Cybersecurity
INSIDERS

2024

Security Service Edge Adoption Report

HPE aruba networking

Introduction

Hybrid work is the new reality for many businesses, but it also poses new challenges for cybersecurity. CISOs and security architects need to rethink how they protect their critical resources from cyber threats, as they have to deal with a diverse and distributed workforce, a multitude of applications, and a complex network environment. Traditional access solutions are no longer adequate for this dynamic and demanding scenario.

This is why more and more security leaders are turning to Security Service Edge (SSE) services to enable secure, unified access for the modern business. SSE platforms are the next generation of enterprise access solutions, as they integrate ZTNA, SWG, CASB, and DEM technologies into a single cloud-based service. With SSE, any user can access any application from any location, with optimal performance and security.

The 2024 Security Service Edge Adoption Report provides a comprehensive analysis of the SSE market's current state and future trends, based on a survey of 631 cybersecurity professionals. The report reveals how SSE is transforming the way businesses secure their hybrid work environments, as well as the key drivers and benefits of adopting SSE.

Key findings from the report include:

- 94% stated their workforce is primarily hybrid or fully remote
- 59% say that adopting a SASE strategy is highly important to their business
- 57% of organizations plan to start their SASE strategy with a Security Service Edge (SSE) platform
- 69% of businesses want to adopt a Security Service Edge (SSE) platform within the next 24 months
- 44% plan to begin SSE implementation with Zero Trust Network Access (ZTNA) deployment

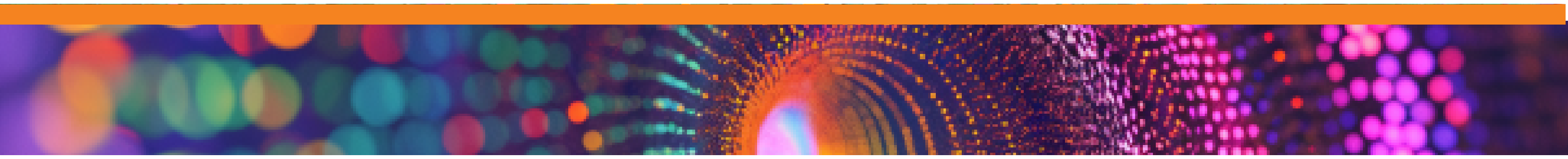
We are grateful to HPE Aruba Networking for their valuable collaboration on this report. Their expertise in SASE, SSE, and Zero Trust has enriched our research and findings.

We hope this report will serve as a useful guide for IT and cybersecurity professionals on your path towards SSE.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders



2024 SSE Adoption Report

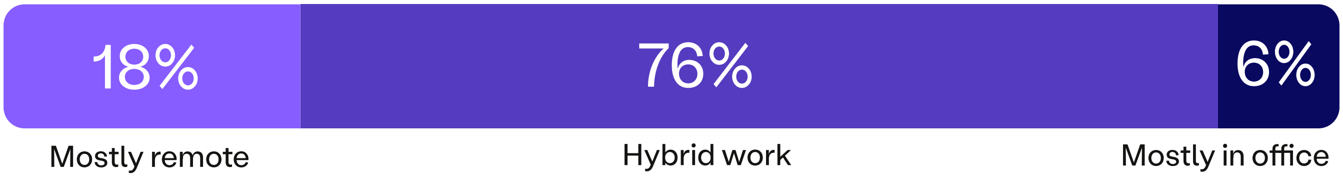
The Modern Workplace

The Risk in the New Workplace

As we approach the fourth anniversary of COVID-19, which acted as the catalyst for the rapid shift to remote and hybrid work, it is evident that businesses are not reverting back to traditional in-office operations. Instead, they have adeptly adjusted to meet the demands of their workforce. Specifically, hybrid work arrangements have remained consistent for 76% of organizations, while remote work environments have surged by 80% compared to last year. Conversely, in-office work has declined by 50% during the same period.

Overall, the widespread adoption of hybrid and remote work models is here to stay. Consequently, businesses must adapt their cybersecurity strategies to effectively support this distributed workforce. Consider your organization's unique needs and explore secure access solutions for business applications, catering to users accessing them from any location.

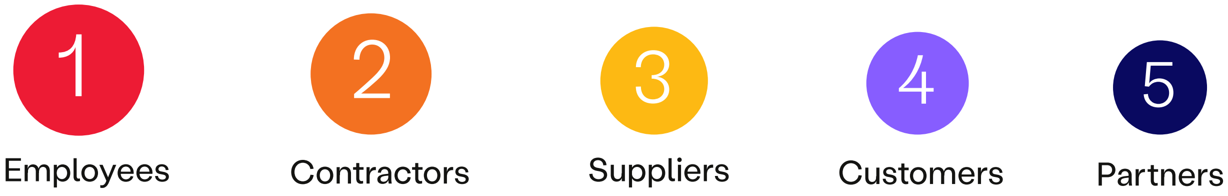
What best describes your current employee workforce model?



Just as people are working from anywhere, many different types of users are gaining access to critical business resources. When assessing risk, it is unsurprising that employees — pose the highest risk to the business (rising from last year's second place) likely due to their direct access to sensitive data and applications. Contractors follow closely as the second-highest risk category, given the nature of external users requiring access to internal business resources.

Suppliers and customers also present significant risks, albeit to a lesser extent, while partners are perceived as the least risky user group. These responses underscore the critical nature of insider threats, whether from direct employees or those slightly removed, such as contractors and suppliers.

When securing access for your business, which group presents the most risk?



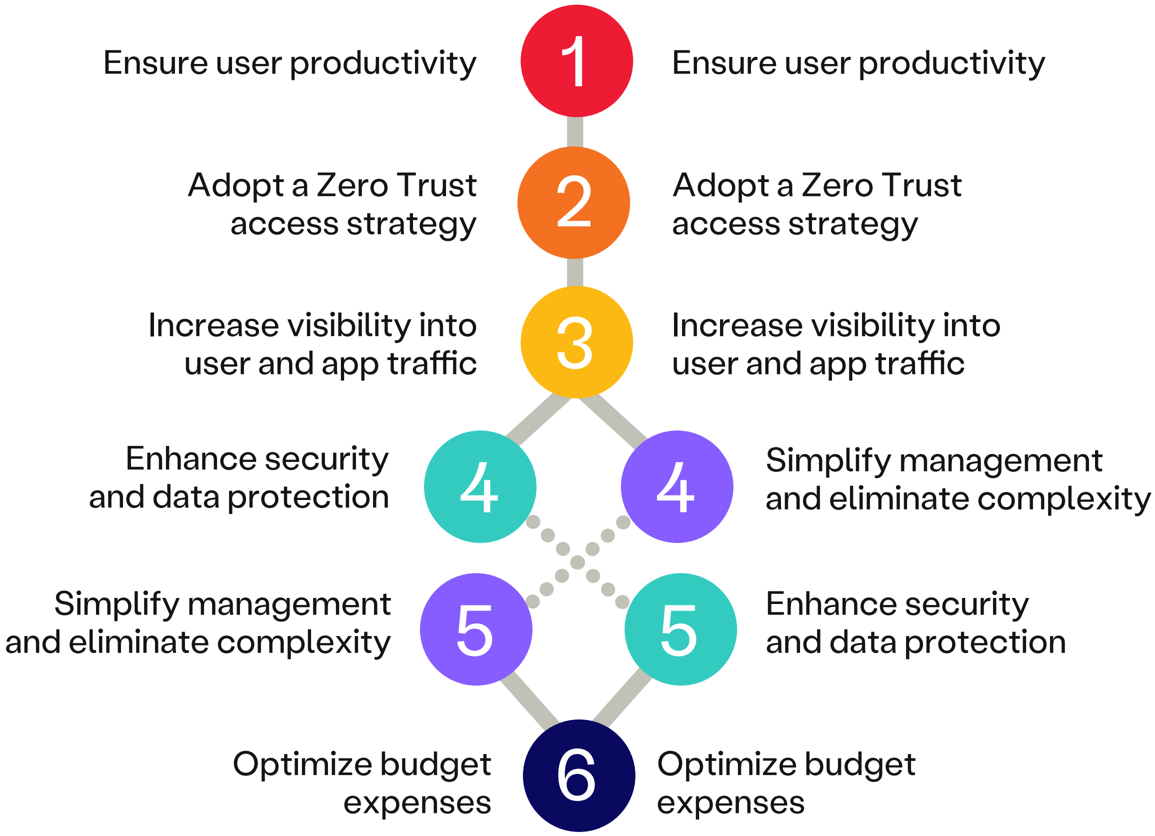
This statistic strongly emphasizes the need for implementing Zero Trust measures, not only for "trusted" internal users but also for external ones. Teams must critically evaluate their business processes to transform employees, currently the highest risk group, into allies for security strategy and overall business success. A well-functioning business cannot afford to have its employees driving the most risk; the right security approach is essential.

