Cybersecurity INSIDERS

2023

Security Service Edge (SSE) Adoption Report

axis

Securing the modern business

The rapid emergence of hybrid work has placed pressure on CISOs and security architects to transform the way they secure access to their critical business resources. Security teams are being asked to ensure the mix of employees, partners, suppliers, and customers can safely access the wide variety of internal business apps, the Internet, and SaaS apps. However, all these moving parts heighten the risk of cyberattackers exploiting this new work environment.

To solve the challenge of securing hybrid work, CISOs and security architects are forgoing traditional access solutions in favor of Security Service Edge (SSE) services to deliver secure, unified access for the modern business. **Security Service Edge (SSE)** platforms simplify enterprise access by consolidating ZTNA, SWG, CASB, and DEM technologies and provide secure connectivity for any user to any application, from any location.

Based on a comprehensive survey of 355 cybersecurity professionals, the **2023 Security Service Edge (SSE) Adoption Report** delivers insight on the shift away from legacy access solutions and the rapidly growing SSE market in light of the modern workplace.

Key findings include:

- **67%** of organizations plan to start their SASE strategy with a Security Service Edge (SSE) platform rather than WAN Edge Services.
- **65%** of businesses want to adopt a Security Service Edge (SSE) platform within the next 24 months.
- **47%** plan to begin SSE implementation with Zero Trust Network Access (ZTNA) deployment.
- **48%** say their primary SSE use case is securing access for their remote and hybrid employees.

We would like to thank Axis Security for supporting this important research.

We hope you enjoy this report.

Thank you,

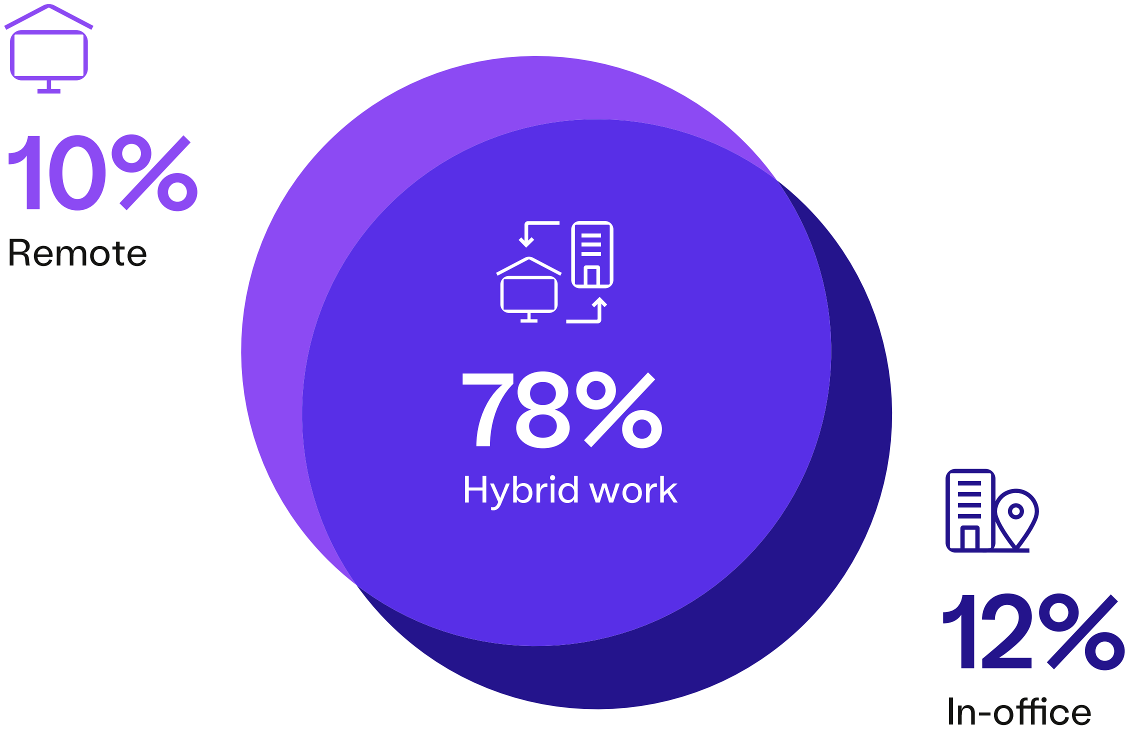
Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

The new workplace

It's no surprise that hybrid work models have grown dramatically over the last few years to better balance employee preferences and work requirements. Today, 8 of 10 organizations support a mix of employees working remote and in-office (78%). Additionally, with only a 2% gap, organizations that now operate fully remote have nearly caught up to the conventional in-office work model.

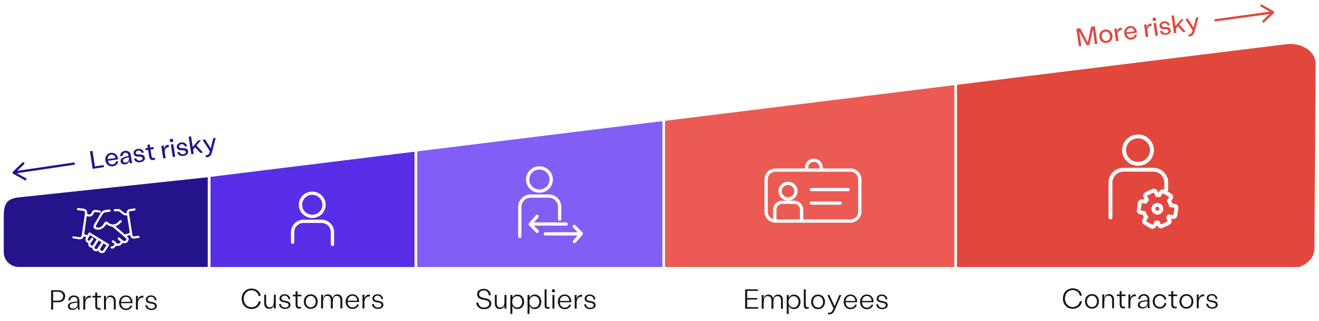
How would you describe your employee workforce today?



