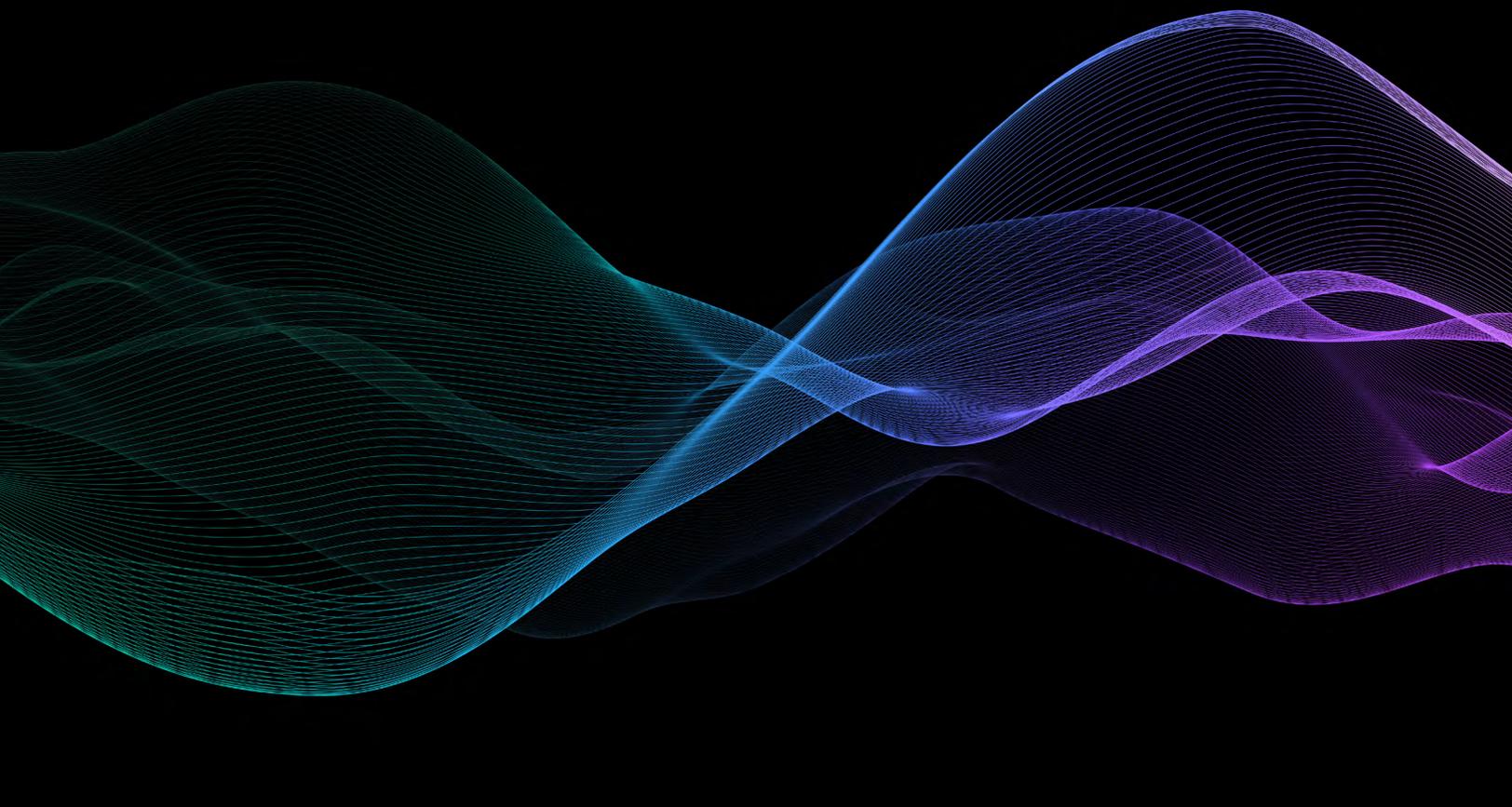




Guia do comprador de SD-WAN

The Forcepoint logo consists of a stylized 'F' icon followed by the word 'Forcepoint' in a bold, sans-serif font.

