RELATÓRIO

O estado de Zero Trust

FORTINET

Resumo executivo

Redes distribuídas e uma força de trabalho híbrida estão transformando rapidamente os ambientes de rede atuais. Os trabalhadores dividem seu tempo entre escritório, casa e algum lugar no meio disso. As aplicações são divididas entre implantações no local, na nuvem e de Software como Serviço (SaaS). E os dados, outrora a única província do data center, são cada vez mais distribuídos em vários locais. Nos últimos anos, garantir que todos os usuários e dispositivos tenham acesso seguro e confiável aos recursos críticos de que precisam tem sido uma das principais prioridades das equipes de TI. E o acesso precisa ser fácil, não importa onde o usuário esteja ou onde as aplicações e os ativos tenham sido implantados.

O relatório "O estado de Zero Trust" de 2023 da Fortinet analisa o progresso das equipes de TI ao estabelecer um novo senso de normalidade após a turbulência da rede iniciada pelo início da pandemia. Com a maioria dos funcionários trabalhando repentinamente fora do perímetro da rede, as equipes de TI se esforçaram para manter as empresas funcionando. Esse esforço geralmente assumia a forma de correções rápidas e soluções alternativas que expunham os pontos fracos de sua estratégia de trabalho remoto. Ele também destaca os desafios de colocar seus ambientes de rede em rápida expansão sob um guarda-chuva de segurança unificada.

Ambientes externos, como escritórios domésticos desprotegidos ou soluções em nuvem mal configuradas implementadas por equipes de DevOps com pouca experiência em segurança, tornaram-se novos vetores de ataque para cibercriminosos. Logo, acabou ficando óbvio que o modelo de confiança implícita em muitas organizações era um problema. No entanto, muitas equipes de TI tentaram resolver o problema da maneira tradicional, lançando tecnologia no problema. E não demorou muito para que elas enfrentassem um novo problema: fazer com que diferentes soluções de pontos trabalhassem juntas. Esses desafios são refletidos neste relatório, que inclui uma série de descobertas importantes.

Organizações de todos os tamanhos estão implementando ativamente estratégias de Zero Trust, mas os desafios permanecem.

- Desde 2021, as empresas implantaram consideravelmente mais soluções como parte de suas estratégias de Zero Trust.
- As empresas estão procurando habilitar a Zero Trust em todos os lugares para minimizar o impacto de uma violação.
- Embora as empresas estejam avançando, elas ainda enfrentam desafios, incluindo interoperabilidade entre soluções, visibilidade consistente, aplicação de políticas de ponta a ponta e problemas de latência de aplicações.
- Os entrevistados também reclamaram da falta de informações confiáveis para ajudá-los a selecionar e projetar uma solução.

As soluções devem abranger usuários locais e remotos com uma política consistente de acesso a aplicações, e o sucesso foi variado.

- Muitas soluções, como acesso à rede Zero Trust (ZTNA) e Secure Access Service Edge (SASE), são apenas na nuvem. No entanto, as empresas precisam proteger o acesso seguro a aplicações no local e fora da rede. Notavelmente, quase 40% das organizações ainda hospedam mais da metade de suas aplicações no local.
- O desafio mais significativo em qualquer estratégia de Zero Trust é a necessidade de mais integração entre ambientes de nuvem e de local.
- Três quartos dos entrevistados encontraram problemas com sua força de trabalho híbrida por dependerem apenas do ZTNA na nuvem.
- As prioridades máximas para as soluções SASE variam, mas a "eficácia de segurança" é a mais significativa, com 58% colocando-a em suas três principais prioridades.

