
# State of Cloud Security 2021

An Ermetic report based on a funded research study
by International Data Corporation (IDC)

# About this report

In mid-2021, IDC conducted a research study – funded by Ermetic – of 200 U.S. CISOs and other security decision-makers regarding their cloud security strategies, practices and experiences. It was the second annual study of its kind.

**This report summarizes the key findings and implications for cloud security stakeholders.**

# State of Cloud Security 2021

An Ermetic report based on funded IDC research

## Contents

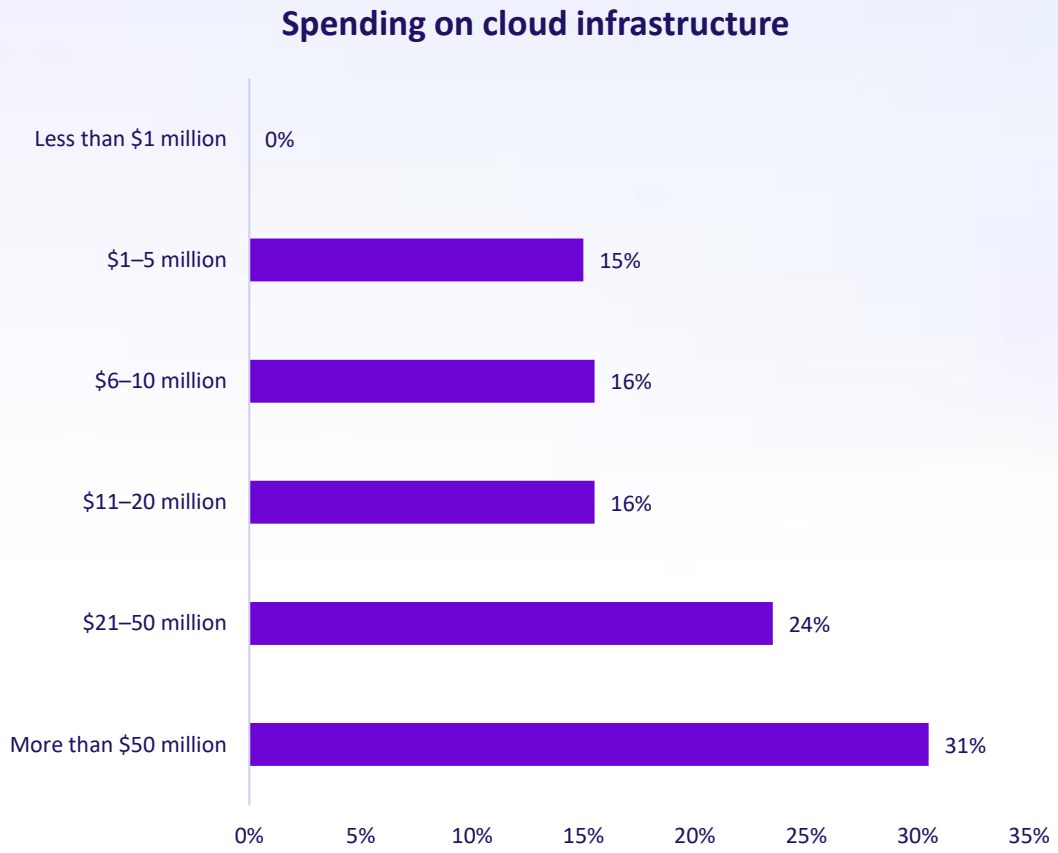
# State of the cloud

# 70%

of organizations are spending more than **$10M** yearly **on cloud infrastructure**

... and 31% spend more than **$50M** yearly

Organizations are making massive investments to grow their cloud infrastructure.

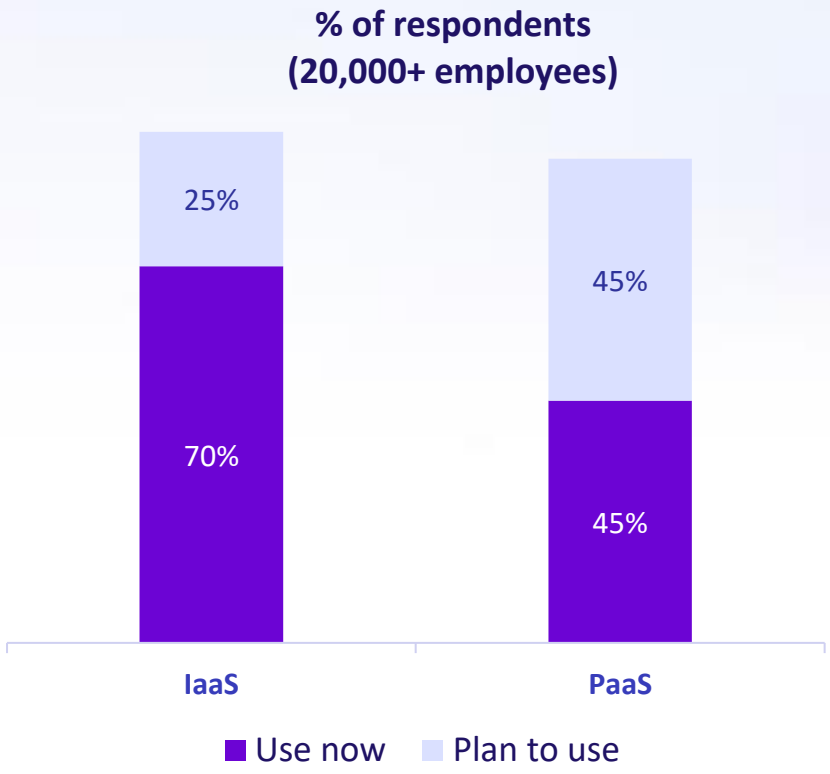


# 95%

of very large organizations **use or plan to use IaaS**. PaaS is rapidly catching up.

