Skyhigh Security

REPORT

The Data Dilemma: Cloud Adoption and Risk Report

TABLE OF CONTENTS

Introduction

Welcome to the *Skyhigh Security Cloud Adoption and Risk Report.* Although it's our first report as Skyhigh Security, we've produced it on a (mostly) annual basis for years. As Skyhigh Security, our goal has remained the same: to identify cloud security trends that affect businesses of all sizes and across many geographies and industries. We offer this holistic view of cloud transformation, and key learnings, to help you evolve your own security practice.

And, when we say "mostly" a yearly report, by that we mean the last survey data was from 2019. In 2019, we were already seeing rapid cloud adoption and were shining a light on visible gaps in how to control and secure data. 2020 brought with it a shift the world couldn't have imagined: the global pandemic. This catapulted organizations headlong into digital transformation, with the cloud at the center of it all. They turned on a dime to adapt their technologies, infrastructure, and software to fit modern hybrid working requirements, including the expansion of cloud applications, the growing remote workforce, a myriad of devices and users, and the increasing weight of regulatory and compliance requirements. It's been a learning curve, to say the least.

This year, we're focused on data, because the data dilemma is still real. At its heart, security is a data protection problem, and it's difficult to protect data that's everywhere—throughout the fabric of devices, the web, cloud applications, infrastructure, and among users. To put it simply, data isn't just on endpoints anymore. It's outside the corporate network, and this creates security gaps. Organizations are constantly faced with the challenge of controlling how data is used, no matter the source.

And, as if this weren't enough to deal with, the increasing use of cloud applications, Shadow IT, and various economic factors are adding to the complexity of the problem. Cloud services have replaced many applications formerly run on-premises, which means more sensitive data is migrating to the cloud. And, with more devices accessing the cloud, the traditional solutions everyone had relied on for so long have outlived their usefulness.

As any security professional can tell you, the job of defending data is not getting any easier. To provide remote workforces with a secure and productive user experience, organizations need to understand where their data is and how it's shared. Adopting a Zero Trust architecture is a critical step in that direction. We hope this report will help you get a more complete picture of that and will help you better shape your cloud data protection strategy.

The Skyhigh Security Team

Key Findings

Since our 2019 study, we've seen increased adoption of cloud services. At the same time, organizations are having to tackle new security challenges

75% have experienced a cybersecurity breach, threat and/or theft of data, indicating that they need stronger security controls to stop breaches and attacks from impacting them.

Organizations store about 61% of sensitive data in the public cloud, on average.

While **75%** of organizations admit Shadow IT impairs their ability to keep data secure...

...only **42%** experiencing Shadow IT use a Cloud Access Security Broker (CASB) to monitor unauthorized cloud usage.

Securing data in the cloud is a **responsibility shared** by an **average of two roles**. This requires **strong communication** and **delineation of duties** for each party and their respective department.

Issues become even more evident when we look at the private cloud, with the percentage of organizations experiencing challenges jumping from:

82% in 2019 to **97%** in 2022...

...a worrisome 15% points increase.