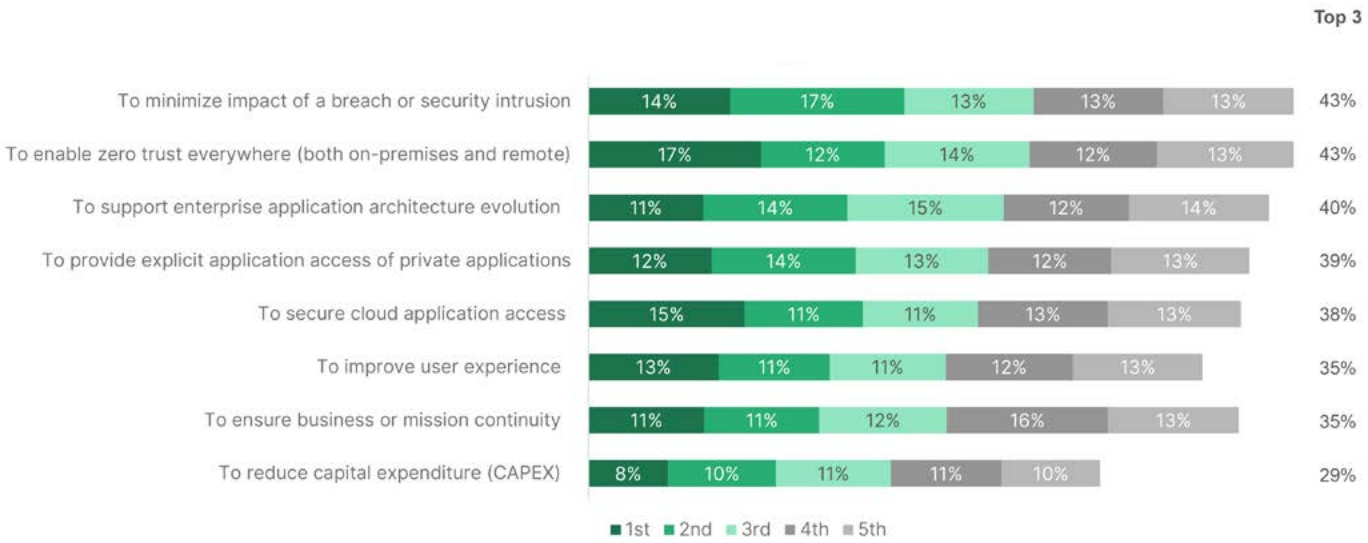
A consolidação de fornecedores e a interoperabilidade da solução são cruciais.

- A implantação de soluções de vários fornecedores criou muitos desafios para as organizações, incluindo a introdução de novas lacunas de segurança e altos custos operacionais.
- As empresas maiores estão especialmente interessadas em consolidar soluções para simplificar as operações e reduzir a sobrecarga.

Prioridades da estratégia de Zero Trust

A pandemia iniciou uma drástica transformação da força de trabalho, com a grande maioria dos funcionários que tradicionalmente trabalhavam no local de repente trabalhando em casa. Essa mudança desencadeou uma reviravolta tão drástica quanto nas redes, essencialmente virando-as do avesso. Quase que da noite para o dia, as organizações precisaram criar acesso seguro à rede para aplicações e recursos críticos em todo o perímetro, o que muitas vezes exigia a atualização de tecnologias de acesso remoto, como ferramentas de segurança de borda. Ao mesmo tempo, as limitações das VPNs tradicionais tornaram-se aparentes quando os hackers começaram a acessar os recursos corporativos sequestrando túneis de VPN através de redes domésticas desprotegidas. Os planos para mover aplicações para a nuvem foram acelerados para descarregar a pressão no perímetro da rede e melhorar a experiência do usuário.

Claro, nenhuma dessas mudanças foi totalmente inesperada. A mudança para uma força de trabalho híbrida estava em andamento há algum tempo, mas a pandemia acelerou o processo. Muitas organizações não estavam prontas para a transição repentina para o trabalho remoto e não dispunham das tecnologias que as circunstâncias exigiam. Apesar desses problemas, dois terços das organizações decidiram manter uma força de trabalho híbrida, sendo que os empregadores maiores se mostraram mais propensos a apoiar trabalhadores remotos do que os menores. O desafio tem sido fornecer acesso consistente e experiência do usuário excepcional para os trabalhadores que transitam entre o trabalho remoto e no local. Tem sido particularmente difícil para as 72% das organizações que optaram por uma solução ZTNA somente na nuvem fornecer acesso seguro a aplicações críticas.

