Deconstructing Application Connectivity Challenges in a Complex Cloud Environment

CSA cloud security alliance®

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Ryan Gifford
Frank Guanco
Sean Heide
Alex Kaluza
John Yeoh

Designer

Claire Lehnert

Special Thanks

Ami Streit, Marketing Content Lead, AlgoSec

Table of Contents

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 cybersecurity in cloud computing and IT technologies. CSA also educates 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 provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

AlgoSec commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding application connectivity security in the cloud. AlgoSec financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in August 2022 and received 1551 responses from IT and security professionals from organizations of various sizes and locations. CSA's research analysts performed the data analysis and interpretation for this report.

Goals of the Study

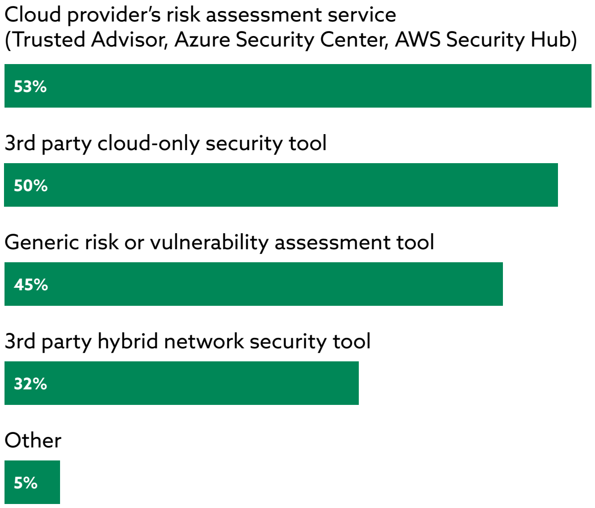
The goals of this study were to understand the following:

- Application connectivity security and risk management
- Application orchestration
- Use of cloud security solutions
- Security incidents over the past year

Key Findings

The production and use of SaaS applications in organizations has grown exponentially over the past several years. Application Security has become an integral part of many organizations' security strategies. However, there are still many pain points organizations face with application connectivity security and risk management.

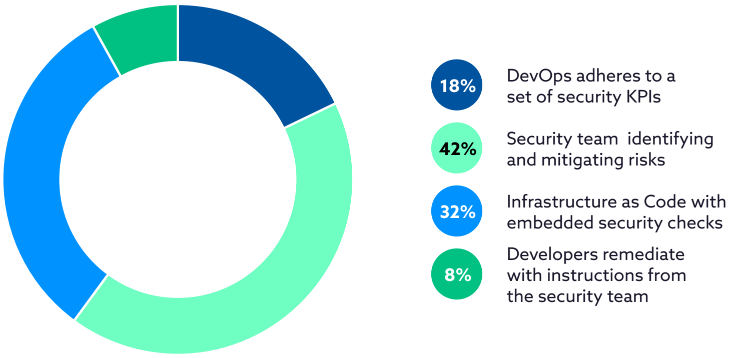
Key Finding 1:
Managing risk for application connectivity is a complicated task



In a 2022 CSA survey found that organizations struggle with risk management in general and application connectivity is no exception. Organizations are utilizing many different tools in order to help manage their application connectivity risk. Fifty-three percent of organizations use a cloud provider's assessment service, half use a third-party cloud-only tool, another 45% use a generic risk or vulnerability assessment tool and approximately 1/3 use a third-party hybrid network security tool. In part this is due to the complex SaaS environments organizations operate within, but it may also be in part with a lack of satisfaction with a single tool. Organizations are trying to use multiple methods to get similar information which can become confusing when there is not a single source of truth for teams to work from.

Key Finding 2:
Managing application connectivity risks in the deployment process is changing

The complexity of managing risk doesn't stop with the tools, it is further complicated with who and how application connectivity risks are managed. Traditional security teams are responsible for identifying and mitigating risk and this still holds true for 42% of organizations. However, there is a shift happening: 32% of organizations utilize infrastructure as code with embedded security checks suggesting organizations are beginning to use more automation which leaves less room for human error. Another 26% have their developers involved either by having DevOps adhere to a set of security KPIs or having developers remediating risk with instructions from the security team. This suggests that organizations are beginning to embrace a DevSecOps or shift left model.

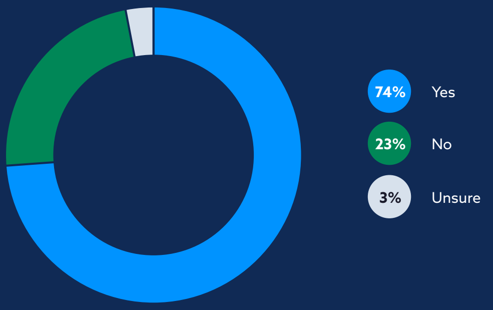


Key Finding 3:

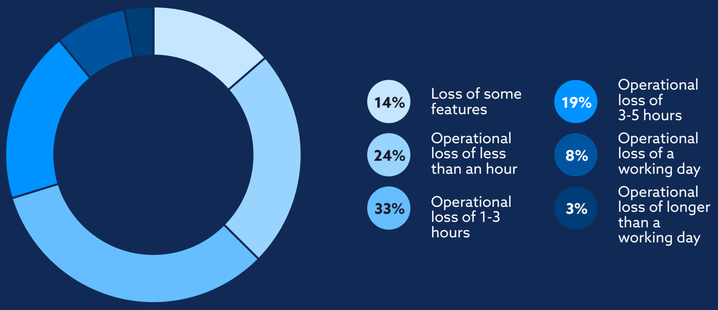
Human error is leading to significant application downtime

Nearly 3 out of every 4 organizations have experienced an application outage in the past 12 months. These disruptions impact 63% of those organizations for more than an hour. According to Gartner, average cost of downtime is $5,600 per minute and about $300,000 per hour. These outages have an impact on organizations bottomline. It also appears that these outages are on the rise. A survey CSA conducted in 2021 found that 52% of organizations had cloud incidents that caused operational loss of over an hour. While not a perfect comparison, it does indicate a general increase in the impact of these incidents. Understanding these causes of these incidents can help organizations to take control and address the outages head on.

