State of Cloud Security Concerns, Challenges, and Incidents

algosec

CSA cloud security alliance®

Acknowledgments

Lead Authors:

Hillary Baron
Sean Heide
Shamun Mahmud
John Yeoh

Designers:

Stephen Lumpe
AnnMarie Ulskey

Special Thanks:

Yitzy Tannenbaum, Product Marketing Manager, AlgoSec

Table of Contents

Survey Creation And Methodology 4
Goals of the study....4
Executive Summary....5
Key Findings....5
- Key Finding 1: Organizations are continuing to move to complex cloud environments....5
- Key Finding 2: Cloud provider's native security controls not enough for many organizations 6
- Key Finding 3: Organizations look for security tools that can supplement their workforce 7

Public Cloud Usage 8
- Public cloud platforms organizations are using. 8
- Expectations being met by public cloud....8
- Past, present, and future cloud workloads....8
- Team Responsible for Managing Security in Public Cloud 9

Cloud Security Concerns....10
- Concerns when adopting cloud 10
- Addressing staff expertise in cloud security.... 11
- Concerns when running applications in pubic cloud 11

Tools 12
- Network security controls 12
- Tools for Application Orchestration 13
- Sought after benefits in cloud security management tools....14

Cloud Security Incidents And Outages....14
- Cloud-related operational incidents 14
- Outage contributors 15
- Downtime from most disruptive outage....16

Demographics....16
- Industry 16
- Organization Size 17
- Role 18
- Location....18

Survey Creation And Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

AlgoSec, a leading network security solution provider, commissioned CSA to develop a survey to add to the industry's knowledge about hybrid-cloud and multi-cloud security, and to prepare this report of the survey's findings. AlgoSec financed the project and co-developed the initiative by participating with CSA in the development of survey questions addressing hybrid cloud security. The survey was conducted online by CSA from December 2020 to January 2021, and was submitted to nearly 1900 IT and security professionals from a variety of organization sizes and locations. The data analysis was performed by CSA's research team.

Goals of the study

- Understand current and estimated future cloud usage
- Determine the current security concerns during cloud adoption and deployment
- Identify the security tools organizations are using to address security concerns
- Understand occurrences and causes of cloud-related security incidents

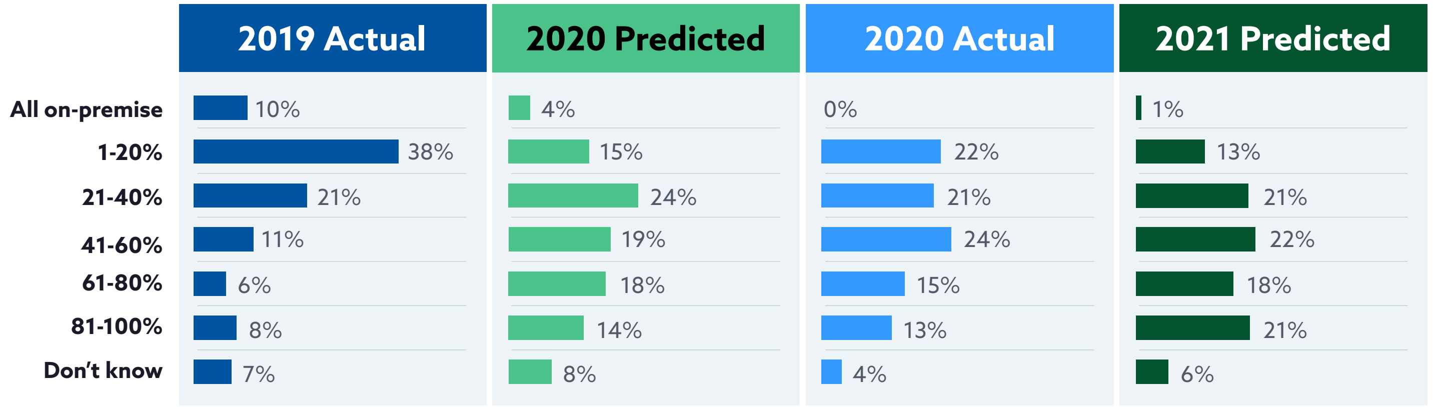
Executive Summary

The use of cloud services have continued to increase over the past decade. Particularly in the wake of the COVID-19 public health crisis, many enterprises' digital transformations are on an accelerated track to enable employees to work from home. CSA developed and distributed a survey to better understand the current cloud security concerns, challenges, and incidents.

Key Finding 1

Organizations are continuing to move to complex cloud environments

Over half of organizations are running 41% or more of their workloads in a public cloud. This is up significantly since 2019, which found that just 25% were running 41% or more of their workloads in public cloud. In 2021, 63% of respondents expect to be running 41% or more of their workloads in public cloud, indicating this trend toward public cloud will only continue. No doubt encouraged by the increase in remote workers due to the recent health crisis.