Guia de compradores



O que procurar ao escolher uma solução SD-WAN

A Wide Area Networking (WAN) tradicional usa um modelo de hub-and-spoke no qual o tráfego é direcionado sobre conexões caras Multiprotocol Label Switching (MPLS) para um data center central por fins de segurança. Essa tecnologia encontra problemas de escalabilidade com despesas operacionais e desempenho, e a rápida mudança de muitas empresas para um modelo de força de trabalho híbrida e aplicativos baseados na nuvem dificulta encontrar o equilíbrio certo entre segurança e eficiência.

Uma solução de Software-Defined Wide Area Network (SD-WAN) resolve esses desafios usando a tecnologia Software-Defined Networking (SDN) para criar uma sobreposição que virtualiza e abstrai as conexões de rede, em vez de empregar hardware, como roteadores e switches. Isso permite o uso agnóstico de diferentes tipos de conexão — incluindo MPLS, LTE e serviços de internet de banda larga — em combinação para conectar de forma flexível usuários remotos a aplicativos e recursos de TI. O roteamento de tráfego eficaz pode otimizar a velocidade e a largura de banda, levando a melhor desempenho e menores despesas operacionais em comparação com a arquitetura de WAN tradicional.

O SD-WAN desempenha um papel crucial na cibersegurança ao permitir que as funções de segurança sejam distribuídas para filiais e endpoints remotos, em vez de exigir que o tráfego seja reencaminhado para um data center central para inspeção. Os fornecedores oferecem uma variedade de soluções, incluindo serviços de SD-WAN e serviços gerenciados, além de appliances físicos e virtuais e licenças de software.

Ao selecionar uma solução de SD-WAN, os avaliadores devem levar essas cinco principais considerações em consideração:

1. Desempenho
2. Custos operacionais
3. Proteção contra ameaças
4. Escalabilidade
5. Inclusão dentro de uma oferta de SSE ou SASE

Desempenho

Uma solução de SD-WAN deve ser capaz de direcionar automaticamente o tráfego de rede para garantir que aplicativos de missão crítica recebam os recursos necessários para o desempenho ideal. O roteamento de tráfego avançado, o monitoramento de link dinâmico e a identificação detalhada de aplicativos são funcionalidades que podem ajudar a diferenciar soluções líderes. O roteamento com reconhecimento de aplicativo ocorre quando uma solução de SD-WAN reconhece as necessidades de largura de banda de diferentes aplicativos e garante que os aplicativos de missão crítica tenham a largura de banda de que precisam para funcionar sem latência ou perda de pacotes.

As soluções SD-WAN usam monitoramento contínuo e autoaprendizagem para responder automaticamente em tempo real a quaisquer alterações no estado da rede, o tráfego de roteamento em torno de gargalos ou serviços de transporte que estão enfrentando problemas. O monitoramento de integridade de aplicativos é o processo de aplicação dessa abordagem a aplicativos que funcionam na rede, e qualquer boa solução de SD-WAN deve coletar dados sobre o desempenho do aplicativo para antecipar mudanças nas necessidades e possíveis problemas.

A conectividade multi-link permite desempenho otimizado e menores despesas equilibrando a banda larga do ISP e as linhas de MPLS privadas. Essa abordagem oferece desempenho máximo para reduzir o tempo de inatividade e remover quaisquer barreiras

à produtividade dos funcionários. Os recursos listados acima oferecem maneiras de detalhar as afirmações sobre o desempenho aprimorado para qualificar como uma solução de SD-WAN funciona para oferecer conexões mais rápidas com menos latência ou tempo de inatividade.