Top Priorities and Challenges

In the context of the modern workplace, it is crucial to understand both the business' priorities and the challenges they face. Within the survey findings, a striking alignment emerges: the top three areas of business challenges also happen to be the highest priorities. This alignment emphasizes the critical nature of these areas.

What is your top priority when enabling the modern workplace?

What is the biggest challenge in securing the modern workplace?



Ensure user productivity	1	Ensure user productivity
Adopt a Zero Trust access strategy	2	Adopt a Zero Trust access strategy
Increase visibility into user and app traffic	3	Increase visibility into user and app traffic
Enhance security and data protection	4	Simplify management and eliminate complexity
Simplify management and eliminate complexity	5	Enhance security and data protection
Optimize budget expenses	6	Optimize budget expenses

Firstly, the foremost priority and challenge revolve around ensuring user productivity. As users access applications across data centers or the cloud, on various devices and networks, maintaining seamless access to essential resources within the distributed environment becomes paramount. Teams must guarantee fast, reliable, and consistent access, regardless of the user's context or situation.

Secondly, adopting a Zero Trust strategy stands as the second priority and challenge. As demands for better experience increase, it's important that security isn't compromised for the sake of productivity. Striving for solutions that achieve both objectives is the goal.

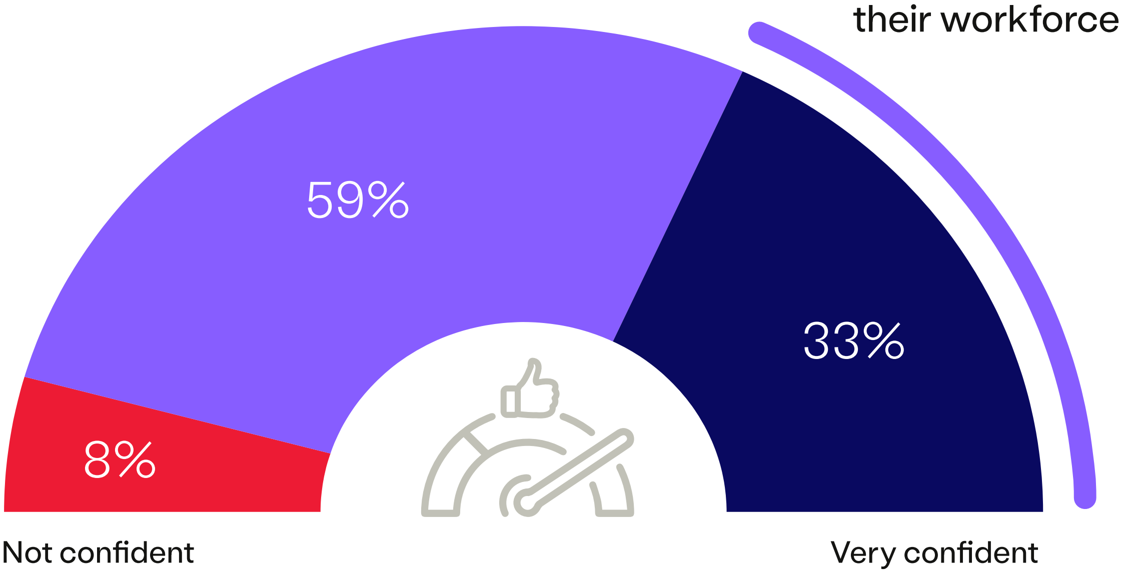
Lastly, the third priority/challenge focus on the business's ability to increase visibility into user and application traffic. Traditional secure networking solutions often lack visibility due to mobile users and extended app locations. To remain competitive in the evolving threat landscape, businesses don't just need visibility, but actionable insights that proactively addressing security gaps and hidden risks.

Confidence in Security

Gauging how well an organization can protect workforce access is crucial for improving its cybersecurity. The survey data shows that only one-third (33%) of organizations feel very confident in their security teams' ability to secure workforce access. On the flip side, two-thirds (67%) express low confidence levels.

In today's cyber-risk landscape, security teams must be confident in securing business access. The reported lack of confidence reflects doubts about the effectiveness of the current tools and technologies. Remember: the right technology empowers security teams, while the wrong ones can leave businesses vulnerable.

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



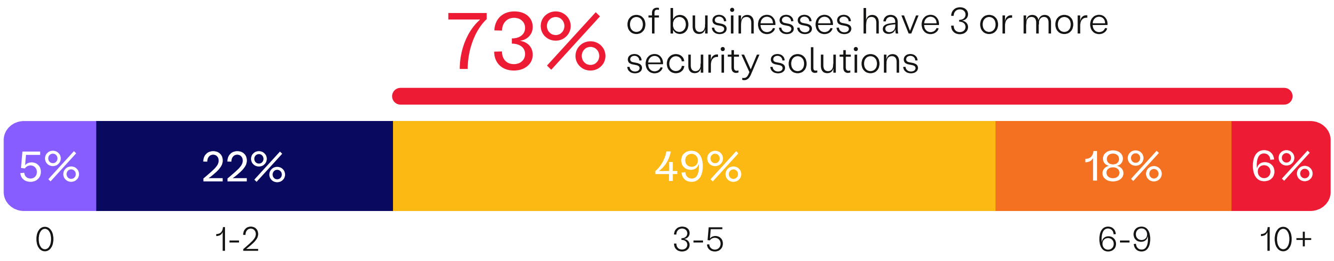
Only 33% are highly confident in their ability to secure access for their workforce

Legacy Access Solutions

The number of solutions deployed to secure resource access highlights organizations' security infrastructure complexity. According to the survey, 73% of organizations now utilize three or more distinct security solutions, marking a 10% increase year-over-year. The share of organizations utilizing 3 to 5 security solutions has surged by 19.5%, while the share of organizations deploying one or two security solutions has declined by 29%. This shift suggests that many companies previously in the 1-2 range have transitioned to the 3-5 range.