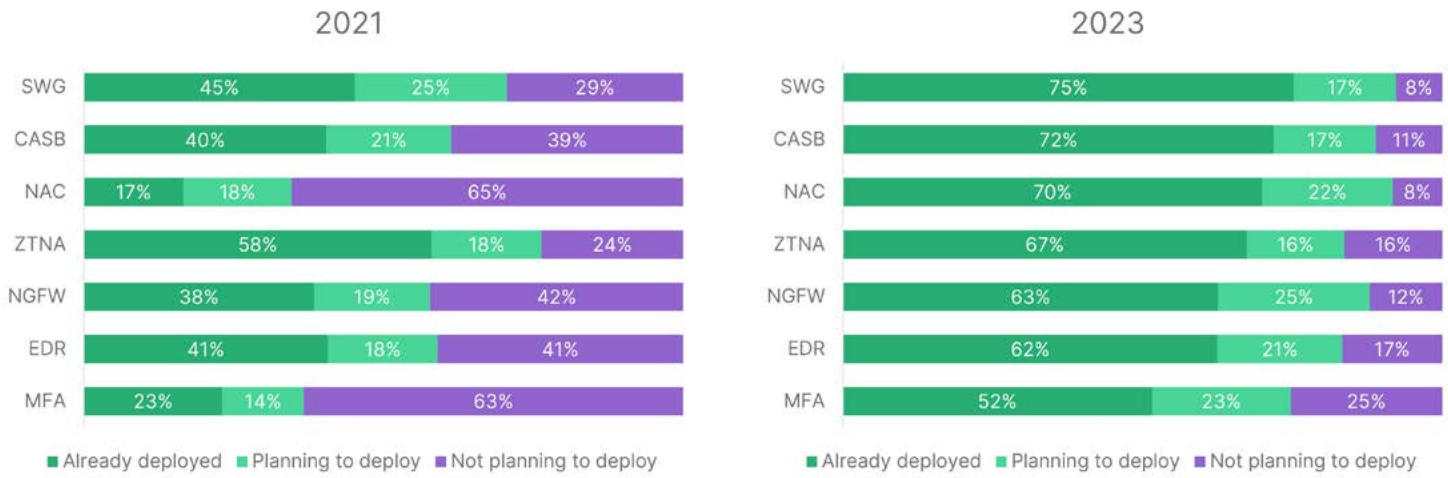


Prioridades da estratégia de Zero Trust

Logo no início, ficou claro que a melhor abordagem para gerenciar e garantir uma força de trabalho sem localização permanente era iniciar uma estratégia de Zero Trust que eliminasse a confiança implícita com base na localização e aplicasse o princípio de privilégios mínimos. Há diversas razões para implementar a Zero Trust, mas 34% identificaram a minimização do impacto de violações e invasões e 29% citaram a ativação da Zero Trust em todos os lugares como seu principal incentivo. Curiosamente, apenas 18% selecionaram a redução das despesas de capital. Embora seu principal objetivo ao escolher uma solução de Zero Trust (classificada como extremamente ou muito importante) fosse garantir a segurança da camada de aplicações (85%), a compatibilidade com as configurações no local e na nuvem (82%) e a integração com o restante de sua infraestrutura de rede e segurança (82%) também eram muito altas.

As organizações também relatam estar mais bem preparadas para apoiar e proteger sua força de trabalho híbrida com uma ampla variedade de soluções já em vigor para apoiar suas estratégias de Zero Trust. As soluções que foram implementadas incluem Secure Web Gateways (SWGs) a 75%, agentes de segurança de acesso à nuvem (CASB) a 72%, controle de acesso à rede (NAC) a 70%, ZTNA a 67%, Next-Generation Firewalls (NGFWs) a 63% e detecção e resposta a ameaças de endpoints (EDR) a 62%. A única surpresa foi a implementação relativamente baixa da autenticação multifator (MFA), com apenas 52%, o que é fundamental para impedir o acesso não autorizado a aplicações e outros recursos.

As organizações que ainda não implementaram uma estratégia de Zero Trust indicam que planejam investir em muitas dessas mesmas tecnologias como parte de sua estratégia de Zero Trust. Os números aumentaram significativamente a partir de 2021: SWG (de 45% para 75%), CASB (de 40% para 72%), NAC (de 17% para 70%), ZTNA (de 58% para 67%), NGFW local (de 38% para 63%), EDR (de 41% para 63%) e MFA (de 23% para 52%).