Risks & challenges of the modern workforce

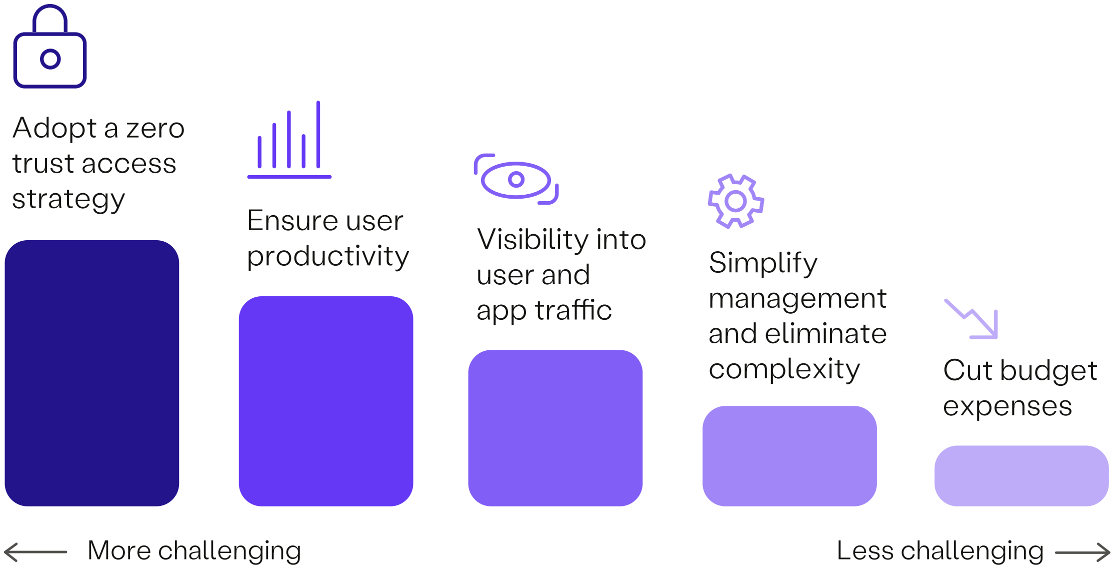
With hybrid work becoming the new norm, new risks and challenges arise. When addressing the top areas of user risk, it was found that contractors pose the greatest threat, mainly due to external users requiring access to internal business resources. It was also found that internal employees present the second highest risk, as the increasingly distributed workforce creates various points of entry for cybercriminals.

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



These findings also validate the main security challenges faced today. According to the study, implementing a zero trust strategy is the top challenge for cybersecurity experts, closely followed by ensuring user productivity and having adequate visibility into user and application traffic.

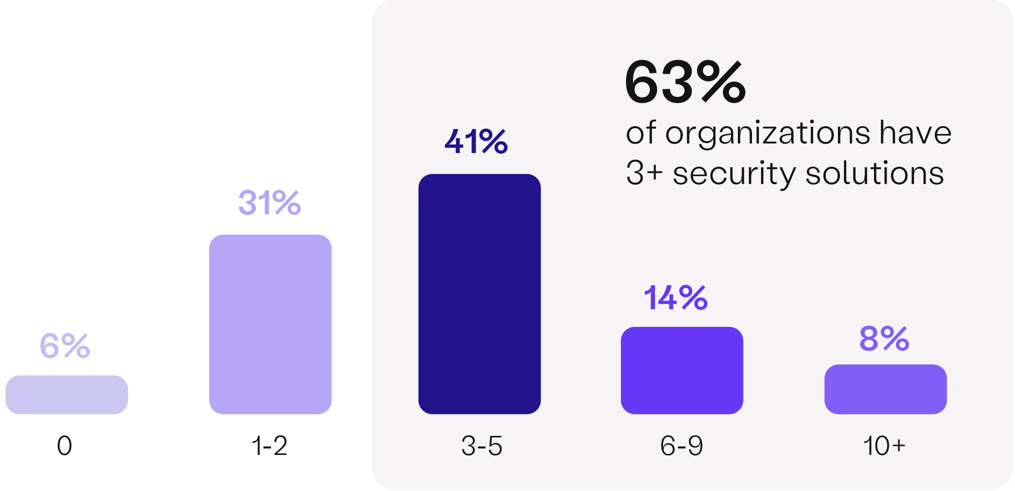
What is the biggest challenge in securing the modern workplace?



Legacy access solutions

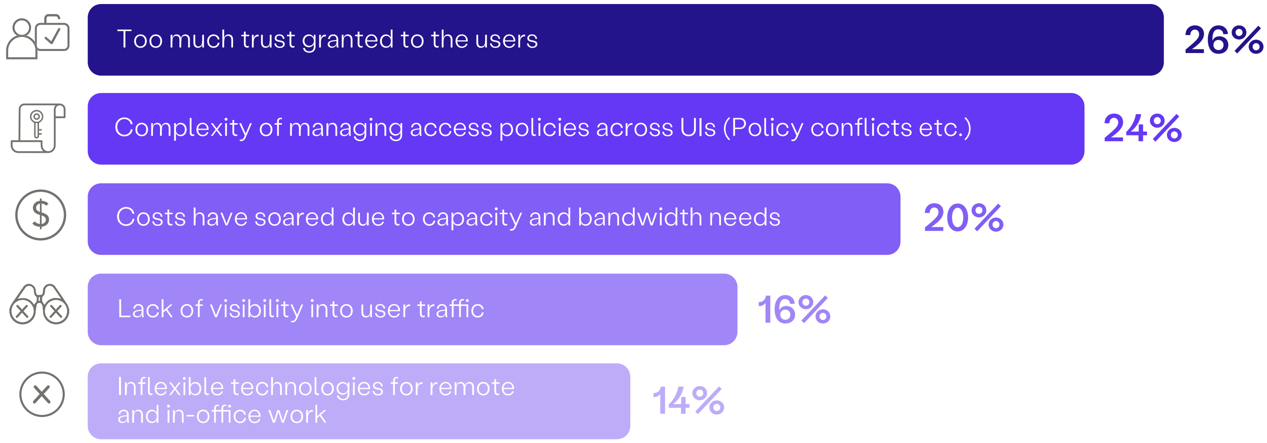
The size and complexity of an organization typically drives the complexity of its access infrastructure and management proportionally. 63% of companies require 3+ security solutions to protect access to business resources, with the largest percentage of companies sitting between 3-5 solutions. Even so, nearly ¼ of surveyed organizations have 5+ solutions deployed. This proliferation of security solutions has driven many organizations to seek solution consolidation for the sake of easier manageability.

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



With the majority of businesses boasting over 3 security solutions, it's no surprise that 24% of cybersecurity professionals claim management complexity across various UIs as their second greatest challenge with current access solutions. At the top of the list is the challenge of excessive user privilege and granting inherent trust to users (26%).