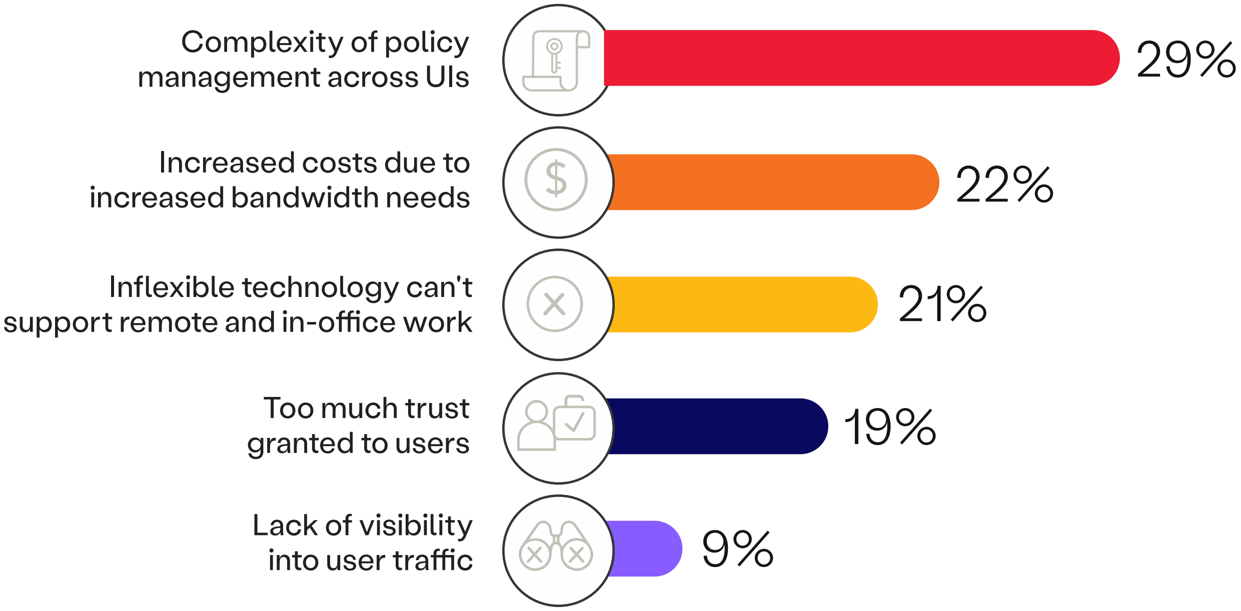
As the traditional network security stack continues to expand, it's essential to assess when this approach becomes unmanageable for teams. Consider the impact of an ever-growing array of security appliances on your business and security team, and perhaps explore alternative security strategies.

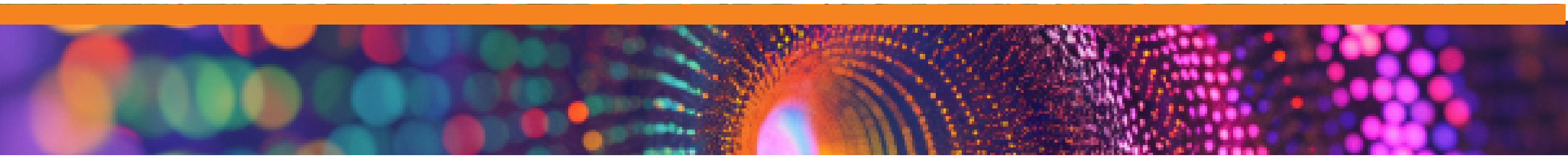
How many different security solutions are you using to provide employees and partners with access to business resources?



With most businesses boasting over 3 security solutions, it's no surprise that 29% of cybersecurity professionals claim policy management as their greatest challege with current access solution—whereas last year's primary challege was granting too much trust to users. Other top challenges include include increased cost (22%) and inflexibility of exisiting security solutions (21%).

What is the greatest challenge you face with your existing secure access solutions?





2024 SSE Adoption Report

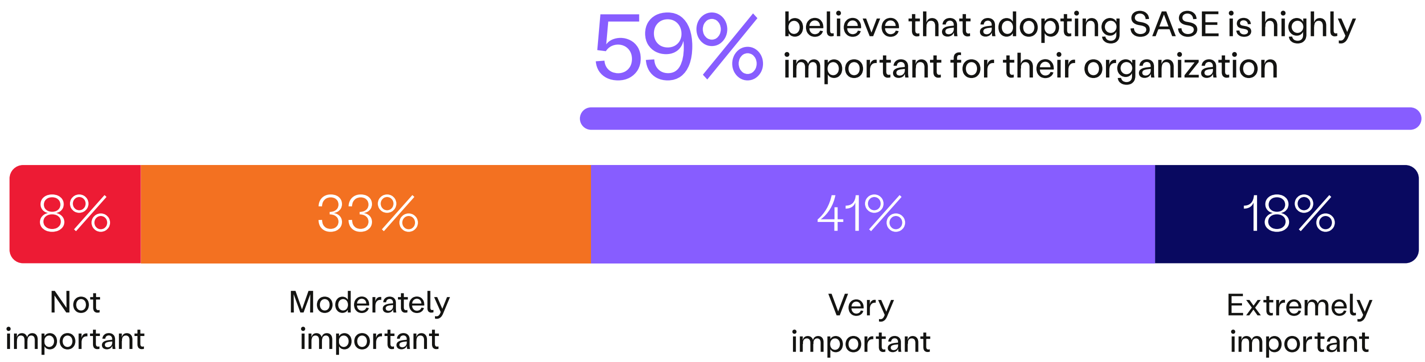
A Modern Solution

Prioritizing a SASE Strategy

The term Secure Access Service Edge (SASE) has generated significant interest in recent years. Coined in 2019, businesses were initially unaware of the profound impact the SASE framework would have in the post-COVID world. Survey results unequivocally demonstrate its significance: 59% of respondents deem SASE adoption highly important for their business, while a mere 8% dismiss it as inconsequential.

As organizations evaluate the potential benefits of SASE—such as enhanced security efficiency, reduced complexity, and heightened security agility—they must also recognize its role in promoting integrated network and security strategies, thereby mitigating tensions between these critical functions.

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

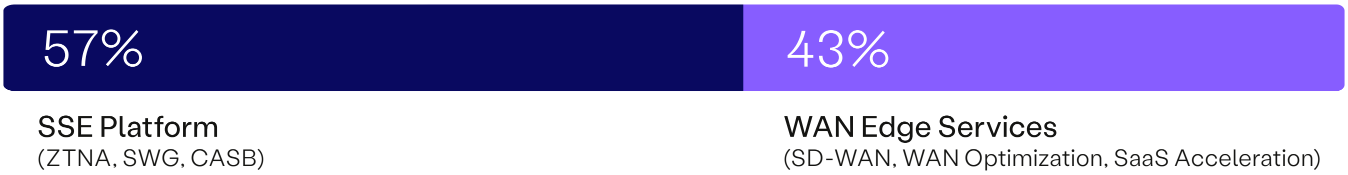


SSE as a Strategic Initiative

Determining the starting point for your Secure Access Service Edge (SASE) strategy is pivotal, as it sets the foundational direction for integrating network and security functions. A majority of organizations (57%), plan to begin their SASE strategy with Security Service Edge (SSE) platforms, including Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Secure Web Gateway (SWG). This preference highlights the emphasis on the security aspect of SASE, prioritizing secure access and threat prevention. However, WAN Edge Services has increased in mindshare since last year's survey, as previously 67% said they preferred to start with SSE. This shift could be due to the increased demand for greater unification and consolidation as Unified SASE platforms have begun merging SSE and WAN Edge Services rather than treating them as two separate parts.

