SASE Evaluation Guide

Your Roadmap to the Right SASE Fit

Executive Summary

Cloud-first strategies and legacy network designs are colliding, creating an untenable situation. Technical leaders and architects have wrestled with networks that were built when employees sat at desks and applications lived in data centers. But for businesses to be successful, operations require a stronger backbone with visibility and insights across the entire digital footprint. Only then can there be seamless connectivity and end-to-end digital experiences across cloud, internet, and the enterprise network.

Today's pressures are opening eyes to modernization options, including Zero Trust Network Access (ZTNA). Still, not every app is ready. At the same time, it's not acceptable to continue to juggle fragmented security tools across inconsistent environments, driving up both risk and cost.

The critical question becomes: How do you deliver secure, seamless, and trusted access—for everyone, everywhere, on any device or network? That's where Secure Access Service Edge (SASE) comes in.

Single-vendor SASE addresses the core tension between security and productivity that has long plagued enterprise IT. By converging networking and security capabilities into a unified, cloud-delivered service, SASE enables true ZTNA while ensuring consistent, high-performance user experiences.

To help you cut through the complexity and decide which SASE solution is right for your organization, we've created a blueprint for comparing vendors, prioritizing capabilities, and aligning investment with real-world needs. In this guide, you'll find must-ask questions, key technical criteria, and insights on how SASE solves the most pressing networking and security issues of our time.

Contents

Overcoming Legacy Networking Shortcomings

When branches connect to campuses, challenges creep in for security, performance, and manageability. Differences in network design, limited bandwidth, and inconsistent security controls have exposed the hard truth that there are critical limitations to legacy tools.

The MPLS Burden

For decades, MPLS circuits promised reliable branch-to-headquarters connections. As work patterns morphed and cloud adoption spiked, MPLS became more of a burden than a benefit.

- **Cost Reality:** MPLS circuits carry a premium price tag that escalates quickly with demands from bandwidth-intensive applications. A single circuit can cost thousands monthly, making scaling across branch locations prohibitively expensive.
- **Agility Gap:** Managing MPLS requires specialized networking expertise that's increasingly difficult to find and retain. Circuit changes require coordination with carriers, lengthy provisioning windows, and complex configurations. When one branch requires more bandwidth, it could be weeks or months of lead time. This makes it difficult to be nimble with changing business needs. Adding to the inflexibility, MPLS contracts often lock customers into long-term agreements with limited changes.
- **Cloud Connectivity Problems:** MPLS forces cloud traffic through an inefficient path—backhauling from branch offices to headquarters before reaching cloud applications. This "hairpinning" effect degrades performance for the very applications that are supposed to drive business productivity.

How SASE Transforms Branch Connectivity

Single-vendor SASE solutions leverage SD-WAN technology to overcome MPLS limitations:

- ✓ Uses broadband internet connections to reduce bandwidth costs while maintaining business-class performance.
- ✓ Centralizes control and automation, eliminating the complexity of managing multiple carrier relationships and circuit configurations.
- ✓ Allows for rapid provisioning and changes to network configurations.
- ✓ Provides direct connectivity to cloud applications and services, improving performance and user experience.
- ✓ Integrates with security solutions to provide comprehensive protection against threats.

Limitations of Standalone Security

Legacy security architectures rely on on-premise secure web gateways (SWGs) and firewalls positioned at network choke points. While these solutions served their purpose in traditional network designs, today, they are simply bottlenecks.

- **Scalability Challenges:** Traditional on-premise firewalls and standalone SWGs are too rigid for the scale of hybrid workforces. When hundreds of remote workers simultaneously access data and cloud applications, these single-purpose appliances quickly become overwhelmed.
- **Visibility Blind Spots:** Legacy firewalls and SWGs provide limited insight into user behavior and application traffic patterns. IT teams struggle to understand what's happening across their distributed environment, making threat detection and response difficult.
- **Performance Gridlock:** Resource-intensive functions like SSL decryption and deep packet inspection can severely impact application performance. Users experience delays accessing critical business applications, leading to productivity loss and user frustration.
- **Management Complexity:** Operating multiple standalone security appliances across different locations creates administrative overhead. Each device requires individual configuration, updates, and monitoring—multiplying the operational burden and creating potential policy inconsistencies across sites.
- **Policy Inconsistency:** Maintaining consistent security policies across distributed locations becomes increasingly difficult with standalone solutions. Different sites may have different security postures, creating vulnerabilities and compliance gaps.