O FlexEdge Secure SD-WAN otimiza o desempenho de aplicativos aproveitando os recursos de direção de aplicativos dinâmicos, como identificação detalhada de aplicativos e monitoramento preciso de links. A direção dinâmica de aplicativos roteia o tráfego com base no desempenho da rede e nos requisitos de aplicativos, garantindo que os aplicativos de missão crítica sempre recebam os recursos necessários para o desempenho ideal. A capacidade de failover automático garante que os aplicativos permaneçam disponíveis e com bom desempenho, mesmo diante de problemas de rede.

O FlexEdge Secure SD-WAN aproveita a tecnologia Forcepoint MultiLink™ para aprimorar a resiliência da rede e o desempenho de aplicativos. Ao combinar dinamicamente várias conexões, como MPLS, LTE, banda larga e LTE, o FlexEdge Secure SD-WAN oferece conectividade perfeita em toda a rede, garantindo que aplicativos críticos recebam a melhor conectividade possível.

O FlexEdge Secure SD-WAN também incorpora um dashboard de monitoramento de integridade de aplicativos, permitindo que os administradores monitorem métricas de qualidade (tráfego, latência, jitter, perda de pacotes) para aplicativos de rede, links de ISP e túneis de VPN, tudo em uma única visualização. O monitoramento de integridade de aplicativos também fornece histórico de status para detectar quaisquer falhas. Ter o histórico de status de integridade dos links do ISP na mesma tela que o status de integridade do aplicativo de rede capacita os administradores a identificar se há conexões causais entre a qualidade do link e aplicativos, ou se há problemas mais isolados em relação a um aplicativo específico ou conectividade de filial.

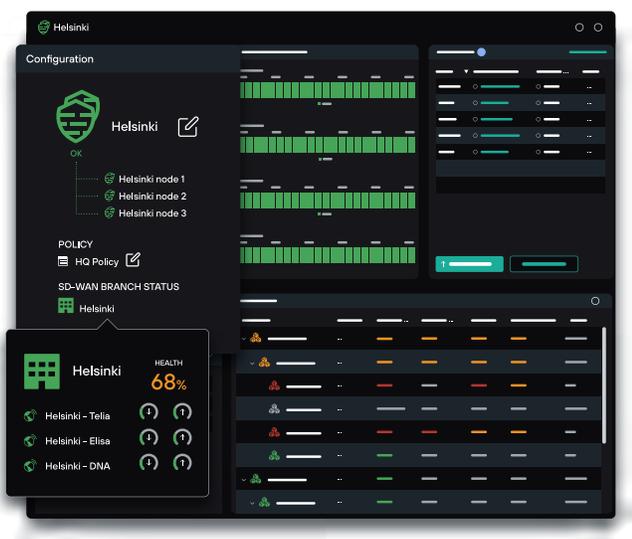


Figura 1: monitoramento de integridade de aplicativos

Perguntas a serem feitas ao avaliar soluções

- Que funcionalidade integrada essa solução fornece para priorizar aplicativos críticos para os negócios?
- Quais capacidades, como o Monitoramento de integridade de aplicativos e direção de tráfego, essa solução oferece para evitar gargalos e maximizar o desempenho?
- Essa solução fornece conectividade Multi-Link?
- Quanto tempo de inatividade normalmente pode ser esperado com uma solução como essa?

Custos operacionais

Além de melhorar o desempenho, uma boa solução de SD-WAN deve funcionar para manter os gastos operacionais da sua organização baixos. Como mencionado anteriormente, o primeiro passo é o uso agnóstico de diferentes tipos de conexão com a conectividade MultiLink, o que evita ter que depender exclusivamente de conexões MPLS de custo mais alto.

Dentro do SD-WAN, o clustering de alta disponibilidade é uma capacidade crítica na mitigação do tempo de inatividade da rede e os custos associados. O clustering de alta disponibilidade minimiza as interrupções de rede ao redirecionar rapidamente o tráfego durante falhas de links, garantindo conectividade ininterrupta. O tempo de inatividade em qualquer empresa significa perda de receita, produtividade e satisfação do cliente.