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

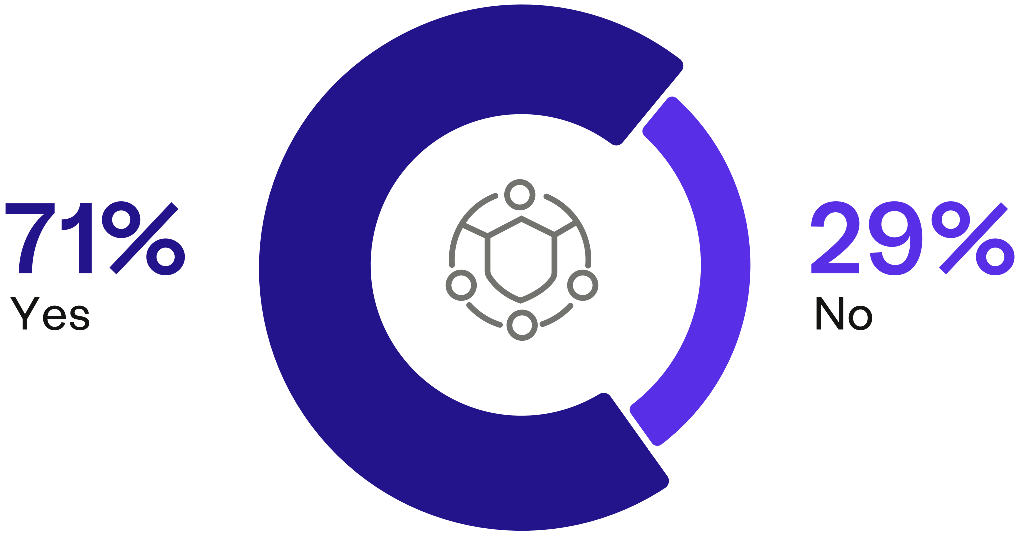


Familiarity with Security Service Edge (SSE)

While the concept of Security Service Edge (SSE) was only introduced by Gartner in early 2021, the survey shows that 71% of cybersecurity experts are aware with the idea of SSE.

Security Service Edge (SSE) solutions provide a modern alternative to traditional secure access technologies by unifying security services such as Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and often times Digital Experience Monitoring (DEM) into a single offering to enable secure access to the web, cloud services, and private applications.

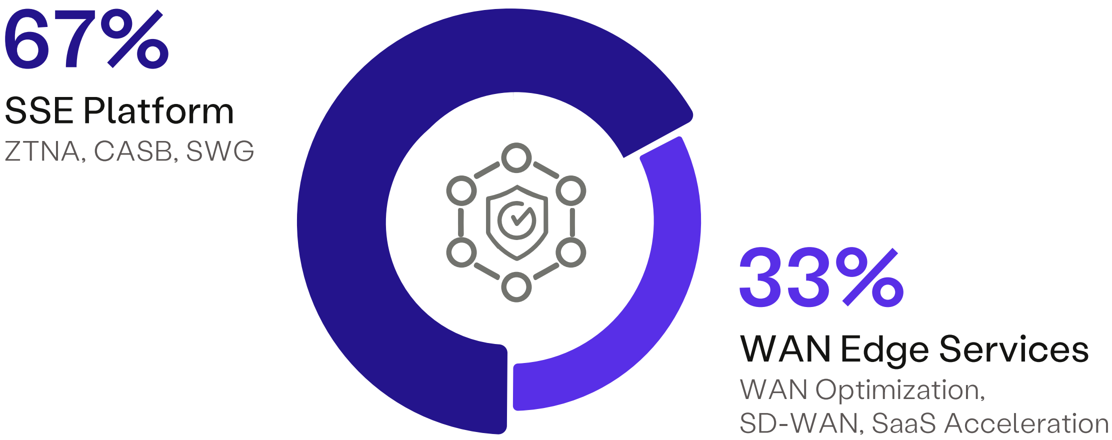
Are you familiar with the term Security Service Edge (SSE)?



SSE as a strategic initiative

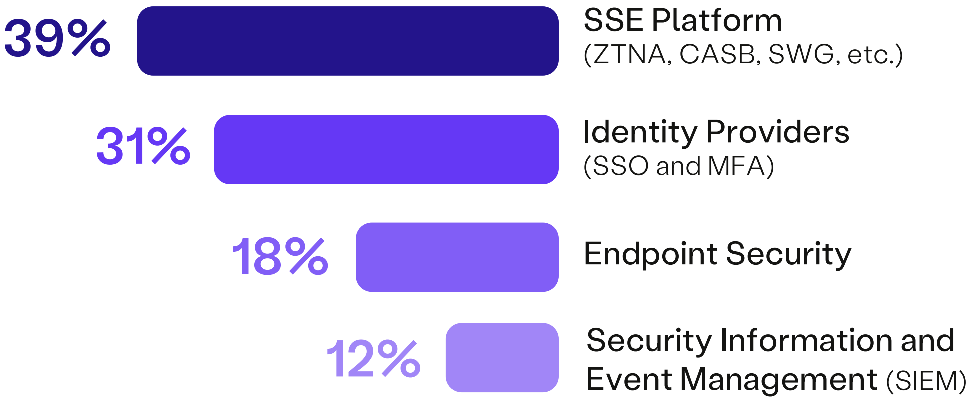
Although SSE has only recently emerged, it has already become a staple in many organizations' strategic planning. When asked about Security Access Service Edge (SASE) implementation and where they plan to begin, 67% of organizations plan to deploy a SSE platform (including ZTNA, CASB, and SWG) before considering WAN Edge Services (33%). This shows that within the SASE framework, SSE is seen as holding more value and significance than its WAN Edge Services counterpart.

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 were ranked first at 39%. SSE even ranks higher than identity solutions like SSO and MFA (31%), endpoint security (18%), and SIEM solutions (12%). 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.

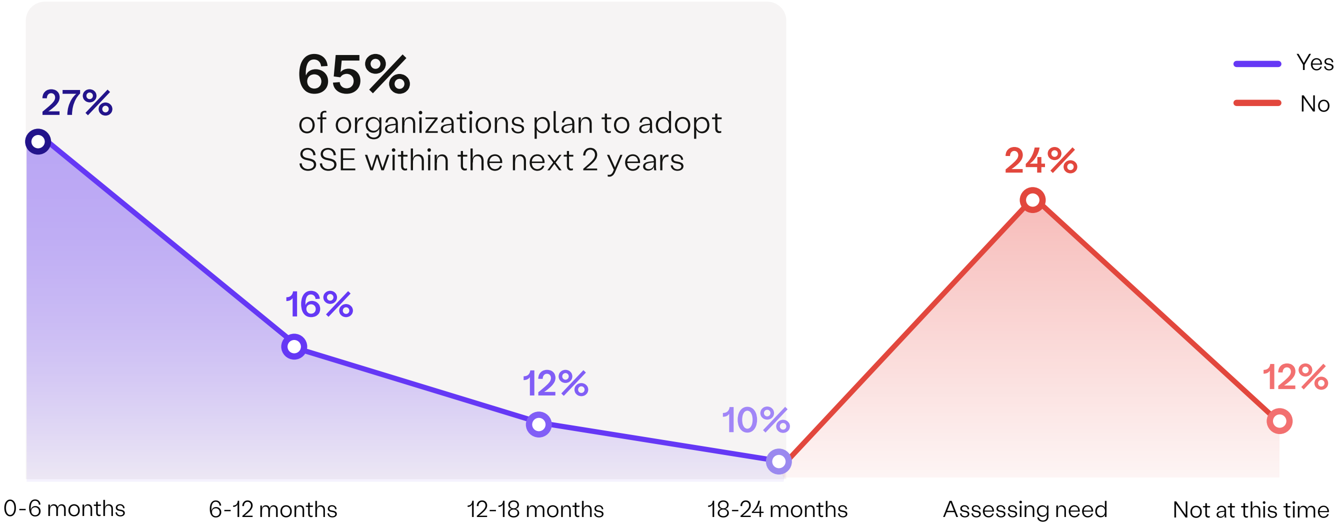
Which of the below technologies do you see as the most critical for a zero trust strategy?