Application outage in the last 12 months

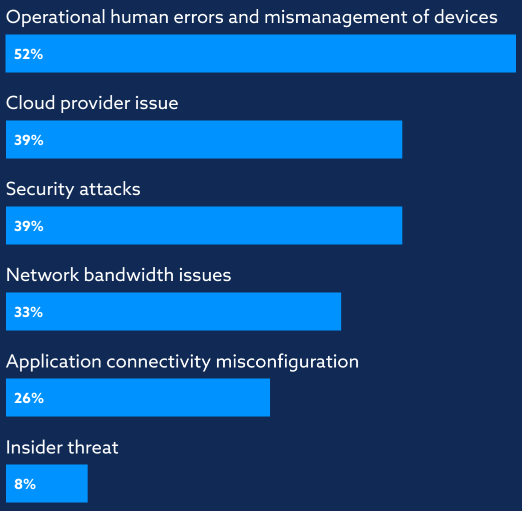


Impact of the most disruptive application downtime



The primary cause for over half (52%) of the outages was operational human error and mismanagement. This is unsurprising as the skills gap has plagued the information security industry. It's clear that a lack of knowledgeable staff can lead to errors. However, this skills gap can also lead to knowledgeable professionals to become stressed and overworked with fewer people shouldering the workload which also leads to errors. To prevent outages caused by human error, organizations need to supplement their workforce with tools such as automation. Use of automation will reduce the workload for staff and allow them to focus less on monotonous and more on more complex issues.

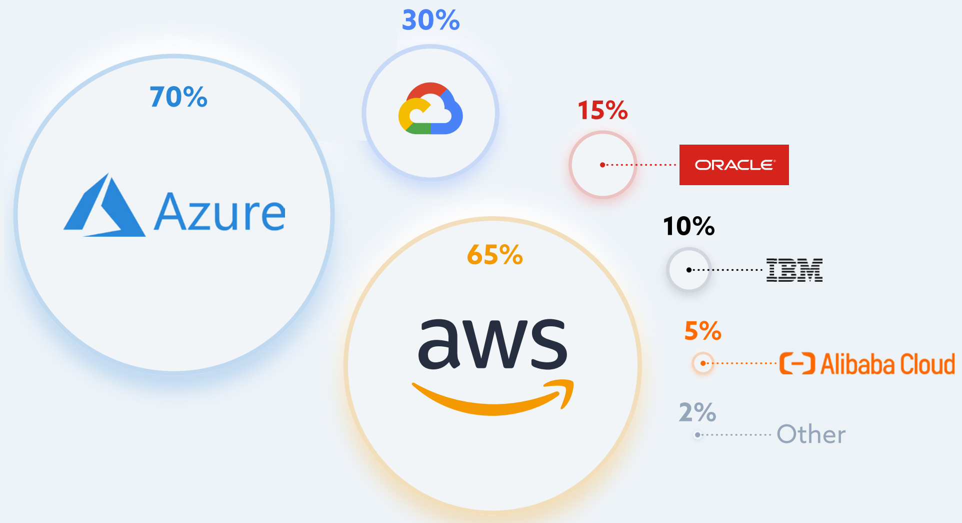
Main contributors(s) to the application outage



Overview

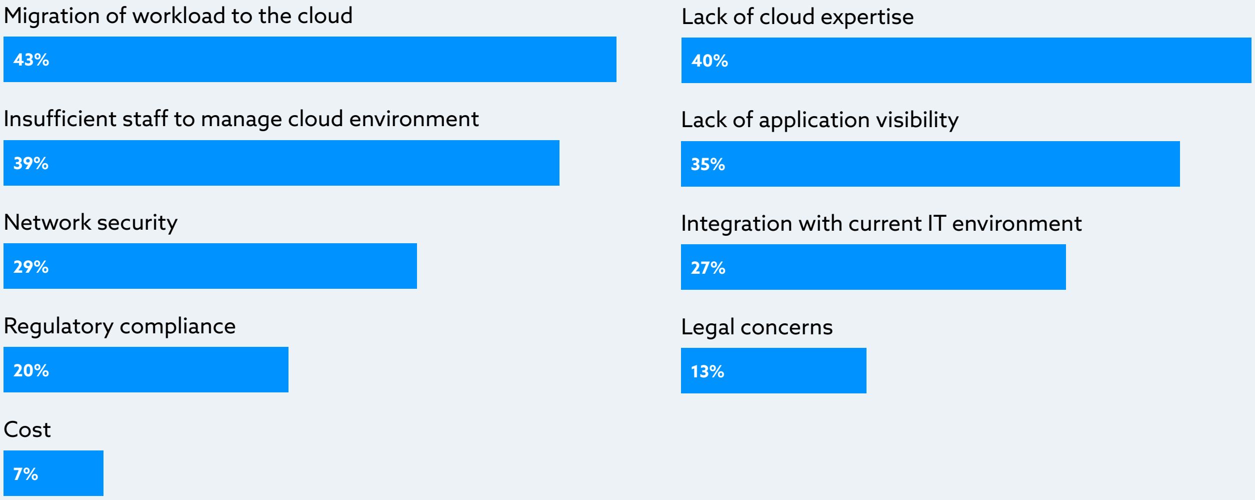
Cloud service providers companies use

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 65% of organizations surveyed with Azure slightly higher at 70%. This also indicates that organizations are continuing to deploy a multi-cloud strategy in their organizations, an observation noted in a 2019 and 2021 CSA survey report.



