State of Infrastructure Access and Security Report

2022

Teleport

2022 State of Infrastructure Access and Security Report

Executive summary

Over the past three years, organizations across the world have experienced fundamental changes in how they build and run applications, access their infrastructure, and communicate within and across teams. While these changes have been underway for years, the Covid-19 pandemic dramatically accelerated their pace.

Converging dynamics including an industry-wide movement to the cloud, cloud-native and microservices architectures, and widespread work-from-home models have created a perfect storm for DevOps, security engineering and other security professionals trying to protect their organization's infrastructure and assets. Employees are using personal devices to access sensitive information from home, and businesses are relying on third-parties to provide critical development and support services in an effort to cut costs. At the same time, employee and contractor turnover has increased significantly, with each personnel change carrying the possibility that a former team member maintains access to something they should not. Amid all this complexity, organizations are still too dependent on secrets like passwords, keys and tokens to protect their infrastructure. Secrets, the number one source of data breaches, are always at risk of being shared, lost or stolen, and they cannot be relied on as part of an effective security posture — yet they are still widely used.

The *2022 State of Infrastructure Access and Security Report* seeks to understand the specific challenges facing DevOps, security engineering and other security professionals. Using survey data collected by Schlesinger Group, an independent research company, from 500 respondents,

the report offers a representative sample of the common beliefs and observations shared by industry professionals, as well as the actions they take to keep their organizations safe. More information on the survey methodology can be found at the end of the report.

Key findings

The report uncovers significant trends in the fields of DevOps, security engineering and information security:

- **Organizations are at serious risk from messy breakups:** Less than a quarter (24%) of respondents are fully confident that ex-employees no longer have access to company infrastructure.

- **Access management is becoming more complex — with no signs of slowing down:** Organizations use on average 5.7 different tools to manage access policy, making it complicated and time-consuming to completely shut off access.

- **Security leaders want to move past secrets, but may not be ready to take the next step:** Secrets still represent the most common way of providing access, with 80% of respondents reporting that they still use passwords as a security method. But there is hope for a future without secrets, as more than three-quarters (87%) of respondents are actively moving towards passwordless access. Biometrics make it possible for organizations to move beyond secrets, but 62% of respondents cite privacy concerns as their biggest challenge when adopting biometrics.

- **Despite awareness of the problems, organizations are struggling to adapt:** More than half (57%) of respondents said their organization has implemented new security methods that failed to be adopted by employees.

- **Security spending is on the rise:** Despite economic uncertainty, 85% of respondents say their security spending increased within the last 12 months, indicating that organizations recognize the critical importance of solving the security challenges highlighted in this report.

Analysis of key findings

DevOps, security engineering, and other security professionals are clear on the challenges they face, as well as the best tools for meeting those challenges. For many organizations, the biggest roadblock to success is the employees themselves. Without security practices that are easy to implement and follow, engineers and other individuals accessing critical applications and infrastructure are more likely to stick with what they know and prioritize convenience over safety.

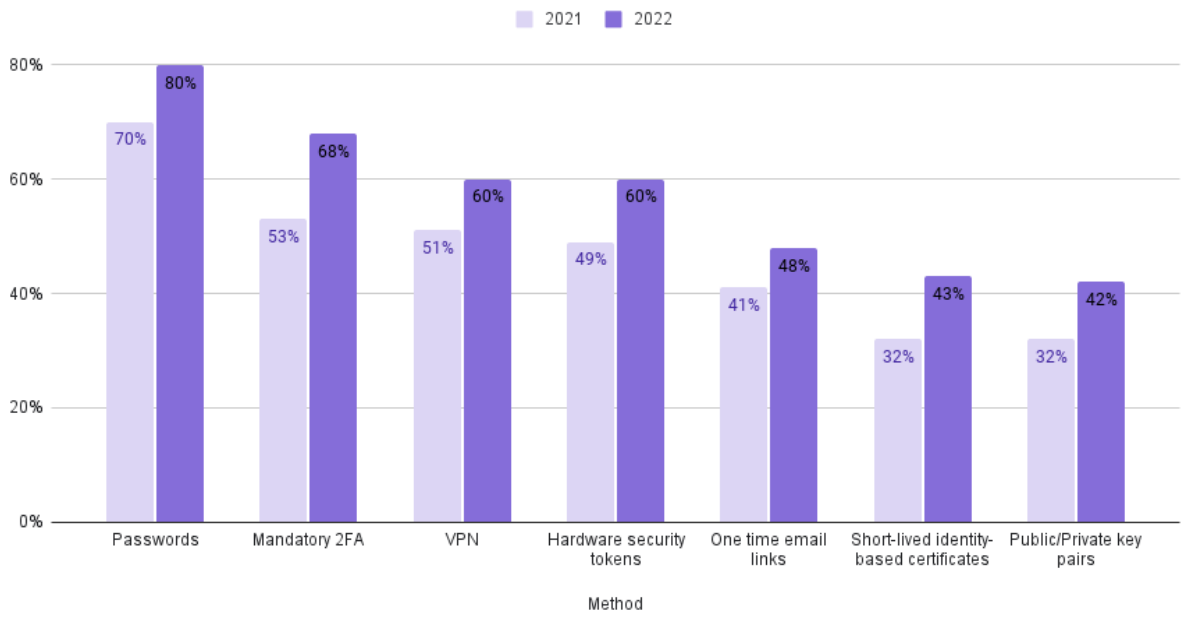
The *2022 State of Infrastructure Access and Security Report* finds that even those with good intentions struggle to make positive changes, particularly regarding the urgency with which they move towards secretless infrastructure access. However, survey responses show that we may soon reach a tipping point, as increased security budgets are applied to new secretless security methods..