Já planejou ou está planejando implantar como parte da estratégia de Zero Trust

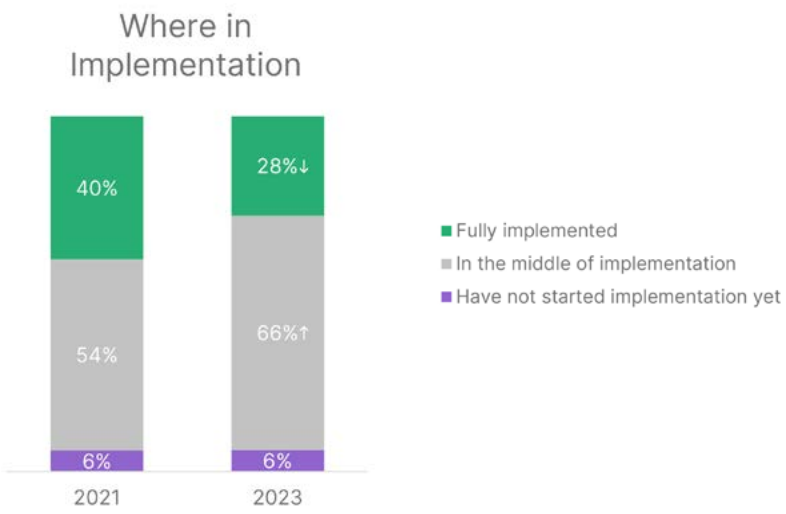
No entanto, as organizações também enfrentam sérios desafios na implementação de uma estratégia de Zero Trust. Quase metade dos entrevistados (48%) indicou que a falta de integração entre as soluções de Zero Trust implantadas no local e na nuvem é a lacuna mais significativa que eles precisam resolver. Esse achado também pode estar vinculado às respostas mais comuns subsequentes, que são a incapacidade de autenticar consistentemente usuários e dispositivos (46%), a incapacidade de fornecer uma experiência do usuário consistente (40%) e a incapacidade de monitorar os usuários após a autenticação (38%).

Outra descoberta significativa foi que quase um terço (31%) também relatou problemas de latência como um desafio significativo, e quase um quarto (22%) lamenta sua dependência excessiva de VPNs tradicionais. A implementação de uma solução de baixa latência é claramente fundamental para uma implantação bem-sucedida do ZTNA.

Status da implementação e desafios

O status da implementação da Zero Trust mudou surpreendentemente entre as pesquisas de 2021 e 2023. Em 2021, 40% dos entrevistados indicaram que sua estratégia de Zero Trust foi totalmente implementada. Mas em 2023, apenas 28% relataram ter uma solução completa de Zero Trust em vigor. E apenas 36% dos fabricantes afirmam estar totalmente implementados, talvez por também terem que lidar com a integração de redes de TI e tecnologia operacional (TO). O número de entrevistados que agora relatam estar em processo de implementação é de 66%, acima dos 54% da pesquisa anterior.

Existem várias razões por trás dessa mudança no status de implementação. A primeira é que o escopo da adoção da Zero Trust evoluiu. O ímpeto inicial foi conectar de forma rápida e segura os trabalhadores remotos às aplicações. Mas a transição para um modelo híbrido, no qual os usuários transitam entre o trabalho remoto e no local, e os dados e aplicações são divididos entre a nuvem e os data centers, expandiu esse objetivo. Os dados precisam estar igualmente disponíveis, independentemente da localização de qualquer coisa, o que significa que são necessárias mais tecnologias do que se supunha no início.