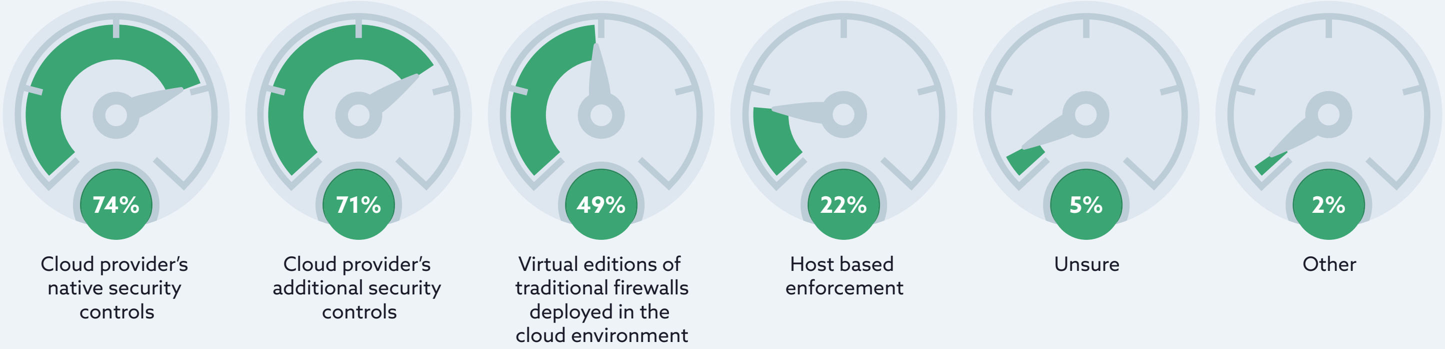


Another survey conducted by CSA in 2020 also indicated that the diversity of production workloads (e.g. container platforms, virtual machines) is also expected to increase. Combine this with the continued use of multi-cloud (62%) found in this current survey and the growing remote workforce, and an ever-more complex cloud environment continues to emerge. This complex environment will inevitably lead to a need for supplementary security tools to improve the organization›s public cloud security.

Key Finding 2

Cloud providers' native security controls are not enough for many organizations

Organizations have increasingly turned to cloud providers' additional security controls and virtual firewalls. The use of cloud providers' additional security controls jumped from 58% in 2019 to 71% in 2021. Approximately half of the organizations turned to third party providers for virtual editions of firewalls for network security controls. This could indicate that while many organizations are moving to public cloud, many are still utilizing legacy and hybrid environments, and need uniform control across many different environments. Additionally, with the current health crisis and the dramatic increase in remote workers, many organizations are unable to secure their network as they have previously and must turn to additional and alternative security controls.



1 Clear visibility (topology, policy) for the entire hybrid network estate (multi-cloud and on-prem)

2 Proactively detect network risks

3 Proactively detect misconfiguration risks (e.g. IAM)

4 Automation, uniform change management across the different security controls

5 Regulatory compliance reports

6 Clean up cloud security controls with excessive rules

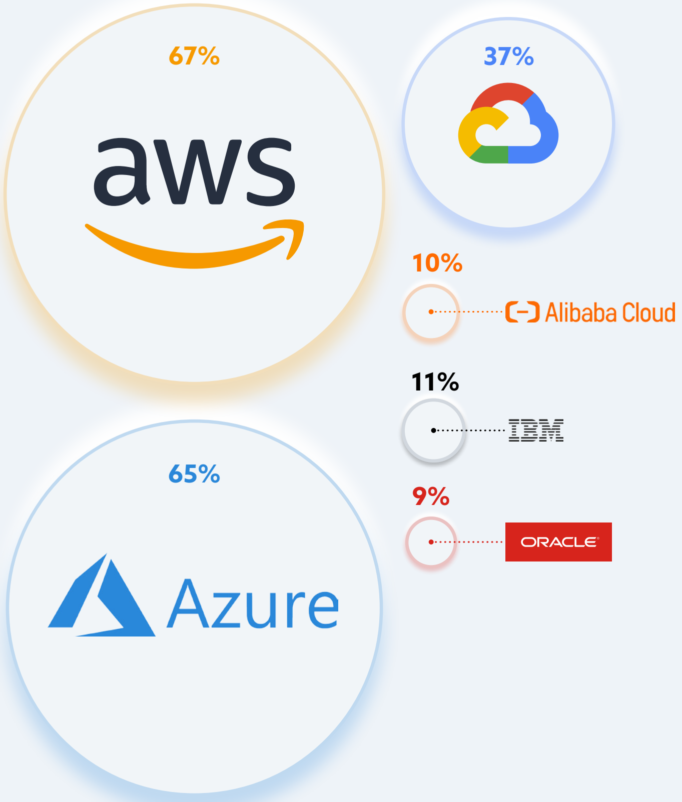
7 Ease of migration of workloads from on-prem to cloud

Key Finding 3

Organizations look for security tools that can supplement their workforce

A complex environment, combined with insufficient security staff and a lack of cloud knowledge, has driven organizations to turn to security tools that can help supplement their workforce. Three of the top four benefits organizations look for in security management tools are for proactive detection of risks and automation. These types of tools can supplement the challenges many organizations are experiencing with lack of expertise (47%) and staff (32%) as well as improve visibility as they move toward an ever-changing cloud environment.

