IFP Insights For Professionals

The State of:

Cloud Security

Analyst Report

IFP RESEARCH

Contents

1: **Introduction**

2: **Business operations in the cloud**

3: **Security concerns and threats in the cloud**

4: **Cloud security vendors**

The State of
Cloud Security

Introduction

1

Introduction

IT security has moved way beyond the traditional trio of firewall, antivirus and intrusion detection. The arrival of the cloud, while delivering massive benefits of cost, scale and business flexibility, creates new risks for business and IT leaders. Ransomware, scams, phishing attacks and cloud vulnerabilities through the multiple services a business can use all create risk.

To create viable defenses against the threat, CIOs and CISOs need to understand exactly what the risks are. They must identify what the differences are in native protection from every cloud provider they use, and build a strategy that defends every endpoint, data source, and ensures users can work safely.

With many vendors adding blockchain, AI, tokenization, hashing and encryption tools into the mix, those responsible for sourcing IT and cloud security products also need to understand the fast-moving landscape.

73.5%

of cloud security professionals are extremely concerned about the security of their cloud-based systems and services.

Survey sample analysis

Insights for Professionals surveyed 200 IT professionals responsible for cloud security in their organization across the USA. Our sample shows a good mix of company sizes ranging from those with 250 employees to 1,000+.

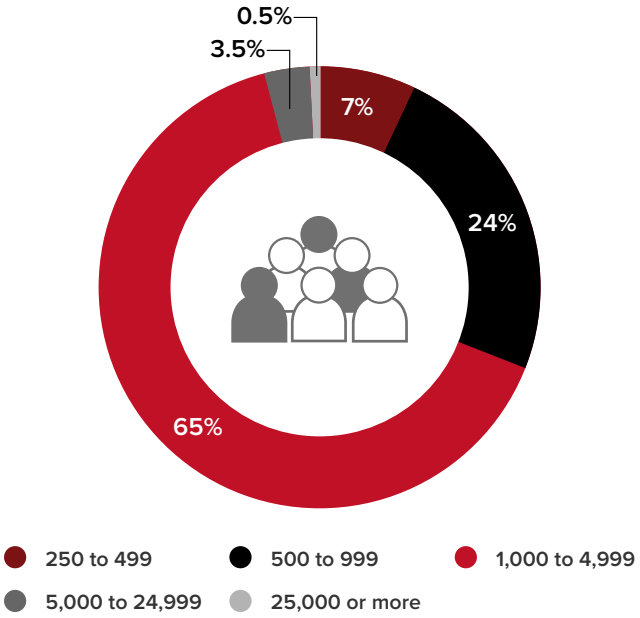
Company size

The largest percentage of respondents (65%) work in large enterprises with 1,000 to 4,999 employees, while the second largest (24%) work in medium-sized businesses with 500 to 999 employees.