As soluções SD-WAN podem reduzir significativamente o tempo e o trabalho ao aproveitar a configuração de nuvem para implantação com zero toque em qualquer local. Isso se aplica à implementação inicial de uma nova infraestrutura de rede, mas também tem o efeito contínuo de simplificar atualizações de políticas e upgrades de software. As implantações com zero toque não são apenas mais rápidas, mas também liberam a equipe para se concentrar em problemas e metas mais relacionados a missões críticas. Esses efeitos se traduzem em custos operacionais menores em todos os aspectos, e uma solução adequada deve fornecer vários caminhos para manter as despesas gerenciáveis.

O FlexEdge Secure SD-WAN fornece a flexibilidade de implantação na nuvem (com integrações com AWS, Microsoft e muito mais). Com a implantação e o gerenciamento de appliances de rede com zero toque, as organizações podem reduzir gastos de capital (CapEx)

e despesas operacionais (OpEx), enquanto se permitem dimensionar sua infraestrutura de rede de forma rápida e econômica.

A capacidade de clustering de alta disponibilidade dentro do FlexEdge Secure SD-WAN garante a continuidade dos negócios ao eliminar pontos únicos de falha. No caso de uma falha, o dispositivo de backup assumirá o controle com zero interrupção, reduzindo o tempo de inatividade e mantendo a conectividade perfeita. A funcionalidade de clustering permite que os administradores gerenciem vários dispositivos a partir de uma única interface, simplificando o gerenciamento de rede e reduzindo os custos operacionais.

O Multi-Link™ no FlexEdge Secure SD-WAN não apenas otimiza o desempenho de aplicativos, mas também ajuda as organizações a economizar em custos de rede. Com a capacidade de rotear o tráfego de forma dinâmica pelo caminho mais eficiente e econômico, as organizações podem evitar links caros e reduzir as despesas de rede.

Perguntas a serem feitas ao avaliar soluções

- › Essa solução utiliza o clustering de alta disponibilidade para reduzir o tempo de inatividade e otimizar a conectividade?
- › Essa solução permite que os recursos de implantação com zero toque economizem tempo e incorporem facilmente locais remotos?

Proteção contra ameaças

Nem todas as soluções SD-WAN fornecem funcionalidades de segurança integradas. Embora a maioria inclua criptografia para proteger a privacidade de dados, essa opção de conectividade pode se tornar um vetor de ataque adicional quando não for integrada adequadamente com outra funcionalidade de segurança. As tecnologias de SD-WAN superiores fornecem capacidades de segurança adicionais também.

À medida que os usuários remotos se conectam diretamente a aplicativos na nuvem, a segurança que antes era fornecida por gateways centralizados e on-premises agora deve ser aplicada em cada local remoto ou na nuvem. As soluções de Secure SD-WAN tornam isso possível ao incorporar as principais funcionalidades de segurança:

- O controle de acesso e a tecnologia de prevenção de invasões, normalmente por meio de [Next-Generation Firewalls](#) (NGFW), evitam que os invasores penetrem nas defesas.
- As funcionalidades de segurança da Web oferecem proteção em tempo real contra ameaças avançadas dentro de páginas da web ou conteúdo baixado.
- As soluções de monitoramento de nuvem rastreiam e protegem aplicativos e dados armazenados na nuvem para evitar abuso.

Com as soluções SD-WAN superiores, as empresas podem permitir que os usuários se conectem perfeitamente aos recursos de nuvem de que precisam, enquanto protegem redes, usuários e dados contra roubo, perda e ataque.

As gerações mais recentes de soluções de Secure SD-WAN são construídas com uma mentalidade de segurança em primeiro lugar e apresentam capacidades, como Quality of Service (QoS) e Network Encryption & Decryption. As soluções de Secure SD-WAN avançadas usam o "encadeamento de serviços" para aplicar capacidades de segurança, como proteção de tráfego da web e Cloud Access Security Broker (CASB), que protege automaticamente os dados transmitidos para aplicativos baseados na nuvem. Como abordado abaixo, esses recursos de segurança são mais eficazes quando a solução de SD-WAN é uma parte integrada de uma plataforma de segurança abrangente.