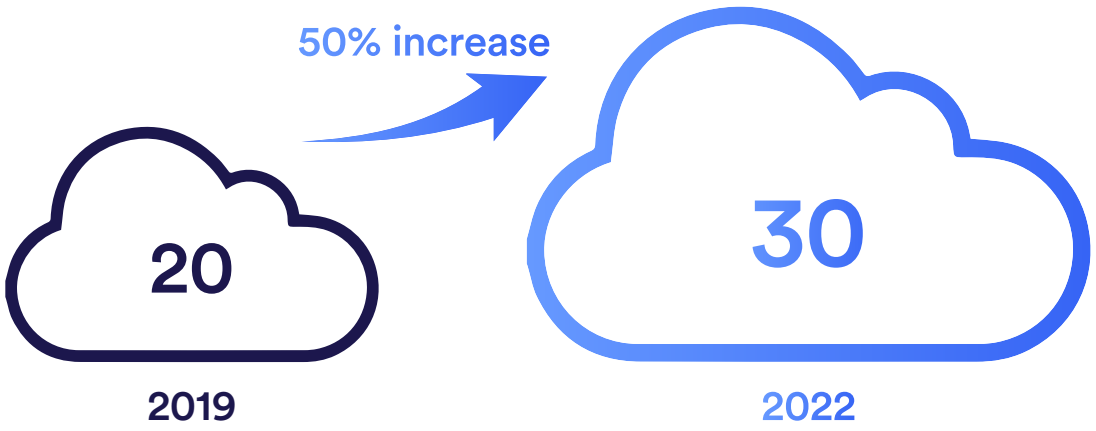
Section 1: The changing cloud landscape

Over the last few years, there's been a big jump in public cloud usage. In 2019, there was an average of 20 public cloud services in use among our surveyed organizations. This has climbed to 30 in 2022, an average increase of 50%.

Largely as a result of the pandemic, which drove the need to work from home and access data from anywhere, more and more organizations are relying on the cloud.

An example of this is the use of Microsoft 365 applications. Microsoft Teams meetings, for example, more than doubled from 2020 to 2021 worldwide, probably due to the shift from on-site to hybrid working.[1] This also means more data is being shared: 41% of organizations report that they are using Microsoft 365 for email and/or file storage. The takeaway from a security perspective is that not only do organizations need to know where data is going in order to protect it, but also where it's going in order to keep it from being exfiltrated.

Average number of **public cloud services** in use



Average number of public cloud services (SaaS, PaaS) in use by organizations participating in the survey, split by survey year. Asked to respondents whose organization is currently using public cloud services [base numbers - 2019: 833, 2022: 1046]

1 *https://www.microsoft.com/insidetrack/blog/five-ways-microsoft-teams-has-transformed-microsoft/*

Section 2: Cloud security challenges

Despite all the advantages of the cloud, organizations continue to struggle with security. For those using Software-as-a-Service (SaaS), more are reporting advanced threats and attacks against their cloud application providers (28%) and an inability to prevent malicious insider theft or misuse of data (23%) than they were in 2019 (23% and 17% respectively). Lack of visibility into data and control over where it goes is also a growing problem, with 28% of organizations reporting lack of visibility into what data is in cloud applications (up from 22% in 2019).

Security in the private cloud is even more concerning. The percentage of organizations experiencing such challenges jumped 15% points, from 82% in 2019 to 97% in 2022. As with the public cloud, these problems result from inconsistent security controls and a lack of visibility. This suggests a need to consolidate security controls into a single holistic solution so that both operations and security teams can have broad visibility and control over the entire cloud-native environment.

