Hewlett Packard Enterprise

2025

SSE Adoption Report

The state of secure access

Research by

Cybersecurity INSIDERS

Introduction

The state of secure access

The modern workforce has fundamentally changed, with most organizations operating in a hybrid model and a growing reliance on cloud applications. However, traditional security architectures—built around VPNs, firewalls, and network perimeters—are struggling to protect users, data, and applications against sophisticated threats in dynamic, distributed environments. The result is a fragmented security model that increases complexity, creates blind spots, and leaves organizations vulnerable to credential theft, ransomware, and insider threats.

Security leaders recognize that stacking more tools on outdated architectures is not sustainable. This is why Security Service Edge (SSE) is emerging as the primary solution for modern access security, delivering Zero Trust enforcement, cloud security, and access control in a single framework. While many organizations plan to expand their security transformation into a broader Secure Access Service Edge (SASE) strategy, most begin with SSE as the security foundation.

The 2025 SSE Adoption Report analyzes exclusive survey data from 713 IT and cybersecurity leaders on how organizations adopt SSE and SASE and their challenges, priorities, and deployment strategies.

Key findings from this report include:

- **SSE and SASE adoption are surging** – 79% of organizations plan to implement SSE within 24 months, and 62% consider SASE very important for their security strategy.
- **Zero Trust is a priority** – 46% of organizations are starting SSE adoption with Zero Trust Network Access (ZTNA) as they prioritize securing the increasingly mobile workforce and their private business applications.
- **Shift towards consolidation** – 61% of organizations favor a single-vendor SASE solution that unifies security and networking, specifically integrating SSE and SD-WAN. This strategy consolidates these services under one provider, offering customers a comprehensive and streamlined solution.
- **Visibility gaps create major security risks** – Organizations report low confidence levels in monitoring employee access (scoring 5.3 out of 10) and third-party users (4.9 out of 10), leaving blind spots that increase risk from lateral movement and credential-based attacks.
- **SSE replaces legacy security appliances** – 62% of organizations plan to eliminate VPN concentrators. At the same time, many seek to reduce reliance on dedicated SSL inspection, DDoS, and firewall appliances, signaling a shift to cloud-delivered SSE security that simplifies infrastructure while strengthening protection.

These findings provide critical, data-driven guidance for security leaders navigating the shift toward SSE and SASE, ensuring a secure, scalable, and simplified approach to modern access security.

Risk of the modern workplace

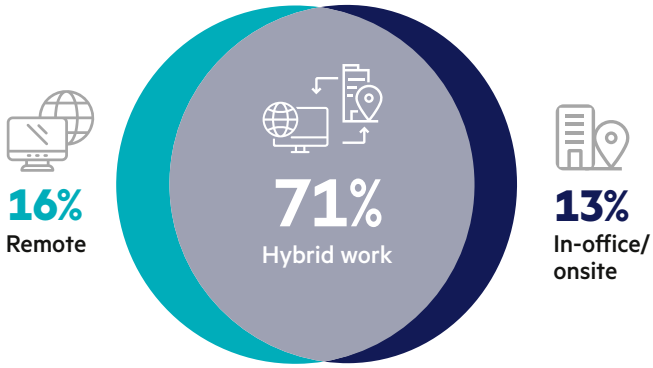
Rising access risks in the new workplace

As hybrid work becomes the norm—adopted by 71% of organizations—the security perimeter has effectively dissolved, requiring security to become less network-centric and more user-and-application-centric.

Employees move fluidly between home, office, and public networks, increasing exposure to threats like credential theft, phishing, and session hijacking.

As a result, organizations must implement security that prioritizes the protection of users and applications, ensuring that sensitive information remains secure regardless of where employees are working.

What best describes your current employee workforce model?



This shift shows why employees, with their wide access to networks and applications, are prime targets for cyber threats and are thus seen as the riskiest user category for businesses. Contractors are the second highest risk group, with customers, suppliers, and partners ranking next.

This hierarchy underscores the critical need for robust security measures and comprehensive training programs tailored for employees. By prioritizing the riskiest user categories, teams can effectively mitigate the most significant areas of risk first, before addressing other important, but less urgent, categories.

When securing business access, which group of users presents the most risk to your organization?

Top priorities and challenges

Understanding business priorities and challenges is crucial today. Survey results show significant overlap in the top four areas: Zero Trust adoption, enhanced security and data protection, ensuring user productivity, and increasing visibility.

Security is the top priority and concern for businesses. Adopting a Zero Trust strategy is their primary goal and presents a significant challenge, ensuring all users are authenticated, authorized, and validated before accessing applications and data. The reason behind this is that as cyber threats become more sophisticated, traditional security models are no longer sufficient. A Zero Trust approach reduces data breaches and unauthorized access risks. Enhancing security and data protection is another major priority and challenge due to the sensitive information businesses handle daily. Data breaches can lead to severe financial losses, legal consequences, and damage to the company's reputation. Strengthened security measures are essential to safeguard information and maintain customer trust.