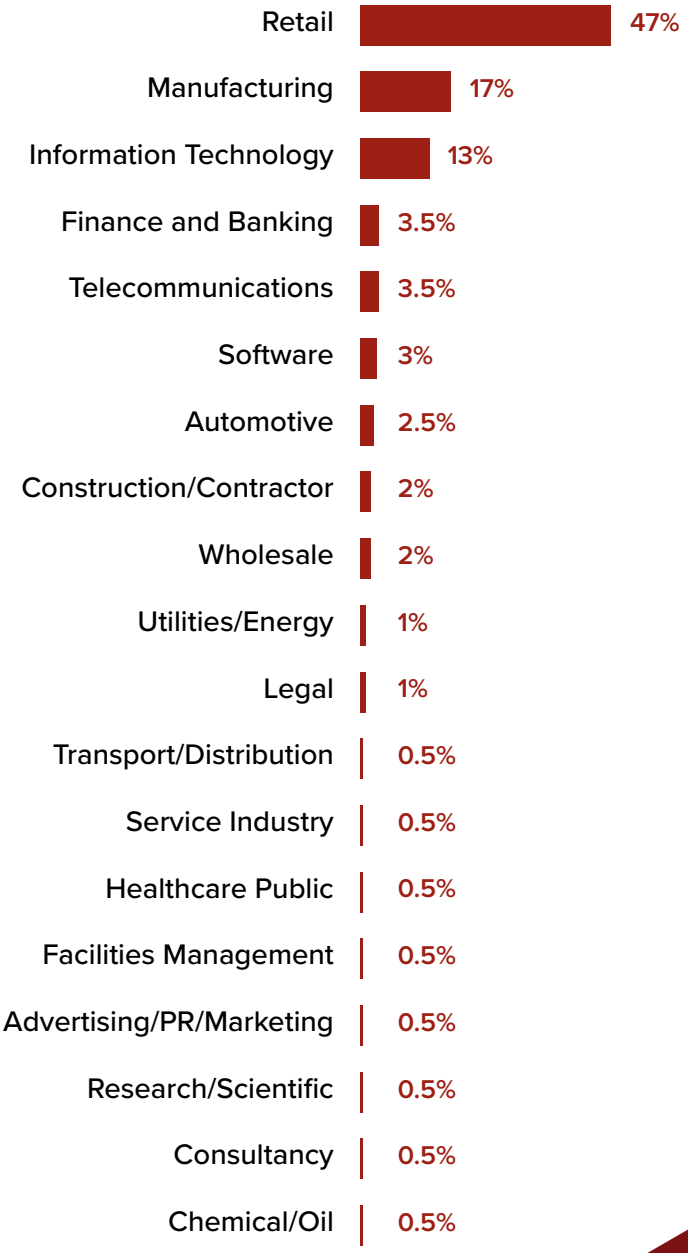
Industry sectors

Our survey shows the largest proportion of participants (47%) are from retail, followed by manufacturing (17%) and IT (13%), all representing organizations with widespread technology footprints and touchpoints.

How many employees are there in your company?



Which industry is your business in?



The State of
Cloud Security

Business operations in the cloud

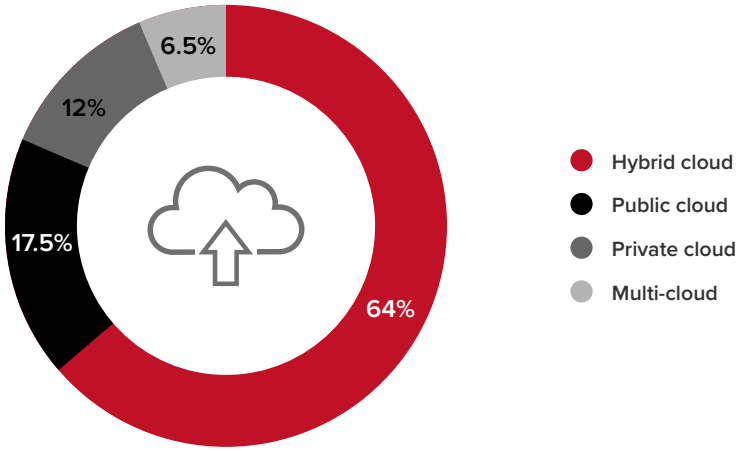
2

Business operations in the cloud

Cloud adoption has accelerated rapidly in recent years due to the Coronavirus outbreak in 2020 and the sudden shift to remote working. Worldwide end-user spending on public cloud services is forecast to grow 20.7% to total $591.8 billion in 2023, according to Gartner - an 18.8% higher growth forecast than for 2022. But not all businesses want to rely solely on the public cloud.

Our survey highlights that 64% of organizations operate a hybrid cloud, 17.5% use the public cloud and the remaining 12% operate in the most secure fashion behind a private cloud.

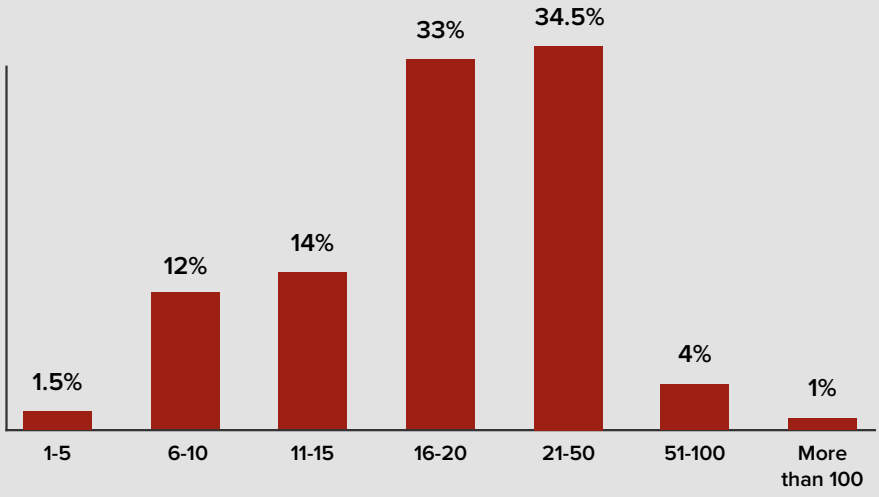
Which cloud deployment model do you use?