Average number of organizations experiencing problems with private cloud

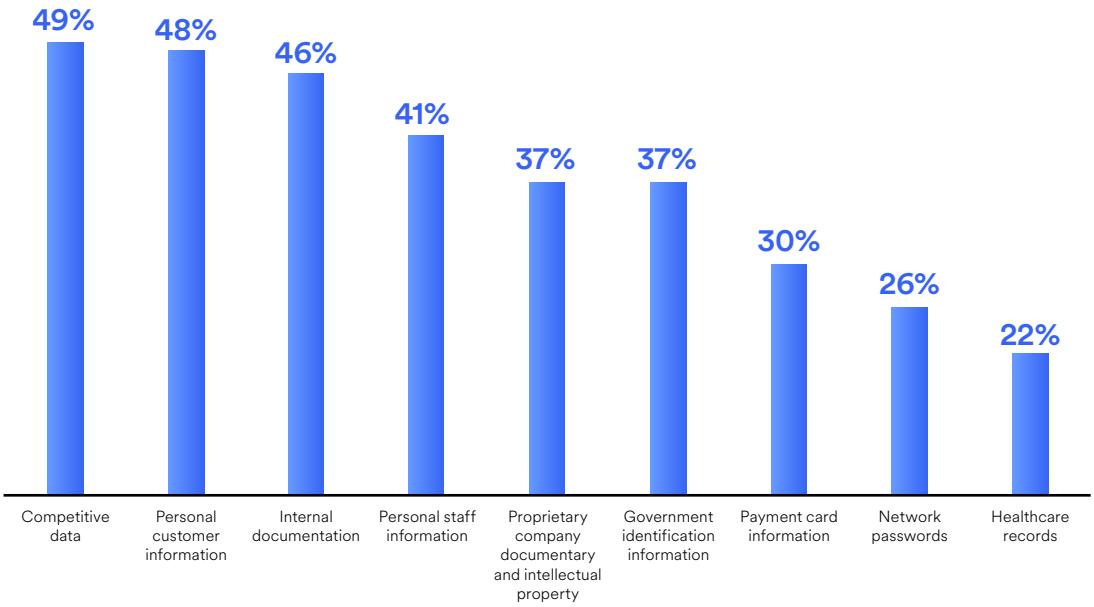
The percentage increase of organizations experiencing issues with private cloud from 2019 [279] to 2022 [528]

38% In addition, for 38% of organizations, remote/hybrid workers are experiencing latency or bandwidth issues with VPN. This puts additional strain on both user productivity and on IT to troubleshoot and improve uptime.

Section 3: Protecting data in the cloud is top of mind

To further complicate matters, there's been a 13% average increase in sensitive data in the public cloud, from 48% in 2019 to 61% in 2022. From the personal information of customers and staff to intellectual property and network passwords, theft of this data could potentially damage a company's reputation and its ability to function and lead to hefty regulatory and compliance fines for failure to secure the data. And, with security issues in the public cloud mounting, data thieves are undoubtedly eager to take advantage of the situation.

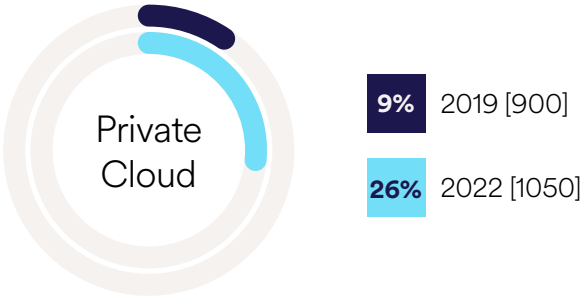
Types of sensitive data stored in public cloud services



What type of sensitive data is stored in your organization's public cloud services? [1046] asked to respondents whose organization uses public cloud services, not showing all answer options.

This could explain why 37% of organizations don't trust the public cloud to keep their sensitive data secure. There's a similar problem for private cloud providers, with 26% of organizations (compared to only 9% in 2019) not trusting that their sensitive data is protected on these platforms. We'll venture to say that the shift in remote work during the pandemic and beyond plays a part in this. Organizations have had to act fast and shift applications to the private cloud—and now they may be facing the consequences.

Distrust in private cloud keeping sensitive data secure



Showing the percentage that 'Completely distrust' or 'Slightly distrust' the private cloud for keeping their organization's data secure. Split by survey year.

There's another factor that adds to the apprehension with data security in the public cloud: an increasing number of organizations are allowing employees to use personal devices to access data in the public cloud. Six in ten organizations allow employees to download sensitive data to personal devices, and this adds another layer of risk.