Adoption of SSE

How quickly are organizations planning to adopt strategic SSE platforms? The survey shows that SSE adoption is an overwhelming priority for businesses, with 65% of cybersecurity experts prioritizing SSE implementation within the next 2 years. In fact, 43% of these organizations plan to adopt SSE by the end of 2023.

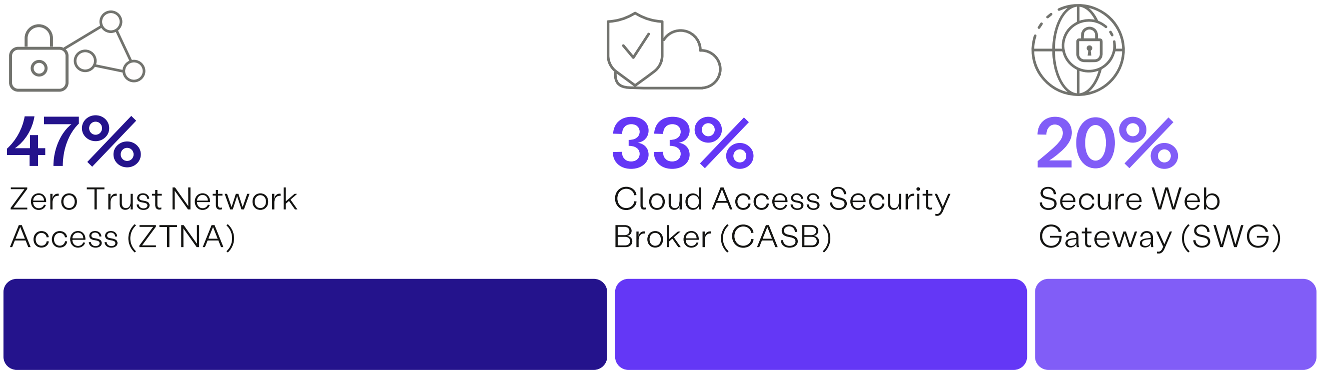
Do you plan to adopt a Security Service Edge (SSE) platform within the next 24 months?



65% of organizations plan to adopt SSE within the next 2 years

As the adoption of SSE technologies continues to grow rapidly, the report found that 47% of organizations plan to start their implementation with **Zero Trust Network Access (ZTNA)** technology. This could be largely due to the increase of remote and hybrid work and prioritizing areas of highest risk. Businesses next plan to tackle Cloud Access Security Broker (CASB) deployment (33%), followed by Secure Web Gateway (SWG) (20%).

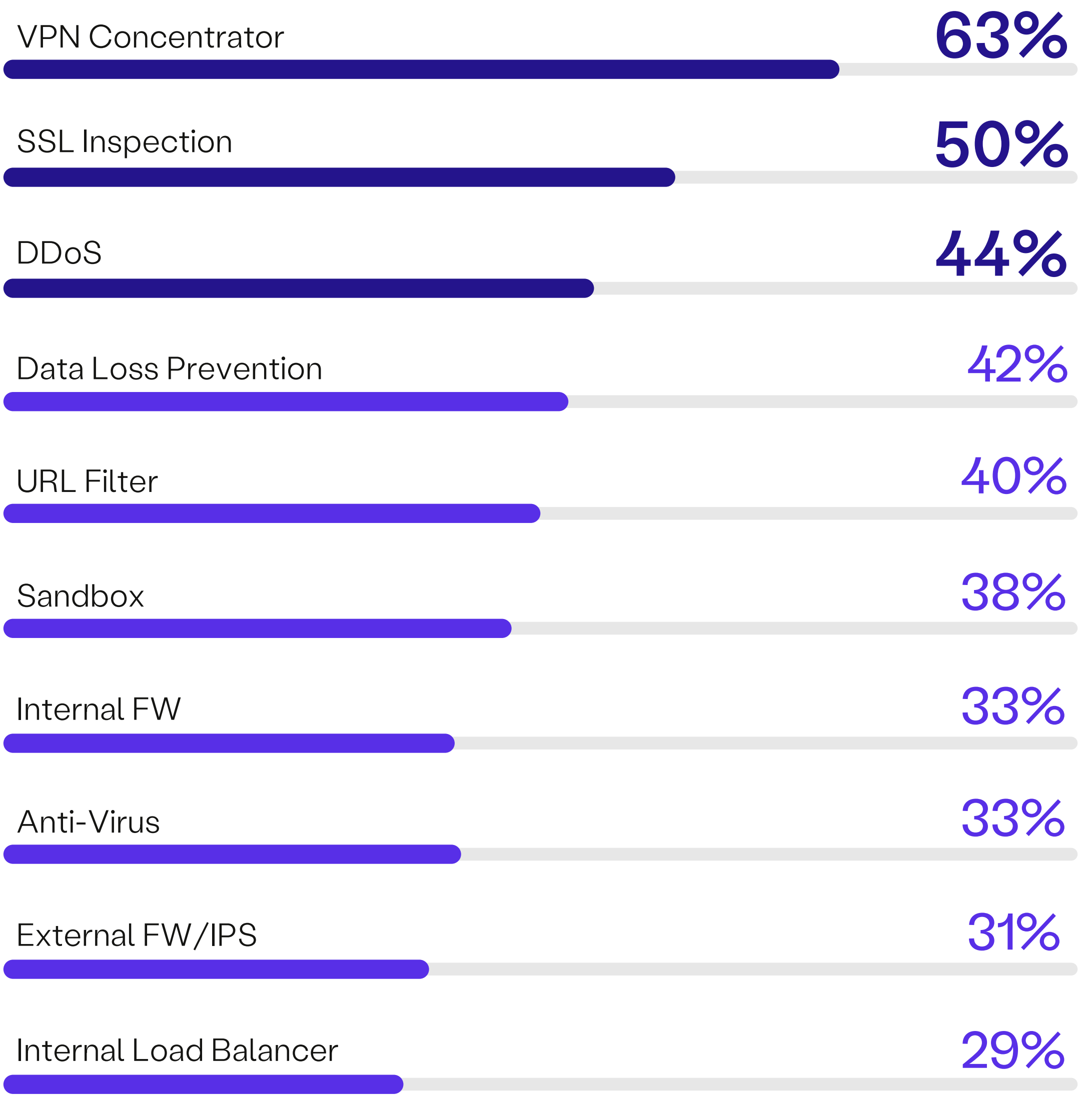
Out of the three core SSE technologies, which do you plan to begin with first?