Access controls are becoming more complex

One year ago, the *2021 State of Infrastructure Access and Security Report* highlighted the incredible diversity of technology architectures and locations organizations use to run applications. This year's survey dug into how this complexity is managed, and the answer reveals a troubling trend towards what we call “access silos.”

Last year's survey highlighted that a typical organization runs applications across multiple clouds, virtual machines and containers, and uses a dizzying number of different SQL and NoSQL databases. This year's survey points out that while each of the engineers responsible for building and maintaining those systems needs varying levels of access, the problem does not stop with human users. Machine users such as CI/CD systems or microservices outnumber developers 10-to-1. This complex matrix of access — human-to-machine and machine-to-machine across multiple physical and logical boundaries — begs the question, how do organizations manage their access?

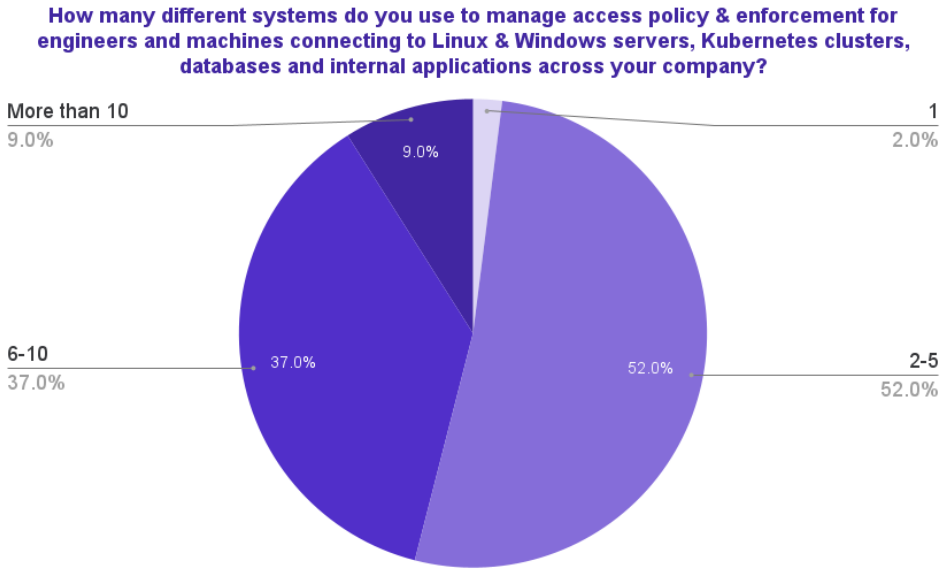
What security methods do you currently use to grant access to infrastructure? Select all that apply.



The survey looked at the specific tools organizations use to grant access (e.g. passwords, VPNs or biometrics) and how these have changed year on year. The number of respondents using passwords to grant access to infrastructure increased by 10% year over year, from 70% in 2021 to

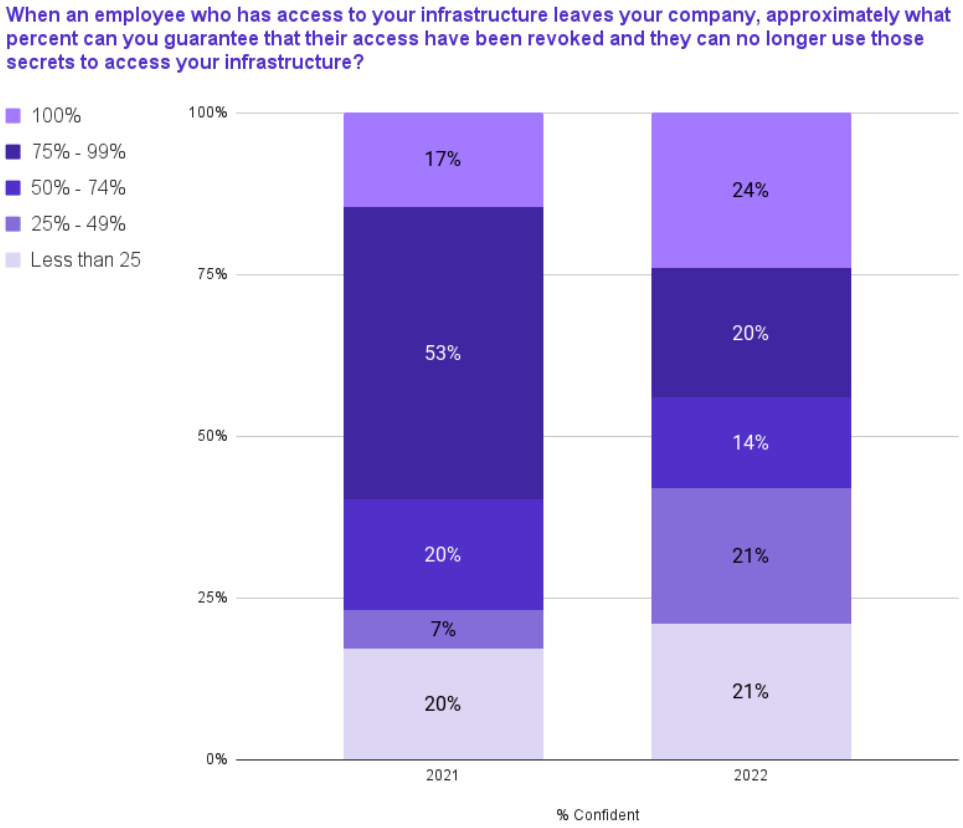
80% in 2022. Organizations must work to reverse this trend, particularly as technology stacks continue to expand with an increasing number of access points that can be exploited.