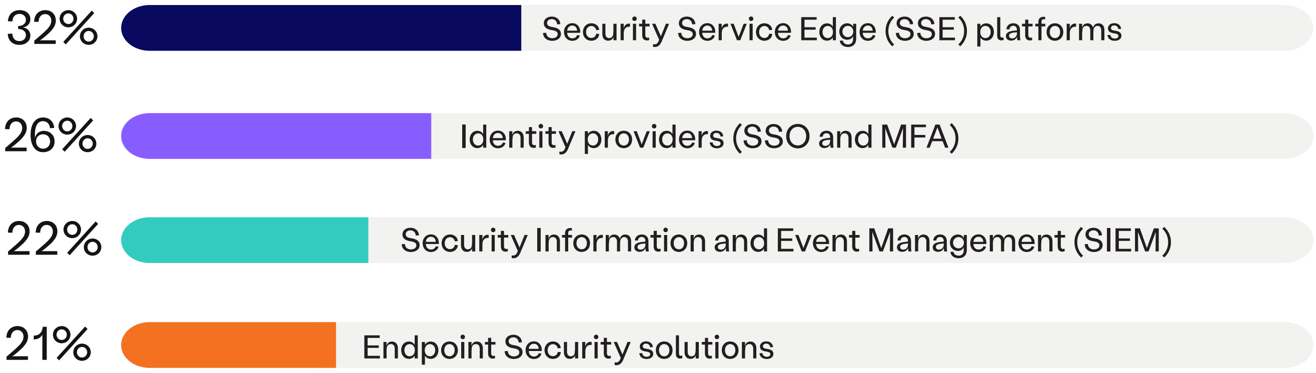
For organizations embarking on the path to SASE, the focus should be on selecting an entry point that addresses the most immediate needs while laying the groundwork for a comprehensive SASE framework. Whether starting with SSE to bolster security measures with Zero Trust or with WAN services to enhance network capabilities, the key is to choose a path that supports seamless expansion and integration of SASE components over time, ensuring a unified and adaptive security approach.

Where do you plan to start implementing your SASE strategy?



Furthermore, when asked which technology is most critical to a Zero Trust strategy, SSE platforms ranked first for the second year in a row at 32%. SSE even ranks higher than identity solutions like SSO and MFA (26%), SIEM solutions (22%) and endpoint security (21%). The implementation of Security Service Edge (SSE) is recognized as a strategic initiative across the industry, as it is central to both an overarching SASE strategy and a Zero Trust approach.

Which technology do you consider most critical for effectively implementing a zero trust strategy in your organization?

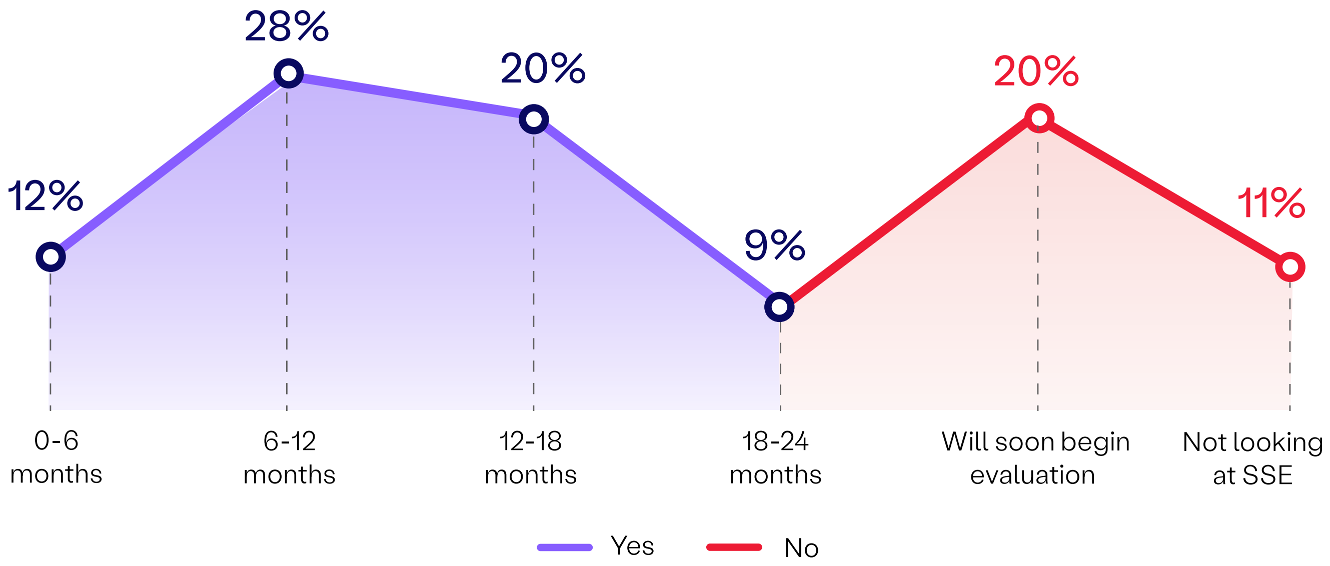


Adoption of SSE

How quickly are organizations planning to adopt strategic SSE platforms? According to the survey, 69% of cybersecurity experts plan to implement SSE within the next two years, up four percentage points from last year. Notably, 40% of these organizations aim to adopt SSE by the end of 2024, indicating a strong priority to bolstering security strategy for the business. Further, only 11% of businesses are not considering SSE at all, while 20% will soon consider evaluation.

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

69% of organizations plan to adopt SSE within the next 2 years



According to the survey, ZTNA is the most popular starting point for SSE adoption, with 44% of organizations choosing it, compared to 47% last year. This is followed by Secure Web Gateways (SWG) rising from 20% to 29% year-over-year. Security teams realize they need to establish Zero Trust with ZTNA first and then secure web access with SWG. CASB adoption fell from 33% last year to 27%, implying a shift in SSE adoption priorities.

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

44%	29%	27%
ZTNA	SWG	CASB

Appliance Reduction With SSE

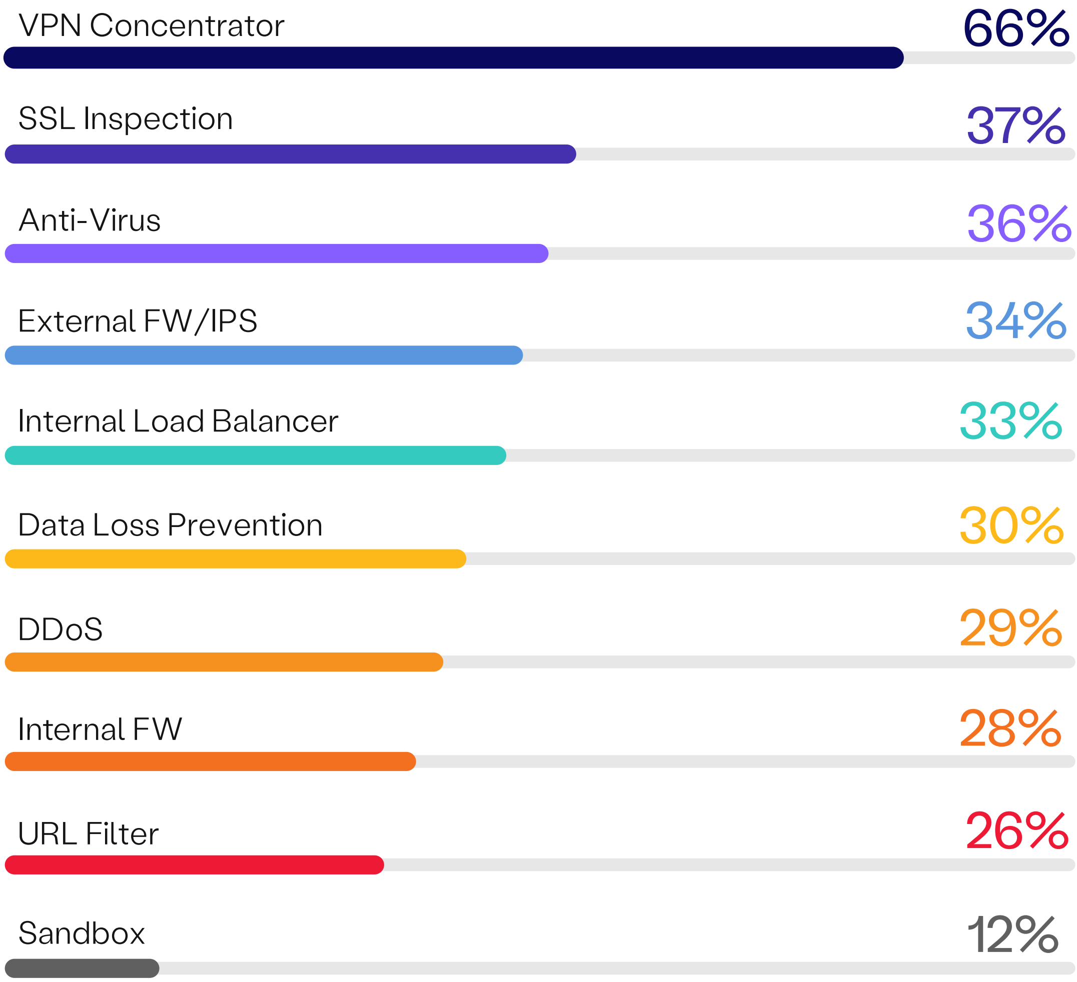
A Security Service Edge (SSE) framework can optimize your cybersecurity infrastructure by streamlining or eliminating traditional security appliances.