Appliance reduction with SSE

SSE offers organizations with an opportunity to remove or reduce the need for a variety of security appliances. With the majority of organizations beginning their SSE journey with ZTNA, it's no surprise that 63% of cybersecurity experts are looking to reduce and even eliminate the use of VPN. Further, organizations would like to see an SSE platform reduce the need for SSL inspection (50%) and DDoS protection (44%), both elements that are often baked into an overarching SSE service.

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

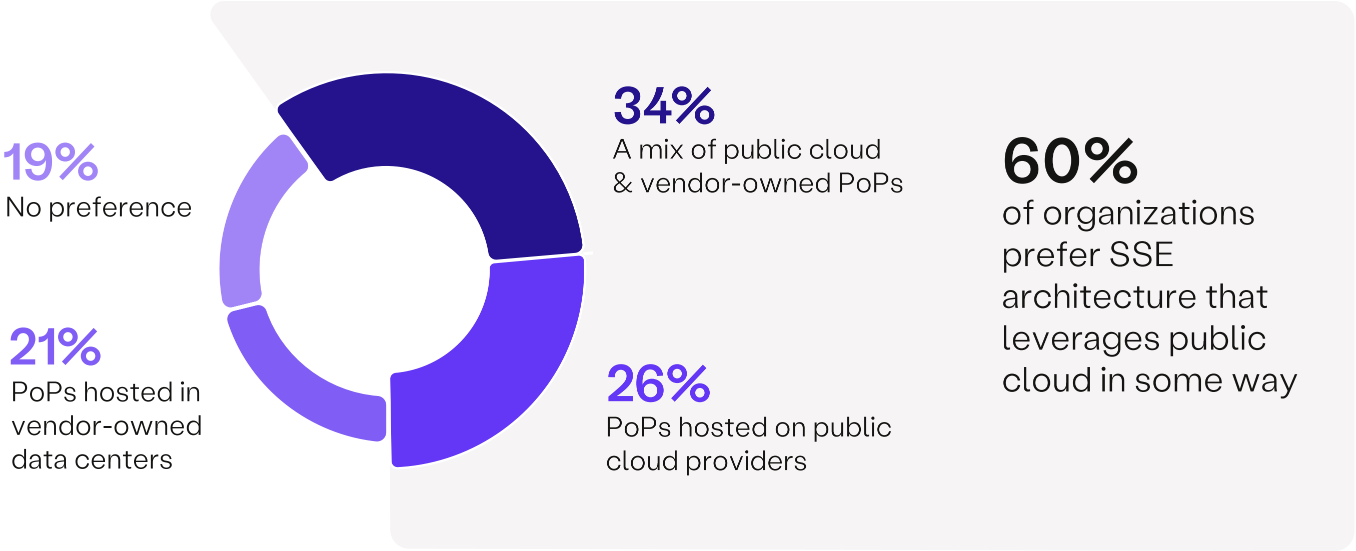


SSE architecture

SSE platforms often fall into two architecture categories: SSE PoPs hosted in Public Cloud Providers or SSE PoPs hosted in Vendor-Owned Data Centers. When asked what type of architecture was preferred, cybersecurity professionals made it clear that they ultimately desire infrastructure that is both flexible and reliable. 34% determined they prefer a mixture of these SSE architectures, both leveraging the power of public cloud and privately owned data centers.

Further, 26% prefer architecture built on the backbone of the major cloud giants (AWS, Azure, and GCP). Overall, we see 60% of organizations prefer SSE architecture that has some reliance on public cloud providers for greater assurance of reliability and performance redundancy.