The SASE Security Advantage

Single-vendor SASE platforms deliver comprehensive security services that address these legacy limitations:

- ✓ Scales with cloud-native security to meet demands without hardware constraints.
- ✓ Provides comprehensive visibility into user activity and application traffic for threat protection.
- ✓ Routes traffic through the most efficient path to optimize application performance.
- ✓ Simplifies security operations through centralized management and automation.
- ✓ Unifies security policies across all locations and devices.
- ✓ Uses ZTNA to enforce per user, per app access consistent with a least privilege, zero trust posture.

Establishing Evaluation Goals

Success starts with clarity of your end goals. Before evaluating potential vendors, define what progress looks like for your organization.

Define Your Top Use Cases

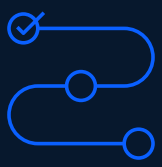
Start by identifying your most critical challenges in these categories:

- **User Experience:** Are remote employees struggling with slow application access? Do branch workers experience inconsistent cloud performance? Are contractors complaining about complex access procedures?
- **Threat Protection:** Where are your most worrisome security gaps? Do you lack visibility into access? Are you struggling to detect threats across distributed environments?
- **Network Performance:** Which applications matter most to your business? Are critical cloud applications suffering from MPLS backhauling? Do bandwidth costs limit your ability to support modern workflows?
- **Operational Simplicity:** Are you managing too many point solutions? How confident are you in achieving the desired result when making policy changes for zero trust?

The Bigger Picture Beyond Feature Comparison

There are many SASE choices, but not all can clear the pathway to your security goals. For many organizations, the first step is to provide better protection across the new, distributed IT environment. This requires a combined set of cloud-native security services that are both more efficient and effective. If this resonates with you, be mindful of this goal when evaluating solutions.

Be aware, roadblocks to your ideal SASE can be subtle. For example, some vendors have extensive feature lists to provide comprehensive protection. While appealing at face value, complex deployment models ultimately cancel out customer satisfaction. In cases like this, SASE buyers seek a unified architecture that integrates networking, security, and observability into a single cloud-delivered platform. Not only does it make initial deployment easier, but it can also set the stage for paced transformation.



Be sure your evaluation criteria balance immediate needs with long-term vision.

Key SASE Evaluation Criteria

With your use cases defined, now it's time to evaluate potential SASE solutions against these critical criteria.

Performance and Latency

- How does SASE maintain an optimal user experience when routing traffic through cloud-based security services?
- Does the provider have global points of presence (PoPs) that minimize latency and offer intelligent traffic routing?

Integration Complexity

- Can the solution integrate with existing infrastructure and third-party solutions?
- Where are the integration opportunities (e.g., sharing policy objects, adding identity context, etc.)?

Scalability and Flexibility

- Is the solution able to scale to accommodate growing bandwidth demands and evolving business needs?
- Can the SASE architecture adapt to different deployment scenarios, such as hybrid cloud or multi-cloud?

Data Privacy and Compliance

- How is sensitive data processed and stored in the cloud?
- Is sensitive data protected in ways to meet compliance standards while providing clear documentation for audits?

Comprehensive Security

- Does the solution combine firewall, intrusion prevention, secure web gateway, and ZTNA, to protect data and applications in the cloud and on-premises?
- Can the solution discover, monitor, and enforce safe and secure use of GenAI apps?