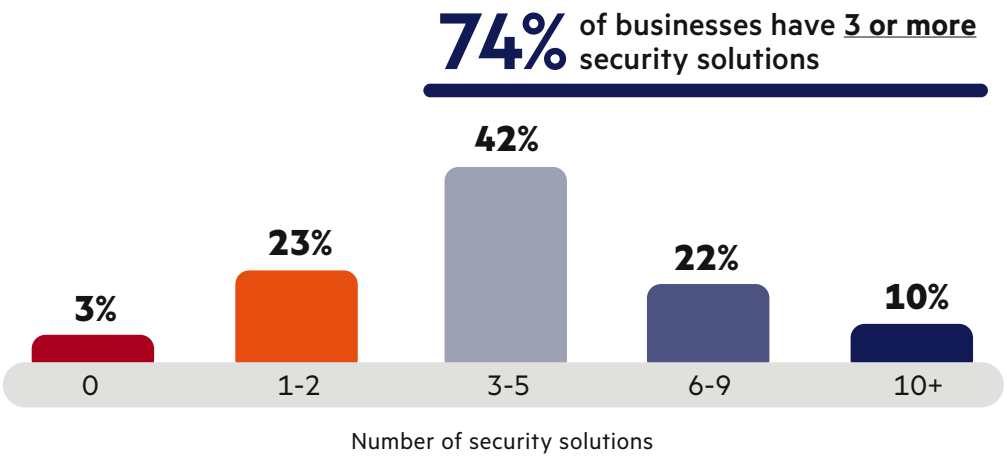
User productivity is essential alongside security. Ensuring a seamless user experience to avoid disruptions in business operations is the second highest priority and third largest challenge. Balance is key: robust security must not hinder employees' efficiency, thus maintaining smooth business operations without sacrificing safety.

Administrators need better visibility into user and application traffic, making it the fourth highest priority and challenge. Improved visibility helps monitor traffic patterns, promptly detect security threats, and mitigate risks. It is essential for optimizing network performance, ensuring compliance, and effectively addressing security and performance issues.

Limited confidence in security

The effects of a fragmented security approach are reflected in the data, as 74% of organizations use three or more security tools, with 42% having between 3-5. Instead of increasing control and protection, layering more tools often only increases complexity, creates security blind spots, and makes it harder to maintain consistent policies across hybrid work environments. More tools can usually create more silos, which can make it harder to secure access across various users, devices, and resources, providing attackers a greater opportunity to exploit IP exposures, misconfigurations, policy mismatches, or authentication fatigue.

How many different security solutions are you using to provide employees and partners with secure access to business resources?



At the same time, confidence in access security remains limited, scoring 6.8 out of 10. In an age where security is more important than ever for business continuity and trust, this isn't acceptable when companies' success, trust, and reputation are at stake. Organizations should consolidate fragmented security products into a unified, secure access framework. This means using fewer, smarter platforms that centralize access controls, adaptive trust, and continuous monitoring. The aim is to simplify Zero Trust enforcement by minimizing redundant tools and implementing consistent security policies across all users and access points.

How confident are you in the security team's ability to secure access for your workforce?

Limited visibility undermines security confidence

The complexity of managing multiple security tools has already eroded confidence in access security. However, the problem runs deeper; organizations lack clear visibility into who is accessing their applications, when, and from where. Despite deploying multi-point solutions, respondents report only moderate confidence in their ability to monitor employee access activity (5.3/10) and even lower confidence in tracking third-party users such as contractors, suppliers, and partners (4.9/10). This gap exposes organizations to undetected risks, as attackers often exploit visibility blind spots to move laterally across networks without detection.

How confident are you in your ability to monitor all application access activities of your employees?

How confident are you in your ability to monitor all application access activities of your third-party users (contractors, suppliers, partners, etc.)?

The disparity between monitoring employees and third parties is especially concerning, as third-party users often introduce additional security risks due to weaker authentication controls, inconsistent security policies, and unmanaged personal devices.

Organizations must prioritize real-time access monitoring across employee and third-party users to bridge this confidence gap. Instead of relying on fragmented logs from multiple tools, a unified Security Service Edge (SSE) approach provides centralized, continuous visibility into all access events—regardless of user type, device, or location. This ensures that every access request is authenticated and monitored for anomalies, closing the visibility gaps that attackers continue to exploit.

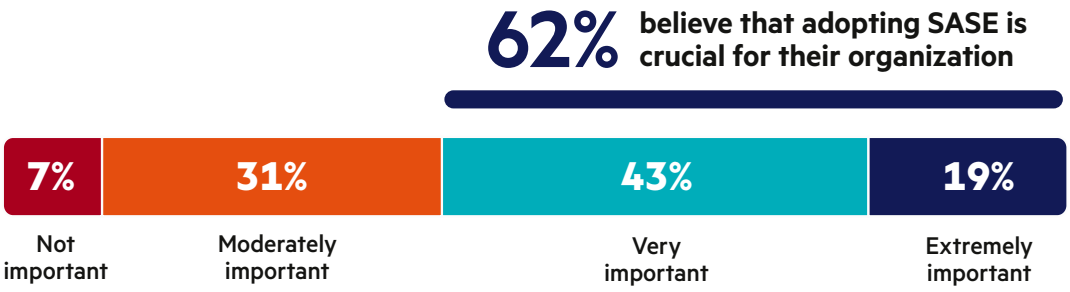
A modern solution

SASE bridges security and networking

Organizations face challenges with visibility gaps, fragmented security tools, and inconsistent access controls. To address these, many are adopting a Zero Trust strategy via Secure Access Service Edge (SASE), which unifies security and networking. Notably, 62% of organizations consider SASE crucial for their security strategy, underscoring the importance of integrated security and networking solutions.

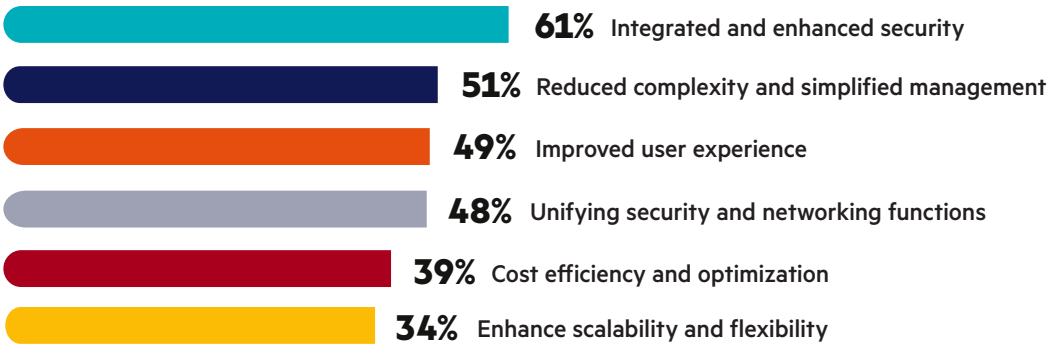
Despite its importance, SASE adoption is ongoing, with organizations only 47% of the way through their Zero Trust journey. Businesses understand that Zero Trust requires a comprehensive approach to secure networking, leading many to explore SASE.