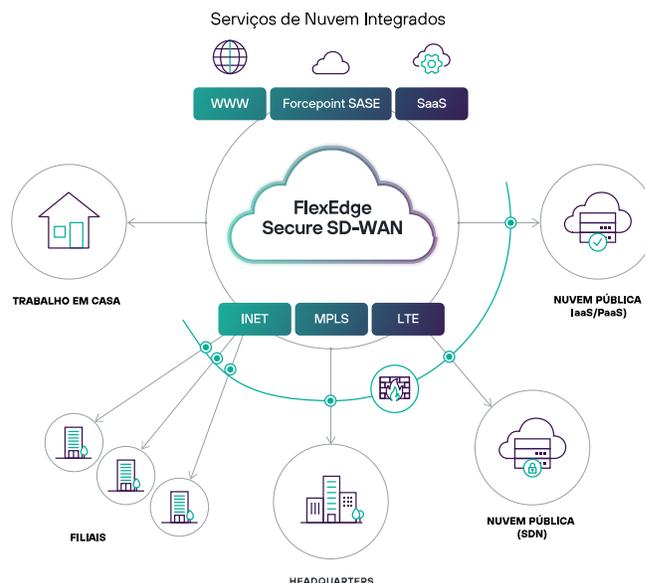


Figura 2: arquitetura do FlexEdge Secure SD-WAN

O FlexEdge Secure SD-WAN fornece detecção e proteção em tempo real contra uma série de ameaças, incluindo malware, tráfego de botnet e ataques de comando e controle (C2), juntamente com outros tipos de exploits. Com a inspeção detalhada de pacotes e as capacidades de detecção de ameaças avançadas, os administradores ganham uma visão abrangente da atividade de rede e podem responder rapidamente para mitigar as ameaças. Pacotes suspeitos são identificados e bloqueados, as sessões de TCP são encerradas e o conteúdo malicioso é removido da rede. Todas essas ações podem ser realizadas em tempo real e de acordo com seus requisitos de política de segurança, garantindo que seus dados e ativos de aplicativos mais críticos sejam protegidos contra danos.

A inspeção multicamadas é uma característica fundamental do FlexEdge Secure SD-WAN, fornecendo uma abordagem flexível e abrangente para a segurança. Ao combinar controle de acesso, identificação de aplicativos, inspeção profunda e filtragem de arquivos, as organizações podem otimizar a segurança e o desempenho do sistema.

Perguntas a serem feitas ao avaliar soluções

- > Quais funcionalidades de segurança integradas essa solução oferece?
- > Como a solução se integra com soluções de segurança externas para proteger os dados transmitidos para aplicativos baseados na nuvem?

Escalabilidade

As capacidades de implantação com zero toque, mencionadas anteriormente, ajudam a tornar uma solução de SD-WAN escalável ao atender remotamente novos locais em todo o mundo. A administração centralizada é outro fator crucial que possibilita a expansão rápida, pois os administradores de rede podem definir políticas de nível superior uma vez e aplicá-las automaticamente em toda a organização. Idealmente, essa administração centralizada deve ser capaz de operar na nuvem para fornecer a velocidade e a flexibilidade necessárias para a solução eficaz de problemas.

Um dos desafios que as organizações enfrentam ao aumentar a escala é o gerenciamento de várias regiões com diferentes fornecedores de ISP. Tais cenários podem levar ao tempo excessivo gasto na configuração manual de novas conexões e na instalação de hardware caro; essas considerações podem fazer com que as organizações incorram em mais custos do que o previsto ao ampliar as operações. Uma solução de SD-WAN que pode tornar esse processo mais eficiente e menos oneroso, como a criação de vários gateways sem a necessidade de conectividade direta, pode aumentar significativamente a escalabilidade para as organizações.