Clear SLAs

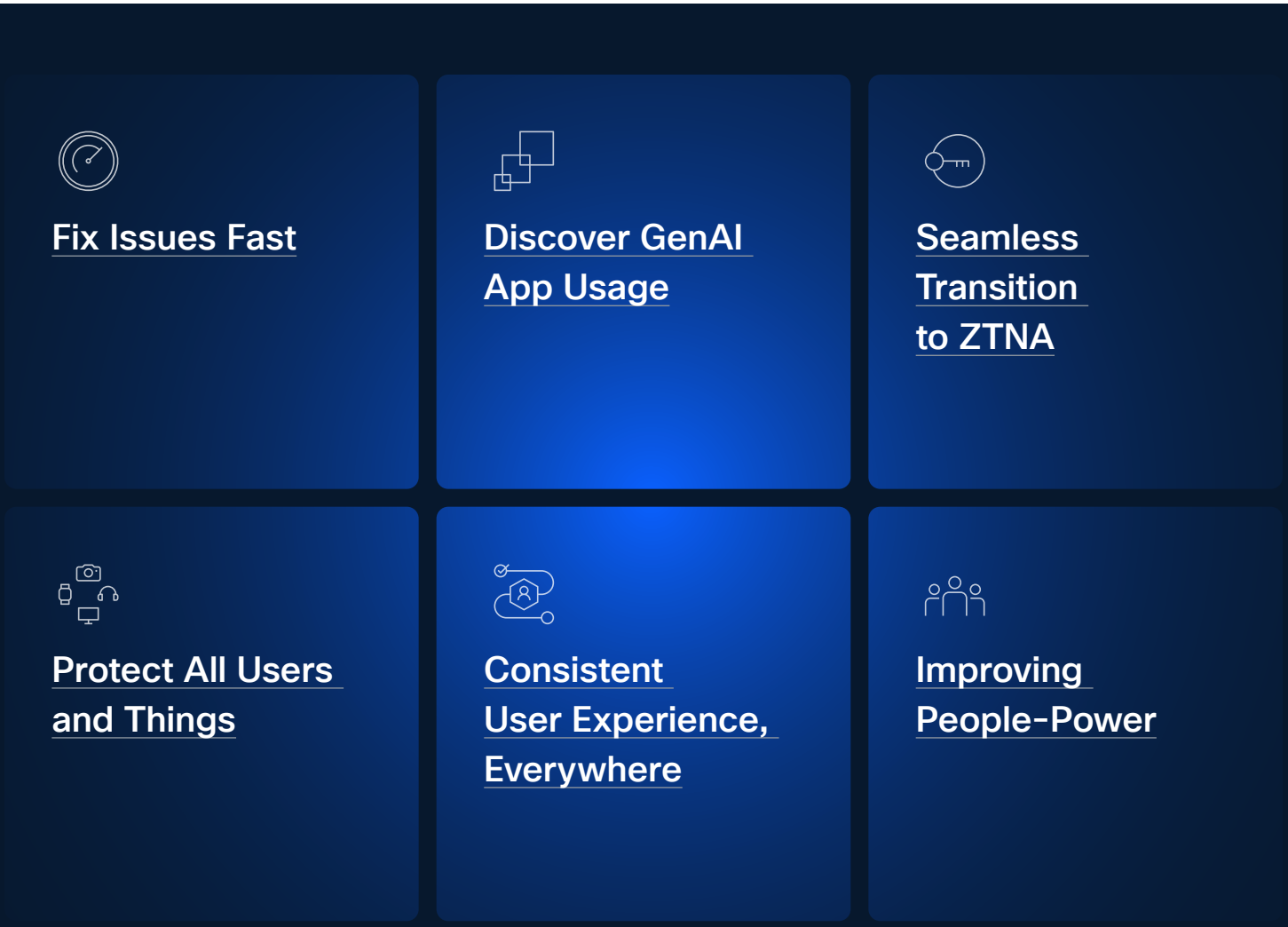
- Does the vendor provide clear SLAs that guarantee the availability, performance, and security of the SASE services?

Cost and ROI

- What is the total cost of ownership (TCO) of the SASE solution, including subscription fees, hardware costs, and operational expenses?
- Is there a clear return on investment (ROI) through improved security, reduced complexity, and increased agility?