Areas most impacted by the skills gap

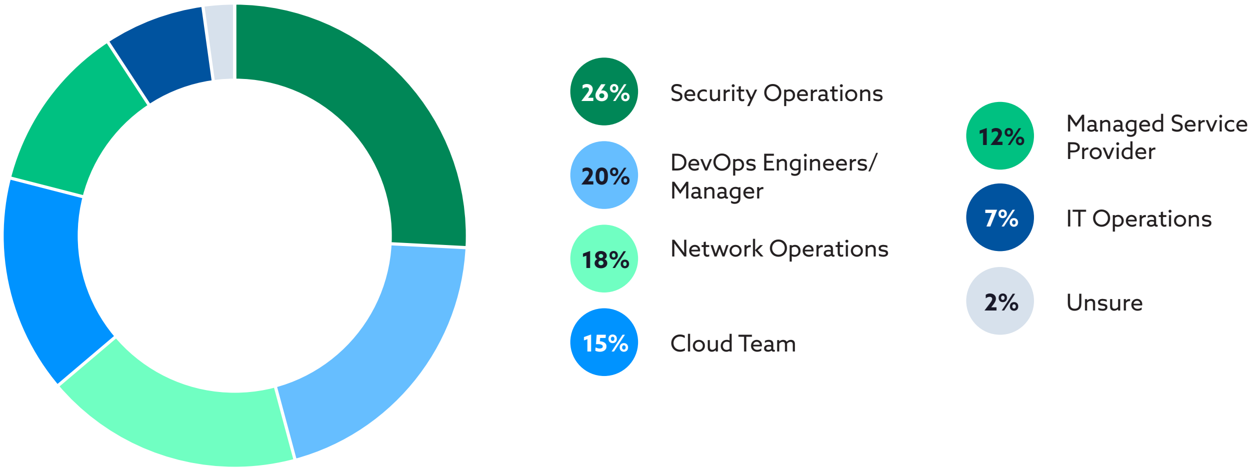
The skills gap in the information security industry is well known. Overwhelmingly cloud knowledge and skills are being impacted, comprising the top three areas of impact. In particular, organizations see migration of workload to the cloud (43%), lack of cloud-specific expertise (40%), and insufficient staff to manage cloud environments (39%) impacted in their organizations.



Cloud-based Applications

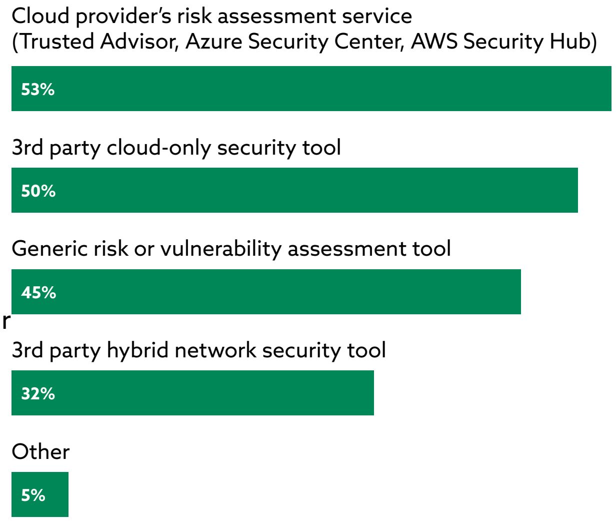
Primary team responsible for securing application connectivity in public cloud applications

Application security teams (26%) are often embedded within security operations teams making it the most common team to be responsible for securing application connectivity in public cloud. These teams are also frequently responsible for the overall public cloud security as found in a 2021 CSA survey report making applications in public cloud a natural extension of their duties. Another common group that is held responsible is the DevOps teams (20%) which indicates a shift toward the DevSecOps or shift left strategies that have grown in popularity.



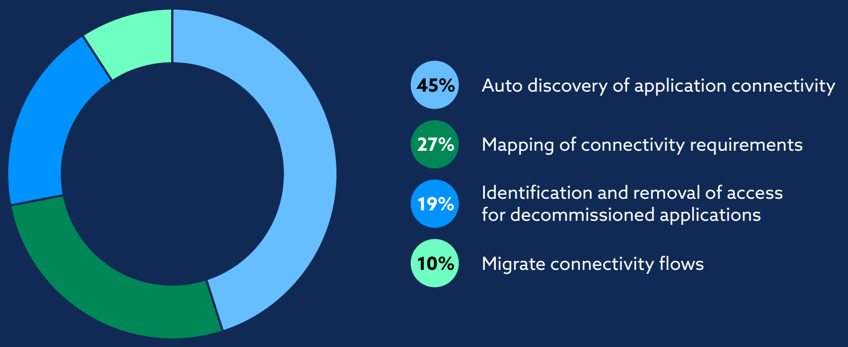
Managing risk for application connectivity

With respect to managing risk for application connectivity, organizations are focused on cloud tools rather than on-premises, indicating that organizations are favoring cloud applications. This finding is likely driven by the large number of smaller organization respondents (<500 employees) who tend to favor cloud over on-premise.