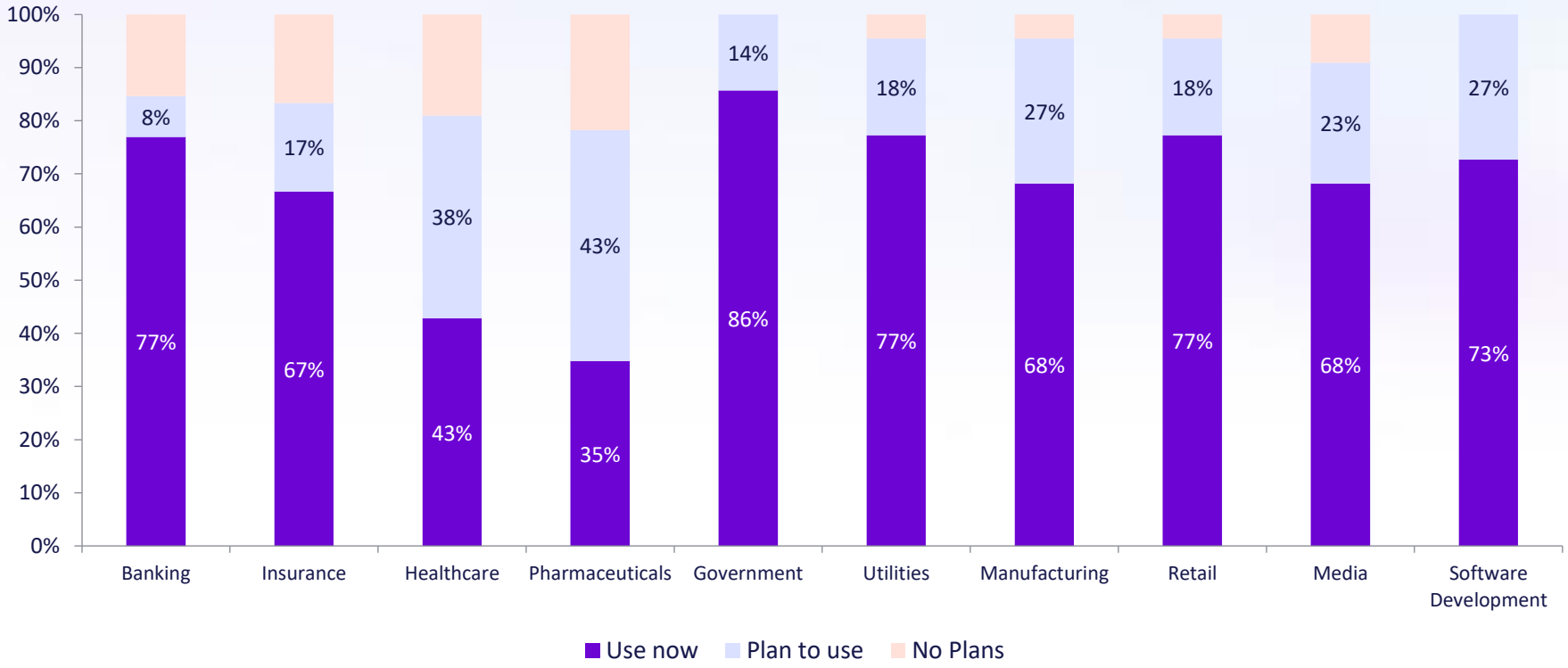
For all organizations, IaaS is reaching mainstream adoption. Among **very large organizations, 95%** are using or plan to use IaaS, and 90% are using or plan to use PaaS.

** Very large organizations = 20,000+ employees*



# IaaS adoption by industry

**Different industries are leading the IaaS adoption charge**. Organizations already using or planning to use IaaS: Government and Software Development (100%!), followed closely by Utilities and Retail.