The survey reveals that VPN concentrators are the technology most security teams want to see replaced by SSE (66%), for the second year. SSL inspection follows this with 37%. As a result, SSE plays a key role in VPN replacement and facilitates scaling out SSL inspection through cloud-delivered SSE approaches.

The report also shows that external FW/IPS (34%) climbed to the 4th highest technology to be replaced, compared to the 9th slot last year. This is likely due to the fact that more and more SSE services are building FWaaS into their platforms which allows greater appliance consolidation in these areas.

Furthermore, internal load balancing solutions rose to the 5th highest technology to be replaced, at 33%, while previously at the bottom of the list last year. This could be emphasizing the need for greater resilience and scalability, both achievable with a cloud-delivered SSE solution.

What security appliances would you like to see SSE remove or reduce the need for?

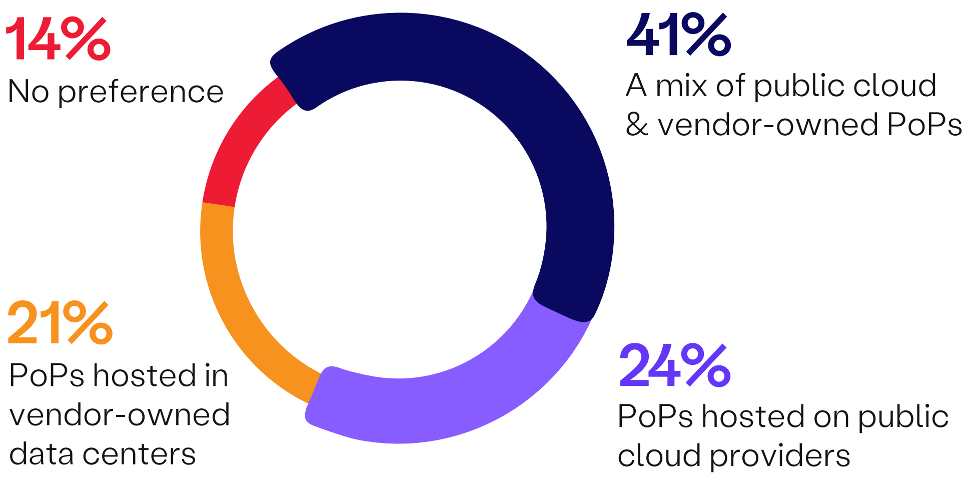


SSE Architecture Preference

SSE architecture is typically categorized into two delivery methods: PoPs via public cloud providers or PoPs in vendor-owned data centers. The report finds that cloud and hybrid SSE architectures continue to grow in preference, with 65% desiring an SSE solution that utilizes public cloud in some capacity, up from 60% last year.

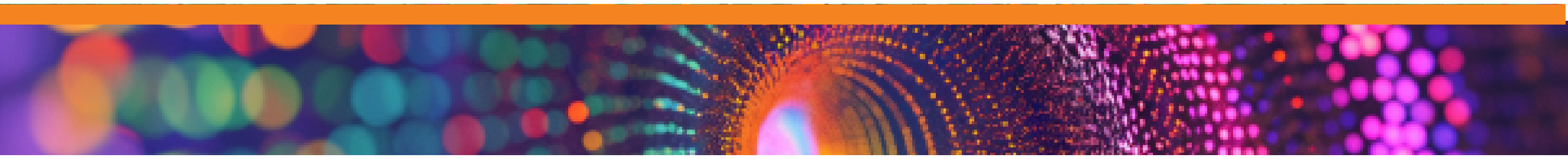
This is the result of 41% of respondents favoring a hybrid approach, a mix of public cloud providers and vendor-owned data centers for hosting SSE PoPs, up from 34% last year. This 20% increase in preference likely results from more teams leaving the "no preference" category, which dropped 26% year-over-year, and joining the hybrid architecture category. Additionally, 24% prefer SSE PoPs hosted on public cloud platforms like AWS, Google Cloud, and Azure, highlighting the cloud agility and global reach these platforms offer. Finally, those who favor vendor-owned data centers has remained constant at 21%, which may indicate a desire for dedicated resources and better security.

What kind of SSE architecture would you prefer?



65% of organizations prefer SSE architecture that leverages public cloud in some way

These preferences highlight the diversity in organizational needs and priorities when it comes to deploying SSE solutions. Embracing a mixed architecture could provide the best of both worlds, combining the cloud's scalability with the control offered by vendor-specific data centers. As companies navigate their SSE implementation, considering the specific advantages of each architecture and how they align with business goals will be crucial in crafting a secure, efficient, and resilient cybersecurity posture.



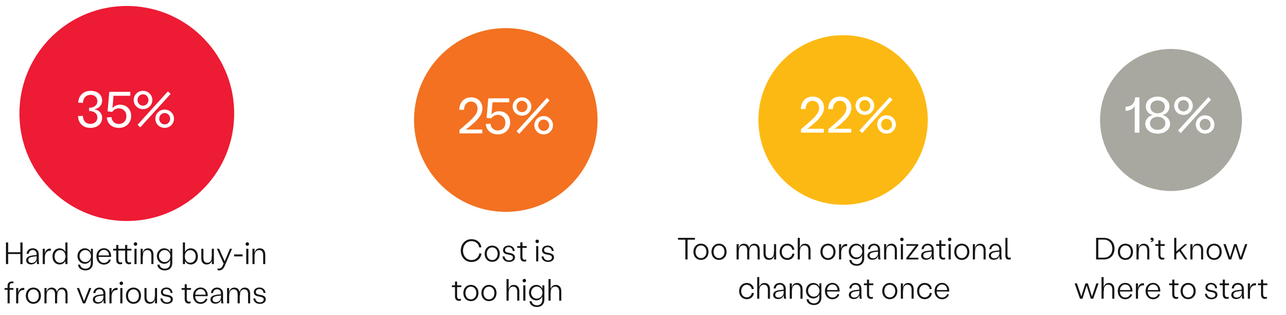
2024 SSE Adoption Report

Challenges & Barriers to Change

Key Barriers to SSE Adoption

When asked about key challenges, the survey participants revealed that getting buy-in from various teams is the most significant barrier to seamless SSE adoption, cited by 35% of respondents. This highlights the organizational and cultural challenges of aligning multiple stakeholders, specifically from security and networking teams, around adopting new security technologies. Following closely are cost issues, identified by 25% as the main obstacle, reflecting concerns over the financial implications of implementing SSE solutions. Additionally, 22% of participants see too much organizational change at once as a challenge.