In addition to the specific tools used to grant access, the survey also asked respondents what systems they use to manage access policy and enforcement. The survey revealed that the mean number of systems was 5.7. The fact that this number is so high creates the very real possibility that the access of an ex-employee or contractor may be turned off in one system while remaining active in another.



Crises of confidence and clarity

Complexity is the defining challenge for infrastructure access today, as architectures grow and evolve on a minute-to-minute basis. DevOps, security engineering and other security experts face a difficult enough task in protecting sensitive assets from those outside the organization. Yet this task is made even more difficult when engineers previously trusted with access leave the organization — taking valuable knowledge with them.



When asked how confident they were that employees who leave the company can no longer use secrets to access company infrastructure, less than a quarter of respondents reported being 100% confident that the access had been revoked. Strikingly, nearly half of organizations are less than

50% confident that former employees no longer have access to infrastructure. This lack of confidence is trending in the wrong direction: the share of respondents with less than 50% confidence increased by 55% year over year.

When organizations rely on outdated security methods such as passwords, keys and tokens, it causes concern about the potential for former employees to access company information — or even sell the credentials onward to bad actors. The *2022 State of Infrastructure Access and Security Report* found that a majority (60%) of respondents are concerned about employees leaving the organization with secrets and knowledge about how to access infrastructure.

The potential for unauthorized access by former employees and contractors increases the need for secretless architectures, eschewing passwords for identity-based access. When an organization's system no longer relies on credentials that can be shared, lost or stolen, there is no longer reason to worry about engineers or others with access to infrastructure leaving with valuable information.

But while DevOps, security engineering and other security leaders fret about users who have left the organization, they must also pay close attention to the actions of their current employees. More than half (57%) of respondents said their organization has implemented new security methods that failed to be adopted by employees. Despite the immense security challenges facing today's companies, employees frequently push back against the tools chosen to solve them.

Organizations face a litany of challenges when dealing with infrastructure access. Top challenges cited by respondents include:

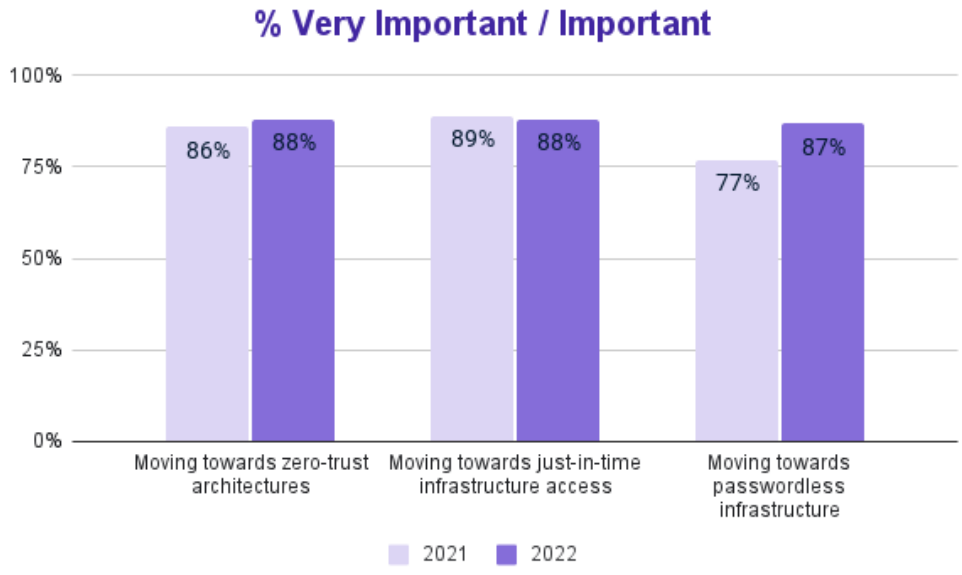
1) Establishing secure connection to infrastructure resources spread across the globe
2) Managing Key and password rotation
3) Implementing zero-trust access

DevOps, security engineering and other security leaders must strike a delicate balance as they aim to address these complicated challenges. Employees are resistant to change and to tools that will disrupt their workflows, so any security solution must be easy for employees to use while simultaneously delivering the desired result.

