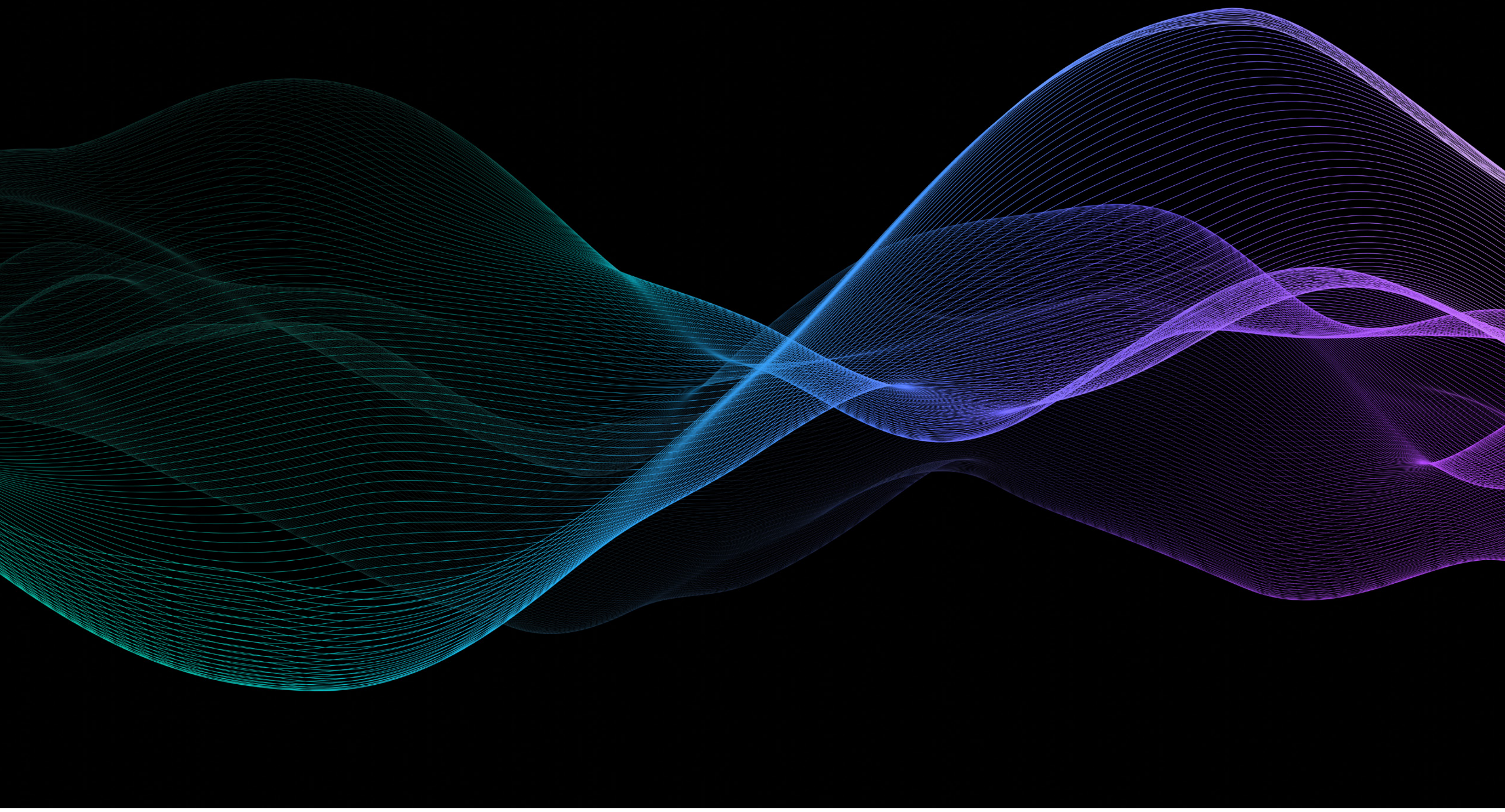
Software-Defined Wide Area Network Buyer's Guide