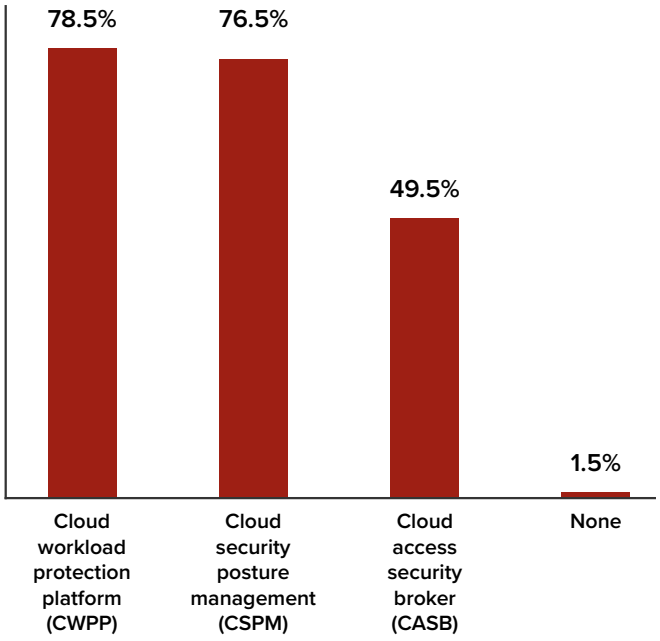
Each cloud deployment model has its own advantages and disadvantages, with more work required to defend public and hybrid operations. However, no cloud is totally secure, so CIOs must use the right tools to maintain security and constantly monitor for breaches or suspicious activity.

That level of surveillance increases as the number of cloud services and platforms across the business also increase, with two-thirds (67.5%) operating between 16 and 50 services. This figure will most likely rise year on year as more businesses start to allocate a greater proportion of their IT budgets toward cloud computing.

How many cloud applications and services do you currently operate?



What cloud security tools is your organization using? (select all that apply)



To defend these growing footprints, CIOs and CISOs must go beyond traditional IT security tools and adopt a range of cloud security solutions to secure and protect their applications, infrastructure and data.

Our research shows that approximately three-quarters of organizations utilize cloud workload protection platforms (CWPP) and cloud security posture management (CSPM) tools. While 1 in 2 companies (49.50%) currently use cloud access security brokers (CASB), further research shows that **60% of large enterprises** will be using CASBs by 2022.