Com o Forcepoint FlexEdge SD-WAN, os administradores podem supervisionar e manter até 6.000 sites a partir do SD-WAN Management Center, gerenciando e monitorando toda a rede em tempo real. E o orquestrador do Forcepoint SD-WAN simplifica a configuração de novos locais de SD-WAN. Basta adicionar um novo local ao orquestrador do SD-WAN e ele se comunicará automaticamente com os sites novos e existentes.

O orquestrador do Forcepoint SD-WAN pode gerenciar a conectividade de malha completa em milhares de gateways, permitindo que as organizações escalem as operações para vários locais.

Perguntas a serem feitas ao avaliar soluções

- › Como essa solução facilita a visualização e o gerenciamento centralizados dos fluxos de tráfego de rede?
- › Essa solução fornece assistência com o gerenciamento de várias regiões, enquanto minimiza os requisitos de configuração manual e aproveita o hardware econômico?



Figura 3: os links de banda larga comum do Secure SD-WAN

Inclusão dentro de uma oferta de SSE ou SASE

O [Security Service Edge](#), ou SSE, é o componente de segurança da arquitetura de Secure Access Service Edge (SASE) conceituada pela primeira vez pelo Gartner™. SSE refere-se à consolidação de serviços de segurança de aplicativos privados, na web e em nuvem em uma única plataforma unificada baseada na nuvem. Esses serviços de segurança integrados, incluindo Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) e Secure Web Gateways (SWG), atendem às necessidades modernas das organizações que adotam a nuvem, a transformação digital e o trabalho híbrido.

Com as organizações em todo o mundo já adotando o SASE e o SSE, um investimento sábio significa garantir que a oferta de SD-WAN escolhida possa funcionar como parte de uma plataforma abrangente de SSE/SASE. A plataforma deve ter capacidade para proteger qualquer interação entre qualquer dispositivo, aplicativo, destino da web, recurso privado ou infraestrutura antiga, com tecnologias de segurança baseadas na nuvem. Essas plataformas oferecem benefícios financeiros e de economia de tempo ao remover a necessidade de alternar entre diferentes produtos e soluções, uma obrigação para os departamentos de TI sob pressão para fazer mais com menos.

Procure uma solução que tenha uma única console de administração, um único agente unificado no dispositivo, administração de identidades unificada e um mecanismo comum de Data Loss Prevention (DLP) e capacidades de verificação de malware em todos os recursos.

Integrações sem falhas entre os componentes nativos da plataforma SSE são obrigatórias. Em última instância, a organização deve optar por uma oferta SD-WAN e SSE que forneça todas as necessidades de segurança para a transformação digital.

Integrando-se com os serviços de Security Service Edge (SSE), o FlexEdge Secure SD-WAN fornece uma estrutura SASE completa que oferece políticas de segurança consistentes e aplicação em ambientes de nuvem híbrida. A integração com o Forcepoint CASB (Cloud Access Security Broker) e o ZTNA (Zero Trust Network Access) permite acesso seguro a aplicativos e dados a partir de qualquer local, enquanto a integração com o SWG (Secure Web Gateway) fornece proteção contra ameaças baseadas na web.

Além disso, a integração com os serviços de proteção contra ameaças avançadas, como o Forcepoint Remote Browser Isolation (RBI) e o Advanced Malware Detection and Protection (AMDP), fornece várias camadas de segurança para garantir o acesso seguro a aplicativos e sites da web, mesmo em locais remotos. Essa integração abrangente com os serviços de SSE garante que todo o tráfego seja roteado e protegido com segurança, fornecendo uma experiência de usuário perfeita e segura, independentemente da localização ou dispositivo.