Forcepoint

Buyers Guide



What to look for when choosing an SD-WAN solution

Traditional Wide Area Networking (WAN) architecture uses a hub-and-spoke model in which traffic is directed over expensive Multiprotocol Label Switching (MPLS) connections to a central data center for security purposes. This technology encounters scalability issues with operating costs and performance, and the rapid shift of many enterprises to both a hybrid workforce model and cloud-based applications makes it difficult to strike the right balance between security and efficiency.

A Software-Defined Wide Area Network (SD-WAN) solution solves these challenges by using Software-Defined Networking (SDN) technology to create an overlay that virtualizes and abstracts network connections, instead of employing hardware such as routers and switches. This allows for agnostic use of different connection types – including MPLS, LTE and broadband internet services – in combination to flexibly connect remote users with applications and IT resources. Effective traffic routing can optimize speed and bandwidth, leading to improved performance and lower operating costs compared to traditional WAN architecture.

SD-WAN plays a crucial role in cybersecurity by enabling security functions to be distributed to branch and remote endpoints rather than requiring traffic to be backhauled to a central data center for inspection. Vendors offer a variety of solutions, including SD-WAN services and managed services in addition to physical and virtual appliances and software licenses.

When selecting an SD-WAN solution, evaluators should take these five key considerations into account:

1. Performance
2. Operating costs
3. Threat Protection
4. Scalability
5. Inclusion within an SSE or SASE offering

Performance

An SD-WAN solution should be able to automatically direct network traffic to ensure that mission-critical applications receive the necessary resources for optimal performance. Advanced traffic routing, dynamic link monitoring and detailed application identification are functionalities that can help to differentiate leading solutions. Application-aware routing is when an SD-WAN solution recognizes the bandwidth needs of different applications and ensures that mission-critical applications have the bandwidth they need to perform without latency or packet loss.

SD-WAN solutions use continuous monitoring and self-learning to automatically respond in real time to any changes in the state of the network, routing traffic around bottlenecks or transport services that are experiencing problems. Application Health Monitoring is the process of applying this approach to apps running on the network, and any good SD-WAN solution should collect data on application performance in order to anticipate changing needs and potential issues.

Multi-Link connectivity allows for optimized performance and lower costs by balancing ISP broadband and private MPLS lines. This approach delivers maximum performance to reduce downtime and remove any barriers to employee productivity. The capabilities listed above offer ways to drill down into claims about improved performance to qualify how an SD-WAN solution works to deliver faster connections with less latency or downtime.

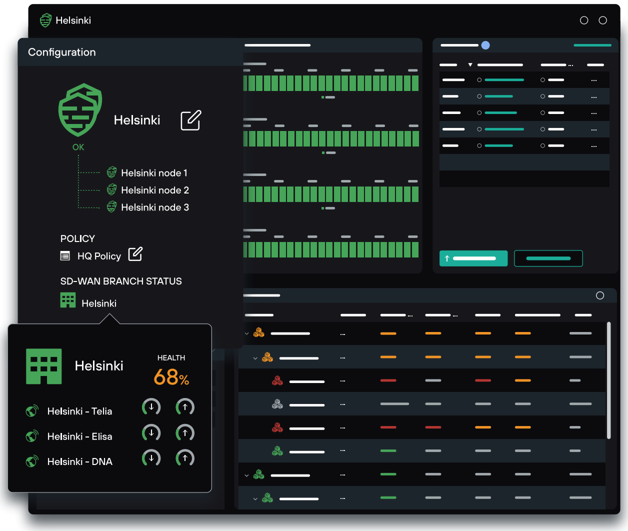


Figure 1: Application Health Monitoring

FlexEdge Secure SD-WAN optimizes application performance by leveraging Dynamic Application Steering capabilities such as detailed application identification and accurate link monitoring. Dynamic Application Steering routes traffic based on both network performance and application requirements, ensuring that mission-critical applications always receive the necessary resources for optimal performance. Automatic failover capability ensures that applications remain available and performant even in the face of network issues.