Mapping Your Business Goals to SASE Solutions

Earlier, we discussed the importance of defining your SASE use cases before looking for your perfect solution. In this next section, we will dive deeper into common SASE goals and the technical capabilities needed to achieve them.



Fix Issues Fast

The Challenge

Quickly troubleshooting performance issues is critical—especially during a ZTNA rollout. When applications slow down or connections fail, IT teams need immediate answers. Legacy monitoring tools stand in the way of this with fragmented views, making it difficult to determine whether the problem lies with the endpoint, network, application, or user behavior.

How SASE Solves the Performance Management Challenge

Your SASE solution should provide end-to-end visibility, from the endpoint to the application, to pinpoint where problems are. Using historical performance data and intelligent recommendations, teams can proactively refine access policies to strengthen resilience and stay ahead of disruptions. Together, SASE naturally supports a zero trust approach.

Key Technical Capabilities:

- **Proactive Performance Optimization:** AI-powered predictive path recommendations forecast network issues before they impact users. The system dynamically selects the optimal path for each application, providing seamless, reliable user experiences and minimizing downtime.
- **Digital Experience Monitoring (DEM):** Utilizes technologies including endpoint agent-based monitoring and synthetic testing, to understand digital satisfaction and correlated behavior insights, particularly where the user's perspective is located across the Internet from the application or service.
- **Mobile Application Insights:** Reveals insights into mobile application performance and user behavior across Android and iOS platforms to ensure a consistent experience regardless of device.

Discover GenAI App Usage

The Challenge

Shadow IT isn't the only problem lurking in the darkness. Generative AI tools have gained traction in the enterprise, supercharging innovation as well as unpredictable behaviors and novel safety and security risks. Much like how visibility combats the negative effects of Shadow IT, we need the ability to discover GenAI app usage and ensure its use is consistent with governance and security objectives.

Because not all AI is created equally, we must understand specific users, data types, and activities occurring within the applications. The problem is, manual analysis isn't fit for the volume of data. It takes too long to identify anomalous behavior patterns, unusual data access, and suspicious activities within sanctioned and unsanctioned apps. The only way to uncover warning signs is to use AI to secure AI.

How SASE Solves the Shadow AI Problem

To move beyond basic identification to understanding and actual risk scoring, you need deep packet inspection and application behavior analysis.

Key Technical Capabilities:

- **Integration with Existing Security Tools:** Integrates with existing security tools, such as SIEM and threat intelligence platforms, to provide a holistic view of the threat landscape.
- **Data Residency and Compliance:** Ensures adherence to regional data residency requirements and industry regulations while providing advanced data loss prevention (DLP) capabilities specifically designed to prevent sensitive data exposure through AI-generated outputs.
- **Performance Support:** Maintains minimal latency impact on application traffic and user experience through intelligent traffic routing and processing optimization.
- **Scalability and Reliability:** Delivers robust, scalable architecture capable of supporting organizational growth and fluctuating AI workload demands with guaranteed uptime and reliability.
- **API Integration:** Provides comprehensive APIs for easy integration with existing systems, enabling automated security workflows and orchestration capabilities.

A Quick Shadow AI Primer

Shadow AI refers to the use of AI tools without IT or security oversight. Understanding this usage is key to setting effective governance and security policies.

For example, organizations may need to monitor and control access to sensitive documents. To do this without blanket approval or denial, the organization would need to decide based on unstructured content, not static labels, where AI can detect intent, such as patent filings or M&A documentation. In a technical scenario, organizations may want to enable developers to use LLMs to debug Python code while restricting access to models with copyleft licensing that could expose proprietary code to open-source requirements. When developers inadvertently use the "wrong" LLM—one trained on copyleft-licensed data—they risk forcing the company to release valuable intellectual property under open-source licenses. Additionally, organizations may want to restrict LLM use with more sensitive languages like C for critical systems. With fine-tuned control, AI can be a powerful tool armed with the right safety guardrails.

