VALTIX

THE 2022 MULTICLOUD SECURITY REPORT

New research reveals why IT leaders either struggle or succeed with the move to multi-cloud

VALTIX

It’s not news that organizations of all sizes are moving to the cloud, but what’s new is that now one cloud isn’t quite enough. To compete, protect customer data, scale, and reach their goals, more companies today are operating multiple clouds than ever before.

While leveraging multiple clouds is an advantage for many companies, managing multi-cloud security is frequently also taxing to IT teams because it multiplies their tasks, staffing needs, and potential for what can go wrong. Complexity, varying security protocols, visibility into the performance of multiple apps, talent scarcity, interoperability and cost controls all enter the picture each time a new cloud does.

Valtix, a multi-cloud security platform, wanted to understand how IT teams are dealing with the growing challenge of multi-cloud management, and what they’re doing to grow and perform better.

Valtix commissioned an independent research firm to survey 200 IT leaders in the US about the problems they face with multi-cloud security, the tools they’re using, the tools they want to use in the future, and the skills they need to scale and secure on multiple cloud platforms.

About this study

This survey used a random sample of US IT leaders and has a margin of error of +/- 6.9% at the 95% confidence level. Respondents were double blind and were carefully screened to verify their expertise and competency. Sampling was conducted in partnership with Lucid, a global leader in survey response and methodology.

Respondent breakout:

100% of respondents were IT leaders, manager level or more senior

33% of respondents were VP level or above

100% of respondents worked in the US

100% or respondents had intimate knowledge of their company's cloud operations

62% of respondents lead at companies that use more than one cloud platform

38% of respondents lead at companies that use just one cloud platform

Respondents represented industries such as computer hardware, software, telcomm, financial services, healthcare and others

ABSTRACT

Many IT leaders resist moving to multiple cloud platforms even though they know at some point growth will demand it. Operating multiple clouds brings both opportunities and challenges. Multi-cloud security, in particular can present problems for IT leaders because it varies by cloud, requires specific skills, causes crisis-level problems if not properly managed, and is constantly evolving.

New research from Valtix reveals the top challenges, opportunities, and strategies IT leaders are dealing with, and how they plan to win at multi-cloud security management.

WHO IS THIS EBOOK FOR?

- IT leaders considering a jump to multiple clouds
- IT leaders who want to optimize their multi-cloud security
- Executives who want to understand how to better support multi-cloud IT teams

WHAT YOU WILL LEARN FROM THIS EBOOK

- Why companies are adopting multi-cloud strategies
- What kind of priority multi-cloud is, and why it's needed
- The top challenges facing multi-cloud operators
- The staffing and skill challenges experienced by IT leaders on multiple clouds
- How businesses are managing security governance for multiple clouds

KEY STATS

Multi-Cloud and Cloud Security Strategy

Companies resist expansion to multi-cloud, but they may be forced to expand anyway.

51% of organizations using one cloud platform **say they don't want to expand to new clouds** because of the added security complexity,

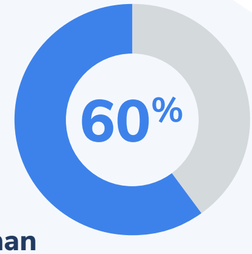
...but 92% of them also think they have no choice if they want to meet their business goals

95%

Multi-cloud security commands attention.

95% of IT Leaders **say multi-cloud is a strategic priority** in 2022

B2B companies feel more pressure to expand to multi-cloud than B2C.



B2B companies on one cloud are nearly **60% more likely than B2C companies on one cloud to feel they have no choice** but to expand to multiple clouds

IT leaders lack tools for successful multi-cloud security.

95% of IT Leaders say **multi-cloud is a strategic priority** in 2022,

...but only 54% feel highly confident that they have the tools or skills they need to execute

Multi-cloud has been trending for years, but in 2022 it becomes a top strategic priority for IT leaders.

IT leaders already struggling with visibility and security challenges are realizing that their problems multiply when each new cloud adds custom security model requirements.

Multi-Cloud and Cloud Security Strategy

CONTINUED

Operational challenges and lack of staff block app security on multiple clouds.

Why IT leaders feel ill-equipped to secure apps across multiple clouds.

Operational challenges

Lack the staff across each cloud for cloud-specific networking, security and automation

Lack the skills for multi-cloud management

IT leaders need budget for successful multi-cloud security.