FlexEdge Secure SD-WAN leverages Forcepoint Multi-LinkTM technology to enhance network resilience and application performance. By dynamically combining multiple connections such as MPLS, LTE, broadband and LTE, FlexEdge Secure SD-WAN delivers seamless connectivity throughout the network, ensuring that critical applications receive the best possible connectivity.

FlexEdge Secure SD-WAN also incorporates an Application Health Monitoring dashboard, allowing administrators to monitor quality metrics (traffic, latency, jitter, packet loss) for network applications, ISP links and VPN tunnels all in one view. Application Health Monitoring also provides status history to spot any hiccups. Having the health status history of the ISP links on the same screen as the network application health status empowers administrators to identify if there are causal connections between the link quality and applications, or if there are more isolated issues regarding a particular application or branch connectivity.

Questions to Ask When Evaluating Solutions

→ What built-in functionality does this solution provide for prioritizing business-critical applications?

→ What capabilities, such as Application Health Monitoring and traffic steering, does this solution offer to avoid bottlenecks and maximize performance?

→ Does this solution provide Multi-Link connectivity?

→ How much downtime can typically be expected with a solution like this?

Operating costs

In addition to improving performance, a good SD-WAN solution should work to keep your organization's operating costs low. As discussed previously, the first step is agnostic use of different connection types with Multi-Link connectivity, which avoids having to rely exclusively on higher-cost MPLS connections.

Within SD-WAN, high-availability clustering is a critical capability in mitigating network downtime and the associated costs. High-availability clustering minimizes network outages by quickly rerouting traffic during link failures, ensuring uninterrupted connectivity. Downtime in any business means loss of revenue, productivity and customer satisfaction.

SD-WAN solutions can greatly lessen time and labor by leveraging cloud configuration for zero-touch deployment at any locations. This applies to the initial implementation of a new networking infrastructure, but it also has the continuing effect of simplifying policy updates and software upgrades. Not only are zero-touch deployments faster, but they free up staff to concentrate on more mission-critical issues and goals. These effects translate to lower operating costs across the board, and a suitable solution should provide multiple avenues for keeping expenses manageable.