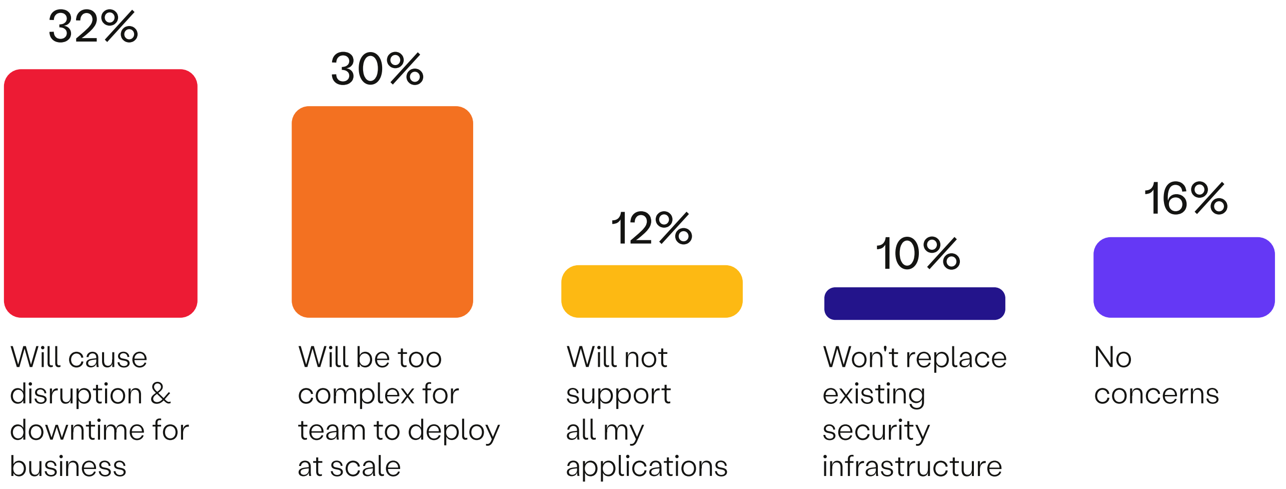
What is the biggest barrier to adopting SSE?



The survey reveals that disruption and downtime (32%) is the top concern for SSE, moving up from second place last year (24%). Complexity preventing SSE deployment at scale (30%) is the second highest concern, up from 22% last year. If you share this concern, evaluate two things when choosing an SSE vendor: (1) Does the vendor have one or multiple UIs? Multiple UIs mean more policies and management scale issues. (2) What is the architecture of the SSE vendor? Do they host PoPs in a public cloud or their data centers? The vendor's scalability affects your scalability.

Lastly, the survey results show a significant drop (decrease by 18% from last year) in the concern that SSE won't replace existing security infrastructure, which was last year's biggest concern. This means SSE is gaining trust and proving its ability to replace legacy solutions like on-premise firewalls, VPNs, etc.

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



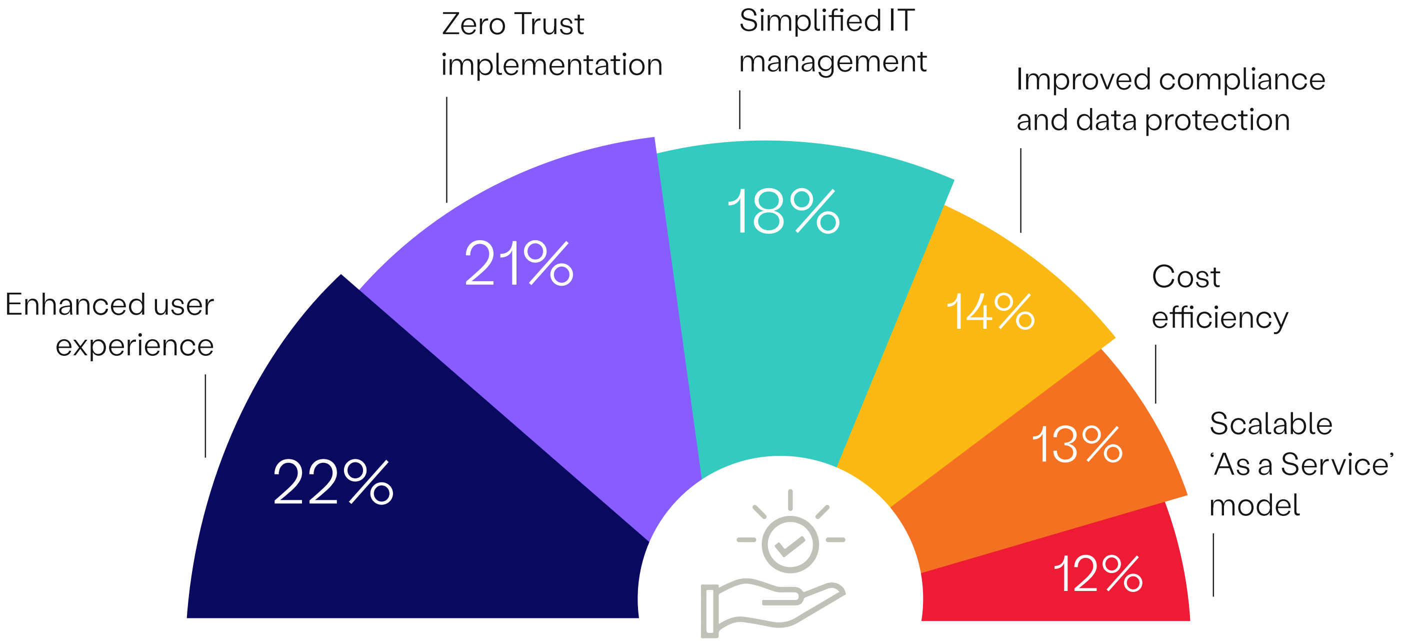
Benefits of SSE

After reviewing the barriers and challenges of SSE, let's look at the benefits. When asked about the most valuable benefit of adopting SSE, the survey results highlight enhanced user experience at the edge as a leading benefit, recognized by 22% of respondents. This underscores the importance of maintaining a seamless and efficient user experience, especially in environments where edge computing plays a pivotal role.

Following closely, Zero Trust implementation is valued by 21% of participants, indicating the critical role SSE plays in facilitating a shift towards more secure access control frameworks within organizations. Simplified IT management through consolidation of tools also emerges as a significant benefit for 18% of respondents, reflecting the appeal of flexible, scalable security solutions that can replace legacy tools.

The benefits we see for SSE map closely to the priorities and challenges we reviewed earlier in the report, specifically in user experience and security. Security teams are looking to find a way to balance the two, and SSE can solve this problem.

What do you consider the most valuable benefit of adopting Secure Service Edge (SSE)?