Reasons for optimism

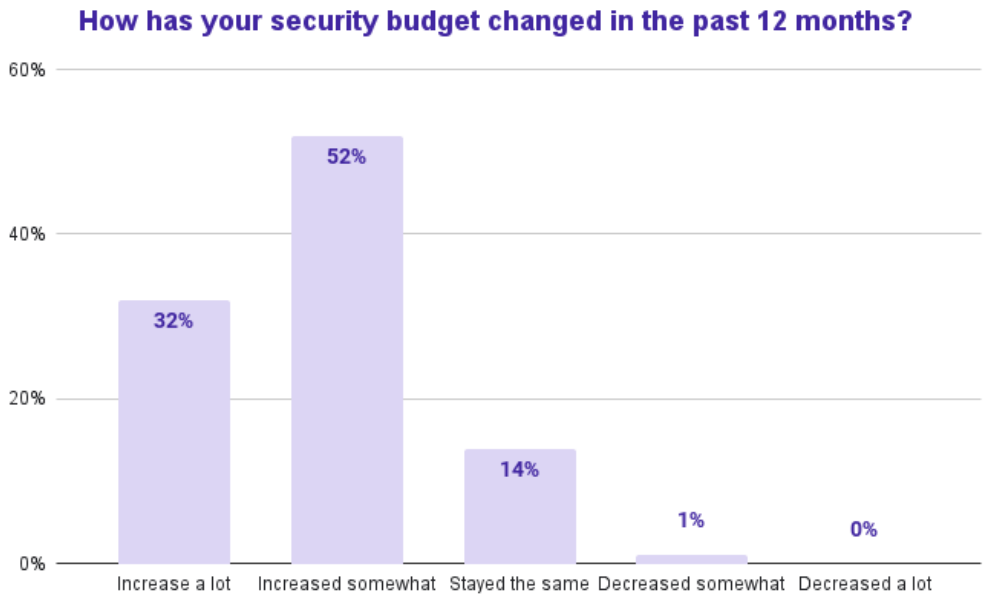
Until now, actions and investments have failed to keep pace with words and goals when it comes to implementing secretless infrastructure access. However, the *2022 State of Infrastructure Access and Security Report* shows that 2023 may be a turning point for effective access management as clear vision meets committed investment.

The vast majority of respondents still use inferior methods to securely access their infrastructure: 80% of respondents use passwords, the leading source of breaches; and 60% still use VPNs, which don't comply with the principles of zero trust.



The report found that respondents recognize the need to adopt passwordless access, and the share of those who view this shift as important increased over the last 12 months. Compared with 77% in 2021, 87% of respondents to this

year's survey said moving towards a passwordless infrastructure is important or very important. This priority is reflected in company initiatives: 77% of respondents have an active initiative to move towards passwordless access; and 78% of respondents have an active initiative to move to biometric authentication, the most effective tool for establishing human identity for secure access.



While adoption of biometric authentication is promising — more than half (55%) of respondents already use biometrics in their systems — there are still significant barriers to widespread adoption. Notably, 62% of respondents cited privacy concerns as a leading challenge when replacing secrets with biometric authentication, while 55% pointed to a lack of devices capable of biometric authentication.

Businesses will only be able to achieve their security goals with a combination of the right technology vision, widespread adoption, and committed investment. According to the report, 85% of respondents say security spending has increased within the last 12 months, demonstrating an

industry-wide appetite for improved security outcomes. Respondents also mentioned the importance of automating infrastructure access for reducing the cost of compliance: almost all (94%) respondents strongly agree or somewhat agree that this automation is critical for streamlining compliance costs.

Conclusion

Today's enterprises have every incentive to effectively manage infrastructure access and secure their most important assets. Vulnerabilities and breaches can result in significant financial, legal and reputational damages. The *2022 Infrastructure Access and Security Report* definitively shows that DevOps, security engineering and other security professionals understand the challenges they face, as well as the most effective tools for securing their infrastructure. But while the vision is clear, execution continues to lag behind. With architectures growing in complexity, and with the number of threats, attack vectors, and bad actors increasing, leaders cannot afford to delay any longer in turning their plans into actions. Secretless, identity-native infrastructure access is the only way forward.