The State of
Cloud Security

Security concerns and threats in the cloud

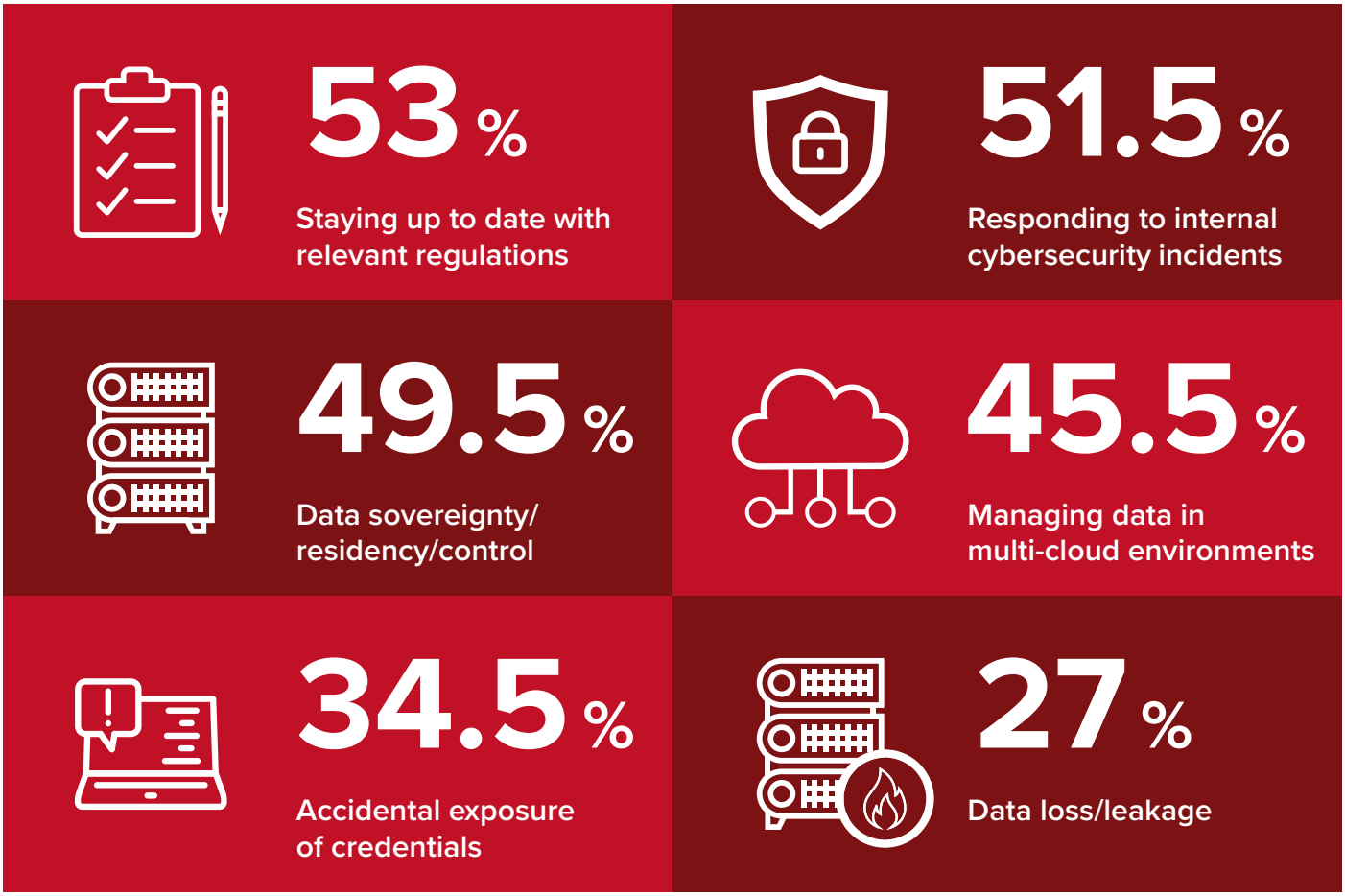
3

Security concerns and threats in the cloud

Most organizations have enough to worry about when it comes to keeping the lights on, and CIOs are facing the twin threats of expanding cloud operations to deliver greater efficiency and creating a more agile business while defending that growing footprint against an increasing armada of threats.

What are your cloud security concerns this year?

Cybersecurity remains a top priority for most CIOs, but as IT departments move from legacy on-premises infrastructure to the cloud, what security concerns do IT leaders share?



Staying up to date with relevant regulations

While most businesses share similar concerns when it comes to cloud security, 1 in 2 cloud security professionals (53%) aren't sure if they're up to date with relevant regulations. This shows the difficulty in following the many regulations of their industry and the increasing need to secure IT infrastructure after recent hacks against high-value targets.

Internal cybersecurity incidents

From unintentional threats caused by negligent staff to former disgruntled employees stealing and exposing sensitive data, half of our survey participants (51.5%) are concerned about internal security. Cloud security tools help minimize the risk of a breach or intrusion, but the rest is often up to good training so staff can identify and avoid falling for spam, phishing or more advanced types of attempts to access credentials.