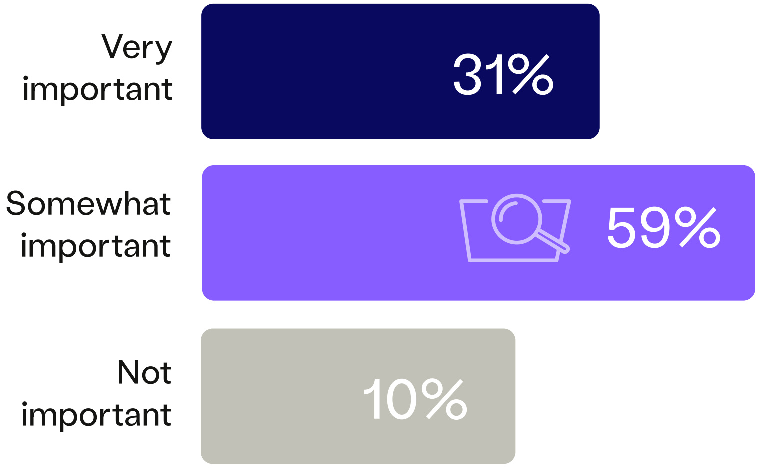


The Importance of User Experience

Integrating Digital Experience Monitoring (DEM) into Security Service Edge (SSE) offerings is becoming increasingly important for organizations looking to gain real-time insights into user experience and how it impacts performance and productivity.

An overwhelming majority of 90% confirm that DEM is important to a holistic SSE platform, indicating a recognition of the value DEM adds in monitoring and ensuring a positive user experience without compromising security. This finding suggests that organizations are increasingly aware of the balance between security and user experience, with many prioritizing solutions that can provide visibility into how security measures impact user interactions.

How important is it that an SSE vendor has a Digital Experience Monitoring (DEM) offering?



90%

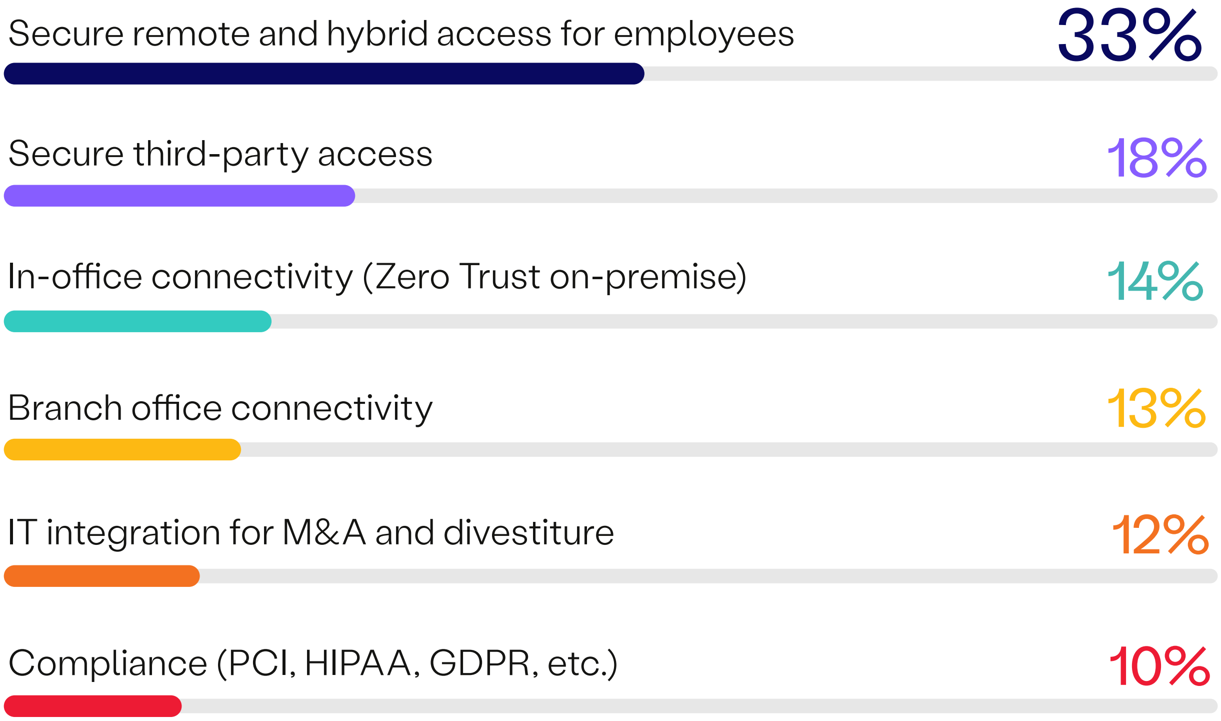
believe that a DEM offering is important to a holistic SSE platform

Getting Started With SSE

Earlier in this report, we confirmed that hybrid or fully remote work is the norm for 94% of organizations. This is a significant factor contributing to the most common starting point for security teams beginning their SSE journey by securing remote and hybrid access for employees (33%).

Following this, the emphasis on securing third-party access has nearly doubled year-over-year, with 18% of cybersecurity professionals selecting it as their primary use case. This shows the underlying importance that teams need to ensure secure access for vendors, contractors, and other external parties, not just employees. Additionally, implementing Zero Trust security on-premise is highlighted by 14% as the third most predominant use case.

Which SSE use case do you plan to start with?



These insights indicate that organizations are keenly aware of the evolving security landscape and are looking to SSE solutions to address their most pressing challenges. Starting with use cases that support remote work and secure third-party access reflects a strategic approach to strengthening security postures while accommodating the needs of a distributed workforce and extended enterprise. As SSE adoption progresses, these initial use cases can lay a solid foundation for expanding into other areas, ensuring a comprehensive and flexible security framework.

Using Security Budget Wisely

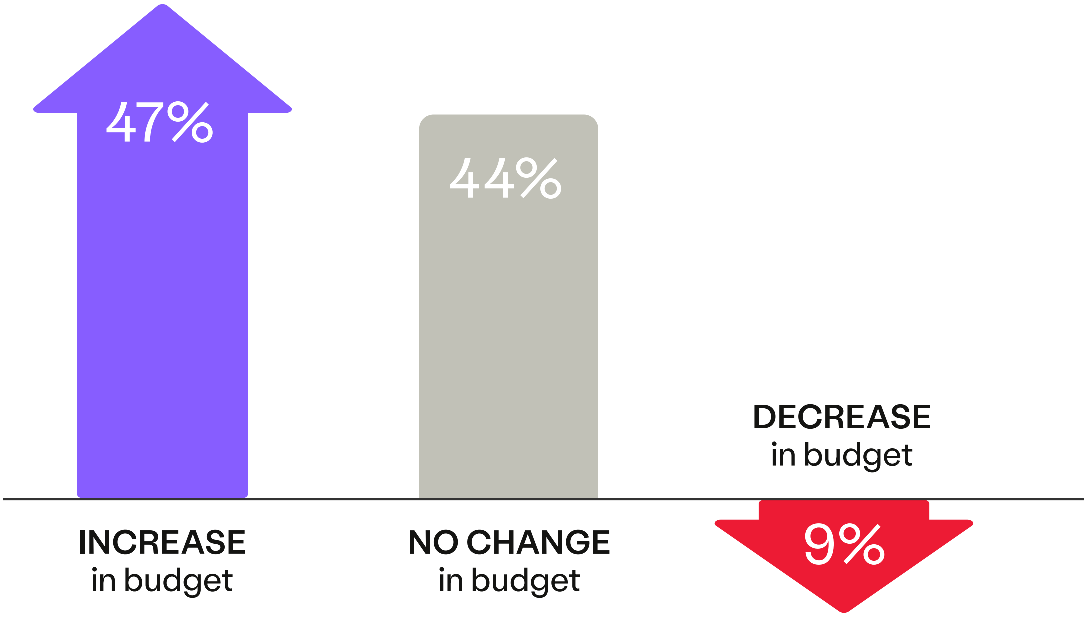
How will your security budgets be impacted in the coming year? Whether your budget is increasing, remaining the same, or decreasing, each category has its own implications and challenges.