Public Cloud Usage

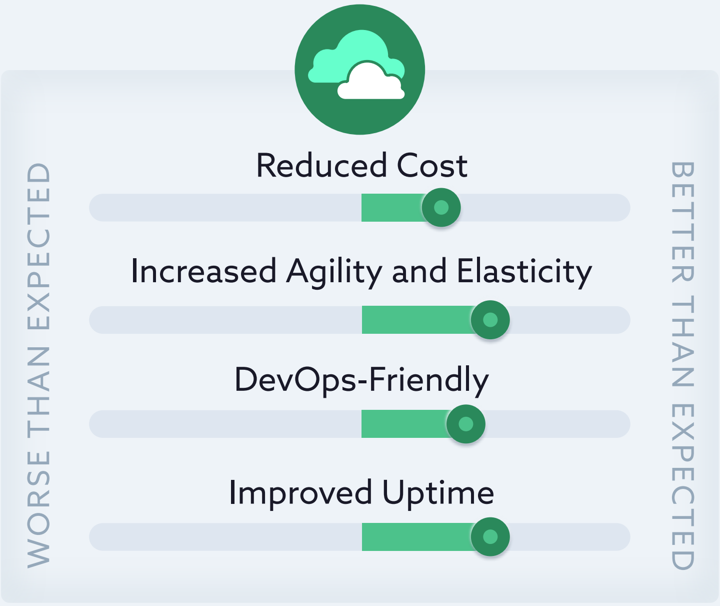


Public cloud platforms organizations are using

There is not one dominant public cloud platform in the market. The market share among the top providers has become more evenly spread. **AWS is used by 67%** of organizations surveyed with **Azure a close second at 65%**. The majority of organizations are also utilizing a multi-cloud strategy (62%) with 27% using three or more public cloud platforms.

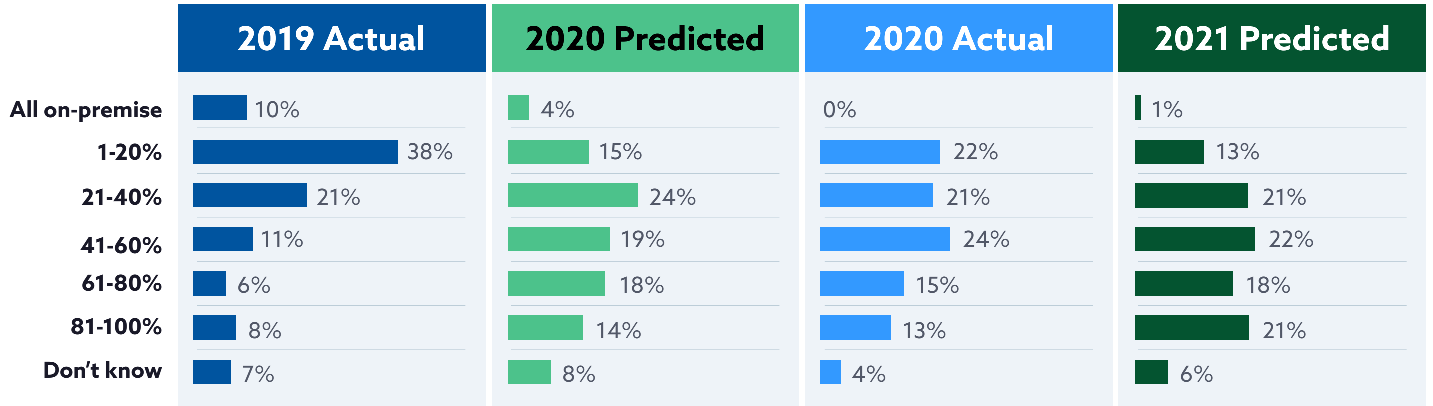
Expectations being met by public cloud

Organizations often migrate to the public cloud due to the promises and expectations made by providers including: reduced cost, increased agility, and elasticity, DevOps-friendly, and improved uptime. On average, organizations are finding that public clouds meet these expectations or even slightly exceed them.



Past, present, and future cloud workloads

Organizations were asked to estimate the percentage of workloads their organization is currently running in the cloud and then predict what they'll be running at the end of 2021.