How important is it for your organization to implement a Secure Access Service Edge (SASE) framework?



Organizations are adopting SASE primarily for enhanced security (61%), but they also see value in simplifying management (51%) and improving user experience (49%). These priorities highlight the need for security solutions that strengthen protection, streamline networking operations, and reduce user friction.

What are the primary drivers for your organization's interest in SASE solutions?



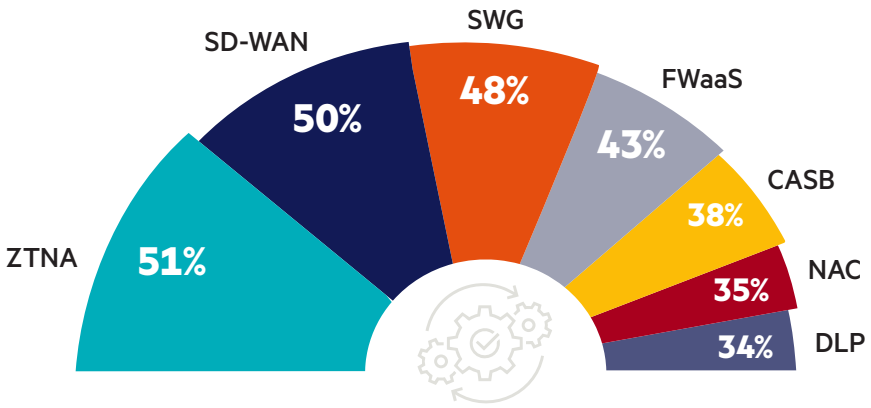
The shift toward single-vendor SASE and integrated security

As organizations push forward with SASE adoption to unify security and networking, they are making key decisions on deployment strategy. The strong preference for a single-vendor SASE model (61%) reflects the same demand for consolidation, simplified management, and integrated security seen in previous survey responses. Rather than managing a fragmented multi-vendor approach, organizations seek a unified security architecture that reduces operational complexity while improving visibility and control—especially as they struggle with confidence in access monitoring and Zero Trust implementation.

Do you prefer a single-vendor SASE or multi-vendor SASE model?

Organizations are prioritizing the integration of essential networking and security elements when adopting SASE components. Zero Trust Network Access (ZTNA) (51%) and Software-Defined Wide Area Network (SD-WAN) (50%) lead in adoption, reflecting the core areas of secure and optimized connectivity, and often serve as the initial step in SASE deployment.

Which components of SASE has your organization implemented or plans to implement?



Organizations are also adopting Secure Web Gateway (SWG) at 48% and Firewall-as-a-Service (FWaaS) at 43%, highlighting the importance of cloud-delivered security controls that protect users, applications, and traffic flows without affecting performance. Lower adoption rates for Cloud Access Security Broker (CASB) at 38%, Network Access Control (NAC) at 35%, and Data Loss Prevention (DLP) at 34% indicate that while these technologies are significant, organizations are currently prioritizing other SASE technology areas.

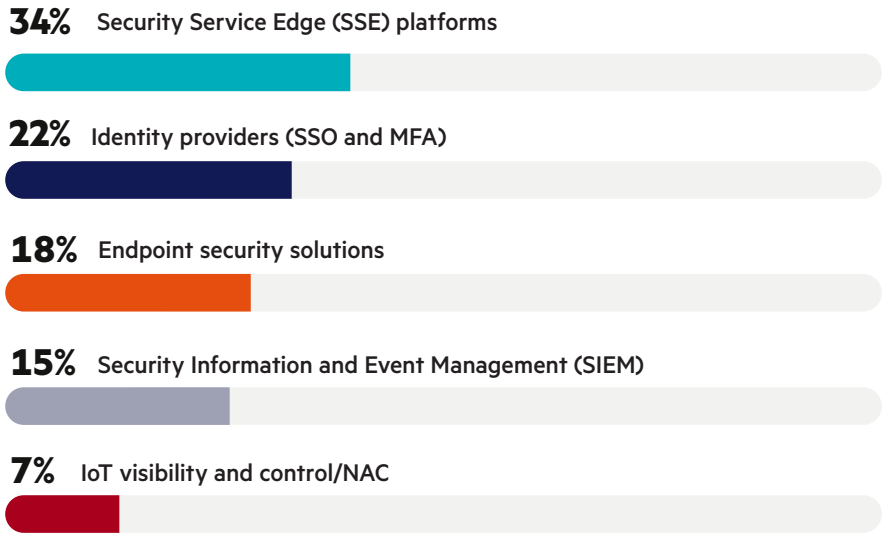
SSE as the strategic starting point for SASE

As organizations consider single-vendor SASE adoption, they are making important decisions about where to begin deployment. The data indicates that 59% of organizations start with Security Service Edge (SSE), while 41% focus on WAN edge services. This suggests a trend seen in previous responses: security is a key factor in SASE adoption, with many addressing Zero Trust access controls followed by optimizing network performance.

Where do you plan to start implementing your SASE strategy?