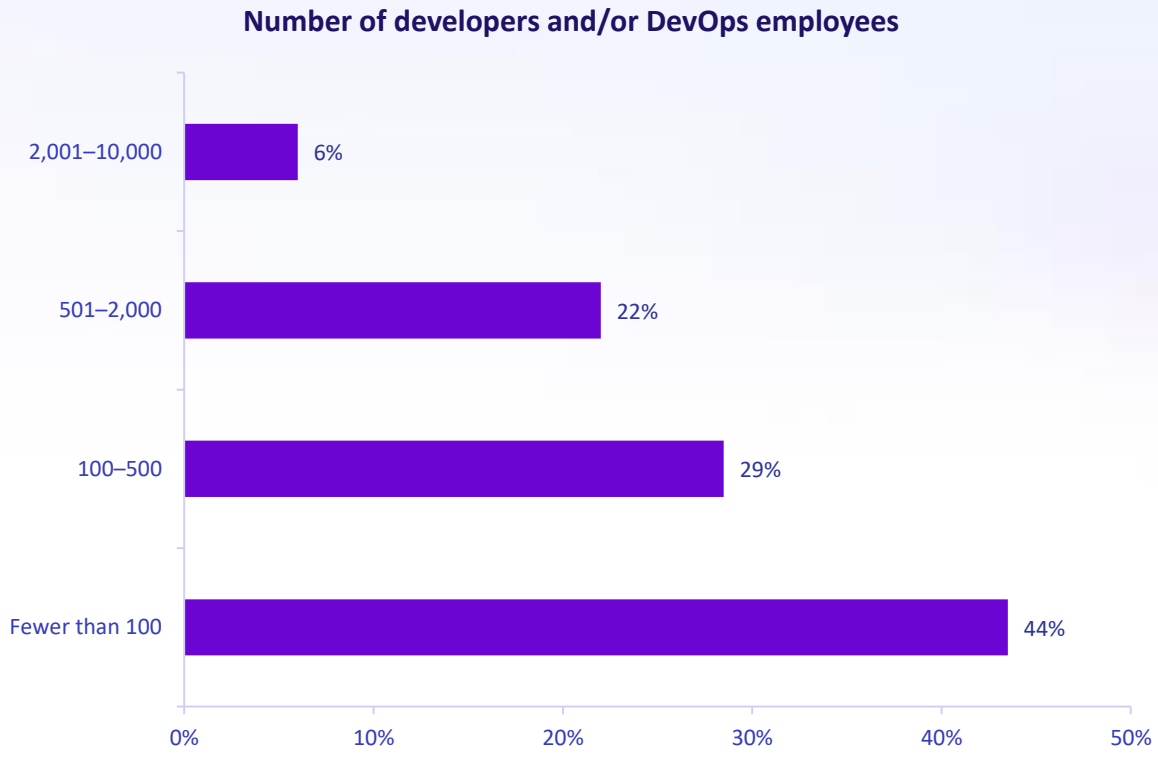


# 56%

of organizations have more than **100 developers** and/or DevOps employees

Organizations that have large development teams potentially also have large numbers of **privileged users**. Such organizations clearly have an **acute need to secure cloud access**.

** Large development teams = more than 100 developers*

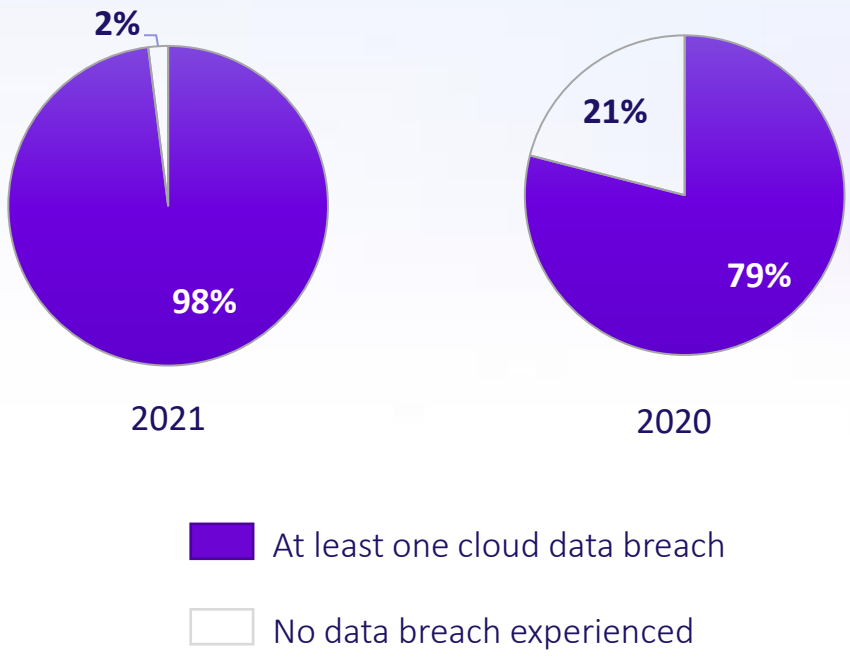


# A world under attack

**Almost every organization** using cloud infrastructure today is experiencing **security failures**. 98% reported having at least one cloud data breach in the past 18 months - and **67% reported three or more incidents**. Organizations are falling prey to more breaches. It's also possible that stakeholders are more aware that breaches are occurring.

# 98%

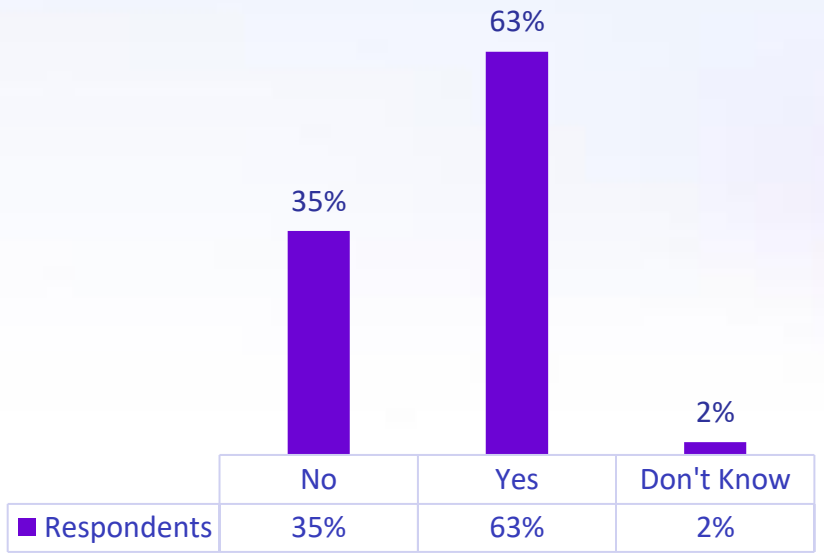
of organizations experienced **at least one cloud data breach** in the past 18 months, compared to 79% in 2020