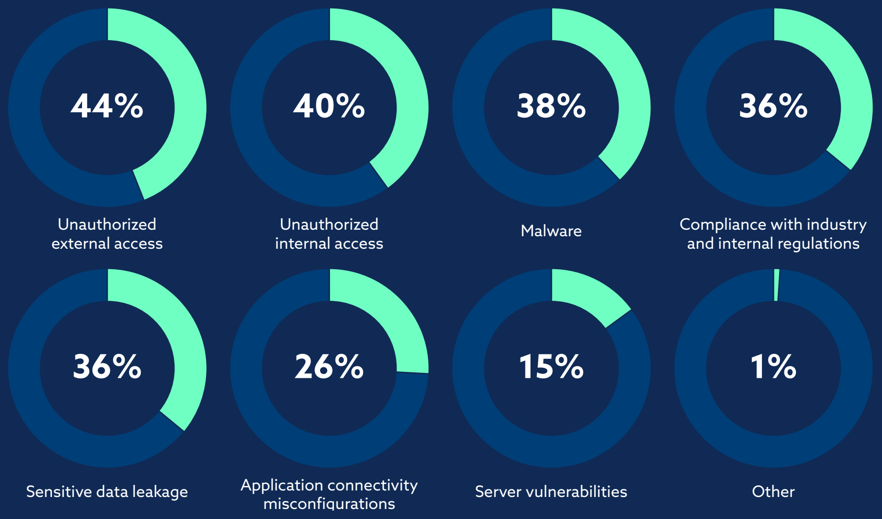
Priority ranking of application connectivity security features

Auto discovery (45%) was the most desirable feature in securing application connectivity. This is likely because auto-discovery is the first step in the process and allows organizations to address the other lower ranked items like mapping of connectivity requirements (27%), and identify and remove access for decommissioned applications (19%). Without auto-discovery organizations cannot move to those steps.



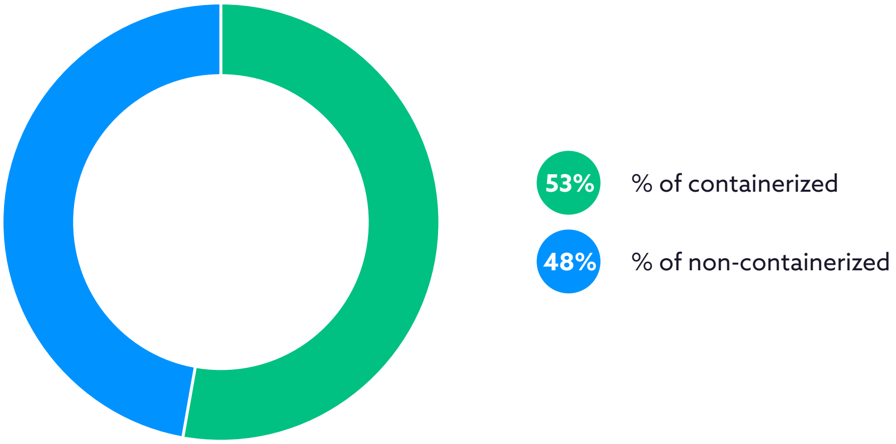
Top security concerns about application running in public cloud

The primary concerns organizations have about applications running in public cloud are centered around unauthorized access, both external (44%) and internal (40%). Another top concern is malware (38%), this is unsurprising as malware, in particular ransomware, has been a top concern for organizations. Malware can also lead to unauthorized external access and data loss. Interestingly, sensitive data leakage (36%) was much lower in the list, but this is likely because it can't happen without some form of unauthorized access. Similarly misconfigurations in application connectivity were rated lower (26%), but again this is likely because organizations are most concerned about the outcome i.e. authorized access.



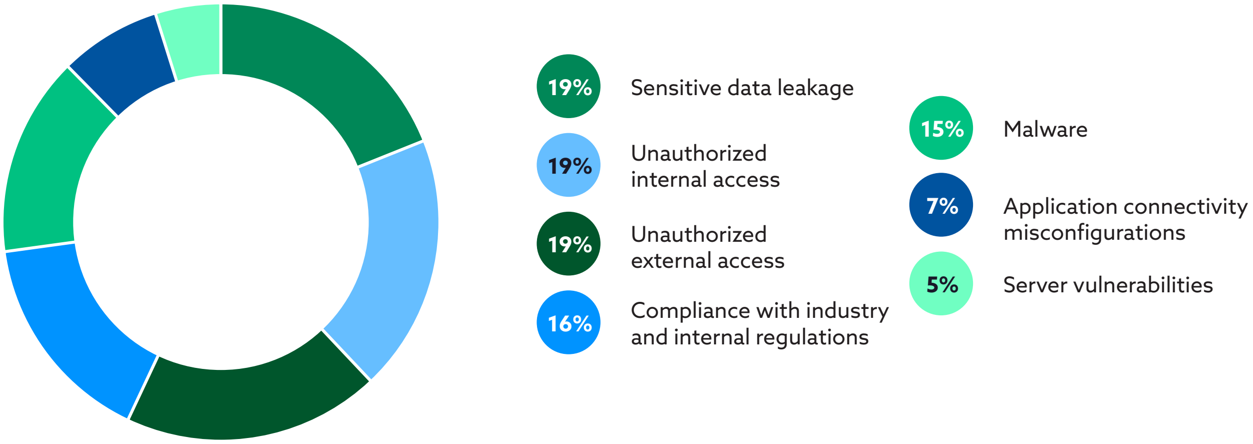
Applications secured using containerized vs non-containerized technology

In this 2020 CSA survey, organizations predicted a significant increase in their use of container platforms. This is likely to support the trend toward DevSecOps and shift left strategies. On average, organizations are roughly split in half with the applications secured using containerized (53%) and non-containerized (48%) technology.