38% of workers share sensitive work information with AI without their employer's knowledge.[1]

1. The National Cybersecurity Alliance, Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024

Seamless Transition to ZTNA

The Challenge

Changes like return-to-office are forcing modernization by replacing legacy VPN and incorporating a cloud-based ZTNA strategy. However, traditional point solutions create a fragmented environment that requires separate management consoles, policies, and expertise for each security function. When operating in silos, it's a struggle to enforce safe and secure access for BYOD devices and contractors, and be able to extend identity context to things and users.

How SASE Eases ZTNA Adoption

A modern SASE architecture makes connecting to applications simple and automatic for everyone—users never have to think about how to access what they need. The system handles all the technical details behind the scenes, providing seamless access regardless of where people are working or what device they're using.

Integrated access policy frameworks make it easier to ensure a consistent enforcement approach and user experience. For older applications that can't use ZTNA, SASE with VPN-as-a-Service seamlessly offers secure connection options, ensuring everything stays protected while maintaining the same easy user experience.

Key Technical Capabilities:

- **Unified Client Experience:** Delivers multiple functions through one client, including DEM, network visibility, and even VPN-as-a-Service if needed for non-ZTNA enabled apps.
- **Automatic Routing:** Intercepts and redirects user traffic seamlessly to the appropriate security services without requiring any changes to the user's device or network configuration.

Protect All Users and Things

The Challenge

Organizations need the ability to deliver the same secure, high-performance experience no matter the type of user, or where a user or application is located. Traditional security architectures create inconsistent experiences, with different access methods, security controls, and performance levels depending on user location or device type. This fragmentation leads to security gaps, user frustration, and operational inefficiencies that undermine both productivity and protection.

How SASE Provides Consistent Experiences

SASE delivers uniform protection and performance across all locations and device types by centrally managing global access policies that adapt seamlessly to user context. Whether users access legacy applications from campus networks or modern cloud apps from remote locations, security enforcement and experience are consistent.

SASE provides continuous identity verification across users, IT systems, and IoT devices. It creates end-to-end identity-based micro-segmentation that maintains uniform security policies across distributed environments. This comprehensive protection covers all devices—from managed corporate equipment to personal BYOD devices—through seamless integration with mobile operating systems and browsers.

Key Technical Capabilities:

- **Mobile Device Integration:** Embeds security across all user devices, managed or unmanaged, with seamless integration for mobile OS and browser.
- **Identity-Based Microsegmentation:** Enforces zero trust policies based on user identity, device posture, and application. Extends consistent identity context across SD-WAN and cloud security enforcement.
- **Unified Policy Management:** Enforces common access control policies uniformly across campus, branch, and remote environments, eliminating security gaps and operational complexity.
- **Comprehensive Threat Protection:** Provides full protection against all web-based attacks, including advanced SSL inspection capabilities, ensuring consistent security coverage regardless of connection method or location.

Consistent User Experience, Everywhere

The Challenge

Organizations accelerating cloud adoption need solutions that eliminate routing inefficiencies while accommodating geo-specific data privacy requirements. With legacy solutions, it's common to be forced into hairpinning traffic through central data centers, creating unnecessary latency. Inefficiencies don't stop there. Organizations often manage multiple networking vendors across cloud environments, increasing operational overhead and security gaps. The challenge intensifies with multi-cloud strategies that use different network approaches across providers, creating inconsistent user experiences.

How SASE Simplifies Routing for Uniform Experiences

SASE can enable multi-environment IT simplicity for greater resilience, from policy assurance to predictive path optimization. By working in the background to intelligently route traffic, end users will always have a consistent experience no matter where they are working without additional steps.

Key Technical Capabilities:

- **Advanced Network Protocols:** Enhances performance and stability with modern network protocols like MASQUE and QUIC, especially in lossy networks, and when moving between networks.
- **High-Performance Processing:** Vector packet processing (VPP) provides modern, high-speed software pipeline capabilities that maintain efficiency and high performance, even with applications like Microsoft Office 365 and resource-intensive cloud services.
- **Unified Client Architecture:** Single endpoint client handles both internet-bound and private application traffic, with support from ZTNA and VPN-as-a-Service without impacting service delivery or requiring multiple connection methods.
- **Intelligent Traffic Management:** Automates directing endpoint traffic to appropriate services—ZTNA or VPN-as-a-Service—without user intervention or configuration complexity with socket-based intercept combined with unified policy management.