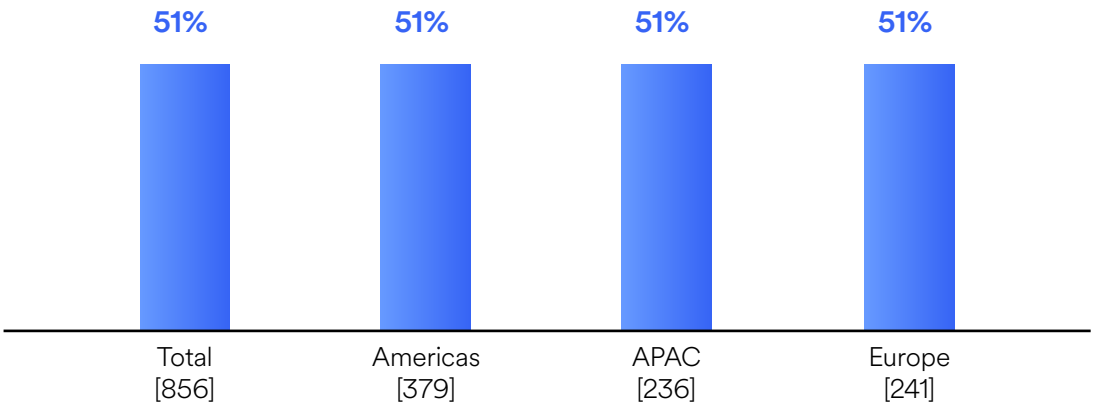
Interestingly, 93% of organizations say that their IT department has control over what sensitive data is uploaded to the cloud from personal devices, suggesting they do have the right controls in place, or worse, they are naïve to the fact they have security gaps that they are not aware of.

Section 4: Control over how data is used in all apps

Modernizing and optimizing data management and security in the cloud to align with business objectives is no small task. It's essential that teams work together to meet this common goal.

But our survey results show otherwise. Over half of SaaS services on average are commissioned without IT involvement. This trend is consistent across all regions. Why is this cause for concern? Business decision-makers often lack expertise in security, and those that don't involve IT may be putting their organizations at risk.

Average percentage of SaaS services in use that are commissioned by departments outside of IT and without direct involvement of the IT department

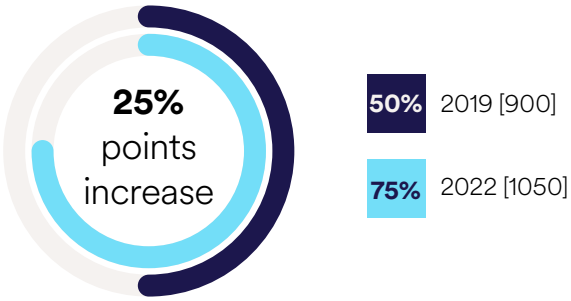


Showing the average percentage of SaaS services in use that are commissioned by departments outside of IT and without direct involvement of the IT department. Split by region.

To make things worse, respondents say they lack visibility to an average of 46% of SaaS services that are commissioned without IT. And it doesn't matter where in the world they're located because it's a consistent issue across all regions. Without this visibility, data loss prevention is near impossible, putting organizations at greater risk of unauthorized access.

But Shadow IT has been around for some time, and there is no evidence of it going away any time soon. There has been a remarkable 25% points increase in organizations that report Shadow IT is impairing their ability to keep data secure—up from 50% in 2019 to 75% in 2022. This drives home how organizations are increasingly aware of the negative impact Shadow IT is having on data security. It also indicates that high demand for public cloud usage is compromising existing data security systems.

Percentage that say shadow IT impairs their organization's ability to keep data secure