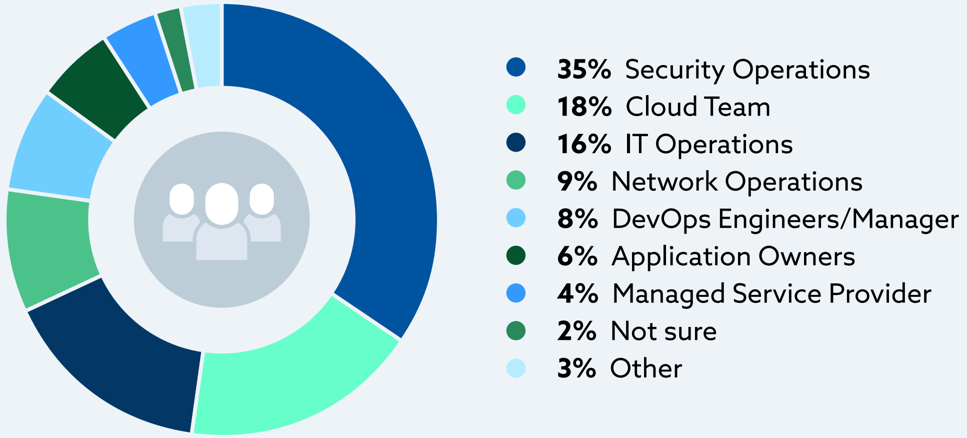


	2019 Actual	2020 Predicted	2020 Actual	2021 Predicted
All on-premise	10%	4%	0%	1%
1-20%	38%	15%	22%	13%
21-40%	21%	24%	21%	21%
41-60%	11%	19%	24%	22%
61-80%	6%	18%	15%	18%
81-100%	8%	14%	13%	21%
Don't know	7%	8%	4%	6%

In our previous survey, we asked a similar question regarding their current workloads in 2019 and predict what they'll be running at the end of 2020. We have included all four estimates in the graph below. When comparing the 2019 actual workloads to the 2020 actual workloads, there are significant increases seen in the ranges 41-60%, 61-80%, and 81-100%. The 1-20% range saw a corresponding decrease although not quite as dramatic as predicted in the previous report. The percentage of organizations in the 21-40% range, on the other hand, remains relatively unchanged, sitting at the 21% mark indicating that it is taking a bit more to get past the 40% mark. Perhaps this is due to a focus on more diverse workloads, which was noted in a previous survey by CSA, rather than the lift and shift method.

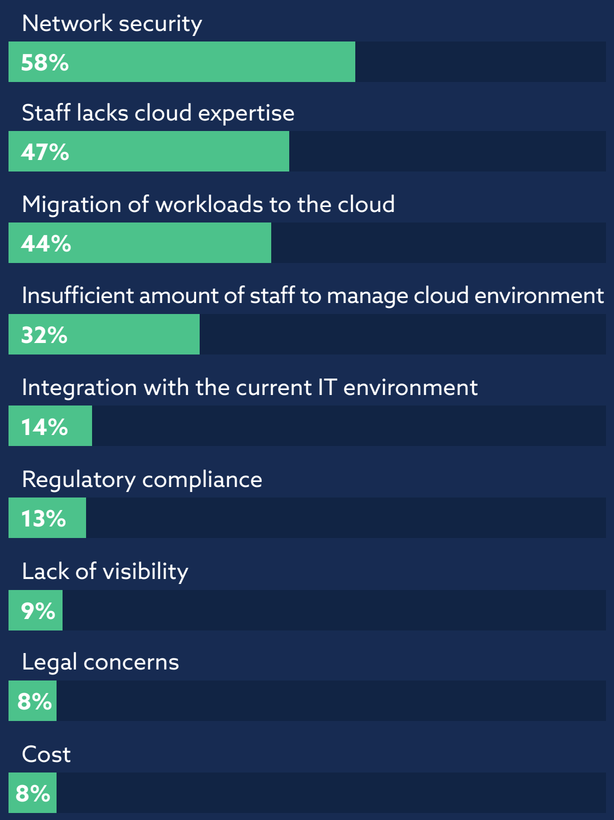
Team responsible for managing security in public cloud

Respondents reported a wide variety of teams who are responsible for managing security in the public cloud. Security operations was the most common response with 35%, followed by the cloud team at 18% and IT operations with 16%. All other teams, including network operations, DevOps engineers/managers, application owners, and managed service providers, all fell below 10%. This is an area where either there is not as much consistency from organization to organization or perhaps confusion regarding which team owns public cloud security.