The prioritization of SSE facilitates both SASE adoption and Zero Trust strategies. According to 34% of respondents, SSE platforms are seen as the most critical technology for implementing Zero Trust. Organizations recognize that Zero Trust involves more than just authentication; it necessitates continuous verification, adaptive access controls, and deep traffic inspection, all of which are core SSE functions.

Which technology do you consider most critical for implementing a Zero Trust strategy?

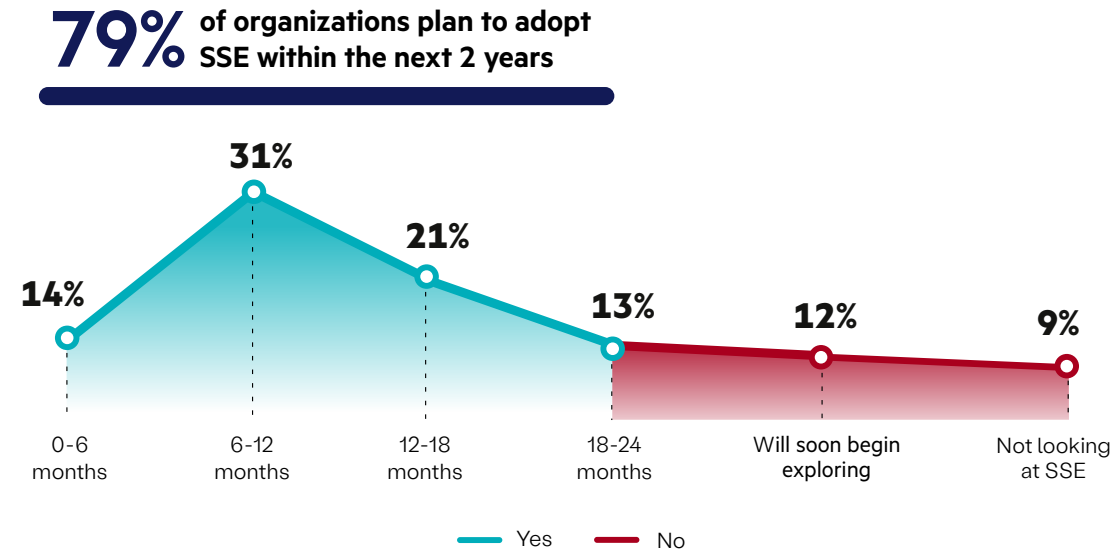


Other 4%

Accelerating SSE adoption

As organizations advance their SASE strategies, the adoption of SSE is accelerating, with 79% planning to implement an SSE platform within the next 24 months (up from 69% in 2024)—and nearly half (45%) moving forward within the next year. This underscores a growing urgency to unify access security, enforce Zero Trust policies, and transition away from perimeter-based security models.

Do you plan to adopt a Security Service Edge (SSE) platform within the next 24 months?

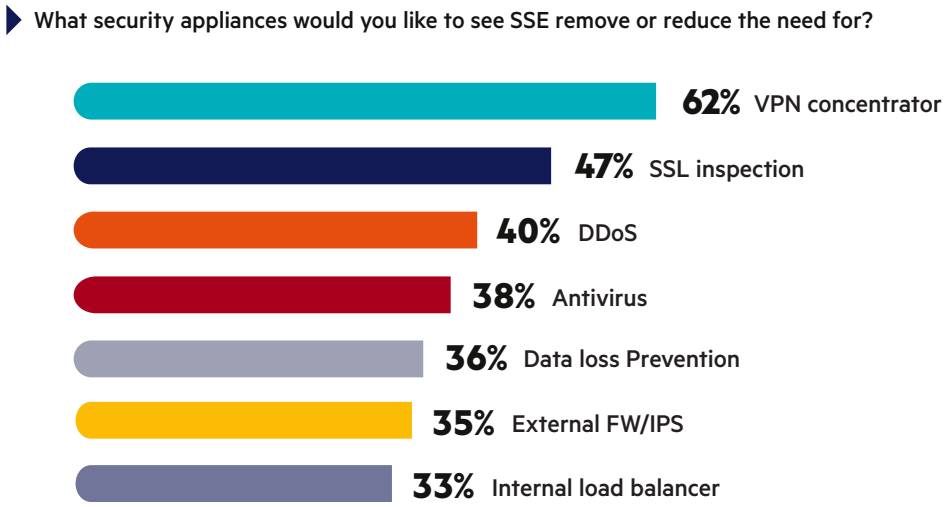


Among core SSE technologies, 46% of organizations prioritize ZTNA to modernize secure private access, followed by SWG (30%) and CASB (24%). This phased SSE deployment strategy first secures private access and then expands secure access to web and cloud applications, addressing the highest risk areas initially with a gradual deployment approach.

Out of the three core SSE technologies below, which do you plan to begin with first?

Eliminating legacy security appliances with SSE

Organizations are adopting SSE to unify security and enforce Zero Trust, but also to reduce reliance on costly, complex legacy security appliances.



The survey reveals that 62% would like SSE to eliminate VPN concentrators, reinforcing the trend of organizations moving away from traditional perimeter-based remote access toward cloud-delivered SSE.