▶ **What kind of SSE architecture would you prefer?**

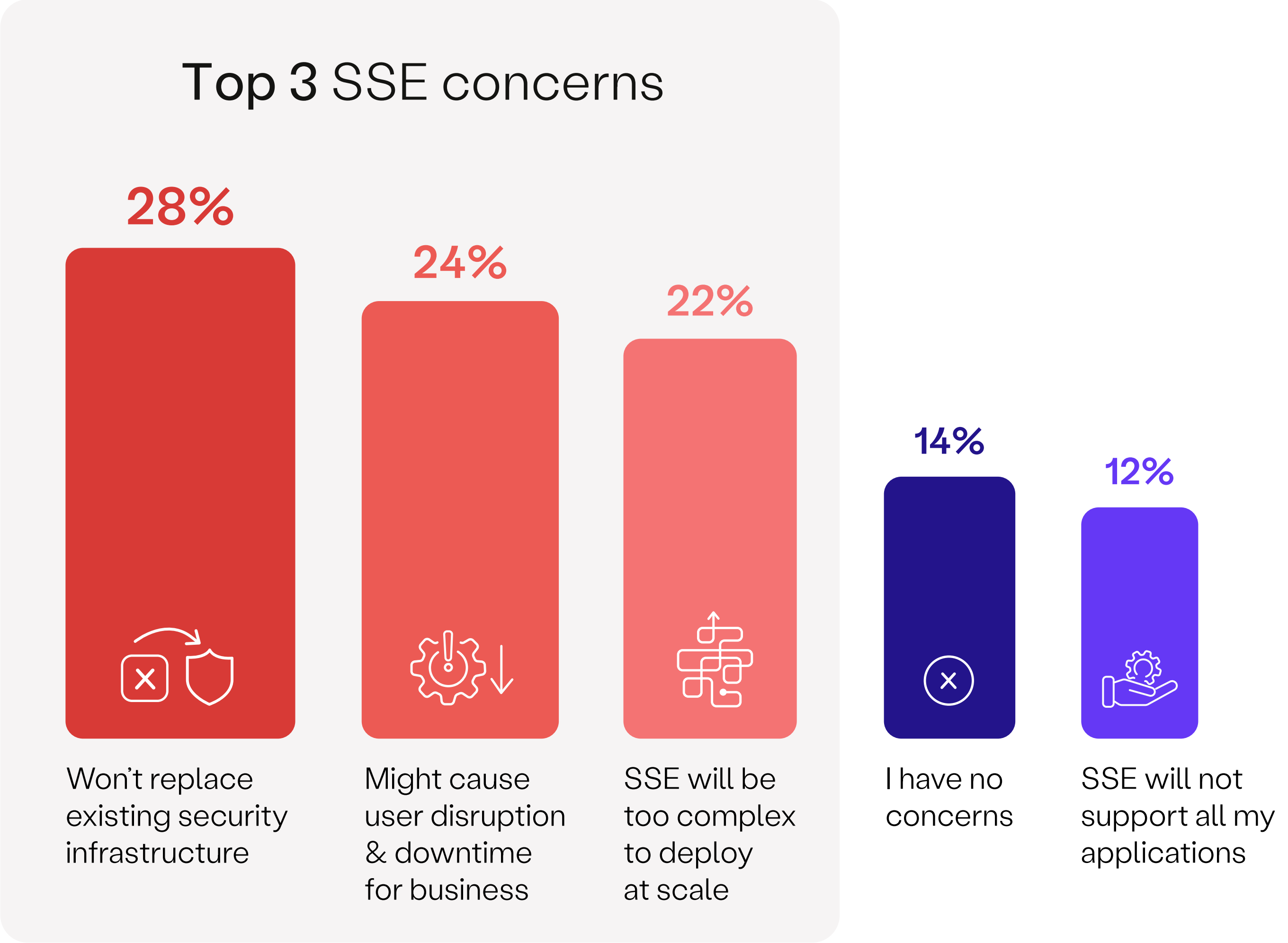


60%
of organizations prefer SSE architecture that leverages public cloud in some way

Top SSE concerns

SSE adoption is not without pitfalls. Cybersecurity professionals in this survey are most concerned that an SSE solution will not be able to replace their existing access security infrastructure (28%). This is why it's important to evaluate SSE platforms that fully eliminate legacy technologies, one example being VPN. Other concerns include the fear that an SSE service will cause user disruptions and downtime for the business (24%) and that it might be too complex to deploy at scale (22%).

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

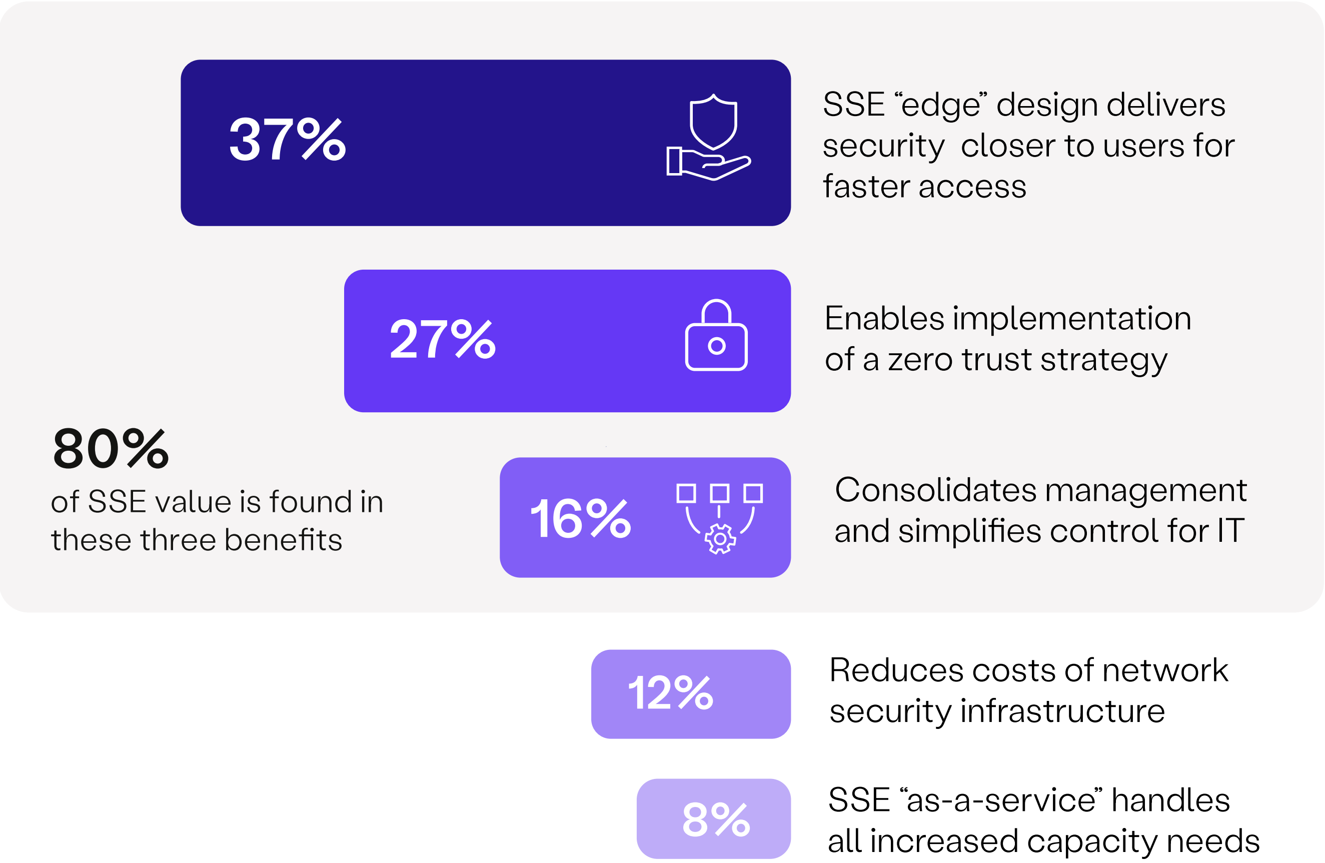


Top SSE benefits

When asked what the most valuable benefit of a SSE platform was, 37% of cybersecurity experts agreed that bringing security and streamlined access to the user with edge locations provides the greatest advantage. Traditionally, organizations may have only a handful of data center locations for users to backhaul to; however, SSE platforms can provide 100s of edge locations, providing fast front door access to users from around the globe.

The second highest value of SSE is its ability to enable a zero trust strategy for the business (27%), followed by the fact that SSE consolidates management and makes it easy for IT to control their environment (16%).