Improving People Power

The Challenge

SASE implementation requires a broad range of skills that many organizations lack internally, spanning networking, security, and cloud computing. Because traditional IT structures operate independently, with networking and security teams using different tools, processes, and priorities, collaborating can be an uphill battle.

The transformation to SASE demands significant changes to existing workflows and processes, which some may resist. Organizations must navigate not only technical complexity, but also organizational change management. This requires substantial investment in training and development to ensure teams can manage converged networking and security platforms.

Role confusion and overlapping responsibilities further complicate SASE adoption, as traditional boundaries between networking and security teams blur. Without clear role definitions and structured collaboration frameworks, organizations risk deployment delays, security gaps, and operational inefficiencies.

How SASE Prepares Your Team

Leading SASE solutions recognize that technology alone cannot overcome organizational readiness hurdles. The most successful implementations provide comprehensive support structures that address both technical and human factors, enabling organizations to solve skill gaps and operational barriers.

Effective SASE platforms reduce complexity. Through intuitive management interfaces and automation capabilities, the solution minimizes the need for specialized expertise for day-to-day operations. And by providing structured pathways, it creates a space for organizational transformation.

Key Technical Capabilities and Support:

- **Simplified Management:** Minimizes specialized skill requirements for routine management tasks using automation and intuitive interfaces that reduce operational complexity.
- **Integration with Existing Tools:** Simplifies deployment and reduces learning curves for existing teams by seamlessly working with current security and networking infrastructure.
- **Training and Support:** Develops internal expertise to manage the SASE implementation effectively with comprehensive educational programs and ongoing support services.
- **Professional Services:** Includes expert consulting to assess organizational needs, design tailored solutions, and guide implementation with proven methodologies and best practices.
- **Partner Ecosystem:** Connects with certified partners and specialists who can provide additional expertise, implementation support, and ongoing managed services as needed.
- **Role-Based Access Control:** Clearly defines responsibilities and ensures appropriate access levels while supporting collaborative workflows between teams using granular permission structures.

A Comprehensive Solution for Enforcing Zero Trust

Cisco supports a zero trust approach by delivering comprehensive capabilities through its SASE architecture. The solution integrates seamlessly with leading identity and access management (IAM) systems to verify both user and device identities, ensuring only trusted entities gain access. Cisco also enforces multi-factor authentication (MFA) for an added layer of protection.

To continually verify trust, Cisco assesses device posture in real time, checking for compliance with security policies. Consistent with a least privilege approach, access is limited to only the specific applications and resources each trusted user and device requires, reducing the attack surface area. Finally, continuous monitoring of user activity and application traffic provides the visibility needed to detect anomalies and enforce adaptive security policies—key components of an effective zero trust strategy.

Specifically, the integrated capabilities from Cisco Secure Access, Cisco SD-WAN, Cisco ISE, Cisco Firewall Threat Defense, and Cisco Duo allow organizations to:

- Implement comprehensive zero trust policies across all network access points for IT, IOT, and OT environments
- Verify identities, assess device posture, and enforce granular access controls
- Extend consistent security policies whether users are accessing resources from the office, home, or anywhere in between

Ready to Transform Your Network Security?

Cisco is the industry leader for security efficacy based on independent Miercom lab testing, and backed by Talos, the world's largest commercial threat intel team analyzing 800B security events every day. Only Cisco empowers customers with visibility and insights across the entire digital footprint, enabling seamless connectivity and end-to-end digital experiences across cloud, internet, and enterprise networks.

Download our comprehensive Proof of Concept (POC) guide to learn how to evaluate and implement Cisco SASE in your environment. The guide includes step-by-step instructions, best practices, and real-world use cases to help you get started.

Download the Cisco SASE POC Guide