What IT leaders need to get ready for multi-cloud security

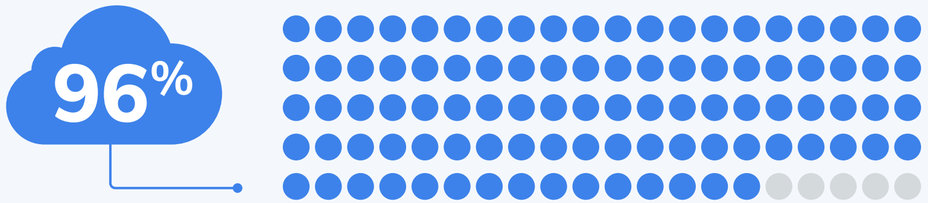
Additional budget

Better multi-cloud operations technology

More people

Multi-cloud security is a top priority.

Security within their multi-cloud strategy is a **top priority for 96% of IT leaders**



IT leaders need to start with gaining confidence in multi-cloud visibility.

From there they should look at security vendors who can make visibility actionable by connecting asset inventory directly to the application of multi-cloud security policy.

Multi-Cloud and Cloud Security Strategy

CONTINUED

Multi-cloud is coming for nearly everyone within 2 years.

62% of organizations **are multi-cloud,**

...and 84% of those that aren't **expect to be within 2 years.**

Low confidence in security across all cloud accounts.

Only 55% of organizations feel highly **confident they have deployed network or host based security** across all of their public cloud accounts and the app workloads that run there

55%

Multi-cloud security budget increases are on the horizon. 83%

83% of companies are committing additional budget to multi-cloud security in 2022

Many public cloud accounts are unknown to IT.

Only 48% feel highly confident that every application workload in their public cloud accounts is known.

IT leaders don't see the extent of public cloud accounts. Only about half of IT leaders feel confident that every public cloud account is accounted for.

48%

Multi-cloud budgets will see a significant bump.

On average, companies that plan additional budget for multi-cloud security **in 2022 expect to bump their budgets by 47%**

Retail organizations use multiple clouds. Industries most likely to be using multiple clouds:

Retail **Restaurant** **Education**

Staffing

Different security policies for different clouds frustrates IT leaders.

Having to **manage different security policy and processes per cloud** is a top pain point for **91% of IT leaders,**

...but only **63% of them have deeply knowledgeable** cloud security staff

Security plus cloud knowledge is key for IT teams.

The top skills needed to manage multiple clouds:

- **Has security knowledge combined with cloud knowledge**
- **Knowledge of provider specific security architecture**
- **Knowledge of provider specific network architecture**

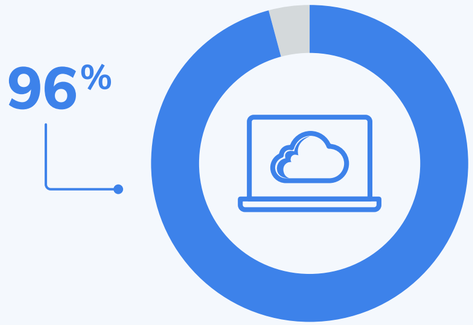
Organizations have sunk time and resources into shifting technology from the datacenter to the cloud.

What they soon realize is that the cloud is different and on prem technologies impose additional maintenance burdens on their teams – thus exasperating the skills gap further.

Cloud Operational Visibility

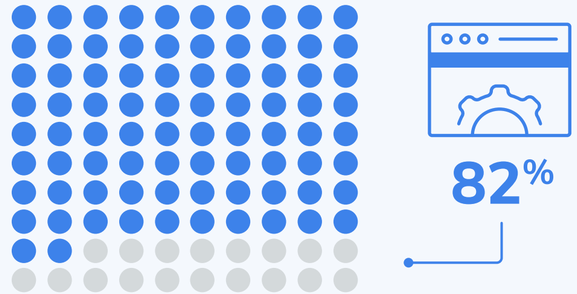
IT leaders want one view for multiple cloud security.

96% of IT leaders say job would be easier if they had one console view to manage their security across multiple clouds.



Fractured visibility means slower work.

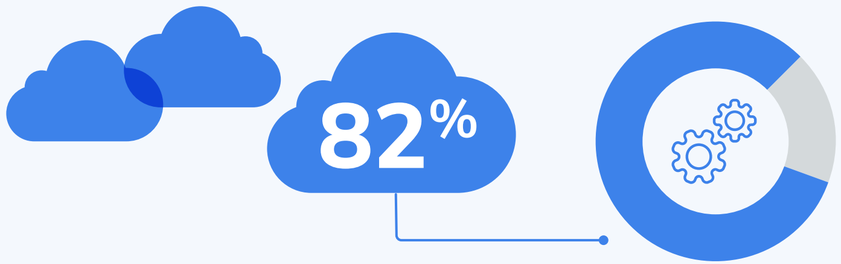
Not having visibility into cross-cloud security controls and policy **creates more work for 82% of IT teams**



Visibility and policy fragmentation have a major impact on the security process.