Data sovereignty/residency/control

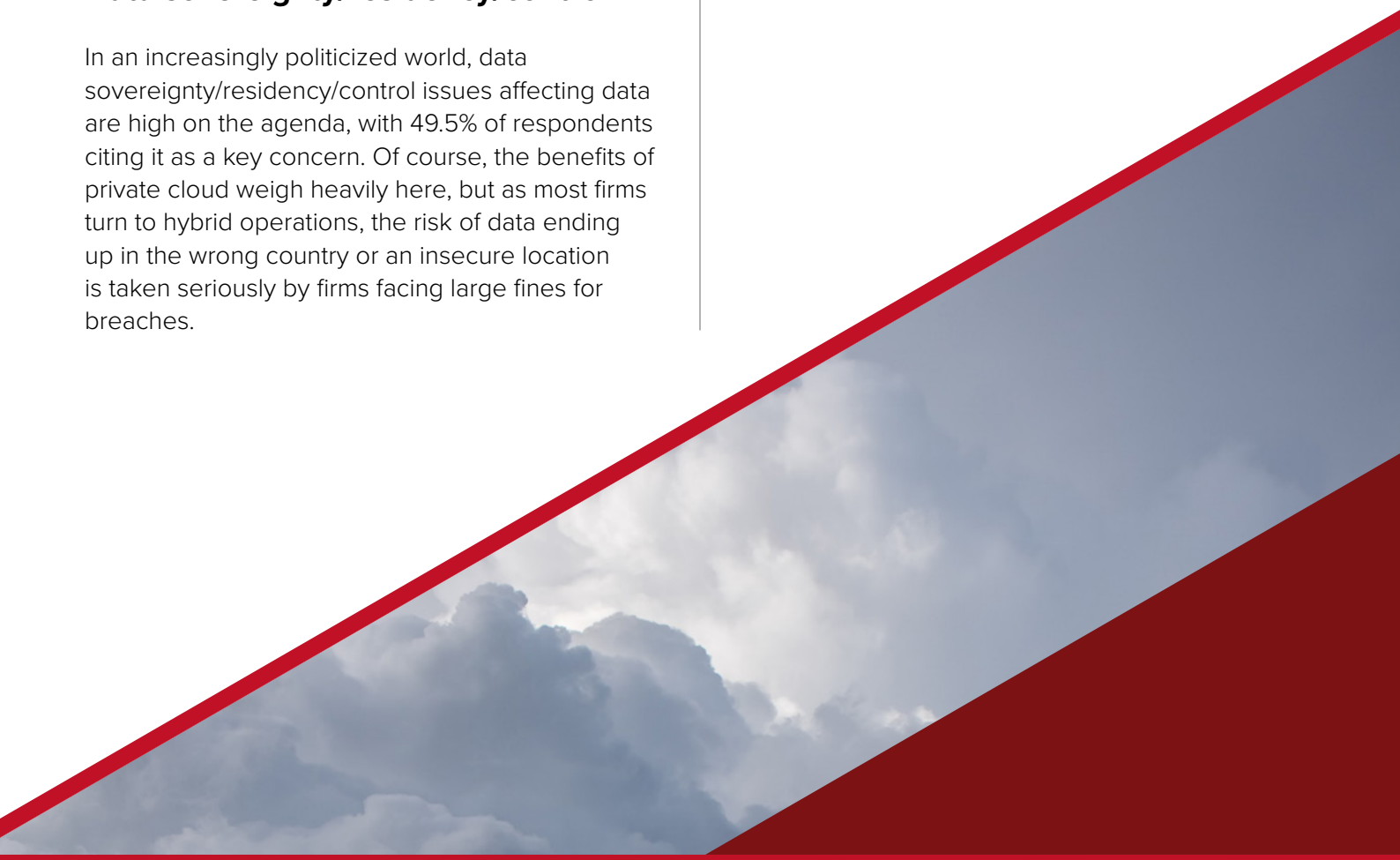
In an increasingly politicized world, data sovereignty/residency/control issues affecting data are high on the agenda, with 49.5% of respondents citing it as a key concern. Of course, the benefits of private cloud weigh heavily here, but as most firms turn to hybrid operations, the risk of data ending up in the wrong country or an insecure location is taken seriously by firms facing large fines for breaches.

Managing data in multi-cloud environments

Managing data in multi-cloud environments is a concern for 45.5% of IT professionals, but is a requirement for any business migrating to the cloud. Strong security, IT and DevOps teams are a requirement for any company operating in this manner and business and IT leaders need to ensure they're well-funded and experienced to support the business.

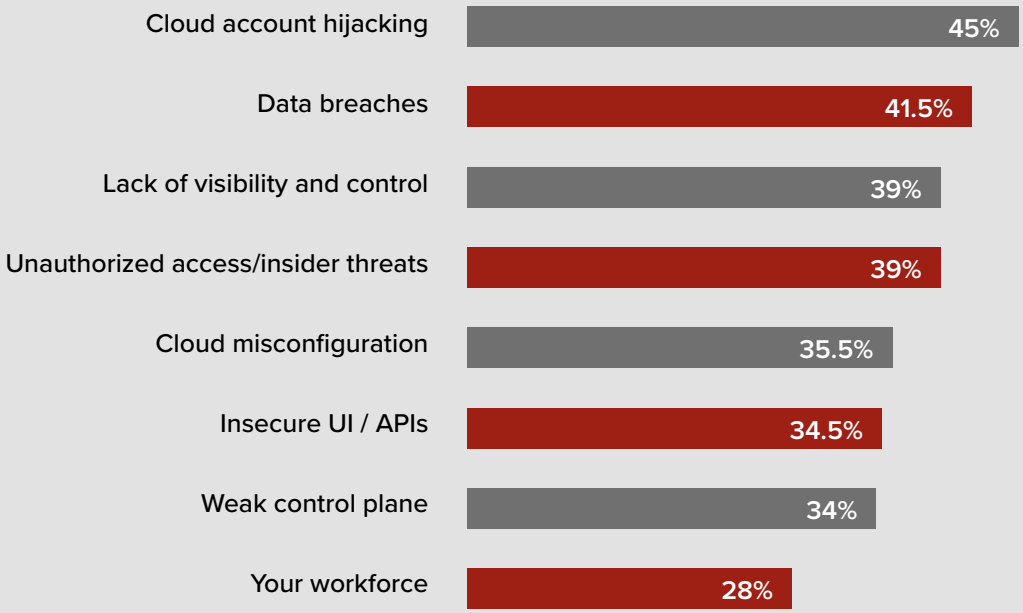
Accidental exposure of credentials and data loss/leakage

Just under 35% of survey participants are concerned about data loss/leakage and the accidental exposure of credentials. That could be because IT leaders consider these operational issues. Given that the majority of attacks on businesses are caused by these methods and go unreported suggest all companies should take them as a high priority across all levels of seniority.