Top concerns about container-based solutions

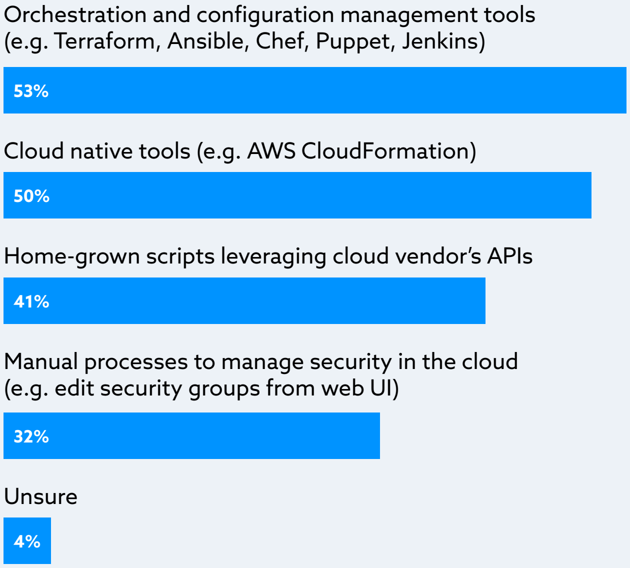
Although organizations are using containerized technology, they are not devoid of any concerns. The top concerns organizations include sensitive data leakage (19%), unauthorized internal access (19%), and unauthorized external access (19%). In many ways this mirrors the overall concerns about running applications in public cloud.



Tools and Technology

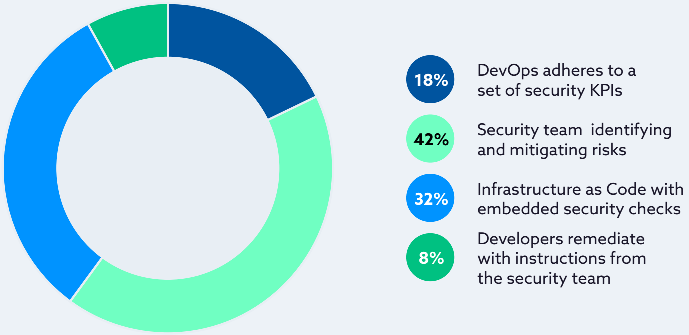
Tools for managing application orchestration process in public cloud

When it comes to managing application orchestration in public cloud, organizations utilize a combination of tools. The most commonly used tool is 3rd party tools (53%) followed closely by cloud native tools (50%). Slightly less common, but still popular is home-grown scripting (41%) which leverage cloud vendor APIs. These organizations are likely building their services rather than purchasing.



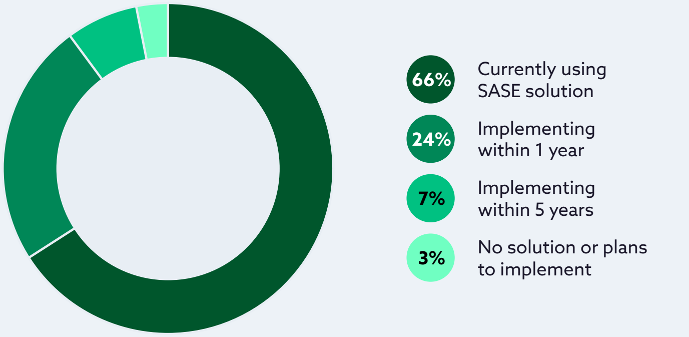
Managing application connectivity risk in the deployment process

The security team is the primary team tasked with managing application connectivity risk (42%) which is to be expected as it follows a traditional DevOps model. However, it is notable that "Infrastructure as code with embedded security checks" (32%) and "DevOps adheres to a set of security KPIs" (18%) are second and third, as they indicate use of automation and that shift left and DevSecOps strategies are being embraced.



Current and future use of SASE Solution

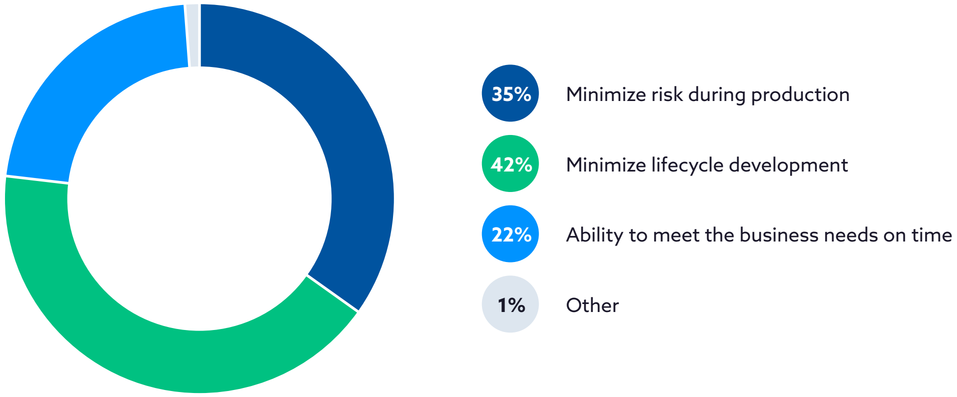
The majority of organizations are already using a Secure Access Service Edge (SASE) solution (66%) or plan to use a SASE solution (31%). Only 3% of organizations report no plans to implement this type of solution.