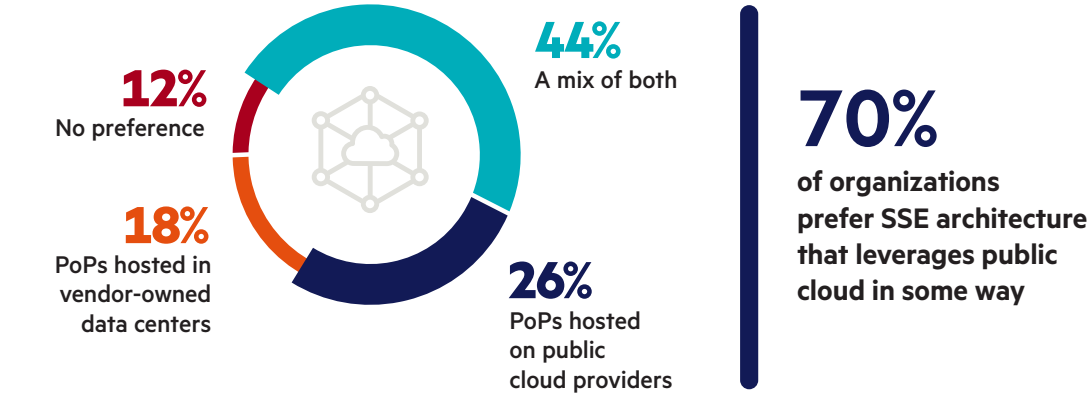
Beyond VPN concentrators, 47% of organizations are looking for SSE to reduce the need for SSL inspection appliances, highlighting the challenge of managing encrypted traffic visibility without performance degradation. 40% cite a priority to eliminate DDoS appliances, while 38% mention antivirus, showing a preference for integrating advanced security functions like threat protection and traffic inspection directly into a cloud-native SSE framework.

Businesses seek to converge security architectures and reduce operational complexities from outdated hardware. By consolidating security functions with SSE and delivering them via the cloud, companies can enhance agility, simplify management processes, and lessen complexity for security and networking teams.

SSE architecture matters

SSE architecture is generally divided into two delivery methods: PoPs via public cloud providers or PoPs in vendor-owned data centers. The report shows a growing preference for SSE architectures incorporating some level of public cloud deployment on AWS, Azure, and GCP, with 70% of respondents favoring this approach, up from 65% in 2024 and 60% in 2023.

What kind of SSE architecture would you prefer?



The SSE vendor-owned data center method has become less and less popular, with an 18% preference, as the adoption and prioritization of cloud has increased for the businesses, along with the growing demand for agility, scalability, and resiliency. At the same time, the 44% favoring a hybrid approach indicates that some organizations still value the flexibility to choose between public cloud and vendor-owned PoPs for additional control, regulatory compliance, or specialized workloads.

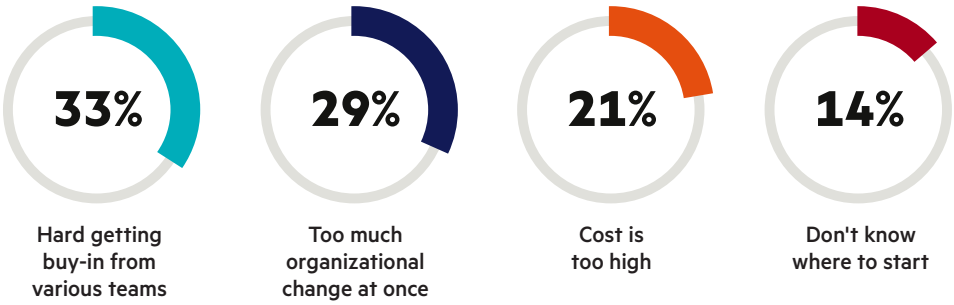
An important aspect to consider is whether an SSE vendor provides private edge deployment for on-ramp or PoP locations. This architectural flexibility can improve on-premises access speeds, enhance business continuity during outages, and comply with data regulations in certain scenarios.

Challenges and barriers to change

Overcoming barriers to SSE adoption

Despite 79% of organizations planning to adopt SSE within 24 months, several barriers may arise. The main obstacle (33%) is gaining support from different teams, necessitating early cross-functional alignment among IT, security, and networking departments. Additionally, 29% worry about significant organizational changes, fearing they may be overwhelming. Concerns over high SSE costs are noted by 21%, making it crucial to prioritize spending effectively. One way to do this is to ensure the SSE vendor provides ROI figures to justify the expense during evaluation.

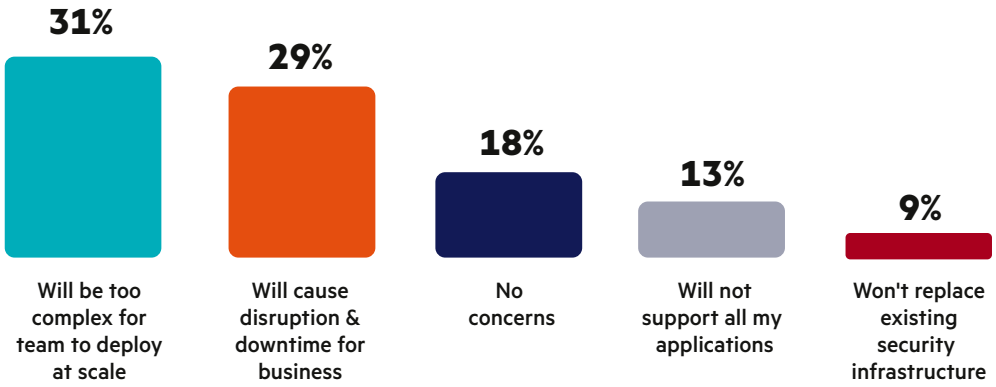
What is the biggest barrier to adopting SSE?



Other 3%

When asked about the top concern for SSE adoption, 31% worried about the service being too complex to deploy at scale, while 29% were concerned about potential user disruption and business downtime. On a positive note, nearly 1 out of 5 respondents had no concerns about SSE adoption. However, if you share any of these concerns, ask your SSE vendor how they plan to address them for your specific use case.