What are the biggest security threats facing your organization today?

With so many security risks in the cloud, our survey respondents were asked to select their biggest threats.



Cloud account hijacking

45% of IT professionals cited cloud account hijacking as their top threat. The ability for criminals to venture into a company's cloud while looking like a legitimate user is a terrifying prospect and one that should see all enterprises using strong account protection and multi-factor authentication (MFA) to ensure that just one leaked password can't immediately impact the business.

Cloud misconfiguration

35.5% of respondents are worried about the threat of misconfigured cloud services. This represents the number one vulnerability found across cloud services and is one of the easiest for hackers and criminals to scan for in an attempt to gain remote access to critical data and other services. Popular targets are Amazon S3 data buckets that are often found unguarded or poorly secured.

Insecure APIs/UIs

Related to that issue are insecure APIs/UIs, a threat for 34.5% of our respondents. APIs connect enterprise services and data to online services, creating a fresh set of vulnerabilities that traditional APIs have faced for many years. Firms can often have hundreds of APIs in operation with minimal oversight of access or data passing through, and one insecurity can lead to a sizeable breach, which might explain why 41.5% of businesses see data breaches as a significant threat. Fortunately, security tools such as CASBs and CSPMS can help improve visibility and minimize the risk of breaches.

Weak control planes

Some 34% are also concerned about weak control planes, the key to security and integrity of business data. A weak control plane puts a business at risk of not being in control of their infrastructure logic, security or verification processes. Control plane security is a growing feature of many security applications to ensure both data and communications remain secure.

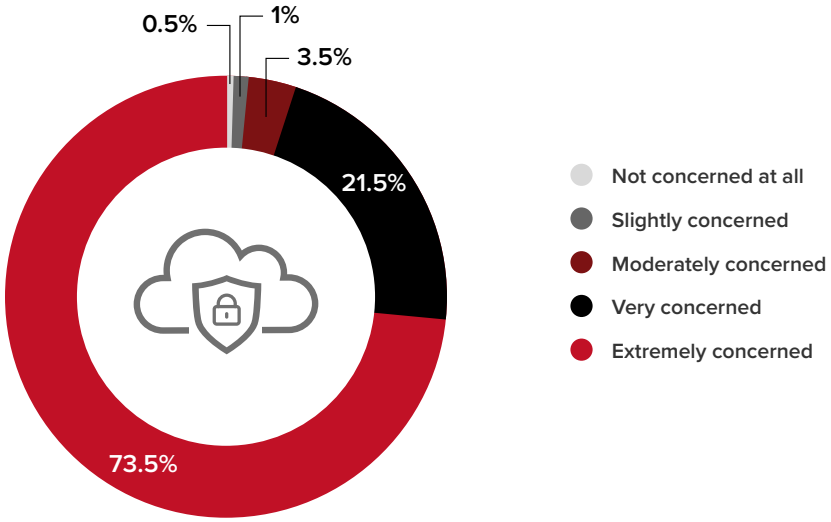
The workforce

28% of respondents consider their workforce to be a major security threat to the business. Only solid onboarding, regular training and testing around the security issues that the cloud presents can teach the human element to respect the cloud. From the security aspect, enforcing strong passwords, MFA, securing devices and rapidly closing unused accounts is key to protecting the business.

How concerned are businesses when it comes to cloud security?