DevOps

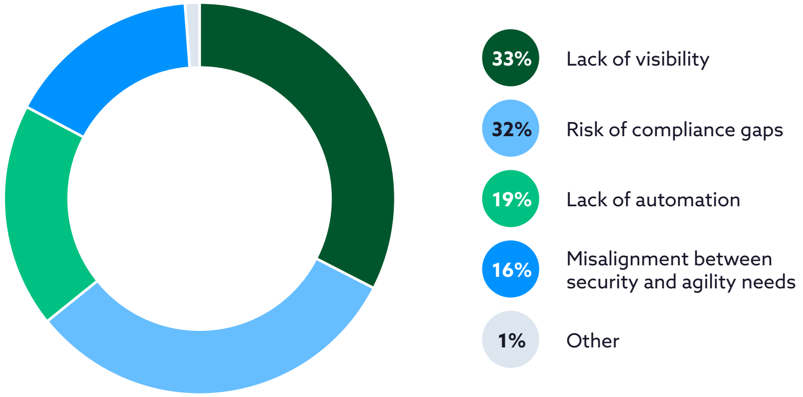
Value of identifying risk during configuration development stage

The top value organizations experience because of identifying risk during configuration development stage is minimizing lifecycle development (42%). This is followed by minimizing risk during production (35%) and ability to meet business needs to time (22%). All of it ties back to integrating security rather than a separate step and potential barrier.



Constraints for application rolling out on schedule

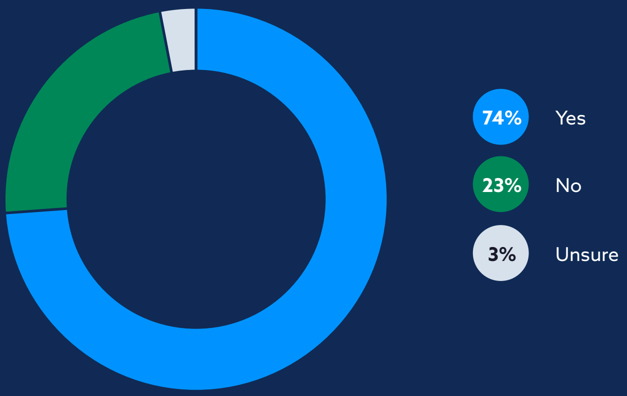
The primary constraint organizations face when rolling out an application is the lack of visibility (33%). If security isn't aware of the project, their involvement will come late in the process, which could hold up critical application roll out deadlines. A similar issue can occur for risk and compliance gaps (32%). To a lesser degree lack of automation (19%) and misalignment between security and agility needs (16%) also hold up the roll out of an application.



Security Incidents

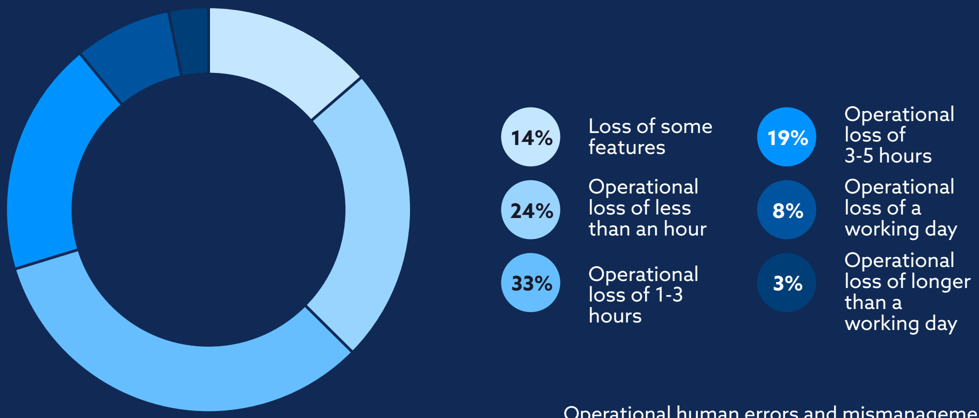
Application outage in the last 12 months

The majority of organizations have experienced an application outage in the past 12 months (74%). Only 23% reported they had not.



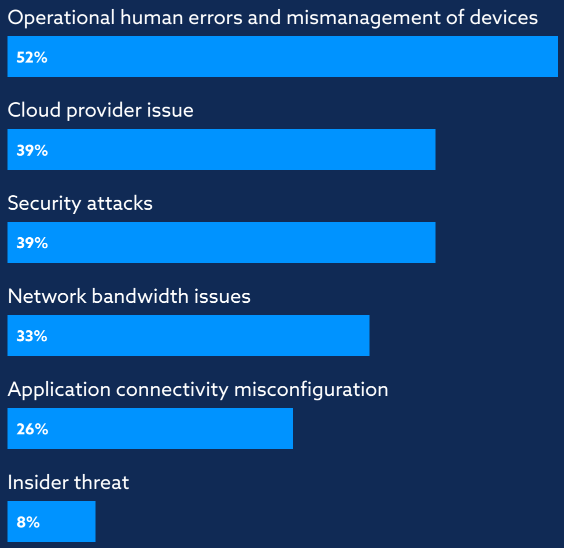
Operational time loss during most disruptive application downtime

For 63% of organizations their most disruptive application downtime was longer than an hour. This can have a serious financial impact on organizations' bottom line. According to Gartner, average cost of downtime is $5,600 per minute and about $300,000 per hour. It also appears that these outages are on the rise. A survey CSA conducted in 2021 found that 52% of organizations had cloud incidents that caused operational loss of over an hour. While not a perfect comparison, it does indicate a general increase in the impact of these incidents.