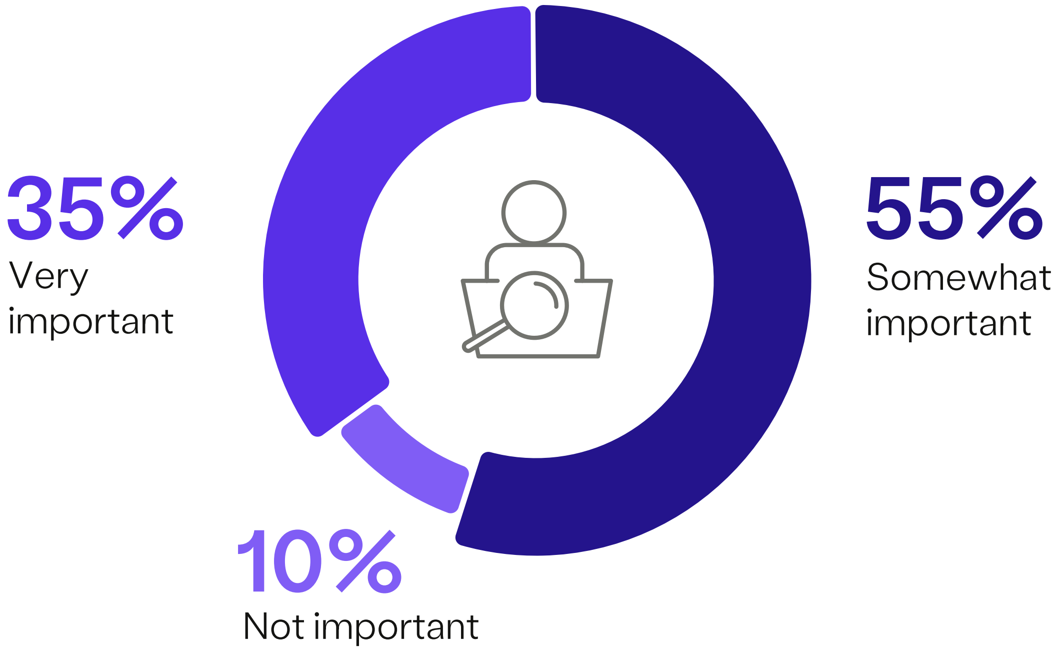
What do you think is the most valuable benefit of SSE?



The importance of experience

The increasingly mobile workforce has led to the increased importance of ensuring access performance doesn't have a negative impact on business productivity. As the report stated earlier, ensuring user productivity and increasing visibility are the second and third largest challenges for teams securing the modern workplace. This is a large contributor to why 90% of businesses believe that a Digital Experience Monitoring (DEM) offering is at least somewhat important to a holistic SSE platform. Thirty-five percent of these cybersecurity professionals believe that the visibility and remediation capabilities of DEM are critical to any SSE offering.

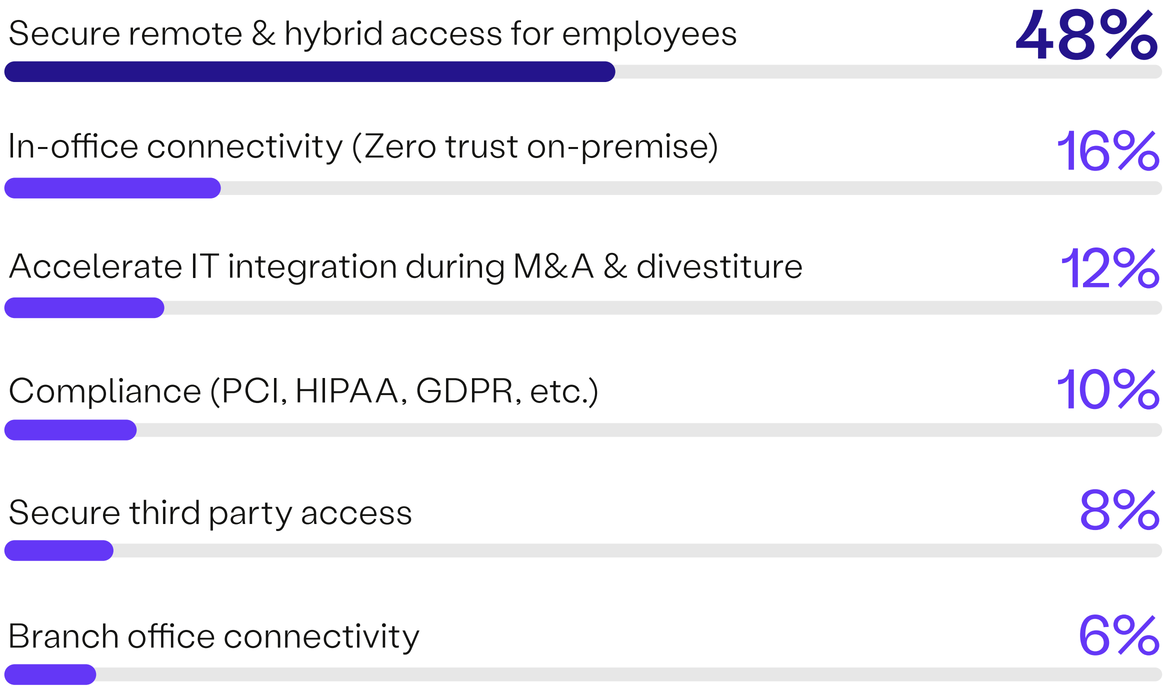
How important is it that an SSE vendor has a Digital Experience Monitoring (DEM) offering?



Getting started with SSE

In the beginning of this survey, 88% of total organizations stated their workforce was primarily hybrid or fully-remote. This shift in the nature of work has led many security teams to rethink their current access strategy, leading nearly half of these organizations to start their SSE journey by first securing remote and hybrid access for employees (48%). Organizations are sensing the urgency in ensuring not just that the workforce has secure connectivity, but that connectivity is adjusted to match the evolving needs of the business.

Which SSE use case do you plan to start with?



The **2023 SSE Adoption report** has illustrated some of the major shifts organizations are seeing today. The shift to a hybrid workforce, the shift to greater zero trust implementation, the shift to consolidating security solutions, the shift away from legacy access solutions, and ultimately the shift towards Security Service Edge (SSE) adoption.

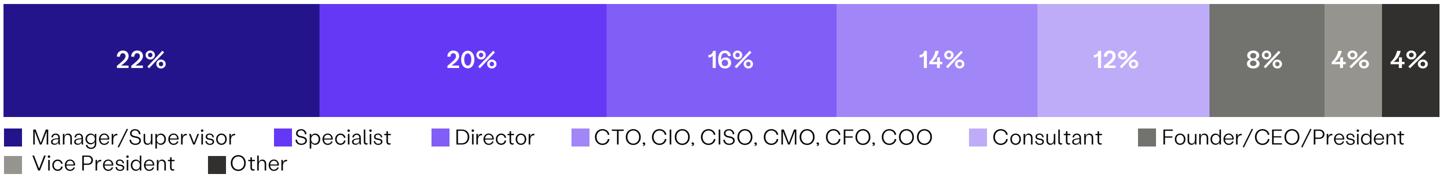
If you are considering a Security Service Edge (SSE) platform or want to learn more, this **interactive value calculator tool** will help your team evaluate your personalized cost-savings with SSE Platform.