Lacking a single source of truth, teams struggle to implement one consistent security policy across the total environment, opening the door to security lapses and gaps that make the organization vulnerable.

Cloud Security Strategy / Policy



Cloud complexity freezes businesses.

82% of companies say that **the complexity of cloud security slows down business agility**

Ultimately, security must be able to move at the speed of business.

The substantial gap between multi-cloud security and the cloud needs of the business will drive the next wave of high-profile security incidents.

A platform that consolidates cloud security and policy enables a more dynamic security function that can move faster, more confidently, and provide better security outcomes.

Multi-Cloud Security Technologies and Execution

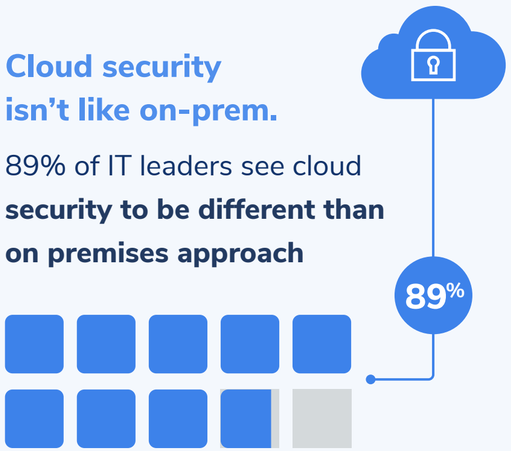
Businesses customize cloud security strategy per cloud.

72% of IT leaders say their **cloud security strategy is different in each of their cloud providers**

72%

Cloud security isn't like on-prem.

89% of IT leaders see cloud **security to be different than on premises approach**



89%

75%

Yet, many see the cloud as an extension of existing data centers.

75% of IT leaders see cloud **as being an extension of their existing datacenter**

There is a divide between how IT leaders almost universally see cloud security as different and yet also see cloud as an extension of the datacenter.

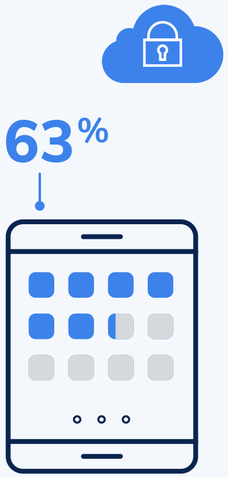
The lesson? Bringing a datacenter mindset to the cloud inevitably results in failure.

Shifting technology from on prem to cloud is challenging and creates risk. IT leaders should look for cloud-native security solutions that are purpose built to secure cloud workloads.

Gaps and Needs

Companies struggle with inefficient multi-cloud security.

Security within multi-cloud **is inefficient at 63% of companies**



Multi-cloud operations are an under-invested necessity.

Multi-Cloud security is a priority and **necessity at 97% of organizations,**

...but it's underinvested at 76% of companies

Employees are underskilled for multi-cloud security.

Security within multi-cloud **is underskilled at 67% of companies**

Under funded, under skilled, inefficient – IT leaders enter 2022 in a precarious state when it comes to multi-cloud.

They must reset their approach for the next decade, not the last.

Gaps and Needs

CONTINUED

Excessive number of apps creates challenges.

Why IT leaders **don't feel confident** that they have the right approach to multi-cloud security

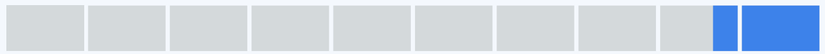
Too many applications to manage

Difficult to manage security policy across clouds

Lack a multi-cloud security policy plane

Lack of executive support

Staff don't have the right skills



13%

Some executives recognize the need for more support.

13% of executives acknowledge that **a lack of executive support is one reason their IT team doesn't have the right approach** to multi-cloud security

Consolidation on multi-cloud security platforms enables IT leaders to simplify the task of managing multi-cloud security policy and close the skills gap.

Consolidated multi-cloud security policy will enable IT leaders to adapt to the new cloud requirements that business agility demands.

VALTIX

Conclusion

Expanding to multiple clouds means more scalability and capability, but requires additional staff with specialized resources, adds complexity to everyday operations, and invites security challenges. But with the right tools, leadership, budget and governance, running multiple clouds can open the door to growth and real competitive advantage.

https://valtix.com