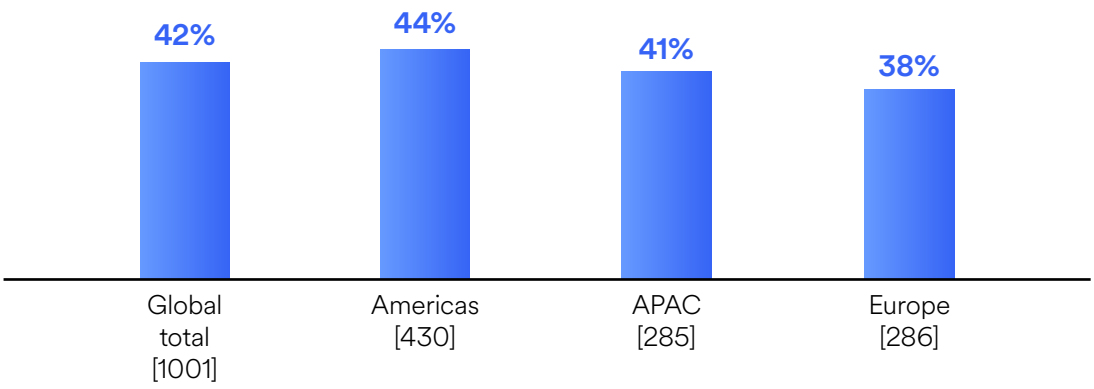
Percentage of organizations that say Shadow IT impairs their organization's ability to keep data secure. Split by survey year.

Section 5: IT departments take multiple approaches

Clearly, data loss is a serious and growing concern for organizations. It's vital to monitor non-IT approved cloud usage to keep data protected. There are several solutions to this: CASB solutions (used by 42% of organizations) and Secure Web Gateways (SWG) (used by 28% of organizations).

The main benefits of these solutions are that they add a much-needed layer of security and they reduce the burden on IT through automated processes.

CASB is used for non-IT approved cloud usage

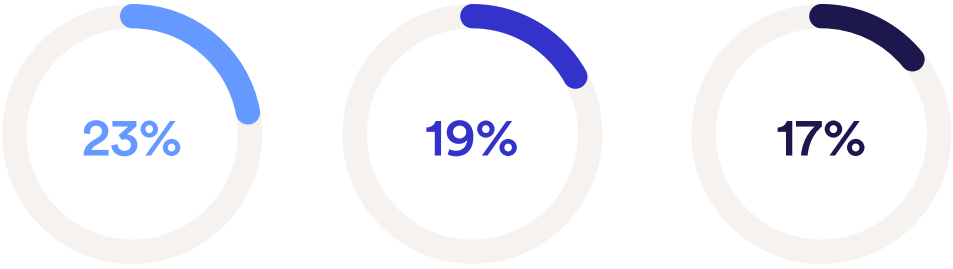


Showing the percentage that say a CASB is used by their IT department to monitor non-IT approved cloud usage, asked to respondents whose organization commissions SaaS and/or IaaS by departments outside of IT and without direct involvement of the IT department. Split by region.

Once Shadow IT is discovered, 23% of organizations use methods like Data Loss Prevention (DLP) and encryption to keep the cloud service secure, which aligns with the methods of protection organizations use to align to the Security Service Edge (SSE)[2] framework.

Some (17%) even block access to unauthorized cloud services, which can help reduce Shadow IT but can impact productivity if employees can't access the information they need to do their jobs. It's also troubling that there are 19% who continue to just monitor usage and take no action at all. Simply sitting, watching, and waiting isn't a recommended security solution.

Some of the ways IT departments secure cloud services once Shadow IT is discovered



Once Shadow IT is discovered in your organization, how does the IT department secure the cloud service? [1001] asked to respondents whose organization commissions SaaS and/or IaaS by departments outside of IT and without direct involvement of the IT department. Not showing all answer options