If you are among the 47% of enterprises that expect an increase in security budgets, you have a great opportunity to enhance your security posture. Your business understands that the security landscape is evolving, and you need more resources to protect it. Use this chance to plan, identify, and eliminate risky or outdated technologies and leverage SSE to support your business.

If you are among the 44% of teams that will have no change in your security budget, you have to optimize your spending and prioritize your goals. Instead of relying on point products that may not work well together, choose holistic platforms that offer more value and efficiency.

If you are among the 9% of teams that will face a decrease in your security budget, you have to make some tough decisions and trade-offs. Security is still your top business priority, so don't settle for solutions that don't meet your needs or expectations. Don't waste dollars on suboptimal products and switch to solutions that deliver better results.

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



8 Actionable Strategies for Effective SSE Deployment

Effective Security Service Edge (SSE) implementation is crucial for bolstering cybersecurity defenses in a rapidly evolving cyber threat landscape. This guide highlights eight essential practices for deploying SSE as you seek to optimize and streamline your organization's secure access.

1 **Reduce Dependency on Legacy Security Appliances**
Leverage SSE to streamline or eliminate traditional security appliances, such as VPN concentrators and SSL inspection appliances, for a more efficient and scalable cybersecurity infrastructure.

2 **Implement Zero Trust Network Access Principles**
Prioritize Zero Trust within the SSE framework, ensuring all users are authenticated, authorized, and continuously validated before granting access to applications and data.

3 **Consolidate Security Architecture on a Unified SSE Platform**
Integrate disparate security tools and platforms into a unified SSE solution that provides ZTNA, SWG, CASB, and DEM functionality. This approach reduces complexity and improves manageability for better security posture and policy enforcement.

4 **Embrace Cloud and Hybrid SSE Architectures**
Opt for SSE solutions that support cloud, on-premise, and hybrid deployments to ensure flexibility and scalability, accommodating the diverse needs of your organization.

5 **Strategically Plan SSE Deployment**
Start with ZTNA to secure remote access to private business applications and replace VPN technology, then gradually expand the SSE framework to include more use cases and areas of secure access needs, ensuring comprehensive coverage.

6 **Secure Hybrid and Remote Work Environments**
Emphasize the security for hybrid and remote work by implementing SSE solutions tailored to distributed workforce needs, ensuring secure and efficient access without compromising user experience.

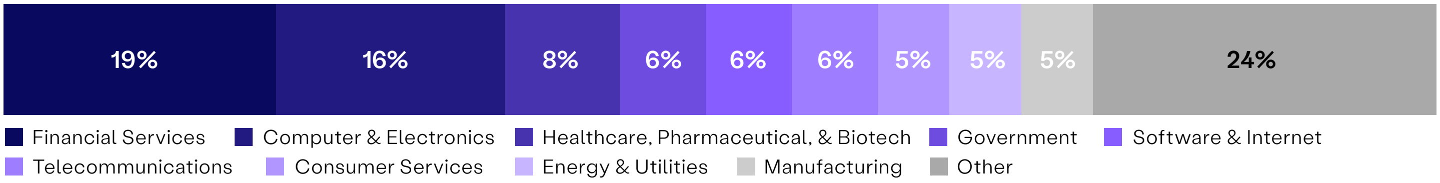
7 **Enhance User Experience with DEM**
Incorporate Digital Experience Monitoring (DEM) within your SSE strategy to ensure an optimal user experience without sacrificing security, which is especially crucial in edge computing environments.

8 **Allocate Budgets Towards SSE Investments**
Prioritize spending on SSE technologies that offer the most significant impact on your security posture. This involves assessing your threat surface, identifying key vulnerabilities, and investing in solutions that address these challenges effectively.

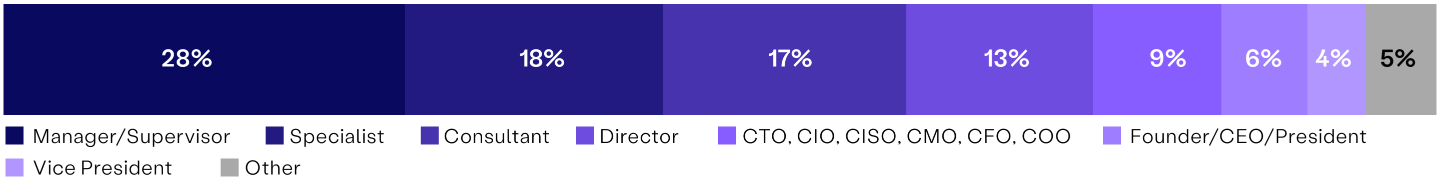
Methodology & Demographics

This survey was conducted in February of 2024 with a sample of 631 respondents, representing a diverse range of industries and organizational sizes. Respondents included IT professionals, cybersecurity experts, and decision-makers responsible for their organization's network security and remote access strategies. The survey aimed to gather insights into current trends, challenges, and attitudes towards Security Service Edge (SSE), reflecting the evolving landscape of cybersecurity and remote work practices. The data collected provides a snapshot of industry perspectives and practices in this domain.

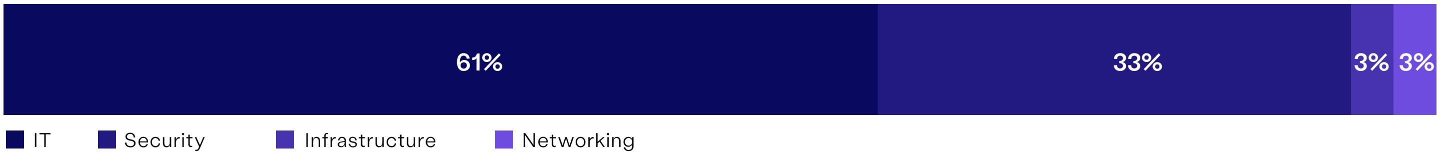
Industry



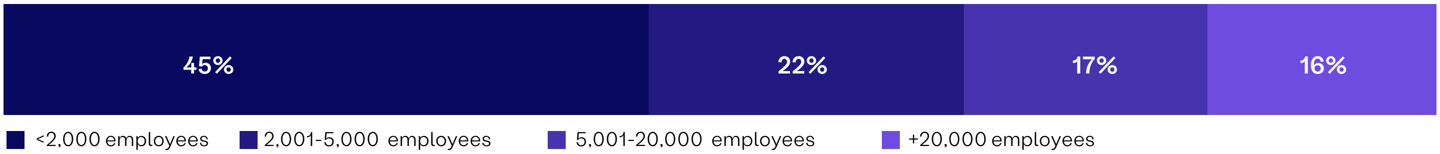
Career Level



Job Function



Company Size



Reuse of content

We encourage the reuse of data, charts, and text published in this report under the terms of this Creative Commons Attribution 4.0 International License. You're free to share and make commercial use of this work as long as you attribute the report as stipulated in the terms of the license. For example: "2024 Security Service Edge Adoption Report by Cybersecurity Insiders."

HPE aruba networking

HPE Aruba Networking helps businesses capture, secure, and transport data to users and applications from edge to cloud. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open, and intelligent technology solutions as a service. With offerings spanning Cloud Services, Compute, High-Performance Computing & AI, Intelligent Edge, Software, Storage, and now Security, HPE provides a consistent experience across all clouds and edges, helping customers develop new business models, engage in new ways, and increase operational performance.

Learn how HPE can help you modernize your security with our holistic HPE Aruba Networking SSE offering.

LEARN MORE

Ready to experience the power of an SSE platform?
Take a free 24-hour test drive today!

SSE TEST DRIVE

Cybersecurity

INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com