Main contributor to application outage

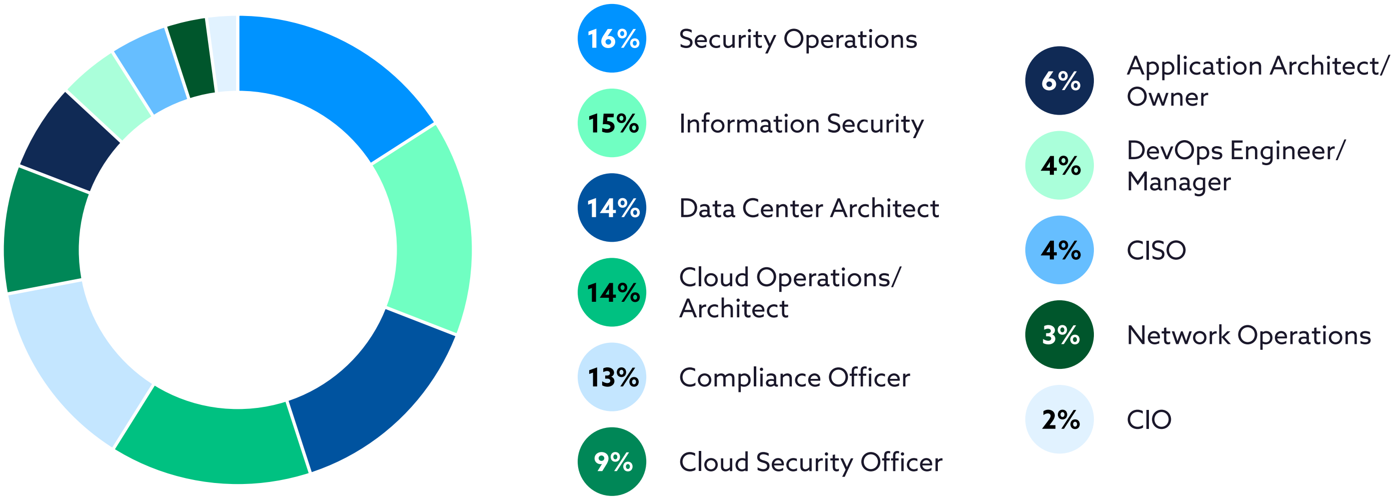
The top reason organizations experience an application outage was because of operational human error and mismanagement (52%). This is likely in part due to the skills gap which impacts cloud knowledge and skills. Lack of knowledgeable staff and stressed knowledgeable staff is going to inevitably lead to error. However, these outages prevent the implementation of automation. Other common contributors included CSP issues (39%) and security attacks (39%).



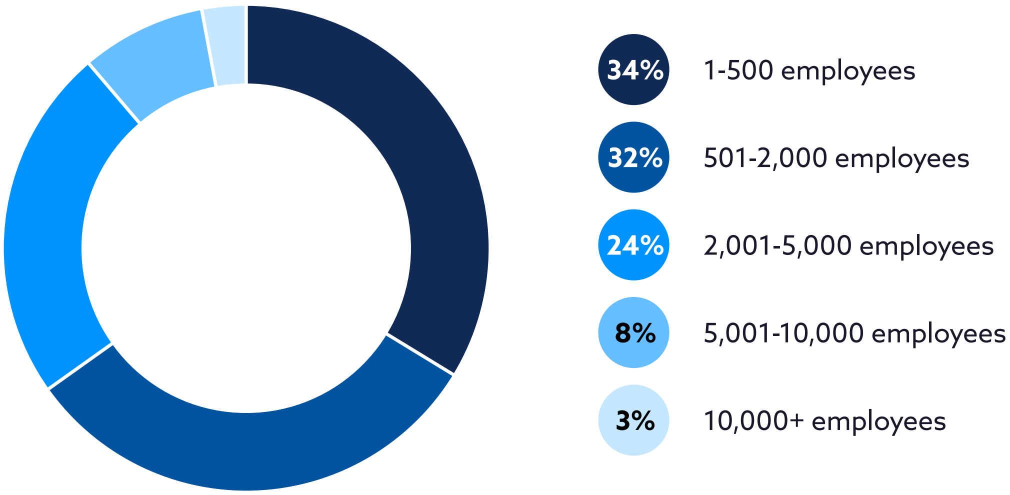
Demographics

This survey was conducted in August 2022 and gathered 1551 responses from IT and security professionals from organizations of various sizes, industries, locations, and roles.