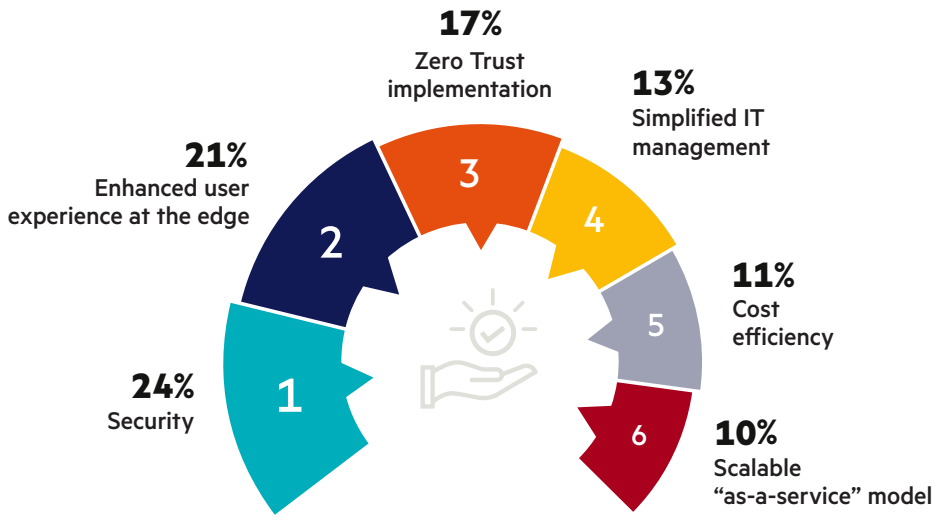
Which is your top concern when it comes to adopting an SSE service?



Maximizing the value of SSE

As organizations consider the barriers and challenges to adoption, the rationale for embracing SSE remains clear—enhanced security, improved experience, and simplified management.

What do you consider the most valuable benefit of adopting SSE?



Other 4%

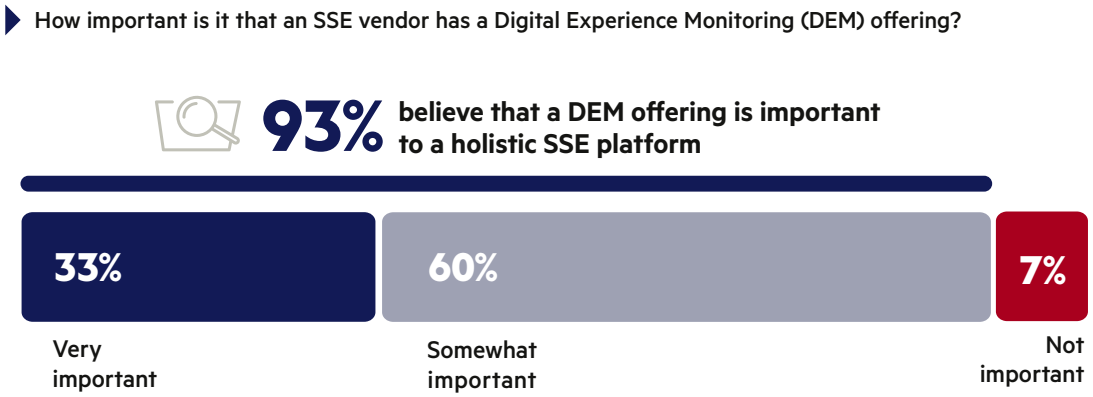
The survey data underscores the primary value businesses derive from SSE, with 24% citing security through data protection and compliance as the chief advantage, and 17% recognizing Zero Trust implementation as their highest priority. This demonstrates that the increasing significance of security across the board can be effectively addressed through the implementation of strategic technologies.

Additionally, 21% of respondents underscore the importance of enhanced user experience at the edge, highlighting the necessity for swift, seamless access to maintain business productivity. While security remains paramount, it should not impede productivity; instead, it should bolster it through strategic implementations.

Simplified management is noted as a significant benefit of SSE adoption by 13% of participants. The essence of SSE and SASE lies in their ability to consolidate for unified security, resulting in streamlined management processes. This consolidation allows for quicker adjustments, reduced manual interventions, and overall easier management, benefiting teams that are often stretched thin.

The role of Digital Experience Monitoring (DEM) in SSE

As organizations embrace SSE to strengthen security and improve user experience, they also recognize the importance of visibility into end-user performance. The survey shows that 93% of respondents consider Digital Experience Monitoring (DEM) important, with 33% rating it as very important. This highlights a growing understanding that SSE success is not just about security enforcement—it's also about ensuring seamless, high-performance connectivity for users across all work environments.



DEM plays a critical role in optimizing the user experience by providing real-time visibility into application responsiveness, network performance, and security policy impacts. In an SSE framework, security enforcement (ZTNA, SWG, CASB) happens in the cloud, which makes continuous monitoring essential to detect performance bottlenecks, troubleshoot latency issues, and proactively address disruptions before they impact productivity.