Uma mudança no status da implementação da Zero Trust

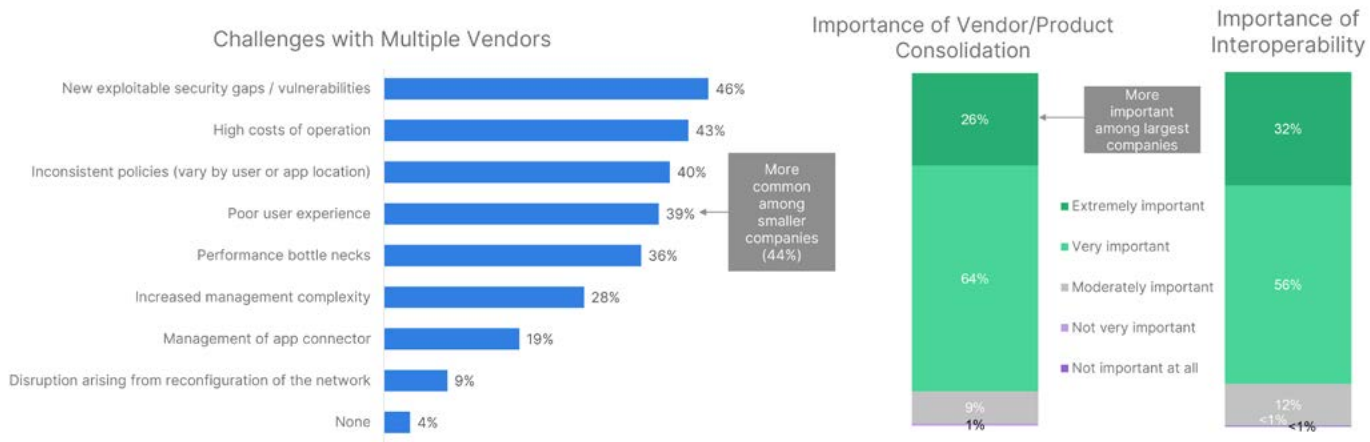
Os fluxos de dados inicialmente pensados para simplesmente ir do usuário para a aplicação e voltar também mudaram. Os fluxos de trabalho geralmente abrangem vários ambientes em uma única transação, o que complicou e ampliou significativamente a implementação. As soluções em nuvem devem se integrar perfeitamente à rede local para detectar e prevenir o movimento lateral de ameaças e a aplicação consistente de políticas de ponta a ponta.

Outra razão para a mudança na implementação é que alguns problemas não se tornaram aparentes até que várias soluções já estivessem em vigor, e a necessidade de interoperabilidade entre soluções de pontos isoladas tornou-se essencial. Criar e solucionar estratégias alternativas para ferramentas que não funcionam juntas de forma nativa pode consumir rapidamente uma parte significativa dos recursos de TI. Duas das maiores barreiras são que 16% das organizações (24% entre empresas menores) reclamam que há informações insuficientes disponíveis para selecionar uma solução de Zero Trust, e um quarto (24%) cita a falta de fornecedores qualificados capazes de fornecer uma solução completa, exigindo que eles montem algo por conta própria. Apenas 4% citaram a falta de recursos humanos (diminuindo de 7%). Uma vez que ficou claro que o trabalho híbrido não era temporário, uma solução mais consistente e confiável se fez necessária e os recursos foram disponibilizados.

Os desafios mais significativos na implementação da Zero Trust

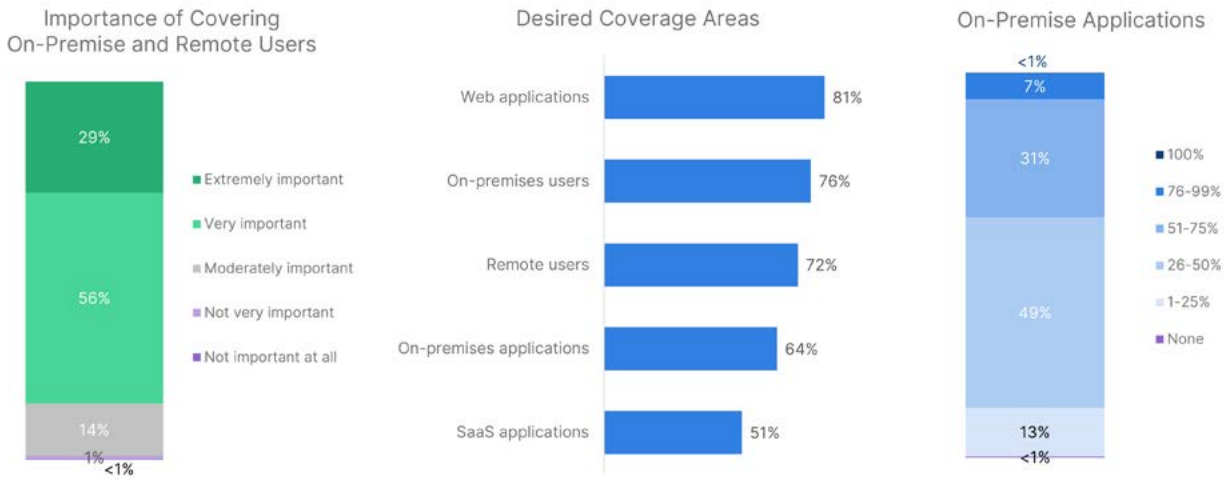
Outra conclusão importante deste relatório é que a implantação de soluções de vários fornecedores criou novos desafios para as organizações, incluindo a introdução inadvertida de lacunas de segurança e altos custos operacionais devido à expansão de fornecedores e soluções. De acordo com a pesquisa, 90% das organizações agora classificam a consolidação de fornecedores e soluções como extremamente ou muito importante, e 88% sentem o mesmo sobre a importância da interoperabilidade da solução. Um resultado disso é que muitas organizações que acreditavam ter implementado totalmente uma solução de Zero Trust agora estão repensando essa conclusão. É claro que a consolidação e a interoperabilidade de fornecedores e produtos são de importância crucial para a implementação.