Cloud Security Concerns

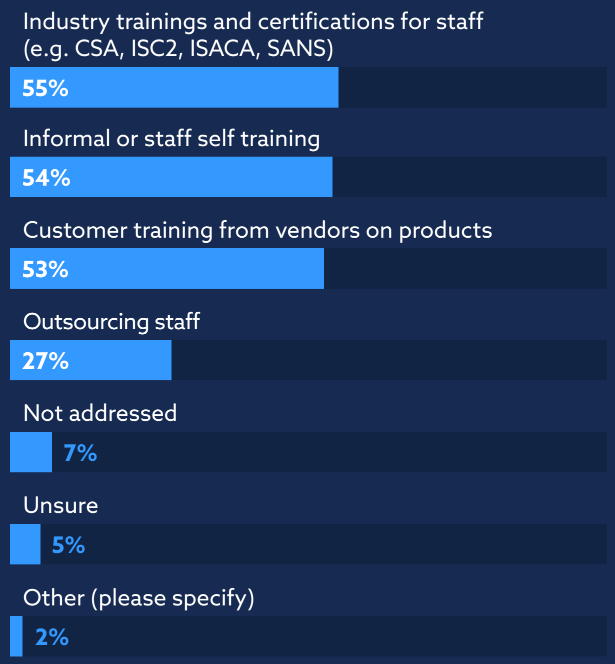
Concerns when adopting cloud



Respondents were asked to select the concerns their organization had while adopting public cloud. The most frequently selected response was **"network security" (58%)**. This was followed by **"staff lack cloud expertise" (47%)**, **"migration of workloads to the cloud" (44%)**, and **"insufficient amount of staff to manage cloud environments" (32%)**. It is worth noting that the second and fourth most commonly selected responses are both related to issues with staff, with a combined total of 79% surpassing the most frequently selected response "network security." In another CSA survey published in 2019, a similar question was asked. A notable shift has occurred as three of the current top four (staff lacks cloud expertise, migration of workloads to the cloud, and an insufficient amount of staff to manage cloud environment) were previously within the bottom four. This rather dramatic shift could be attributed to the current health crisis. Many organizations may be struggling with how to address a largely remote workforce.

Addressing the skills gap in cloud security

The top three ways organizations are addressing the skills gap are **"industry training and certifications for staff" (55%)**, **"informal or staff self training" (54%)**, and **"customer training from vendors on products" (53%)**. Much less commonly selected at 27% was outsourcing staff. The least frequently selected option was "not addressed" at 7%.



Concerns when running applications in public cloud

1 Sensitive data leakage
2 Service outages
3 Configuration and security settings
4 Unauthorized internal access
5 Compliance with regulatory compliance
6 Ransomware
7 Vendor technology vulnerabilities

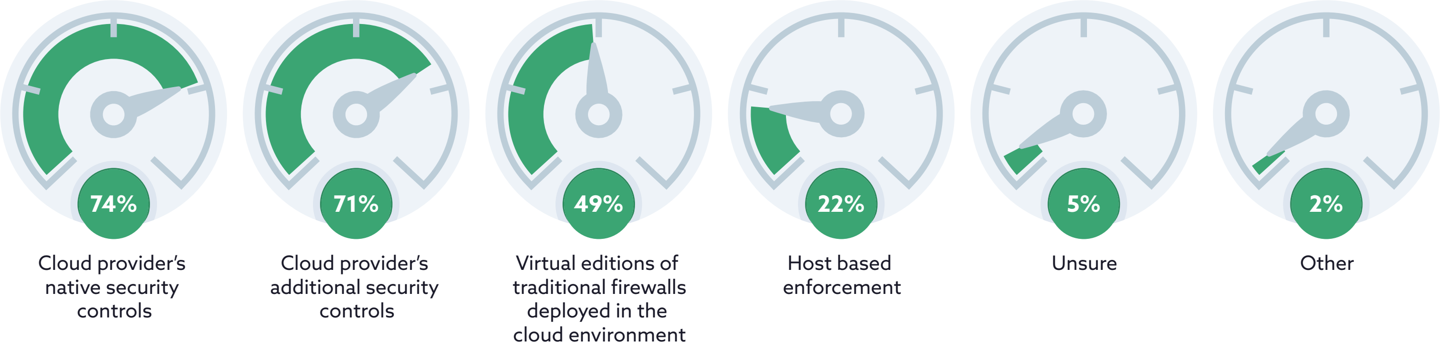
Respondents were also asked about their concerns once applications were running in the public cloud.

On average, the highest ranked security concern was "sensitive data leakage," which is consistent with the previous survey in 2019. "Services outages", "configuration and security settings", "unauthorized internal access", "compliance with regulatory compliance", and "ransomware" received a similar average ranking of about moderate concern. Although "vendor technology vulnerabilities" received the lowest average ranking, it fell just below moderate concern. This was somewhat surprising since the SolarWinds hack was reported while this survey was open. However, even with this issue being more salient, it still was the lowest ranked issue.