63% of all organizations had sensitive data exposed in the cloud. This number **ballooned to 85%** for companies with large cloud footprints.

** Large cloud footprints = Cloud infrastructure spending of more than $50 million yearly*

Most organizations (**63%**) confirmed that their **sensitive data has been exposed** in the cloud




**Respondents who said sensitive data has been exposed in the cloud**
(% of respondents)

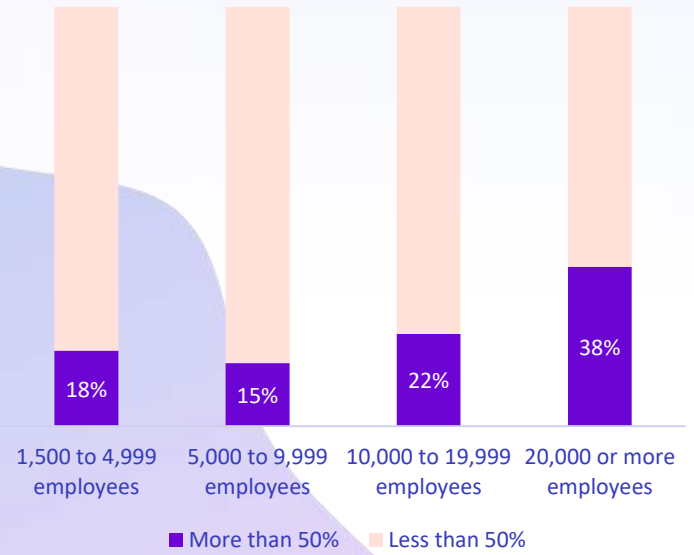
# 83%

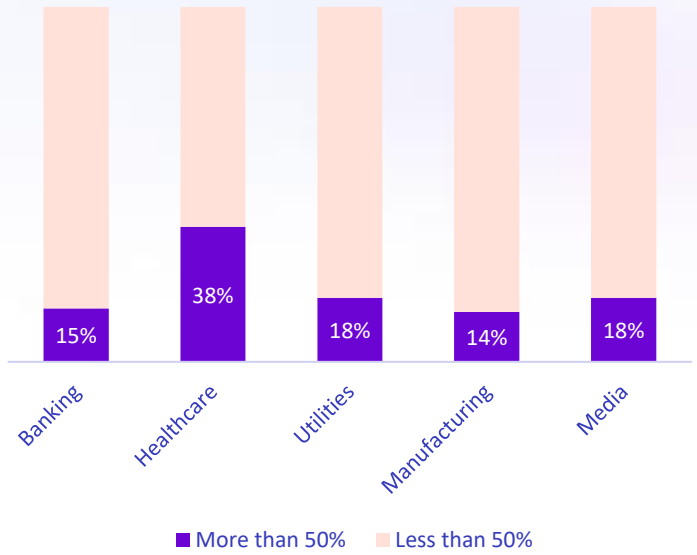
of companies said at least one breach was **access related**

Everyone is vulnerable, but some even more. **60%** of large and very large organizations -- and nearly 40% of healthcare companies -- cited **access vulnerabilities as a primary root cause** of their cloud breaches.