Para quase metade dos entrevistados (46%), as principais preocupações envolvem a criação de novas lacunas e vulnerabilidades de segurança exploráveis porque as soluções não são interoperáveis e não podem se comunicar. E 40% também relatam incapacidade de aplicar e fazer cumprir políticas de forma consistente. Relacionado a essas descobertas está o alto custo de tentar manter uma solução desarticulada em funcionamento, com 43% citando esse problema como um dos principais desafios. Outros desafios relacionados incluem má experiência do usuário (39%), afunilamentos e desempenho (36%) e maior complexidade de gerenciamento (28%).



Por que a consolidação e a interoperabilidade são importantes

Apesar das alegações de que tudo está mudando para a nuvem, a maioria das organizações ainda tem uma estratégia híbrida de aplicações e dados em vigor. Surpreendentemente, 38% das organizações ainda têm mais da metade de suas aplicações no local. E outros 49% têm algo entre 26% e 50% implantadas lá. Portanto, não é surpresa que 85% dos entrevistados tenham identificado a necessidade de soluções ZTNA que cubram usuários locais e remotos como muito ou extremamente importantes. O acesso à rede Zero Trust precisa funcionar independentemente de onde as aplicações e os usuários estejam localizados, e as principais áreas que uma estratégia híbrida de ZTNA deve cobrir incluem aplicações da Web (81%), usuários locais (76%), usuários remotos (72%), aplicações locais (64%) e aplicações SaaS (51%).



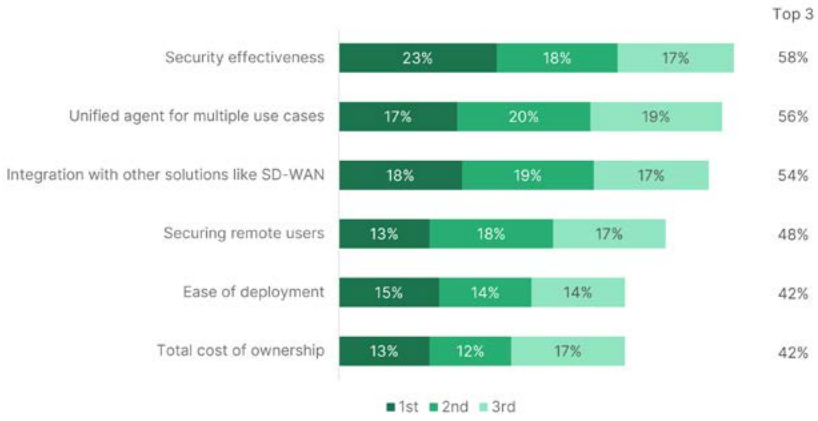
As soluções ZTNA precisam cobrir usuários e aplicações, independentemente de onde estejam localizados

Notavelmente, três quartos dos entrevistados relatam encontrar problemas com sua força de trabalho híbrida por dependerem apenas do ZTNA na nuvem. Eles precisam de uma solução Universal ZTNA que suporte aplicações na nuvem e no local, com recursos e políticas consistentes em todas as implantações e um modelo de licenciamento por usuário para que as proteções (e licenças) possam se mover perfeitamente à medida que os usuários de trabalho de qualquer lugar (WFA) transitam entre suas casas e seus escritórios.