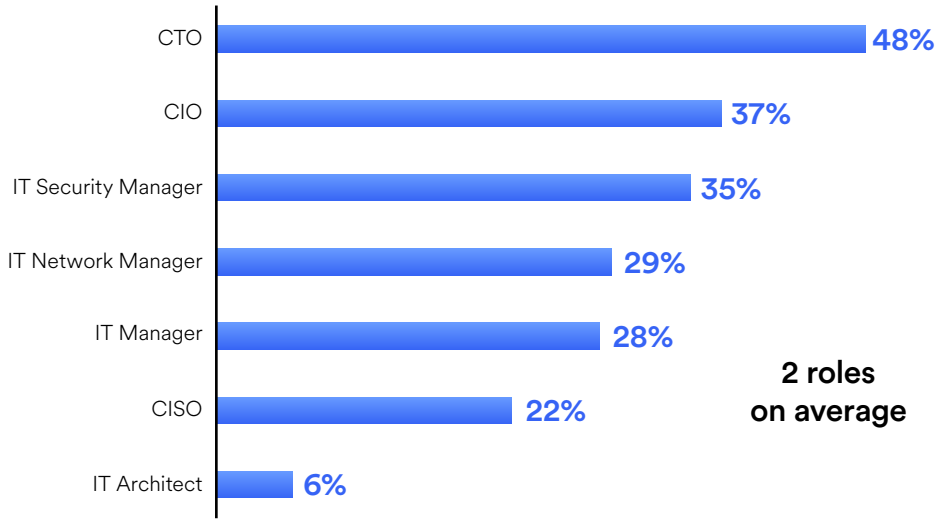
2 *https://www.gartner.com/en/information-technology/glossary/security-service-edge-sse*

Section 6: Looking to the future

Our results suggest that organizations believe securing data in the cloud is a shared responsibility spanning across two roles, on average. While this may be true on some level, many organizations may assume that someone else is taking care of the problem.

But this can be a dangerous and likely mistaken assumption when the security of sensitive data is at stake. Having clear ownership allows for better data governance and control, as it means everyone understands their role in securing data in the cloud.

Department(s) responsible for securing data in the cloud



Who is responsible for securing data in the cloud for your organization? [1050] not showing all answer options.

One of the great advantages of the cloud is scalability and capacity. Because of this, the volume, speed, and complexity of sensitive data being stored and shared in the cloud is soaring, driven, in part, by the increase in remote work. As we noted, organizations store about 61% of their sensitive data in the cloud, on average.

This means securing data is getting to be a complex challenge. From an administrator's perspective, 86% feel that cloud security could be simpler. What's behind this sentiment? It's likely organizations are struggling to get a high-level view of what's going on, especially if there are multiple security tools in use.

And, from a user experience perspective, 79% admit it could be simpler, which could be due to latency and bandwidth issues from an increase in VPN usage in the hybrid work environment. Automation and integrated applications that provide a simpler and more seamless experience for both users and administrators could be the answer to overcoming these issues and to keeping up with rising demand for cloud services.

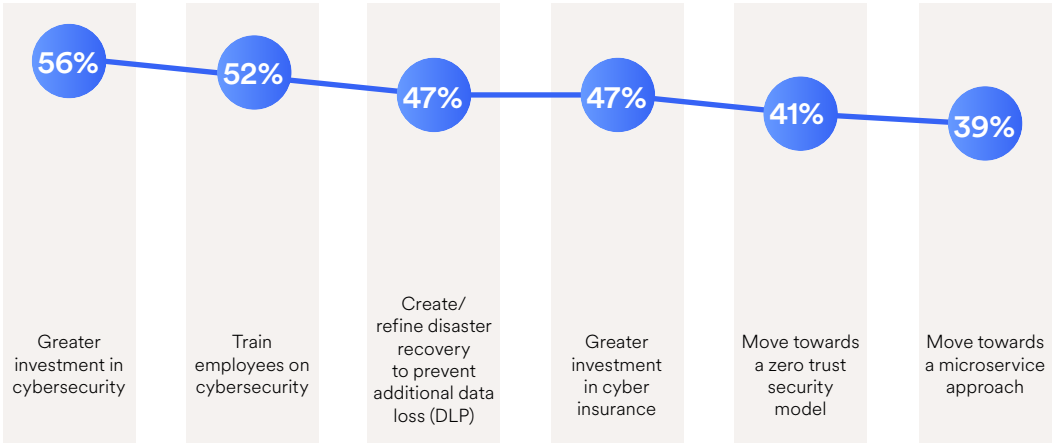
75% of organizations have experienced at least one of the following threats:

The percentage of organizations that have experienced a cybersecurity breach, cybersecurity threat, and theft of data at least once [717] asked to specific respondent types

Advanced, integrated solutions can help organizations manage cloud security more effectively and efficiently. They can also help minimize cybersecurity risks. We've seen that most organizations have suffered a cybersecurity breach (90%), cybersecurity threat (89%), and/or theft of data (80%) at least once. And, unfortunately for some, this has happened more than once. With so many of these issues tying into cloud security, these incidents will likely continue in the future, making it more important than ever to implement the right controls.