Tools

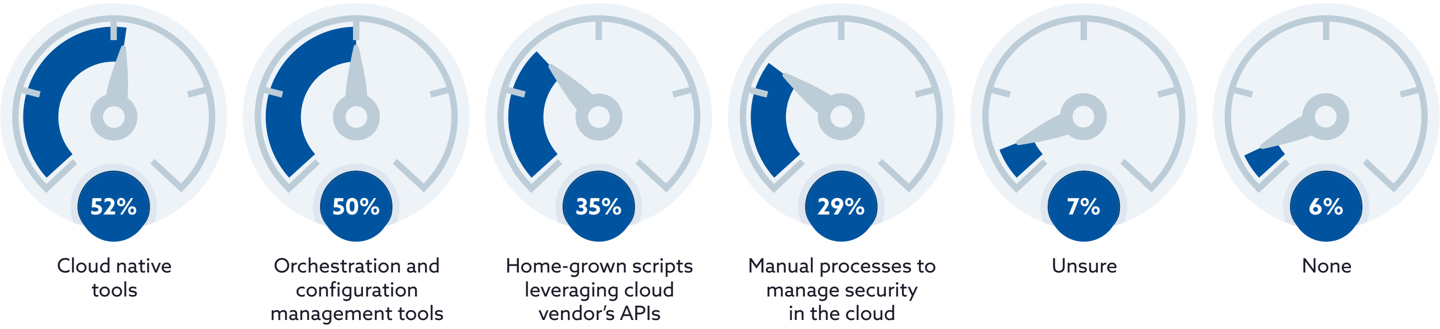
Network security controls

To better understand how organizations were navigating the security of their public cloud deployments, respondents were asked about the network security controls they used. Many respondents reported using a combination of controls. The most commonly selected option was "cloud provider's native security controls" (74%), which remains consistent with a prior survey performed by CSA. A close second was "cloud provider's additional security controls" (71%), which has seen a notable rise from the previously reported 58%. However, nearly 50% of respondents have found these methods alone insufficient and have turned to 3rd party's "virtual editions of traditional firewalls."



Tools for application orchestration

Security management can take many forms within security application orchestration. Respondents were asked about the tools they currently use to manage security as part of their application orchestration process. Over half of respondents reported using cloud native tools (52%) and orchestration and configuration management tools (50%). Around a third reported using home-grown scripts (35%) and manual processes to manage security (29%).



Sought after benefits in cloud security management tools

1 Ease of migration of workloads from on-prem to cloud

2 Clean up cloud security controls with excessive rules

3 Regulatory compliance reports

4 Automation, uniform change management across the different security controls

5 Proactively detect misconfiguration risks (e.g. IAM)

6 Proactively detect network risks

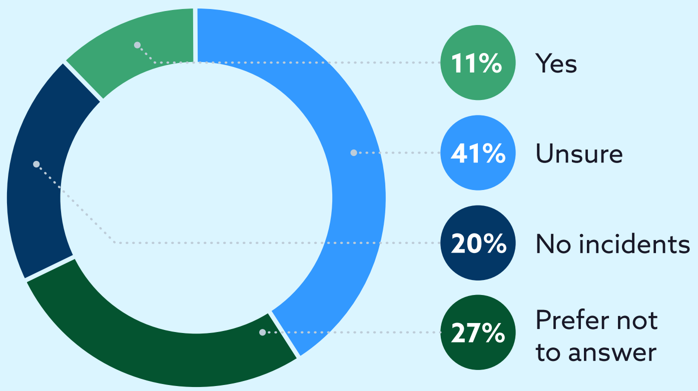
7 Clear visibility (topology, policy) for the entire hybrid network estate (multi-cloud and on-prem)

When asked about the benefits they look for in security management tools, the top ranked response was visibility. This has been a common complaint with regards to cloud environments, especially with the popularity of hybrid and multi-cloud environments. Closely following visibility was the ability to proactively detect network risks and proactively detect misconfigurations. Respondents then ranked automation of uniform change management across different security controls and regulatory compliance fourth and fifth, respectively. The tools that organizations are looking for largely supplement their current challenge with a lack of staffing and cloud expertise.

Cloud Security Incidents and Outages

Cloud-related operational incidents

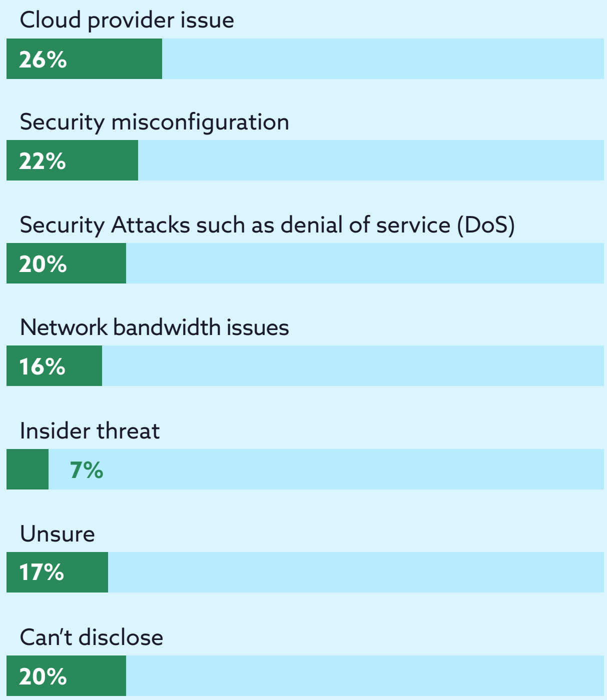
Many organizations attempt to prepare for security incidents, such as breaches and outages. When asked whether their organization had experienced a cloud-related operational incident in the last 12 months, 11% reported definitively having a security incident, 20% reported no incidents, and 27% preferred not to answer. However, the most common response was unsure with 41%, which is a significant change from the 2019 survey in which only 18% didn't know whether an incident had occurred. Equally as interesting, the percentage of respondents reporting that they have had an incident (11%) has remained consistent from the 2019 survey.



