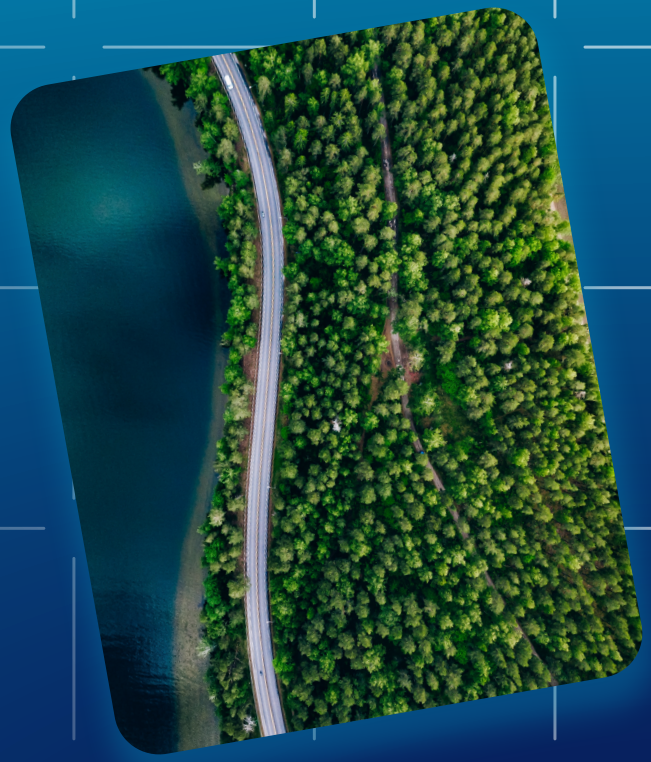
5 Critérios para Selecionar uma Solução Zero Trust para o Acesso à Rede

netskope

5 Critérios para Selecionar uma Solução Zero Trust para o Acesso à Rede

As empresas estão adotando rapidamente o Security Service Edge (SSE) para obter os benefícios de uma arquitetura SASE segura. Uma solução ZTNA (zero-trust network access) é um componente crítico de SSE, permitindo a conectividade específica da aplicação para os usuários, onde quer que eles estejam. A arquitetura Security Service Edge consolida as funções de segurança, reduz o custo total de propriedade e melhora a eficiência operacional a longo prazo, para uma melhor segurança geral.



netskope

A importância da plataforma

Independentemente de você estar selecionando e implementando ZTNA para um projeto de trabalho remoto ou híbrido, um projeto inicial como parte de uma iniciativa maior de segurança de confiança zero ou se você tiver uma visão abrangente sobre SSE e SASE, é melhor trabalhar com um provedor em uma plataforma SSE completa: um único agente, um único console e um único mecanismo de políticas, com suporte para um ambiente multinuvem.

O Gartner estima que "até 2025, 70% das organizações que implementarem o acesso zero trust à rede baseado em agente (ZTNA), escolherão um provedor de security service edge (SSE) para ZTNA, e não uma oferta independente, em comparação com apenas 20% em 2021."*

*Gartner, "Magic Quadrant for Security Service Edge", John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, 15 de fevereiro de 2022

02

Possibilitando o trabalho híbrido em qualquer lugar

Para possibilitar o trabalho híbrido de qualquer lugar, é importante selecionar um provedor que tenha uma área de cobertura que possa corresponder ao seu plano de expansão global e à agilidade de seus negócios. Trabalhe com um fornecedor ZTNA que tenha data centers em todas as principais localizações geográficas de onde seus funcionários poderão se conectar. Sua seleção de provedores não deve se basear apenas na contagem de data centers, mas na escolha de um que tenha a stack de segurança completa disponível em todas as regiões —com computação total na borda perto dos seus usuários— com rotas de entrada de baixa latência e amplo peering para a melhor experiência dos usuários e das aplicações.

Uma política fácil de implementar

Além de um único agente, a configuração de políticas de identidade e acesso utilizando um console unificado deve exigir apenas um passo. Em poucos dias, você poderá habilitar o acesso a aplicações na nuvem e privadas para dar suporte a fusões e aquisições e outras atividades urgentes.

Não fique preso a uma VPN de aplicações e regras de firewall complexas disfarçadas de ZTNA.

Proteja os dados em qualquer lugar

A sua solução ZTNA deve detectar o uso de dados, atividades e anomalias de comportamento (UEBA), impor regras e políticas avançadas de DLP e aplicar uma política de acesso adaptativa com base nos riscos de cada usuário.

O ZTNA conecta os usuários a aplicações e recursos privados com segurança. Muitas vezes, esses recursos são a "joia da coroa" da organização, desde o código até outras formas de dados proprietários, como segredos comerciais.

Selecione uma solução que forneça múltiplas opções para ajudar sua organização a proteger as informações. Por exemplo, uma solução ZTNA moderna deve oferecer tanto a inspeção de tráfego quanto opções de aplicação de DLP para proteger os dados. No entanto, algumas organizações podem preferir UEBA e classificações de risco por usuário para obter contexto em tempo real sem descriptografar o tráfego, minimizando assim o risco interno.

05

Integração eficaz de terceiros

Com as integrações e trocas corretas em ambientes de múltiplos fornecedores, o ZTNA pode fazer grande diferença. As melhores trocas oferecem pontuações de confiança a usuários e dispositivos que são normalizadas em todo o ambiente e podem acionar controles de acesso adaptativos, configurações de grupos de usuários e emissão automática de tíquetes para investigação.

Conclusão

Lembre-se de que confiança zero NÃO significa não confiar em ninguém, pois para viabilizar os negócios é preciso estender o acesso (confiança). O ponto fundamental para otimizar os princípios de confiança zero em toda a sua organização, seja especificamente com o ZTNA ou de outra forma, é usar a tecnologia para tomar decisões melhores e baseadas em contexto sobre confiança e acesso para um determinado usuário e monitorar e adaptar continuamente para minimizar os riscos. Este contexto é baseado em vários fatores, como função e identidade do usuário, identidade do dispositivo, postura de segurança, tipo de aplicação, risco da aplicação e instância da aplicação, além do nível de sensibilidade dos dados. As decisões contextuais resultam em políticas de acesso robustas que são otimizadas para riscos e podem ser aplicadas de maneira uniforme na nuvem, na Web e em aplicações privadas, ao mesmo tempo em que permitem a agilidade nos negócios e a produtividade do usuário.

Mais informações

A Netskope, líder global em segurança cibernética, está redefinindo a segurança de nuvem, dados e rede para ajudar as organizações a aplicar os princípios de zero trust para proteger os dados. A plataforma Netskope Intelligent Security Service Edge (SSE) é rápida, fácil de usar e protege pessoas, dispositivos e dados onde quer que eles estejam.

Saiba como a Netskope ajuda os clientes a estarem preparados para tudo na sua jornada SASE, **visite netskope.com.**