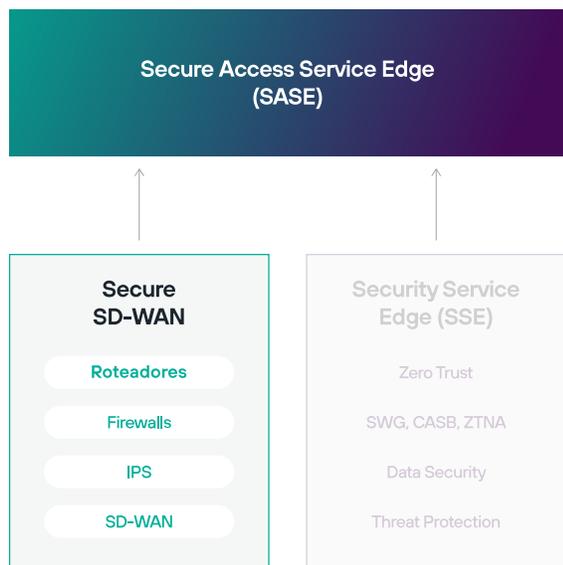


Figura 4: a estrutura SASE

Perguntas a serem feitas ao avaliar soluções

- › Você pode usar essa solução para permitir proteções de segurança consistentes para todas as interações em todos os aplicativos, dispositivos, recursos privados, destinos da web e infraestrutura?
- › O fornecedor utiliza um serviço de segurança de dados comum, serviço de verificação de malware comum e serviço de identificação comum em todos os canais CASB, SWG e ZTNA para reduzir a sobrecarga administrativa?
- › Quais recursos de facilidade de uso e administração a solução SD-WAN oferece? Faz parte de uma plataforma SASE com um único dashboard para configuração simples de políticas?

Principais considerações para a seleção de uma solução SD-WAN

As soluções SD-WAN capazes de atender às necessidades de rede e segurança das empresas modernas fornecem o seguinte:

- Desempenho | Direciona automaticamente o tráfego de rede e emprega monitoramento contínuo e autoaprendizagem para evitar gargalos e reduzir a latência e o tempo de inatividade
- Custos operacionais | Reduz as despesas de tempo, trabalho e infraestrutura com medidas como implantação com zero toque, uso agnóstico de diferentes tipos de conexão e clustering de alta disponibilidade
- Proteção contra ameaças | Inclui funcionalidades de segurança integradas, incluindo criptografia, prevenção de invasões e inspeção multicamada
- Escalabilidade | Facilita a administração centralizada e a configuração e implantação eficientes para novos locais em todo o mundo
- Inclusão dentro de uma oferta SSE ou SASE | Parte de uma oferta SASE abrangente e facilmente gerenciável que fornece capacidades CASB, ZTNA e SWG

Para ver o Forcepoint FlexEdge Secure SD-WAN em ação ou para saber mais sobre nossas ofertas SASE, [solicite uma demo gratuita](#).

O Forcepoint FlexEdge Secure SD-WAN maximiza o desempenho e a escalabilidade, reduz os gastos operacionais e é compatível com as melhores práticas de segurança de dados.

O Forcepoint FlexEdge Secure SD-WAN integra-se à plataforma Forcepoint ONE, uma plataforma de nuvem baseada em hyperscaler com 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,99% para proteger o uso de aplicativos de nuvem perfeitamente e preservar a produtividade do usuário. Outras soluções fazem backup do tráfego de aplicativos de nuvem por meio de data centers proprietários, que não têm a escalabilidade elástica e a alta disponibilidade da infraestrutura de nuvem hiperescalável do Forcepoint ONE. O Forcepoint ONE unifica CASB, SWG e ZTNA para proteger o acesso a aplicativos corporativos SaaS, da web e privados, simplificando a segurança.



forcepoint.com/contact

Sobre a Forcepoint

A Forcepoint simplifica a segurança para empresas e governos globais. A plataforma all-in-one verdadeiramente nativa de nuvem da Forcepoint facilita a adoção de Zero Trust e a prevenção de roubo ou perda de dados confidenciais e propriedade intelectual, independentemente de onde as pessoas estejam trabalhando. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para clientes e seus funcionários em mais de 150 países. Entre em contato com a Forcepoint em www.forcepoint.com.br, [Twitter](#) e [LinkedIn](#).