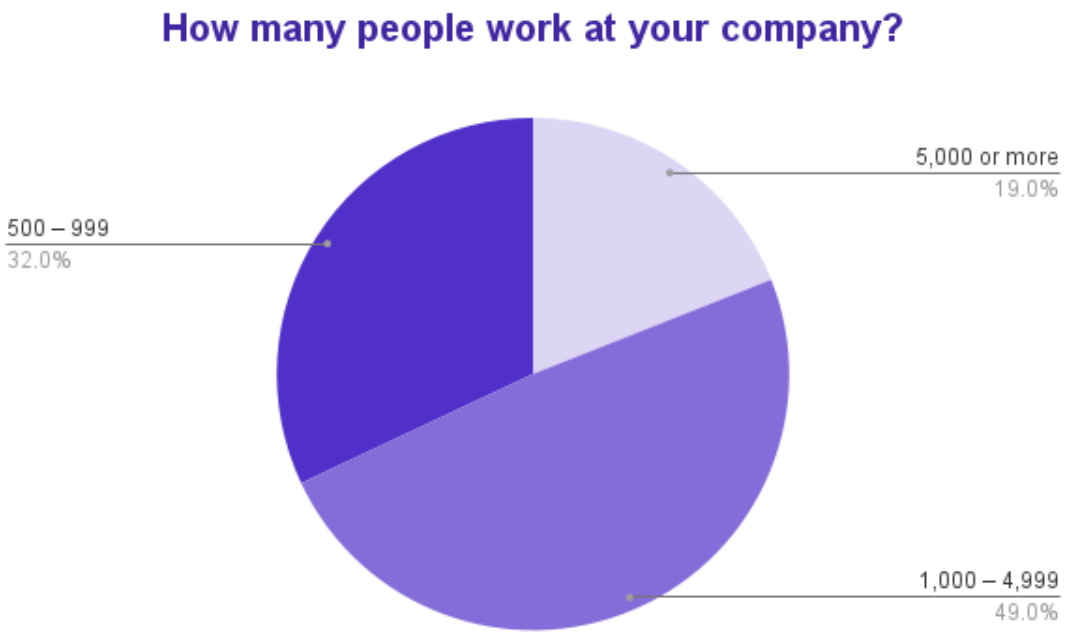
Methodology

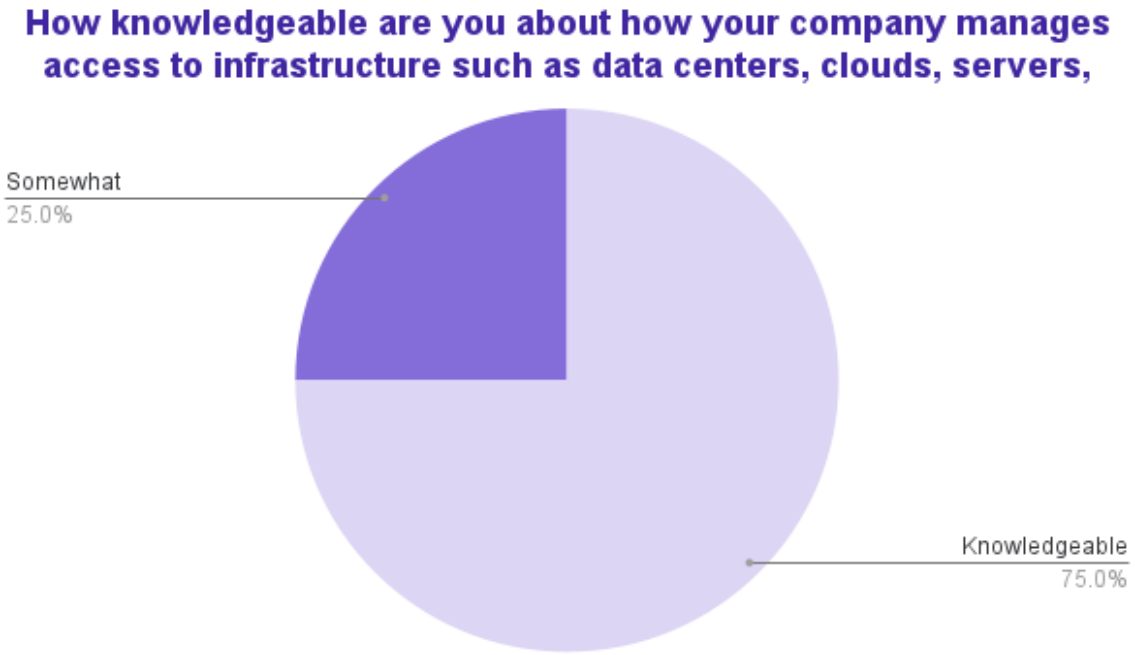
The *2022 Infrastructure Access and Security Report* survey collected a representative sample of DevOps, Security Engineering, and other security professionals with knowledge about how their company manages access to infrastructure. A total of 500 respondents completed the survey, which was conducted by Schlesinger Group, an independent research company.

About Teleport

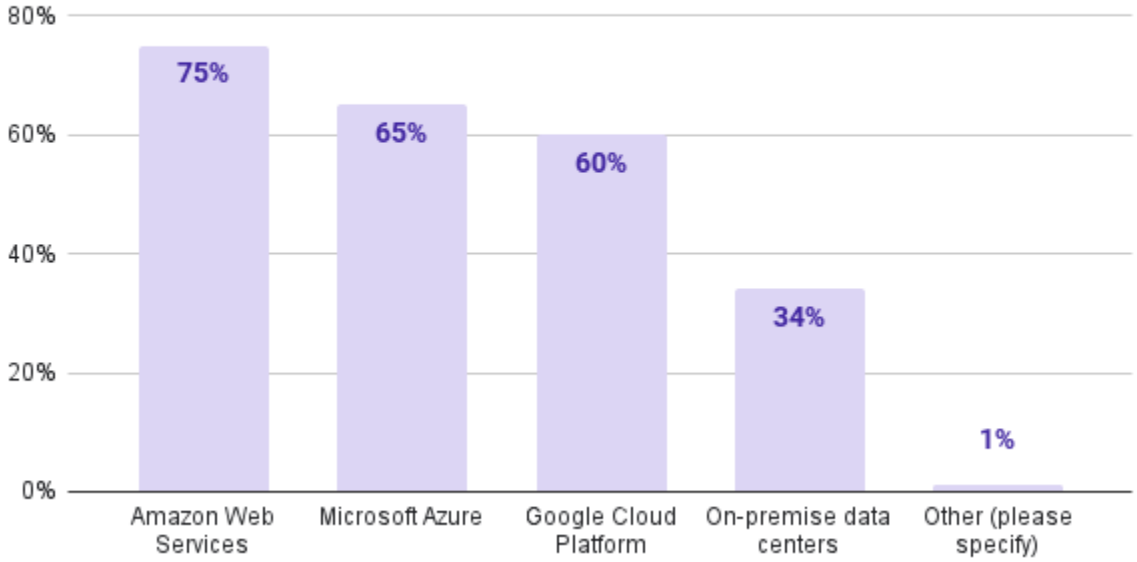
Teleport is the first identity-native infrastructure access platform for engineers and machines. By replacing insecure secrets with true identity, Teleport delivers phishing-proof zero trust for every engineer and service connected to your global infrastructure. The open source Teleport Access Platform provides a frictionless developer experience and a single source of truth for infrastructure access. Teleport is used by leading companies including Elastic, Samsung, NASDAQ, and IBM. The company is backed by Bessemer Venture Partners, Insight Partners and Kleiner Perkins. Headquartered in Oakland, California, the company embraces a remote-first work culture.