The good news? Organizations that have suffered from these attacks recognize that they need to do more to avoid them in the future. Over half of organizations plan to invest more in cybersecurity, which suggests their current investments are incapable of handling the complexities of keeping data secure. Many organizations have their sights set on developing disaster recovery to prevent data loss and adopting Zero Trust security.

Current/future plans as a result of experiencing a cybersecurity breach, cybersecurity threat and/or theft of data



As a result of experiencing a cybersecurity breach, cybersecurity threat, and/or theft of data, has your organization made/are they planning to make any of the following changes? [1006] asked to respondents whose organization has experienced a cybersecurity breach, cybersecurity threat and/or theft of data, not showing all answer options.

Key Takeaways

Whether your organization has a 100% remote, hybrid or onsite work environment, sharing data in the cloud will continue to grow exponentially. Cloud security needs to evolve at pace to handle the complexity of monitoring and controlling data flow and persistent challenges like Shadow IT. Security vendors recognize that security is a data protection issue and have responded by creating sophisticated point solutions to secure data wherever it resides.

But today, data is everywhere. This means that organizations have had to stitch these disparate technologies together to produce a comprehensive solution. We've seen that organizations are beginning to take proactive measures to secure data in the cloud by layering in additional security tools. For example, they are monitoring non-IT approved cloud usage by implementing CASB (42%) and web gateways (28%), and once Shadow IT is discovered, they're securing the cloud services through other measures like DLP and encryption (23%).

While this demonstrates a step in the right direction, this piecemeal, unintegrated approach results in security gaps, inconsistent application of controls and policies, and management complexities, putting a burden on security teams who are already stretched to capacity.

There is a better way: a top-down approach that focuses on the data itself rather than the traditional bottom-up process of starting from where it is stored. This radically simplifies data security by expanding Zero Trust principles to how the data is used rather than how it is accessed.

We recommend a SSE solution that secures data and applies consistent controls and policies across the web, cloud ((SaaS) and platform-as-a-service (PaaS)), and private apps—from anywhere, any application and any device. Consider a single-vendor solution that converges all security services, including SWG, CASB, Zero Trust Network Access, and Cloud-Native Application Protection, into a unified, centrally managed platform for greater efficiency and scalability.

When evaluating an SSE platform, make sure it includes the following capabilities:

- Endpoint and cloud data protection:
  To secure data going to cloud services from employees who collaborate remotely, a CASB provides the most comprehensive security. It gives visibility and control over data to and from cloud services, as well as threat prevention and control over Shadow IT.

- Advanced threat protection and unified data control:
  A cloud-based SWG adds access control, advanced malware prevention, Remote Browser Isolation (RBI), and DLP to any internet connection from a managed device.