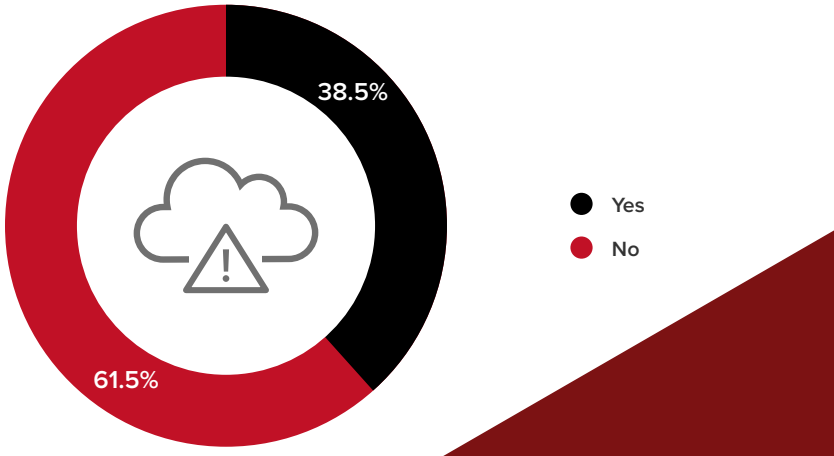
With all the risks highlighted every day in industry, technical and mainstream media, we would expect enterprises to be on high alert. However, around 5% of respondents aren't as concerned about the security of their cloud-based systems and services. This suggests they're either highly confident in their solutions and IT team, or are somewhat unaware of the risks facing them.

How concerned are you about the security of your cloud-based systems, data and infrastructure?



Our research highlights that 38.5% of respondents have faced some type of cyberattack in the past 12 months. 21.5% are very concerned and 73.5% are extremely concerned about the risks to enterprise clouds. But are CIOs taking the right steps to train their workers and defend their IT infrastructure? And is everyone else doing more to protect the business as the range and volume of attacks increases?

In the past 12 months, has your enterprise experienced a cloud data breach or cyberattack?