Appendix: Report Data

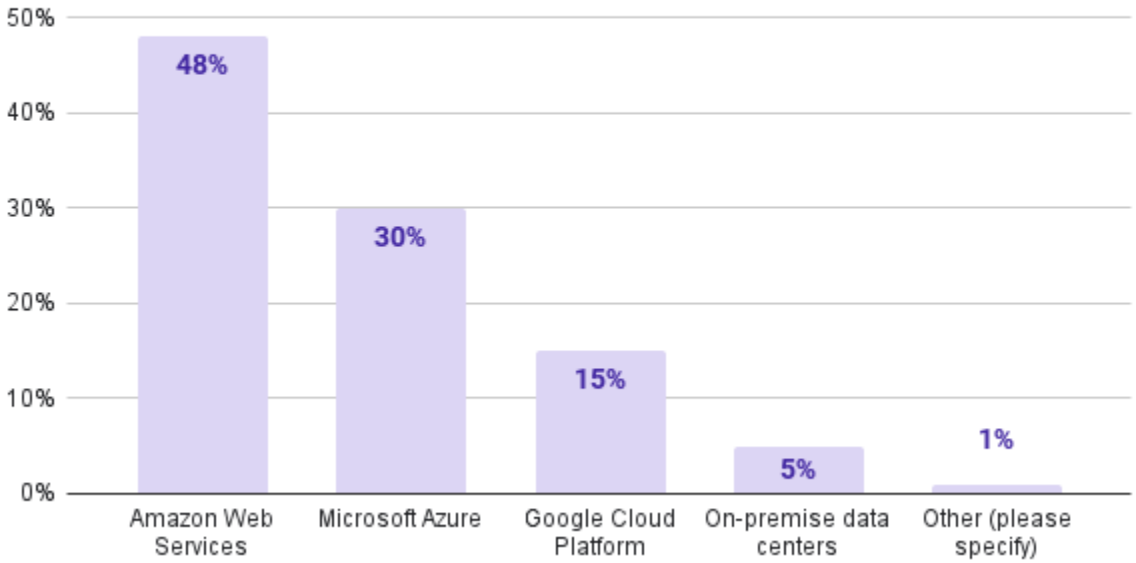




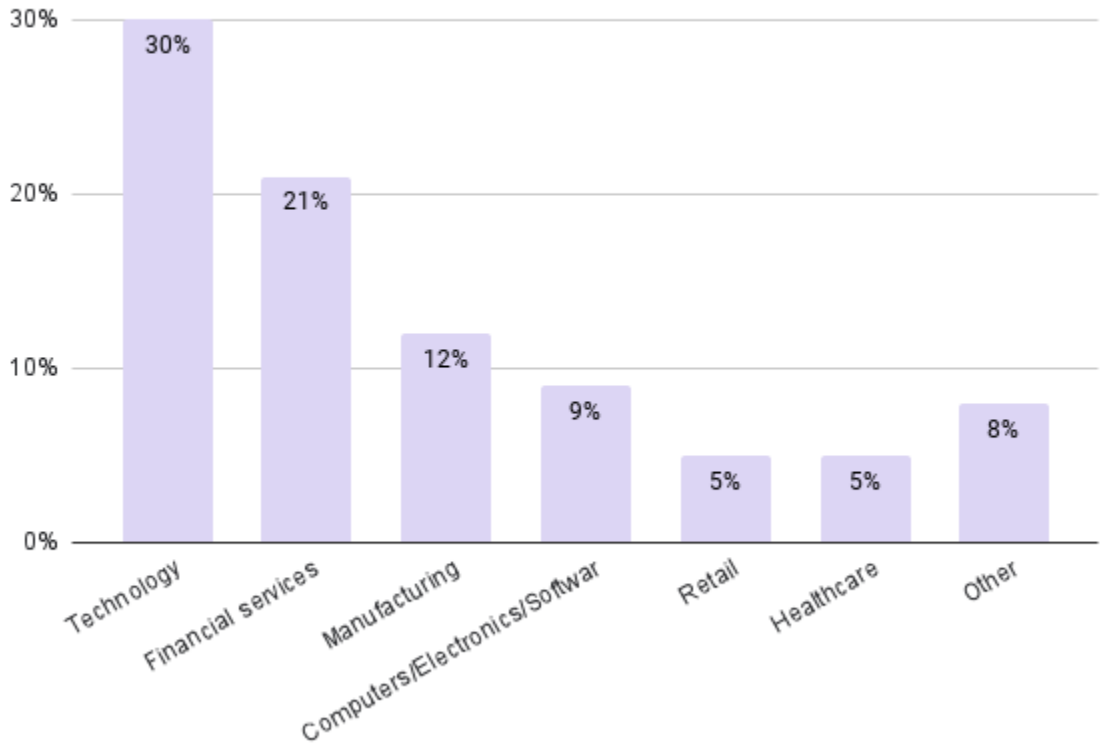
What environments do you currently use to run enterprise applications? Select all that apply.