** Large organizations = 10,000-20,000 employees; very large organizations = 20,000+ employees*

**Percentage of cloud data breaches related to access (by size and industry)**



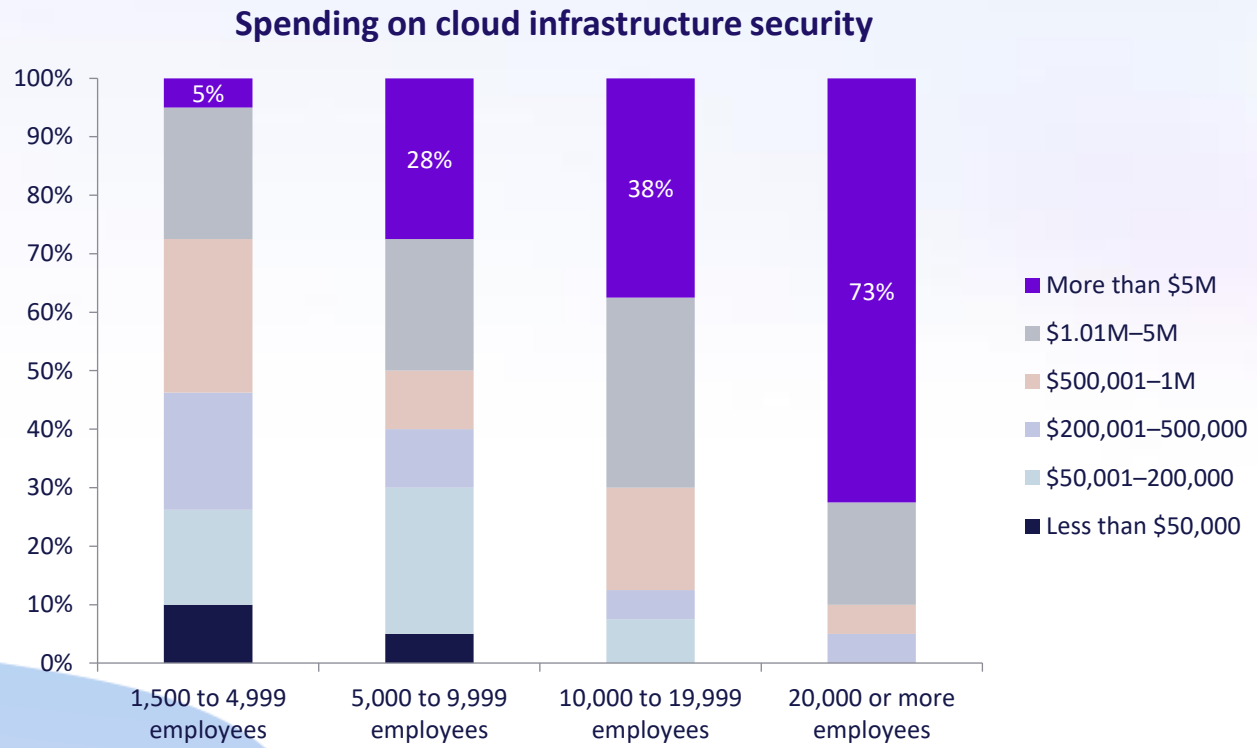
# Guarding the gate

# 85%

of organizations expect to increase their **security spending** this year

For 85% of organizations, **security budgets are on the rise** – and a significant portion is being allocated to cloud infrastructure security. 73% of very large organizations - and almost half of the banks surveyed - plan on spending **more than $5 million to secure their cloud infrastructure**.

** Very large organizations = 20,000+ employees*

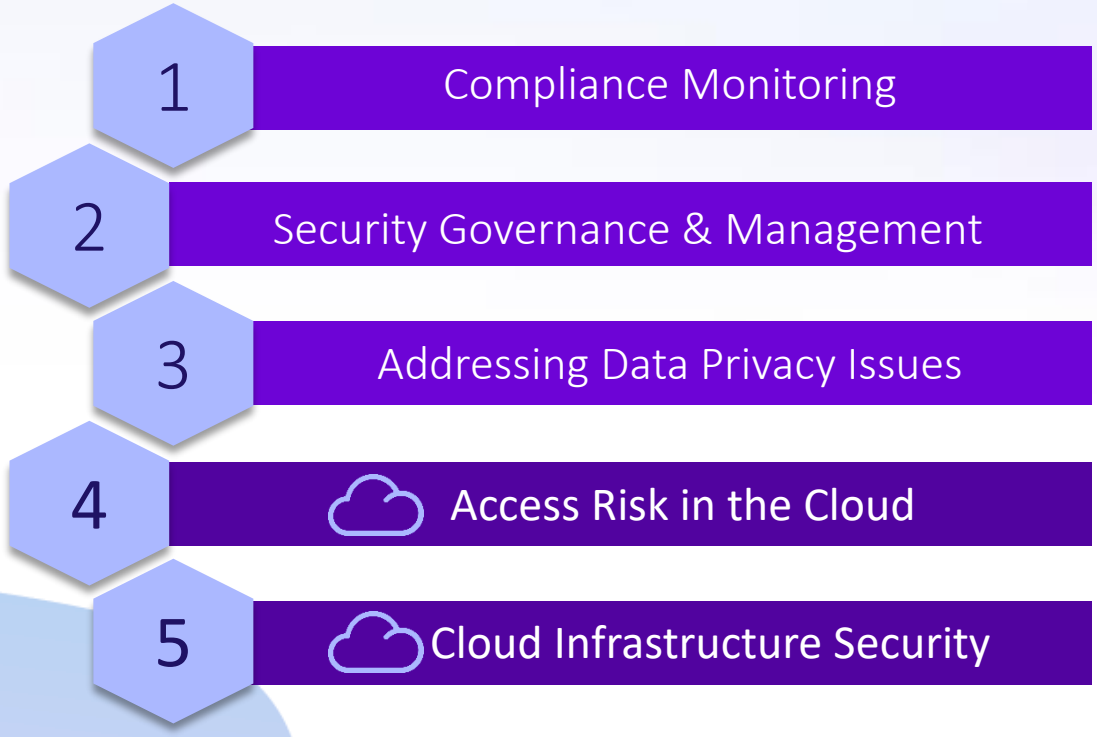


# Top 5 security priorities

for the next 18 months

Two of the **top security priorities** for security decision makers are **uniquely cloud related**: Access risk in the cloud and cloud infrastructure security. Access risk ranks higher for enterprises with large development teams and/or large cloud footprints.