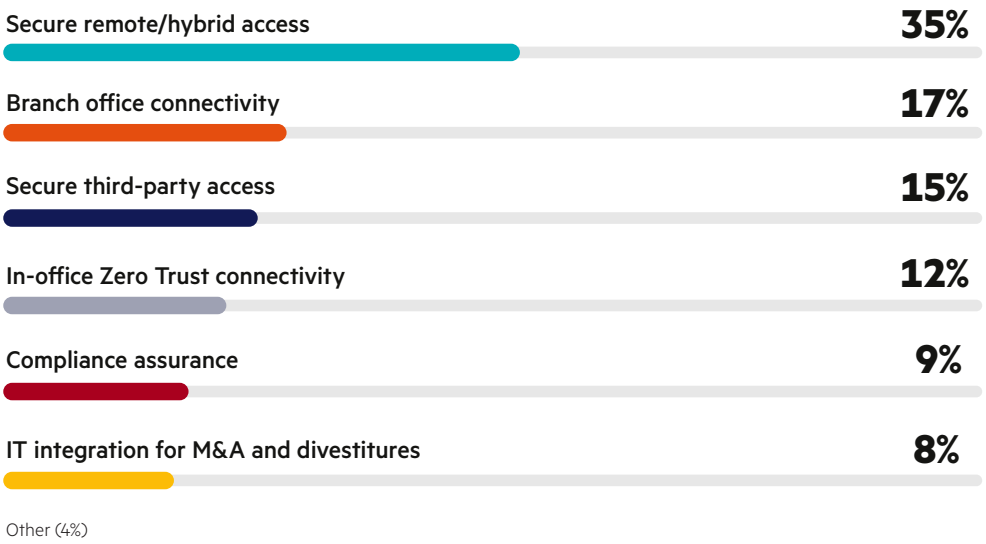
Without DEM, organizations lack insight into how security policies, network routing, and application access impact end-user experience—creating blind spots that can lead to frustration, downtime, and reduced efficiency.

To fully realize the benefits of SSE, organizations should ensure their chosen platform includes integrated DEM capabilities that provide granular insights and proactive performance optimization, as well as real-time visibility across cloud applications, remote workforces, and branch locations. By combining security enforcement with intelligent user monitoring, SSE solutions can deliver not only strong protection but also a frictionless, high-performance experience for users—ensuring that security does not become an obstacle to productivity.

Strategic entry points for SSE adoption

Previously in this report, it was established that hybrid or fully remote work is prevalent in 87% of organizations. This prevalence is a major factor influencing why security teams typically prioritize securing remote and hybrid access for employees (35%) as the initial step in their SSE journey. Following this priority are branch office connectivity (17%) and third-party access security (15%) as key SSE use cases. These findings reflect the reality that organizations must first secure their core workforce before expanding protections to distributed locations and external partners.

Which SSE use case do you plan to start with?



Other (4%)

To achieve the greatest security impact early with SSE, begin by securing remote and hybrid workforces using ZTNA to protect critical assets as users transition between home and office. Next, expand to branch connectivity and third-party security for comprehensive coverage with consistent policy enforcement.

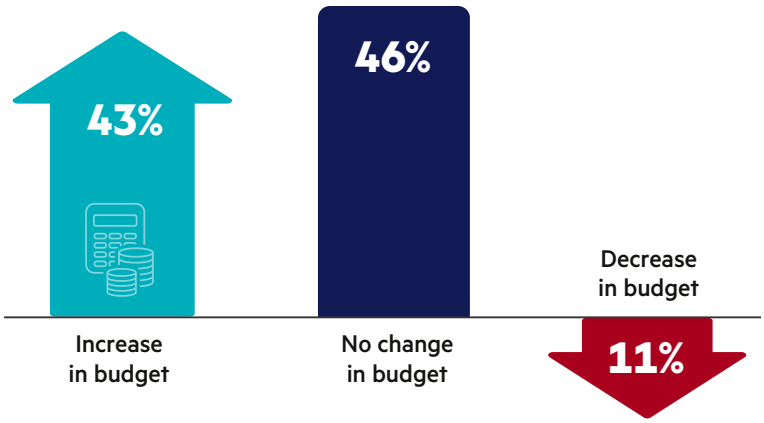
By deploying SSE in structured phases, security teams can prioritize high-risk areas initially and subsequently address other value-add use cases later, allowing them to enhance security at their own pace.

Security budgets reflect stability

As organizations advance their SSE, SASE, and Zero Trust initiatives, budget trends indicate a mix of stability and selective investment. The survey reveals that while 43% expect security budgets to increase, the relative majority (46%) anticipate flat spending, and only 11% foresee reductions.

This suggests that while security remains a priority, organizations are focusing on optimizing existing investments rather than drastically expanding spending.

How do you think security budgets will change in the next 12 months?



The steady or growing budgets align with the need for security modernization, particularly as organizations transition from legacy perimeter-based security to cloud-delivered SSE models. Given earlier findings that SSE adoption is accelerating, with 79% planning deployment within 24 months, budget increases will likely be directed toward consolidating security solutions, replacing aging infrastructure, and improving visibility into access security.

For organizations navigating budget constraints while implementing SSE, prioritization is key. Investing in SSE as an integrated platform—rather than managing multiple siloed security tools—ensures cost efficiency and operational effectiveness. By consolidating ZTNA, SWG, and CASB into a unified framework, organizations can maximize security coverage while controlling costs and aligning spending with strategic security transformation.

Best practices for successful SSE adoption

As organizations accelerate their adoption of SSE to modernize access security, they must navigate key challenges such as visibility gaps, Zero Trust enforcement, and security tool sprawl. To maximize the benefits of SSE—strengthening security, reducing complexity, and ensuring seamless user access—organizations should follow these proven best practices.

1

Prioritize ZTNA adoption as a first step towards SSE

Traditional VPNs create security risks and performance bottlenecks. ZTNA is a great first step in SSE adoption, ensuring that access is granted based on contextual access parameters like user identity, device trust, and real-time risk assessments. If you need a place to start, begin with ZTNA.

2

Focus on users with elevated risk, such as third-party access

Internal employees and external contractors may have increased security risks during remote access. Implement Zero Trust by ensuring third-party users receive only the minimal access necessary for their roles while preventing unauthorized network access.

3

Ensure your SSE platform offers real-time monitoring and risk detection

Select an SSE platform that provides continuous access monitoring, threat detection, and adaptive authentication to identify and address suspicious activity promptly, thereby reducing the risk of threats and limiting their impact.

4

Consider a resilient SSE architecture based on public cloud

70% of organizations use an SSE model leveraging public cloud. Choose an SSE vendor whose services are built on the reliability of reputable public cloud providers while also offering the flexibility to deploy private edge locations at headquarters or branch sites.