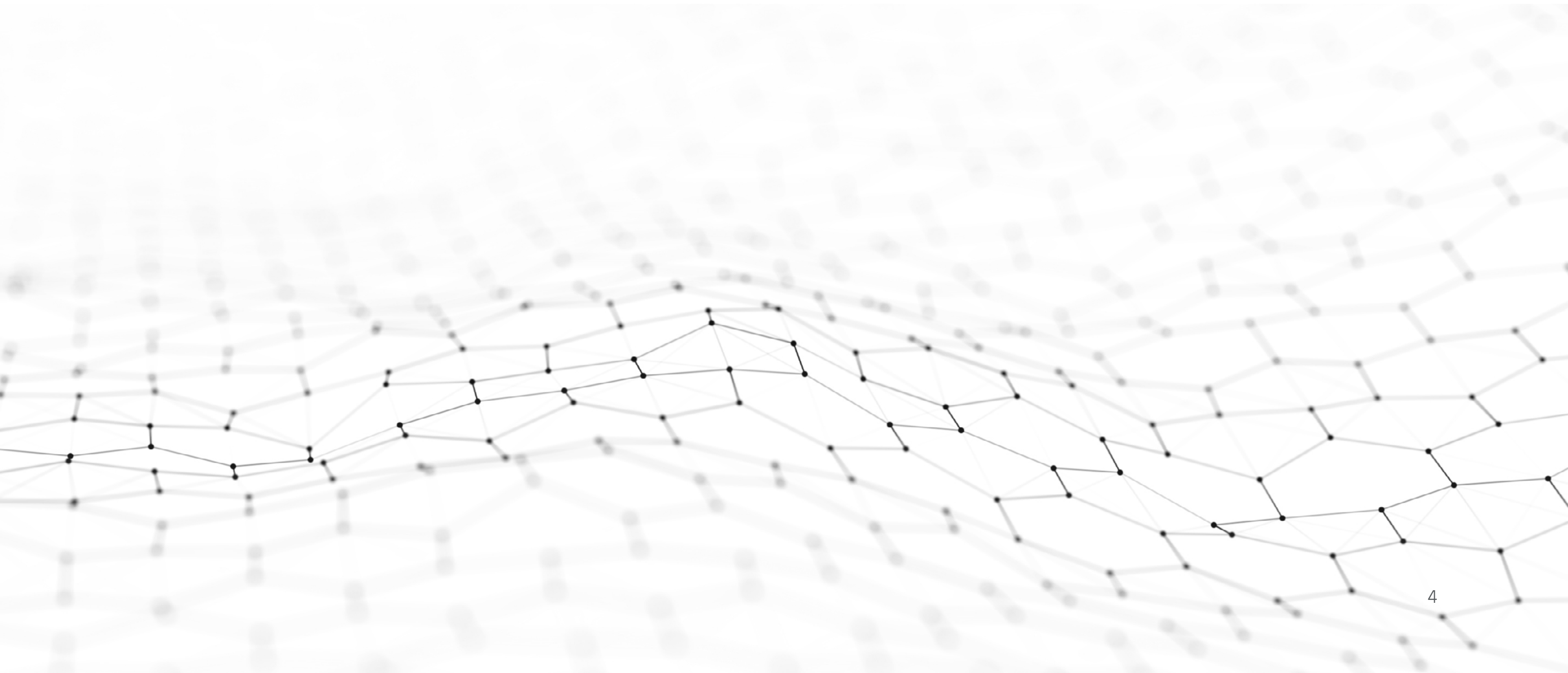
FlexEdge Secure SD-WAN provides the flexibility to deploy in the cloud (featuring integrations with AWS, Microsoft and more). With zero-touch deployment and management of networking appliances, organizations can reduce both capital expenditures (CapEx) and operating expenses (OpEx) while enabling themselves to scale their network infrastructure quickly and cost-effectively.

High-availability clustering capability within FlexEdge Secure SD-WAN ensures business continuity by eliminating single points of failure. In the event of a failure, the backup device will take over with zero disruption, reducing downtime and maintaining seamless connectivity. The clustering feature allows administrators to manage multiple devices from a single interface, simplifying network management and reducing operational costs.

Multi-LinkTM in FlexEdge Secure SD-WAN not only optimizes application performance but also helps organizations save on networking costs. With the ability to dynamically route traffic over the most efficient and cost-effective path, organizations can avoid expensive links and reduce networking expenses.

Questions to Ask When Evaluating Solutions

- Does this solution utilize high-availability clustering to reduce downtime and optimize connectivity?
- Does this solution enable zero-touch deployment capabilities to save time and easily incorporate remote locations?



Threat Protection

Not all SD-WAN solutions provide built-in security features. While most include encryption to protect data privacy, this connectivity option can become an additional attack vector when not properly integrated with other security functionality. Superior SD-WAN technologies provide additional security capabilities as well.

As remote users connect directly to cloud applications, security that once was provided by centralized, on-premises gateways must now be enforced at each remote location or in the cloud. Secure SD-WAN solutions make this possible by incorporating key security features:

- → Access control and intrusion prevention technology, typically through Next-Generation Firewalls (NGFW), prevent attackers from penetrating defenses.
- → Web security features deliver real-time protection against advanced threats within web pages or downloaded content.
- → Cloud monitoring solutions track and protect apps and data stored in the cloud to prevent abuse.