Integração SASE

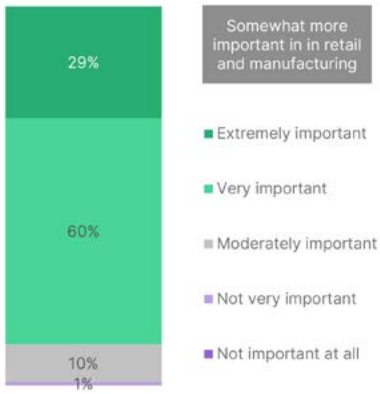
Um elemento crítico de qualquer estratégia de Zero Trust é garantir um mecanismo simples e contínuo para fornecer segurança consistente aos funcionários que trabalham remotamente e no escritório. Um dos problemas mais significativos encontrados no início da transição para um modelo WFA foi que os home offices eram notoriamente desprotegidos. Mas estender a segurança de nível empresarial a esses ambientes exigia custos e recursos intensivos, de modo que as soluções SASE rapidamente se tornaram uma opção poderosa para fornecer acesso seguro e confiável a aplicações baseadas na nuvem para trabalhadores remotos.

No entanto, o desafio é que a maioria das soluções SASE não interage com a rede física. Conexões, políticas e monitoramento precisam ser entregues usando algum tipo de mecanismo extra que precisa ser projetado e gerenciado. Portanto, embora a eficácia de segurança seja a prioridade máxima para soluções SASE (58%), 56% dos entrevistados também querem um agente unificado que possa suportar vários casos de uso e 54% querem que a SASE interopere com outras soluções, como SD-WAN. Além disso, 42% querem que isso inclua facilidade de implantação e um custo total de propriedade gerenciável.



Prioridades da solução SASE

De acordo com 89% dos entrevistados, a integração da SASE com suas soluções locais é muito ou extremamente importante. O valor está em sua capacidade de aprimorar consistentemente a experiência do usuário, simplificar as operações consolidando tarefas, implementar políticas de Zero Trust e proteger o acesso seguro a aplicações na nuvem. Essas descobertas indicam o valor que muitas organizações podem obter de soluções SASE de fornecedor único que fornecem recursos convergentes de rede e segurança para todos os usuários e dispositivos em locais distribuídos.



A necessidade de integração da SASE com o restante da rede

Conclusão

As realidades de uma força de trabalho híbrida permanente e uma rede em expansão que engloba serviços no local, multinuvem e em nuvem, como SaaS, exigiram que as organizações fizessem a transição de um modelo de confiança implícita para uma estratégia de Zero Trust. Garantir acesso confiável à aplicação, segurança consistente e uma experiência do usuário otimizada para cada usuário, independentemente da localização, são os principais impulsionadores dessa mudança. O desafio é que a maioria das redes é complexa, com aplicações divididas entre implantações na nuvem e no local, enquanto os usuários transitam entre suas casas e seus escritórios. Como resultado, a implementação da Zero Trust tem sido mais difícil do que muitas organizações supunham no início. E as organizações geralmente recebem pouca ou nenhuma orientação confiável dos fornecedores, muitos dos quais fornecem soluções projetadas para implantações somente na nuvem.

À medida que o segmento de mercado de Zero Trust continua a amadurecer, fica claro que as organizações que começaram a implementar uma estratégia de Zero Trust devem consolidar sua presença de fornecedores e soluções. Eles precisam de soluções projetadas para abranger vários ambientes e que possam convergir rede, segurança e acesso em uma única estrutura integrada. Ao adotar essa abordagem, eles podem estender sua estratégia de Zero Trust a todos os usuários e aplicações em todos os cantos da rede, mantendo ampla visibilidade e controle de ponta a ponta. Só então as organizações poderão aproveitar ao máximo as oportunidades que as estratégias híbridas de hoje oferecem.

julho 6, 2023 3:11 PM

2167932-0-0-PT