** Large development teams = more than 100 developers; large cloud footprints = cloud infrastructure spending of more than $50 million yearly*



# 92%

of organizations tried to implement **least privilege access**, or will try to in the next 12 months

While 92% seek to implement least privilege, of large organizations that tried, **50% failed**. All organizations cited the greatest **barriers to implementing successful least privilege** as: Lack of personnel/expertise, multi-cloud complexity or implementation difficulty.

Nearly

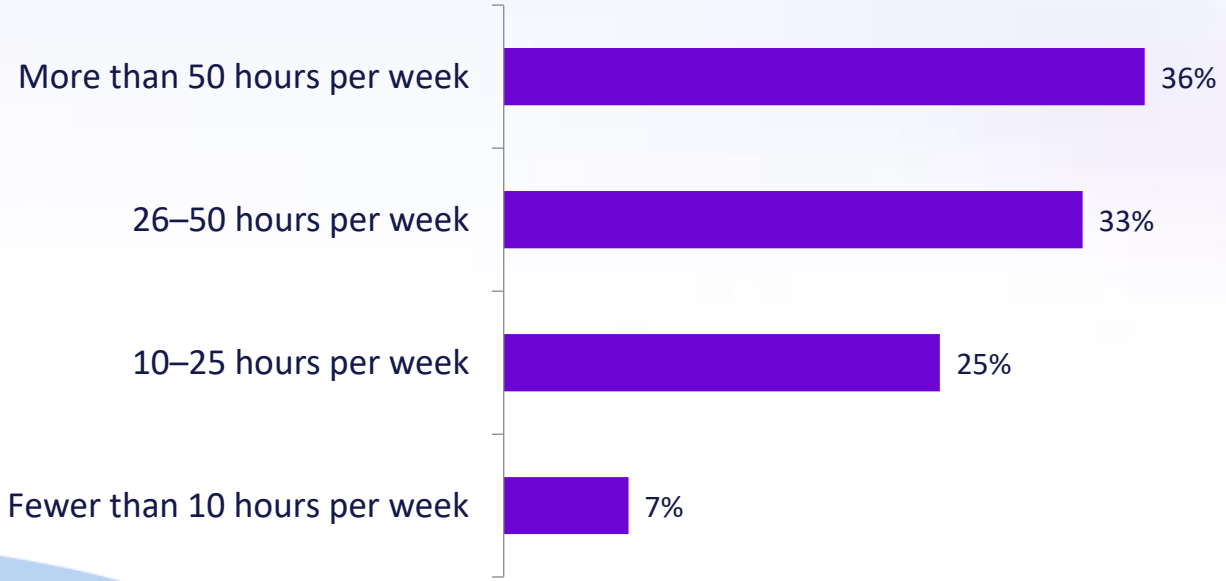
# 70%

of organizations invest more than 25 hours/week **managing IAM in cloud infrastructure**

Nearly 70% of organizations - and 100% of large and very large organizations! - spend **more than 25 hours weekly** dealing with cloud IAM. At $100 an hour, that adds up to at least $130K yearly.