With superior SD-WAN solutions, enterprises can enable users to seamlessly connect to the cloud resources they need while protecting networks, users, and data from theft, loss and attack.

The latest generations of Secure SD-WAN solutions are built with a security-first mindset and feature capabilities such as Quality of Service (QoS) and Network Encryption & Decryption. Advanced Secure SD-WAN solutions use "service chaining" to apply security capabilities like web traffic protection and Cloud Access Security Broker (CASB), which automatically secures data transmitted to cloud-based apps. As addressed below, these security capabilities are most effective when the SD-WAN solution is an integrated part of a comprehensive security platform.

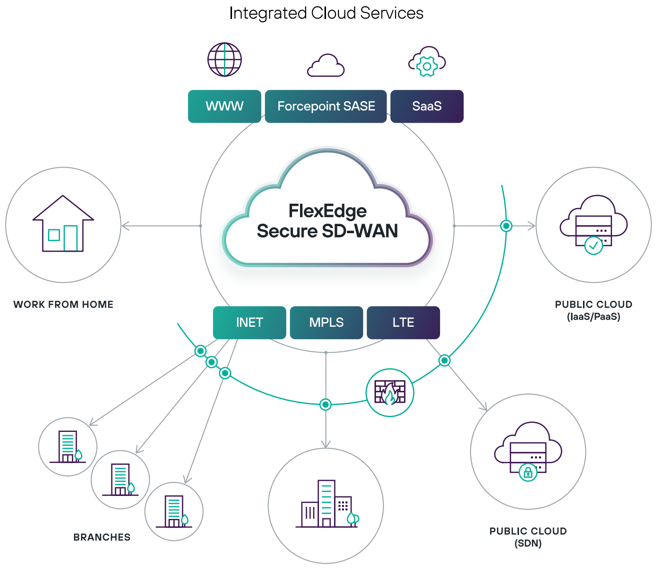


Figure 2: FlexEdge Secure SD-WAN Architecture

FlexEdge Secure SD-WAN provides real-time detection and protection against a range of threats, including malware, botnet traffic and Command and Control (C2) attacks, along with other types of exploits. With detailed packet inspection and advanced threat detection capabilities, administrators gain a comprehensive view of network activity and can respond quickly to mitigate threats. Suspicious packets are identified and blocked, TCP sessions are terminated and malicious content is removed from the network. All of these actions can be taken in real time and in accordance with your security policy requirements, ensuring that your most critical data and application assets are protected from harm.

Multi-layer inspection is a key feature of FlexEdge Secure SD-WAN, providing a flexible and comprehensive approach to security. By combining access control, application identification, deep inspection and file filtering, organizations can optimize both security and system performance.

Questions to Ask When Evaluating Solutions

- › What built-in security features does this solution offer?
- › How does the solution integrate with external security solutions to secure data transmitted to cloud-based apps?

Scalability

Zero-touch deployment capabilities, mentioned earlier, help to make an SD-WAN solution scalable by remotely servicing new locations all over the world. Centralized management is another crucial factor that makes it possible to scale up rapidly, as network administrators can set higher-level policies once and apply them automatically across the organization. Ideally, this centralized management should be able to operate in the cloud to provide the speed and flexibility required for effective problem-solving.

One of the challenges that organizations face when scaling up is managing multiple regions with different ISP vendors. Such scenarios can lead to excessive time spent manually configuring new connections and setting up expensive hardware; these considerations can cause organizations to incur more costs than they anticipated in scaling up operations. An SD-WAN solution that can make this process more efficient and less costly, such as by creating numerous gateways without the need for direct connectivity, can greatly increase scalability for organizations.

With Forcepoint FlexEdge SD-WAN, administrators can oversee and maintain up to 6,000 sites from the SD-WAN Management Center, managing and monitoring the entire network in real time. And the Forcepoint SD-WAN orchestrator simplifies setup of new SD-WAN locations. Just add a new location to SD-WAN orchestrator, and it will automatically communicate with the new and existing sites.

