aplicação de verificações de identidade de logon único ajudou a Delivery Hero a melhorar sua postura de segurança com as práticas recomendadas de Zero Trust e a simplificar a experiência para os usuários finais.

A adoção da Cloudflare também ajudou a Delivery Hero a escalar com mais eficiência, simplificando o processo de integração de novos funcionários e consolidando políticas de acesso em uma única plataforma. Isso liberou tempo e energia para a equipe técnica da Delivery Hero se concentrar na inovação e não na administração.

Escolher um provedor

Embora muitos fornecedores de segurança ofereçam uma capacidade semelhante de criar políticas de acesso Zero Trust, nem todos os provedores são criados iguais.

A solução da Cloudflare, por exemplo, é mais rápida e fácil de implantar, usando uma configuração simples de implantação sem agente com operações uniformes para expansão perfeita para mais vias de acesso e serviços in-line.

E, uma vez implantada, a Cloudflare oferece uma experiência do usuário final de baixa latência com serviços de segurança entregues perto dos usuários finais, disponíveis em todos os lugares para todos em escala global.

Também é resiliente, fornecendo conectividade confiável de ponta a ponta e um backbone privado com roteamento de tráfego e balanceamento de carga automatizado como código, além de inteligência contra ameaças integrada. A arquitetura de rede Anycast da Cloudflare permite um SLA de 100% para planos pagos.

Além disso, com os serviços combináveis da Cloudflare, disponíveis em todos os lugares, você pode facilmente passar para a implantação do restante de uma estratégia SSE ou SASE quando estiver pronto. A substituição da VPN pela nuvem de conectividade da Cloudflare impulsiona a modernização e a consolidação mais amplas da TI/segurança.

Próximas etapas

Superar a complacência e abandonar as VPNs é imperativo. E adiar o inevitável só custará tempo e dinheiro, além de aumentar o risco e as chances de responsabilidade da empresa.

Para obter mais informações sobre como implantar o ZTNA com a Cloudflare, dê uma olhada nos nossos guias de implementação tanto para acesso sem cliente à web como para substituição de sua VPN.

Se quiser, você pode agendar um workshop gratuito sobre arquitetura de quadro branco com nossa equipe de especialistas em segurança aqui.

Outra opção é entrar em contato conosco em caso de dúvidas ou para uma conversa mais detalhada.

Agende um workshop sobre arquitetura de quadro branco para saber mais

Sobre a Cloudflare

Cloudflare, Inc. (NYSE: NET) é uma plataforma unificada e inteligente de serviços nativos de nuvem programáveis que oferece segurança incomparável para proteger pessoas, aplicativos e redes, permitindo que as organizações retomem o controle, reduzam custos e os riscos de proteger um ambiente de rede expandido.

Saiba mais sobre a Cloudflare em **cloudflare.com/connectivity-cloud**. Saiba mais sobre as tendências e insights mais recentes da internet em **radar.cloudflare.com**.

Siga nos: **Blog** | **X** | **LinkedIn** | **Facebook** | **Instagram**

Contato

+55 (11) 3230-4523
www.cloudflare.com/pt-br/

CLOUDFLARE