** Large organizations = 10,000-20,000 employees; very large organizations = 20,000+ employees*

**Time spent dealing with IAM in cloud infrastructure**

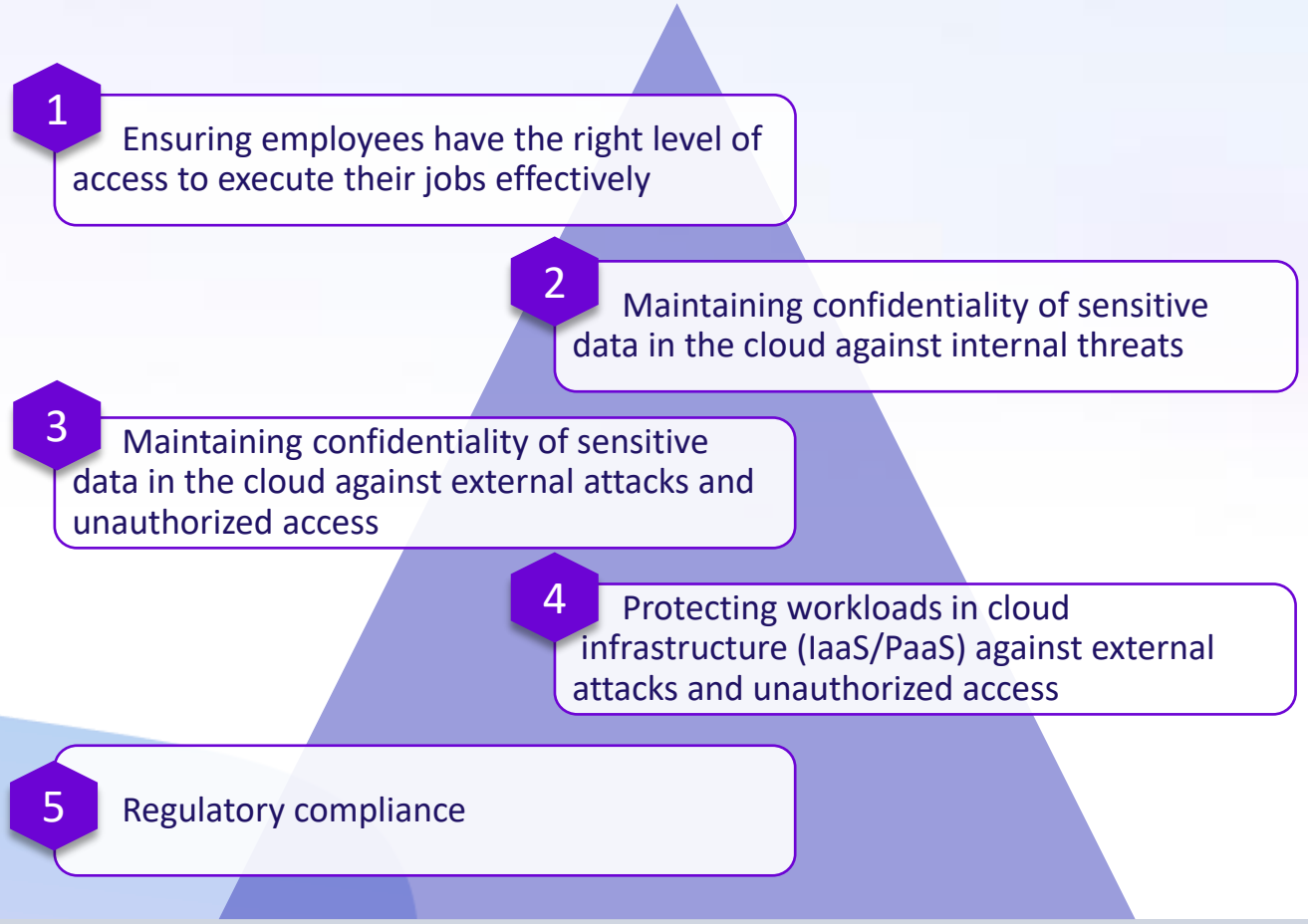


# 60%

Let my people work - that's **why I govern access**

For large organizations, letting employees do their jobs effectively was the top driver for governing access permissions. **Protecting sensitive data from internal and external threats** followed closely.

** Large organizations = 10,000-20,000 employees*



**Multi-cloud** is amplifying cloud security **challenges**

**IDC survey participants speak:**

“The biggest challenge for us is to manage the **complexity** of the multi-cloud environment.”

“**Security controls are inconsistent** across multiple cloud environments.”

“Multi-cloud infrastructure has a chance of **data security breaching**, as data is shared by multiple service providers.”

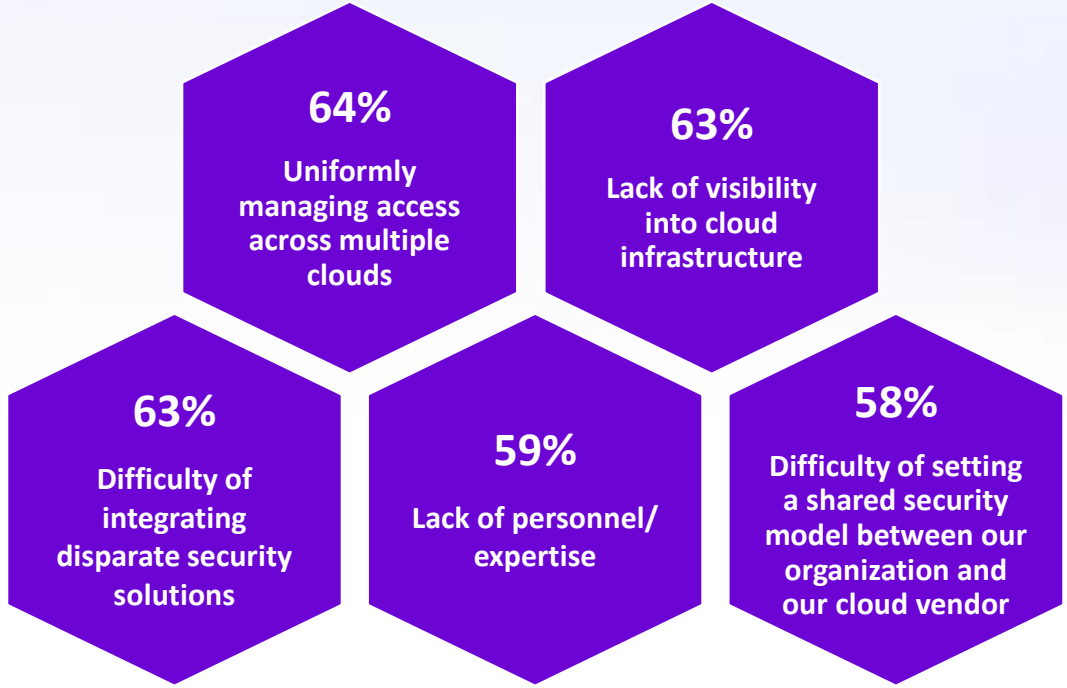
# Recipe for failure

# 43%

of organizations could not say they are satisfied with their **cloud security posture**

Almost half of the organizations **could not say they are satisfied** with their cloud security posture.

When asked about difficulties in managing cloud infrastructure identities and permissions, respondents ranked **multiple challenges** as having **moderate to severe significance**.



# Fragmented decision-making complicates security practices

Few of the surveyed organizations have a dedicated cloud security team. While IT/Operations make most decisions, the overall process is very fragmented, with **many job roles identified as primary decision makers for securing access in cloud infrastructure**.