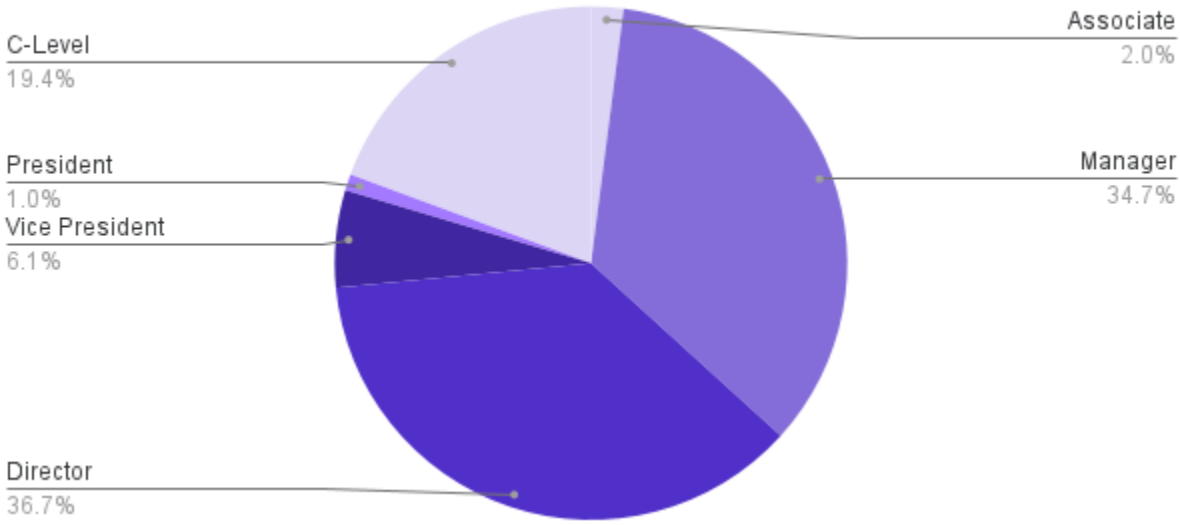
What environment is your primary one to run enterprise applications?