The Forcepoint SD-WAN orchestrator can manage full mesh connectivity among thousands of gateways, enabling organizations to scale operations to multiple locations.

Questions to Ask When Evaluating Solutions

- How does this solution facilitate centralized visualization and management of network traffic flows?
- Does this solution provide assistance with managing multiple regions while minimizing manual configuration requirements and leveraging cost-effective hardware?

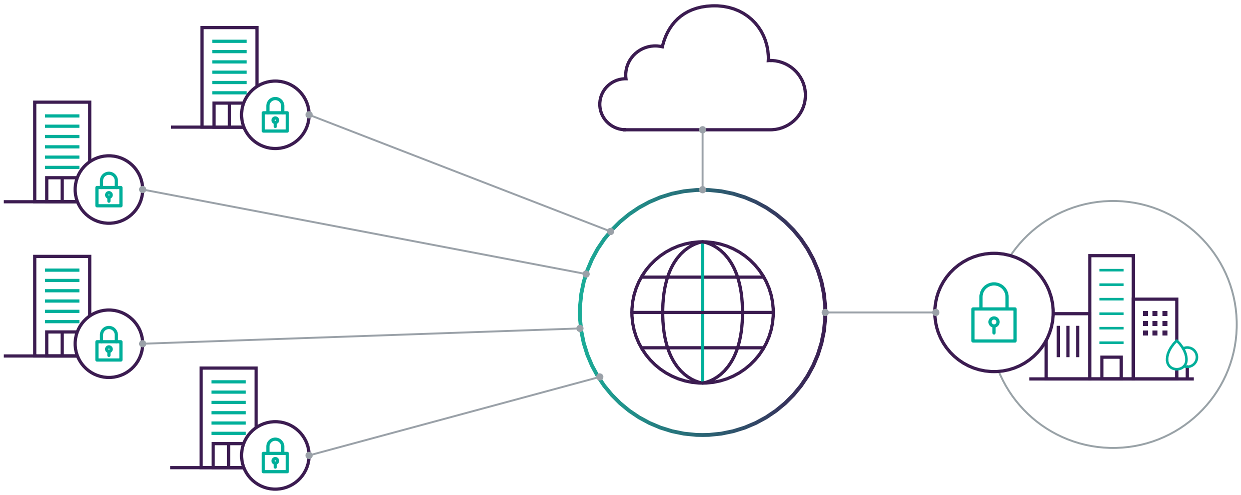


Figure 3: Secure SD-WAN Commodity Broadband Links

Inclusion within an SSE or SASE offering

Security Service Edge, or SSE, is the security component of the Secure Access Service Edge (SASE) architecture first conceptualized by Gartner™. SSE refers to the consolidation of cloud, web and private application security services into a single, unified, cloud-based platform. These integrated security services, including Cloud Access Security Brokers (CASBs), Zero Trust Network Access (ZTNA) and Secure Web Gateways (SWGs), address the modern-day needs of organizations embracing the cloud, digital transformation and hybrid work.

With organizations around the world already embracing SASE and SSE, a wise investment means ensuring the chosen SD-WAN offering can function as part of a comprehensive SSE/SASE platform. Such a platform must be able to secure any interaction between any device, application, web destination, private resource or infrastructure through cloud-based security technologies. These platforms offer time-saving and financial benefits by removing the need to pivot between different products and solutions – a must for IT departments under pressure to do more with less.

Look for a solution that has a single management console, single unified on-device agent, unified identity management and a common Data Loss Prevention (DLP) engine and malware scanning abilities across all resources. Smooth integrations between native components within an SSE platform are a must. At the end of the day, an organization should opt for an SD-WAN and SSE offering that provides all security needs for digital transformation.