Respondents were also asked to report the number of incidents that they experienced, with the average response being five. This seems relatively low when considering that large cloud platforms have many incidents throughout the week, although many may not be disruptive enough to significantly impact users.

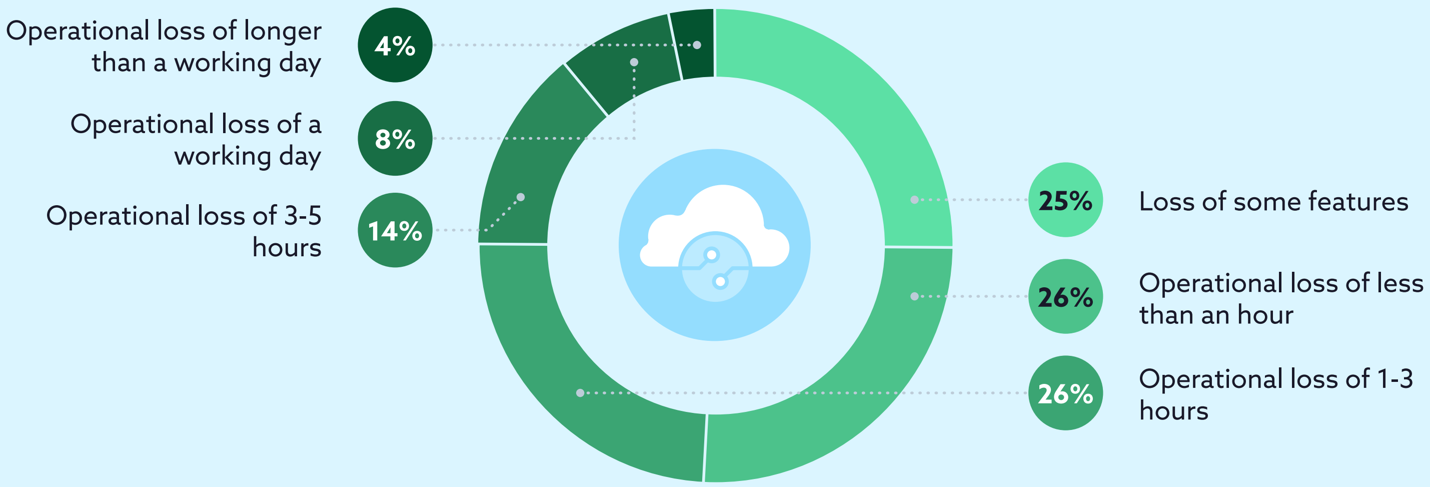
Outage contributors

Following the question about the number of incidents, respondents were asked about the main contributors to these incidents. The most common response was cloud provider issues (26%), followed by security misconfiguration (22%), and security attacks such as denial of service (20%). Less commonly selected were network bandwidth issues (16%) and insider threat (7%). Several of the top contributors can be tied back to human error or misconfiguration, which is very likely due to the lack of staffing and expertise that organizations are currently grappling with.



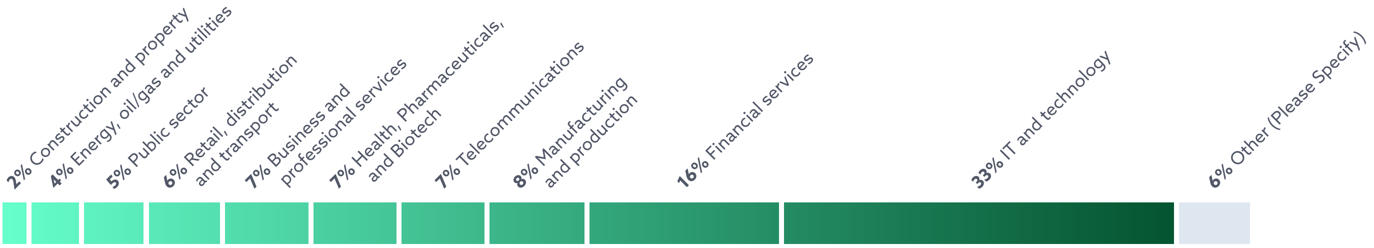
Downtime from most disruptive outage

Respondents were also asked about the impact of the most disruptive cloud outages. For over 25% of respondents it took longer than three hours to restore normal operations. This has remained consistent with the 2019 survey which had similar results. It is concerning that such disruptive outages continue to plague the industry and cost organizations considerable financial and productivity loss.