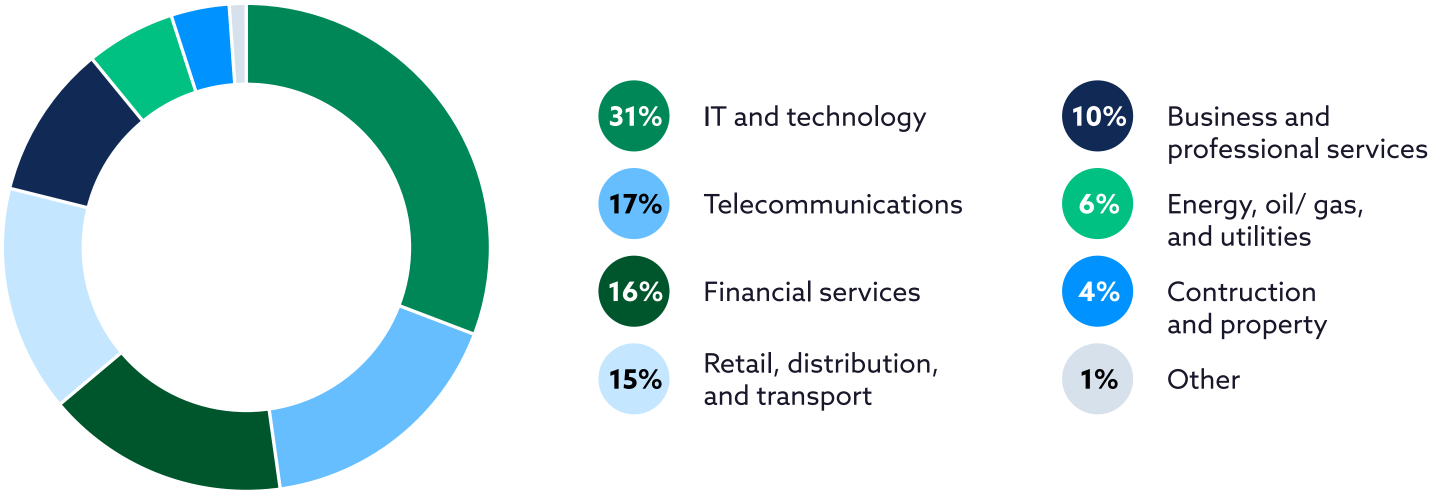
What is your primary role?



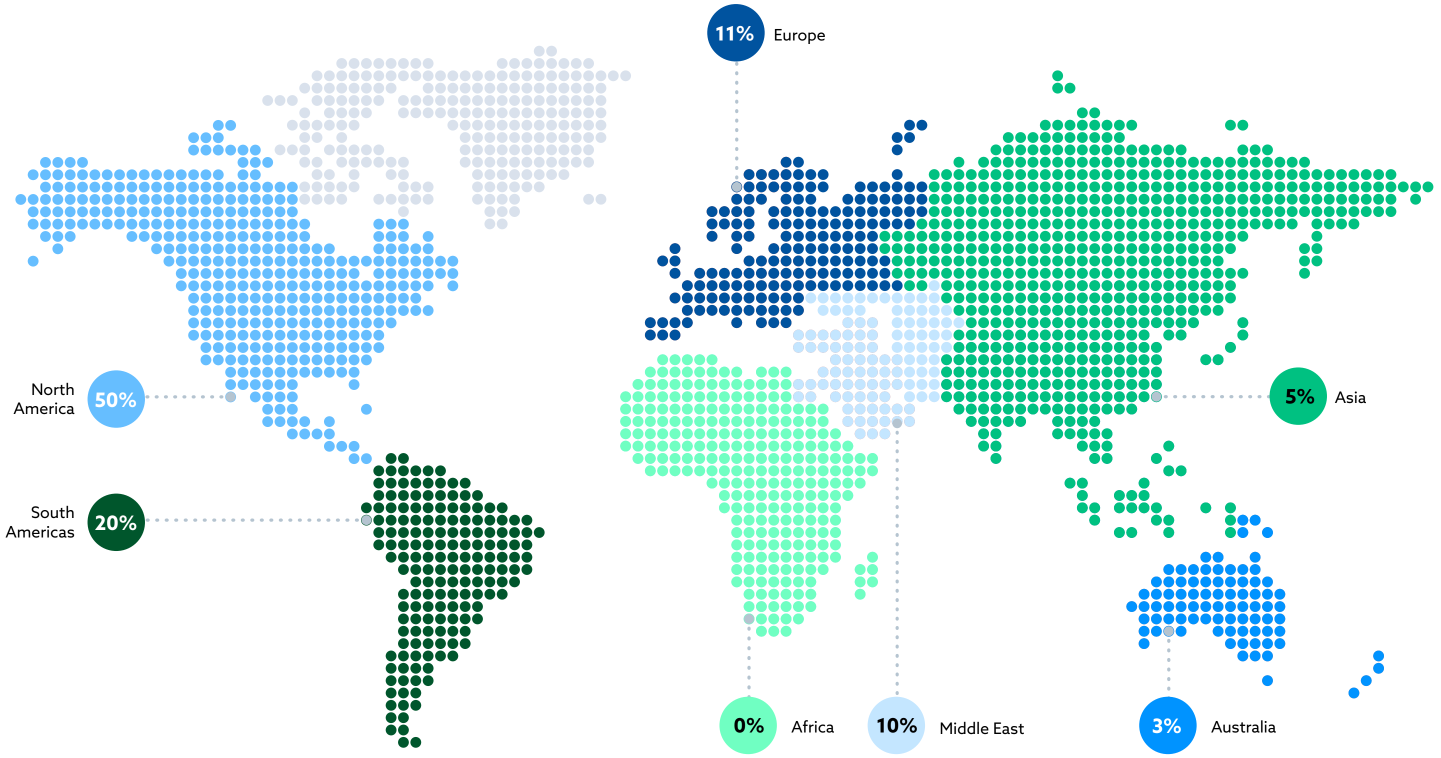
What is the size of the organization you work for?



Industry



What region are you located in?


11% Europe
North America 50%
South Americas 20%
5% Asia
0% Africa
10% Middle East
3% Australia