The State of
Cloud Security

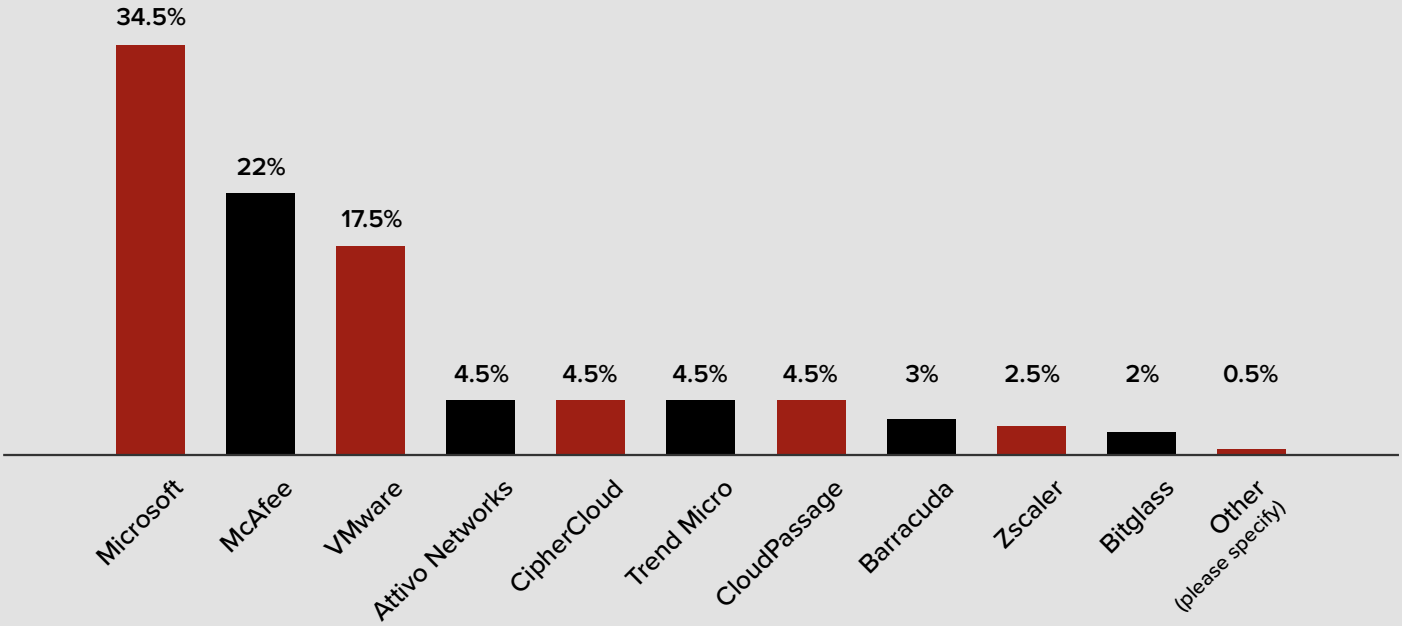
Cloud security vendors

4

Cloud security vendors

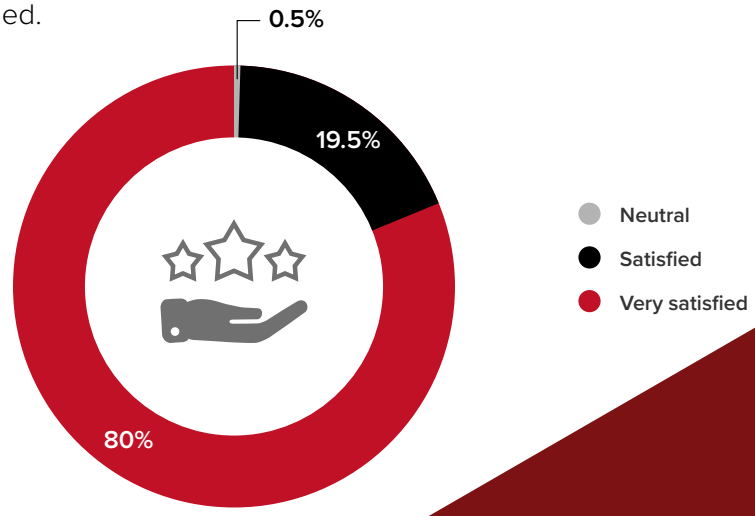
With the massive risk out there, it comes as no surprise there are many vendors offering a complete range of specialist solutions for cloud protection. Yet in the age of cloud-first businesses, Microsoft remains the most popular cloud security vendor at 34.5%.

McAfee (22%) and VMware (17.5%) round out the top three, with a host of specialist brands like Barracuda, Zscaler and CipherCloud clustering around the 5% adoption mark. Whatever the brand, businesses need tools that are collaborative in providing overall protection for the company, with a single end-to-end solution rarely available to cover all eventualities.



Among the respondents, 80% are very satisfied with their choice of vendor and the service they receive while 19.5% are merely satisfied.

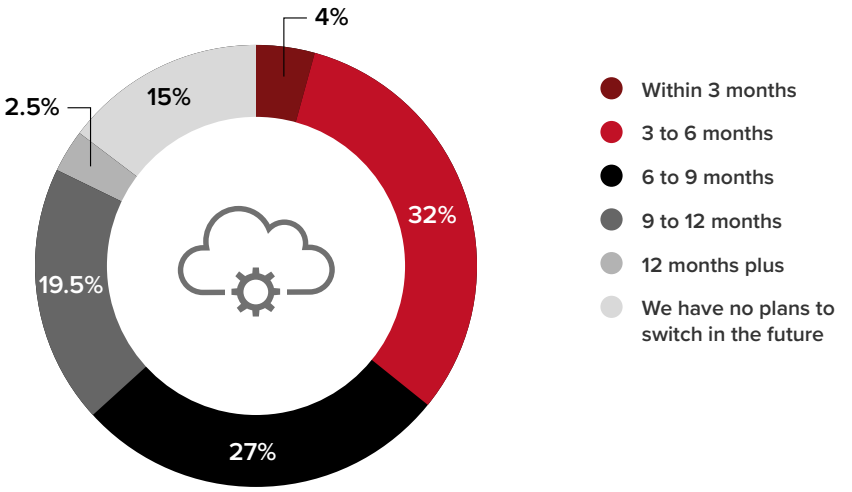
How satisfied are you with your current provider?



However, 36% plan to switch to a new cloud security solution within 6 months, with 46.5% looking to change in the next 6-12 months. Only 15% have no plans to change, which will be good news to vendor sales teams.

As new cloud security services emerge to deal with new threats, enterprises will be looking to adopt them. Many will include AI features to reduce the human workload and improve performance and hunt for the more subtle risks that people are likely to miss. All of this makes for a fast-moving landscape that IT security leaders, CISOs and other roles need to keep on top of.

When are you planning to switch to a new cloud security solution?



Summary

This report highlights that the majority of CIOs and their teams are making good progress in the mission to secure their clouds. However, this is an endless challenge to defend the business against implacable, smart and committed adversaries. And as more firms migrate to the cloud, there are plenty more targets of opportunity.

It's never enough to be "up to date", all enterprises need to remain constantly vigilant about changing threat postures, new vulnerabilities and how their expanding cloud creates new risks.

With many security issues, visibility gaps and challenges lurking in the background, every business and every worker using their cloud services needs to be aware of the latest risks and how the tools that protect them function.

About Insights for Professionals

IFP gives you access to the latest business knowledge that's customized for you. We provide high quality, credible and relevant resources for senior professionals in one place.

An easy to access and personalized library to help you when you are researching specific topics, seeking practical advice, or simply want to stay ahead of what's happening in your industry. To do this we gather the best content from suppliers, brands and industry experts, as well as doing our own research.