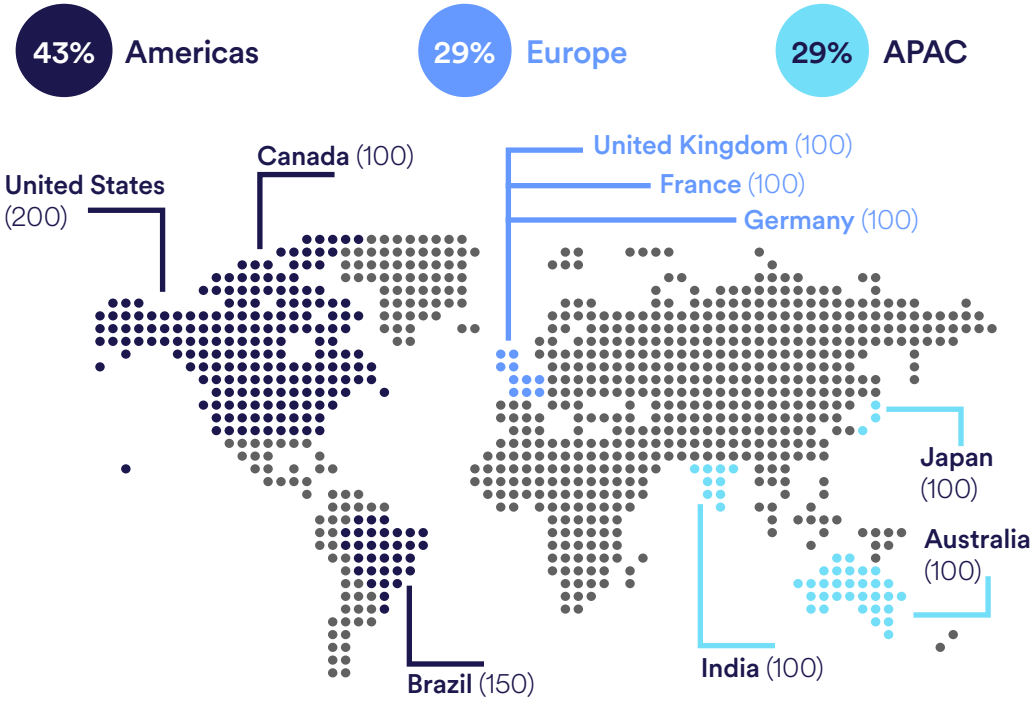
- Secure access to private internal applications and data:
  Move beyond a traditional VPN by implementing technology that continuously assesses the risks associated with connecting devices by providing fast, "least privileged" access to private applications through a hyperscale service edge.

- Simplified management and reporting:
  Look for a platform with a dashboard that provides a consolidated view across all cloud security services to ease administration, save time, and reduce complexity.

For more information on cloud security technology, please visit *www.skyhighsecurity.com*. Ready to begin? *Contact* Skyhigh Security for a personalized assessment of cloud usage in your organization

Methodology

Skyhigh Security commissioned independent market research agency Vanson Bourne to conduct this research, which is based on the results of 1,050 IT decision makers, IT specialists, and senior business decision makers. All organizations participating in the survey use cloud services.



Organization size

20% 500-999 employees
31% 1,000-2,999 employees
29% 3,000-4,999 employees
20% 5,000 or more employees

Industry

20% Retail, distribution and transport
16% IT, technology and telecoms
12% Financial services
12% Manufacturing and production
8% Energy, oil/gas and utilities
7% Public sector
6% Construction and property
5% Media, leisure and entertainment
2% Business and professional services
12% Other

This research makes comparisons to 2019, using data from the Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report. To make robust comparisons, the 2022 scope matches the 2019 scope as closely as possible. This includes the same organization size, sectors, job roles and initiatives. In 2019, there were 50 responses from Mexico and 50 responses from Singapore, but these countries were removed for the 2022 iteration of the survey. Therefore, these countries were removed from the 2019 dataset so that more robust comparisons could be made. This means the base number for 2019 is 900 (rather than 1,000 at the time of 2019 data delivery) and therefore percentages may not match those published in 2019.

About Skyhigh Security

Skyhigh Security protects organizations with cloud-native security solutions that are both data-aware and simple to use. Their market-leading SSE Portfolio goes beyond data access and focuses on data use, allowing organizations to collaborate from any device and from anywhere without sacrificing security.

For more information visit us at *www.skyhighsecurity.com*

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information visit us at *www.vansonbourne.com*

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
www.skyhighsecurity.com

March 2023