Nearly

# 60%

consider lack of visibility and inadequate IAM to be **major threats** to their cloud infrastructure

*"Cloud computing systems are insecure because of their complex networks and various third-party platforms."* Survey participant

As their cloud footprint grows, organizations are struggling to protect it. Nearly **60%** of organizations identified lack of visibility and **inadequate IAM security as major threats** to their cloud infrastructure. In fact, they cited security across the **full cloud stack** - IAM, APIs and network - and security misconfigurations, as major threat concerns.

1. Insecure APIs/other interfaces
2. A lack of visibility and inadequate network security
3. A lack of visibility and inadequate IAM security

Organizations know they **need to govern access** to protect sensitive data from threats but are **pressured to give permissions** that will not impede employee productivity.

# Organizations are **struggling to balance cloud security** without impacting day-to-day operations

**Top drivers for governing access permissions in cloud infrastructure**

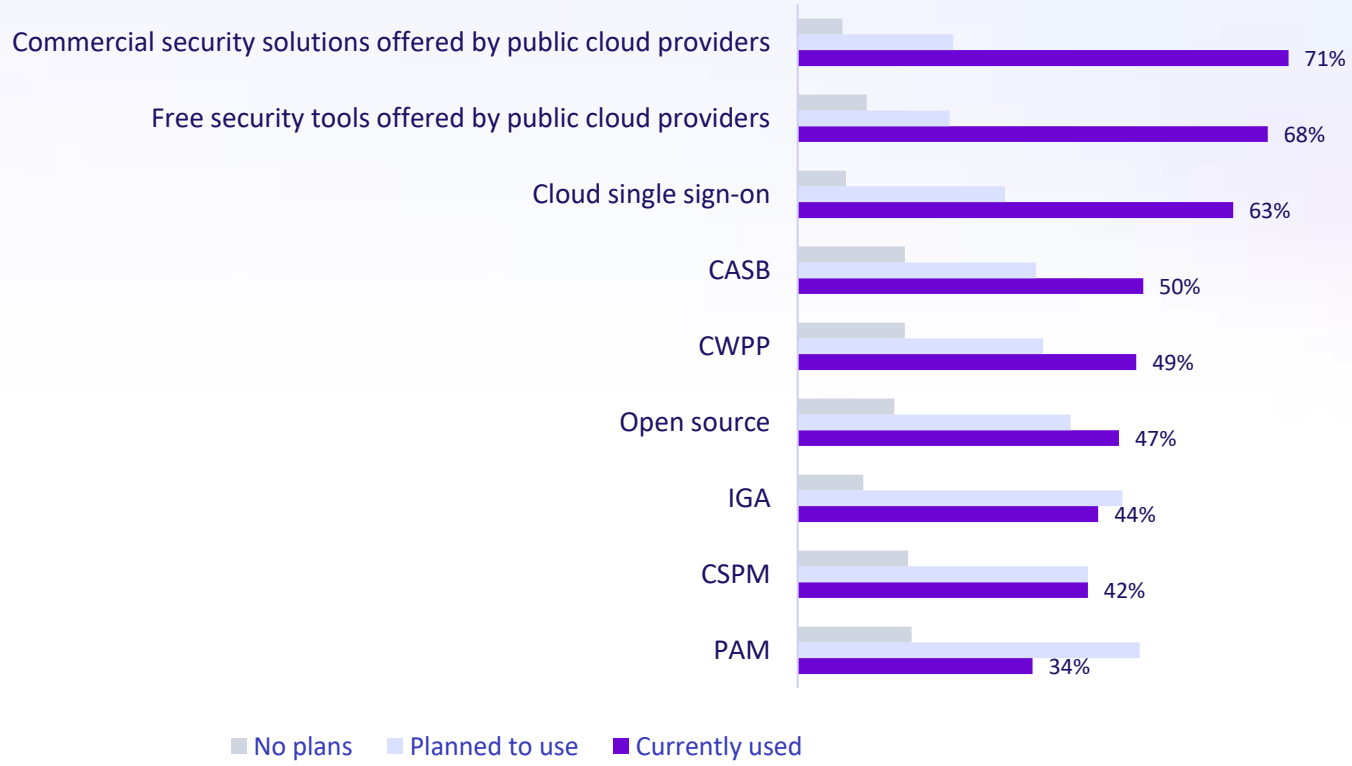
# 71%

**use commercial security tools** by cloud providers

…yet only 20% are very satisfied with their cloud security posture

71% use commercial security solutions/tools by their cloud providers. Respondents said **these tools require a lot of time.** And only 20% of organizations are very satisfied with their cloud security posture.

Together, the widespread use of cloud provider tools, low satisfaction with cloud security posture and universally high instances of cloud breaches suggest the **shared model for cloud security is not working**.



# What's next?

# What’s next?

## The Dilemma

Existing security solutions are not working for cloud infrastructure

Access risk is not understood - and solutions in place can’t address it

## Urgently Needed

- Visibility into identities & other security risks
- Automated governance & remediation
- Unified proactive multi-cloud security

Stakeholders need to see risk, comply and pursue least privilege

## The Answer

**Identity-first cloud infrastructure security**

A solution that prevents cloud security failure at scale and surmounts the expertise gap