5

Ensure your SSE solution is truly consolidated

74% of organizations use three or more security tools, and SSE will not reduce this number if the platform is not fully integrated. Verify that your SSE vendor consolidates ZTNA, SWG, and CASB solutions onto a single cloud, single UI, and single policy for unified security, centralized policy enforcement, and reduced administrative overhead.

6

Adopt SSE in phases to meet business needs

While many plan to embrace full SASE, 59% start with SSE as their security foundation. Organizations should focus first on their greatest area of need; often this is the need for secure remote and hybrid access for their globally distributed business.

By following these best practices, organizations can ensure a smooth transition to SSE, enabling Zero Trust security, reducing risk, and delivering a more secure and efficient access experience for all users.

Understanding SSE and SASE: The future of secure access

As organizations adapt to hybrid work, cloud adoption, and evolving cyber threats, traditional network security models—built around firewalls, VPNs, and perimeter-based controls—are no longer sufficient. These legacy architectures create visibility gaps, policy inconsistencies, and operational complexity, leaving organizations vulnerable to credential theft, lateral movement attacks, and cloud security risks. This shift has driven the adoption of Security Service Edge (SSE) and Secure Access Service Edge (SASE), two modern security frameworks that ensure seamless, secure access to applications, users, and devices—anywhere, anytime.

What is SSE?

Security Service Edge (SSE) is the cloud-delivered security layer of SASE—and the starting point for most organizations modernizing access security. According to our survey data, 59% of organizations plan to begin their SASE journey with SSE, prioritizing security before network transformation. SSE consolidates fragmented security tools into a unified framework, reducing complexity while strengthening Zero Trust enforcement.

Key capabilities include:

- Zero Trust Network Access (ZTNA): Secures private application access while eliminating VPN by granting least-privilege, identity-based access.
- Secure Web Gateway (SWG): Blocks malicious web traffic, phishing attacks, and enforces security policies.
- Cloud Access Security Broker (CASB): Protects cloud applications, ensuring visibility and policy control across SaaS environments.

With 79% of organizations planning to implement SSE within the next 24 months, it is clear that SSE is the top priority for modernizing access security.

What is SASE?

Secure Access Service Edge (SASE) expands SSE by integrating networking performance optimization, including:

- Software-Defined WAN (SD-WAN): Routes traffic dynamically to improve network performance and application responsiveness.
- WAN Optimization: Reduces latency, improves bandwidth efficiency, and enhances cloud application performance.
- A significant majority of organizations favor a single-vendor SASE solution that unifies security and networking, specifically integrating SSE and SD-WAN.

What's the right first step for your organization?

For most organizations, SSE is the first and most impactful step toward a modern, cloud-delivered security framework. As organizations continue their digital transformation, SASE adoption will follow, unifying security and networking into a single, scalable architecture.

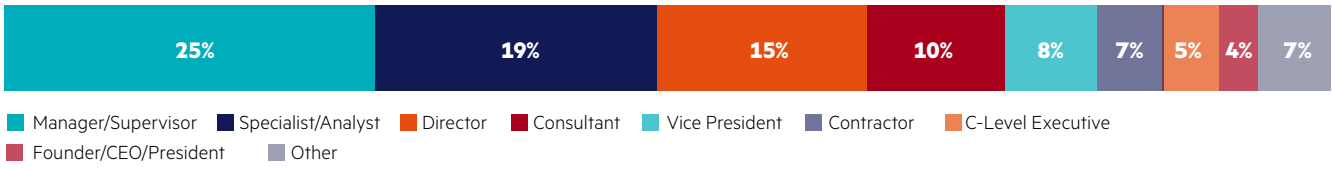
- SSE is the best choice if your priority is enhancing security without making major networking changes. It deploys alongside existing infrastructure and delivers immediate Zero Trust benefits.
- SASE is ideal for organizations seeking a fully integrated security and networking solution. SASE can be adopted in phases. Many organizations start with SSE before transitioning network architecture.

Methodology

This survey was conducted in early 2025, with 713 respondents across various industries and organizational sizes. Participants included IT professionals, cybersecurity experts, and decision-makers responsible for access security and Zero Trust strategies. Using a stratified sampling approach, the survey achieved a 95% confidence level with a margin of error of ±3.75%, ensuring statistically valid industry representation.

The survey explores SSE and SASE adoption, security priorities, and emerging challenges, providing a data-driven snapshot of how organizations are evolving their security architectures. The findings highlight security trends, adoption barriers, and the growing shift toward cloud-first, identity-driven security models.

CAREER LEVEL



DEPARTMENT

COMPANY SIZE

INDUSTRY

Hewlett Packard Enterprise

Introducing the HPE Aruba Networking SASE platform

The HPE Aruba Networking SASE platform offers a powerful, edge-to-cloud solution that seamlessly integrates networking and security functions into a unified solution. By combining our industry-leading SD-WAN with our award-winning SSE, our SASE platform ensures secure, uninterrupted access to applications and data from anywhere, enhancing both user experience and productivity.

The HPE Aruba Networking SASE platform simplifies deployment and management by merging networking and security into a single, intuitive interface. The SASE platform not only streamlines operations and reduces complexity but also provides security at cloud-scale for your modern digital enterprise.

Learn how HPE can help modernize secure connectivity with our unified HPE Aruba Networking SASE offering.

Learn more

Ready to experience the power of SASE in real time? Take a free 24-hour test drive today!

SASE test drive

Cybersecurity INSIDERS

TURNING CYBERSECURITY INSIGHTS INTO STRATEGIC INFLUENCE

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- How-to articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information visit

cybersecurity-insiders.com