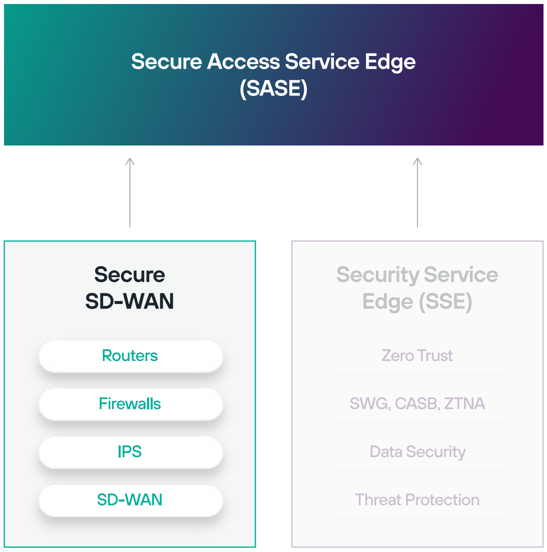


Figure 4: SASE Framework

Integrating with Security Service Edge (SSE) services, FlexEdge Secure SD-WAN provides a complete SASE framework that delivers consistent security policies and enforcement across hybrid cloud environments. The integration with Forcepoint CASB (Cloud Access Security Broker) and ZTNA (Zero Trust Network Access) allows for secure access to applications and data from any location, while integration with SWG (Secure Web Gateway) provides protection against web-based threats.

Furthermore, the integration with Advanced Threat Protection services such as Forcepoint Remote Browser Isolation (RBI) and Advanced Malware Detection and Protection (AMDP) provides multiple layers of security to ensure safe access to web applications and sites, even in remote locations. This comprehensive integration with SSE services ensures that all traffic is securely routed and protected, providing a seamless and secure user experience regardless of location or device.

Questions to Ask When Evaluating Solutions

- Can you use this solution to enable consistent security protections for all interactions across all apps, devices, private resources, web destinations and infrastructure?
- Does the vendor utilize a common data security service, common malware scanning service and common identity service across CASB, SWG and ZTNA channels to reduce administrative overhead?
- What ease-of-use and ease-of-management features does the SD-WAN solution provide? Is it part of a SASE platform with a single dashboard for simple policy configuration?

Key considerations for selecting an SD-WAN solution

SD-WAN solutions capable of addressing the networking and security needs of modern enterprises provide the following:

- Performance | Automatically directs network traffic and employs continuous monitoring and self-learning to avoid bottlenecks and reduce latency and downtime
- Operating costs | Reduces time, labor and infrastructure expenses with measures such as zero-touch deployment, agnostic use of different connection types and high-availability clustering
- Threat Protection | Includes built-in security features including encryption, intrusion prevention and multi-layer inspection
- Scalability | Facilitates centralized management and efficient configuration and deployment for new locations worldwide
- Inclusion within an SSE or SASE offering | Part of a comprehensive, easily manageable SASE offering that provides CASB, ZTNA and SWG capabilities

To see Forcepoint FlexEdge Secure SD-WAN in action or to learn about our SASE offerings, sign up for a free demo.

Forcepoint FlexEdge Secure SD-WAN maximizes performance and scalability, reduces operating costs and supports data security best practices.

Forcepoint FlexEdge Secure SD-WAN integrates with the Forcepoint ONE platform, a hyperscaler-based cloud platform with 300 points of presence (PoPs), global accessibility and proven 99.99% uptime to secure the use of cloud apps seamlessly and preserve user productivity. Other solutions backhaul cloud app traffic through proprietary data centers, which lack the elastic scalability and high availability of the Forcepoint ONE hyperscaler cloud infrastructure. Forcepoint ONE unifies CASB, SWG and ZTNA to secure access to corporate SaaS, web and private apps, making security simple.

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Brochure-Software-Defined Wide Area Network Buyer's Guide-US-EN] 31Oct2023