SSE Value Calculator

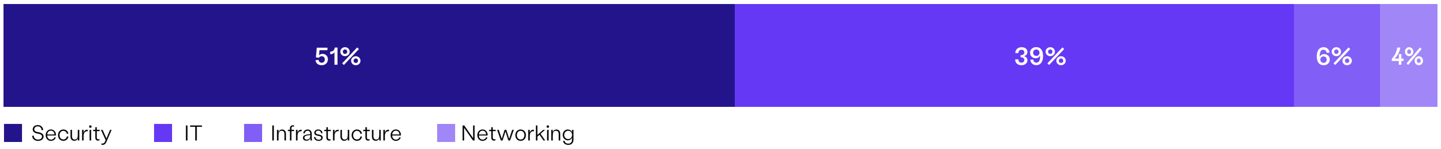
Methodology & Demographics

The 2023 Security Service Edge Report is based on the results of a comprehensive online global survey of 355 cybersecurity professionals, conducted in December 2022, to gain deep insight into the latest trends, key challenges, and solutions. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

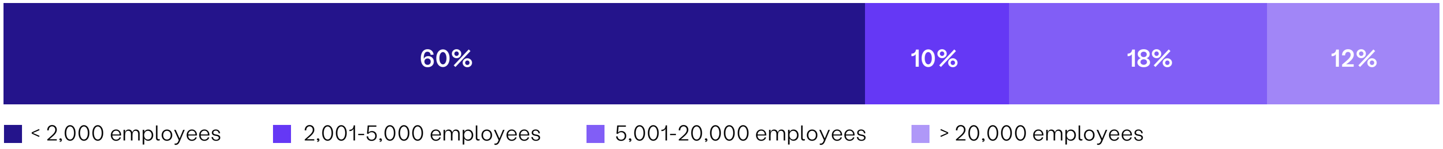
Career level



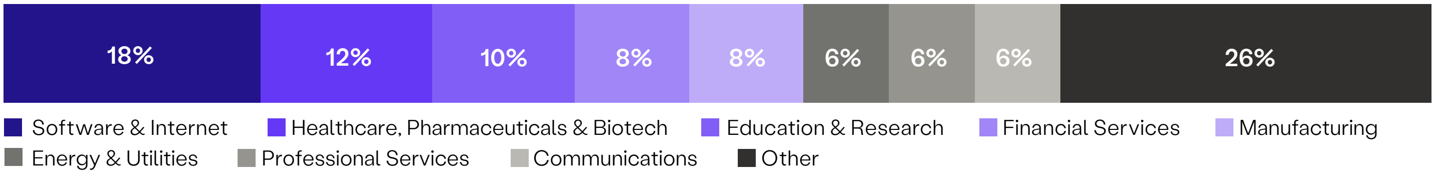
Job function



Company size



Industry



axis

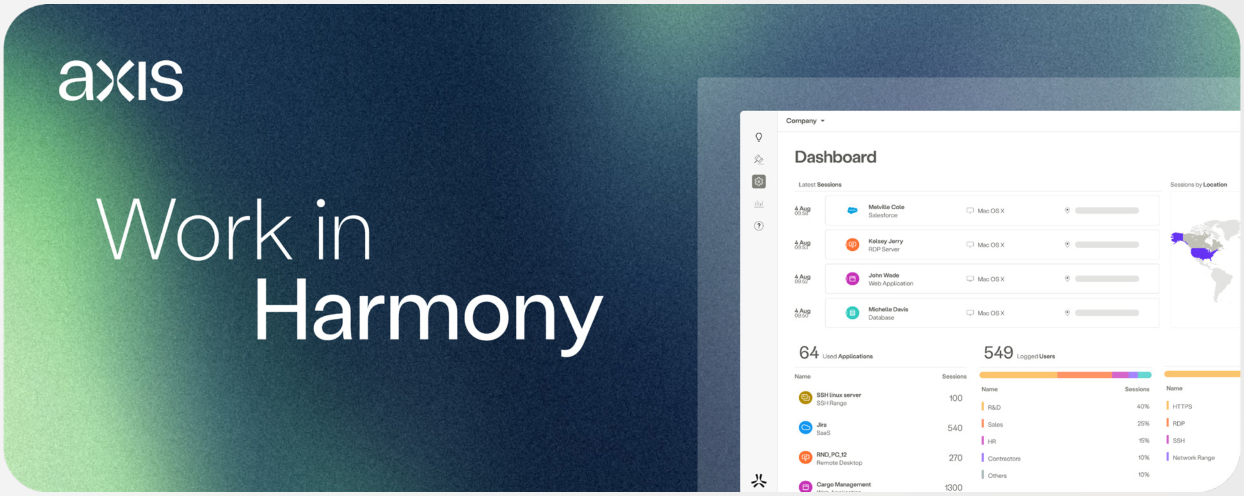
Axis' vision is to bring harmony to workplace connectivity and that the sooner IT adopts zero trust, the sooner we can witness a world where the exchange of information is always fast, seamless, and secure.

With 350 Axis cloud service edges across the world, Axis helps IT leaders enable their employees, partners, and customers to securely access business data without the pitfalls of network-centric solutions or application limitations that every other zero trust service faces.

Through its world-class research and development and founding team which hails from Israel's acclaimed Unit 8200, Axis aims to accelerate the world's transition to a modern workplace where hybrid work is made simple, digital experience becomes a competitive advantage and business data remains protected from cyber threats even as it moves to the cloud.

For more information, visit **www.axissecurity.com**.

Follow us on Twitter and on Linkedin



4 Aug 09:58	Melville Cole Salesforce	Mac OS X	
4 Aug 09:53	Kelsey Jerry RDP Server	Mac OS X	
4 Aug 09:52	John Wade Web Application	Mac OS X	
4 Aug 09:50	Michelle Davis Database	Mac OS X	

64 Used Applications

Name	Sessions
SSH linux server SSH Range	100
Jira SaaS	540
RND_PC_12 Remote Desktop	270
Cargo Management	1300

549 Logged Users

Name	Sessions
R&D	40%
Sales	25%
HR	15%
Contractors	10%
Others	10%

Name
HTTPS
RDP
SSH
Network Range

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit
www.cybersecurity-insiders.com