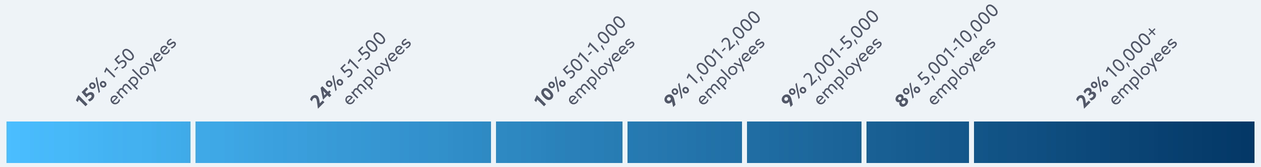
Demographics

This survey was conducted from December 2020 to January 2021 and gathered 1900 responses from IT and security professionals from a variety of organization sizes, industries, locations, and roles.



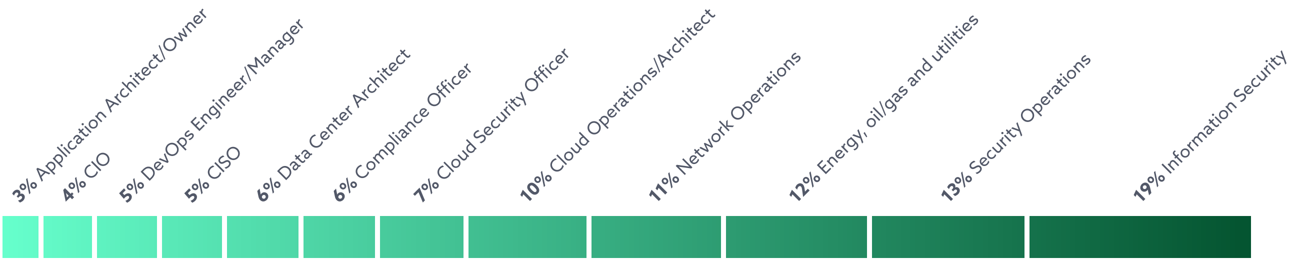
Industry

What industry does your organization belong to?



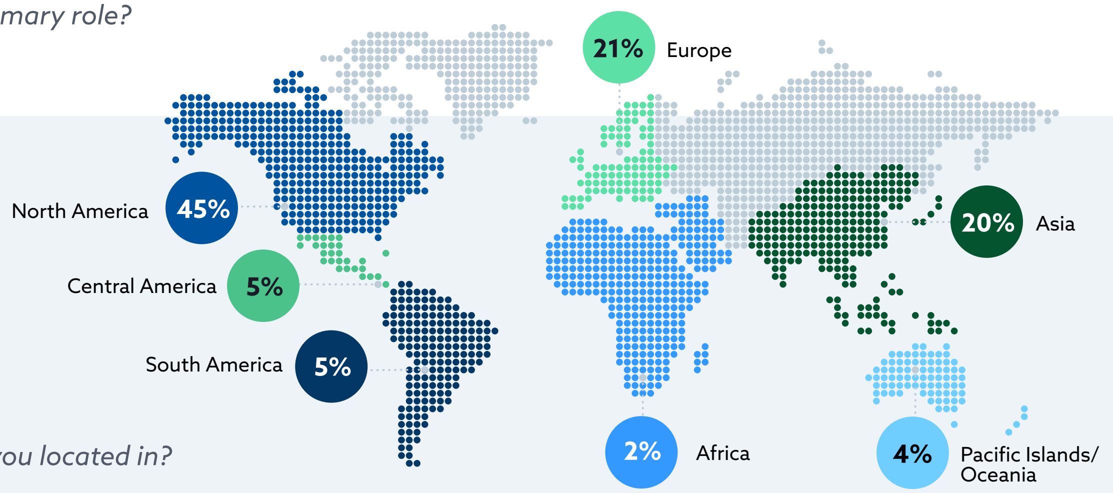
Organization Size

What is the size of your organization?



Role

What is your primary role?



Location

What area are you located in?

About Algosec

The leading provider of business-driven network security management solutions, AlgoSec helps the world's largest organizations align security with their mission-critical business processes. With AlgoSec, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch – across their cloud, SDN and on-premise networks. Over 1,800 enterprises, including 20 of the Fortune 50, have utilized AlgoSec's solutions to make their organizations more agile, more secure and more compliant – all the time. Since 2005, AlgoSec has shown its commitment to customer satisfaction with the industry's only money-back guarantee.

Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.