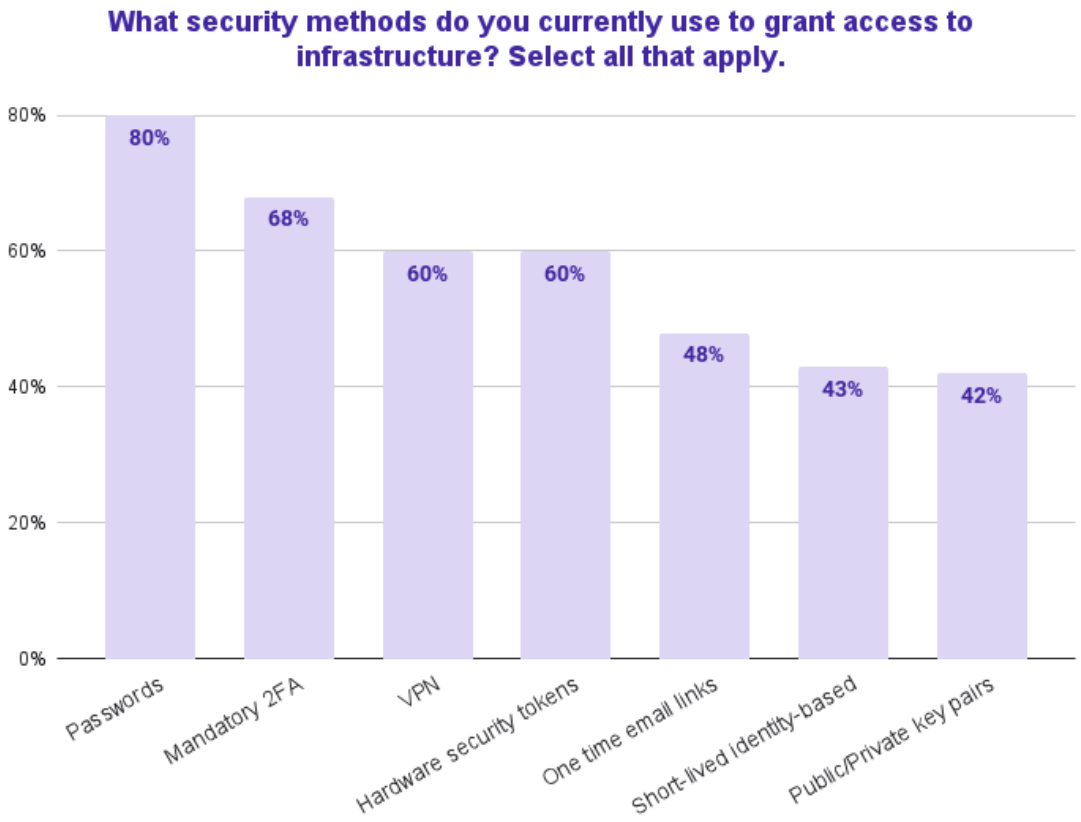


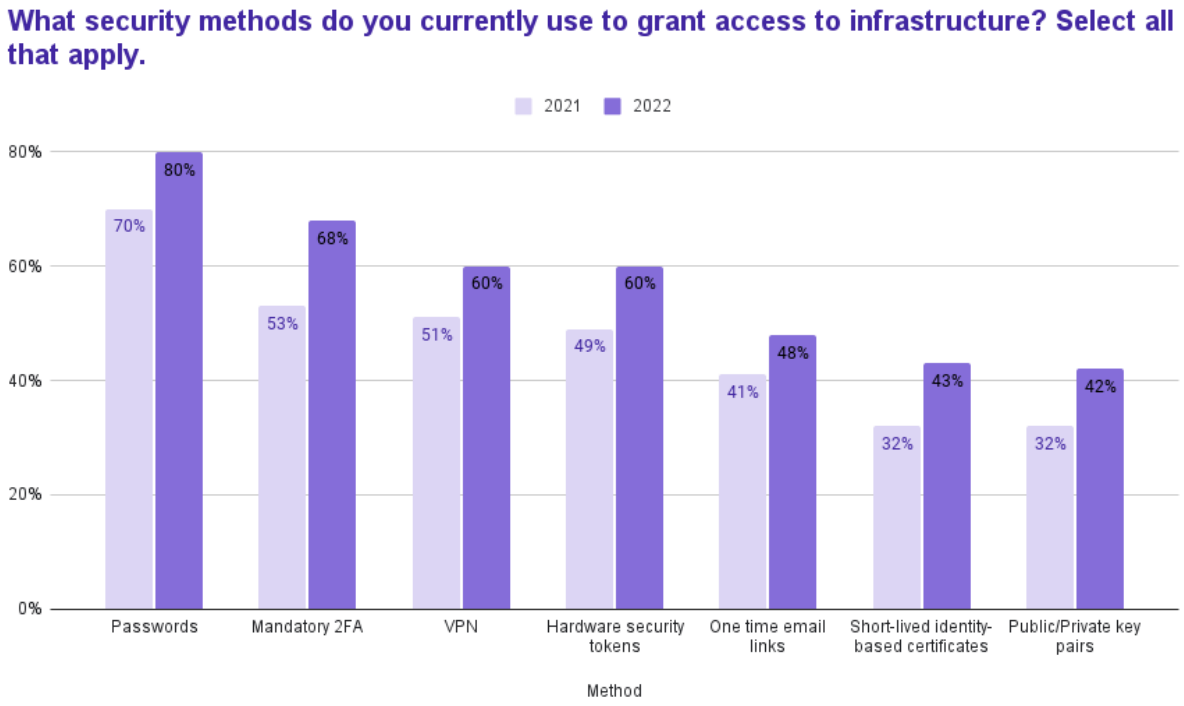
What industry does your company fall into?



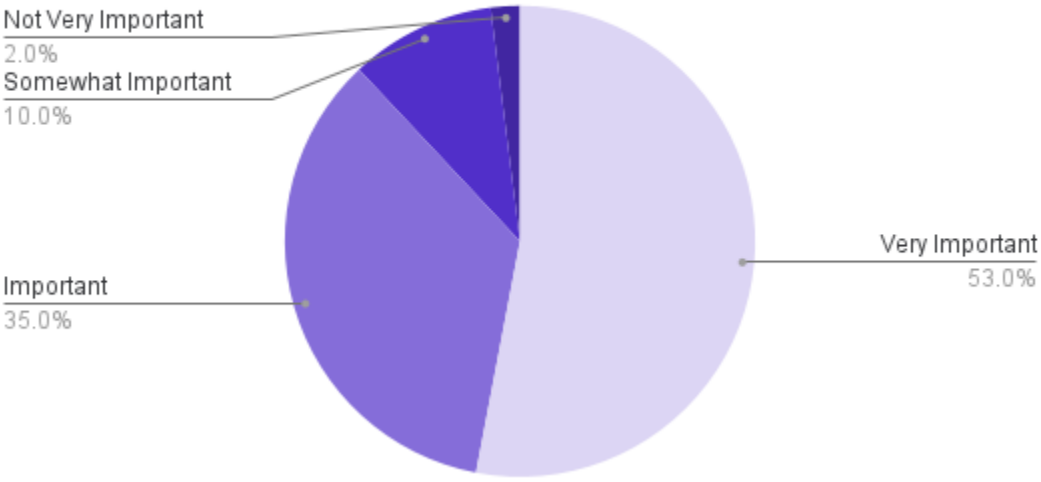
Which of the following best describes your title?



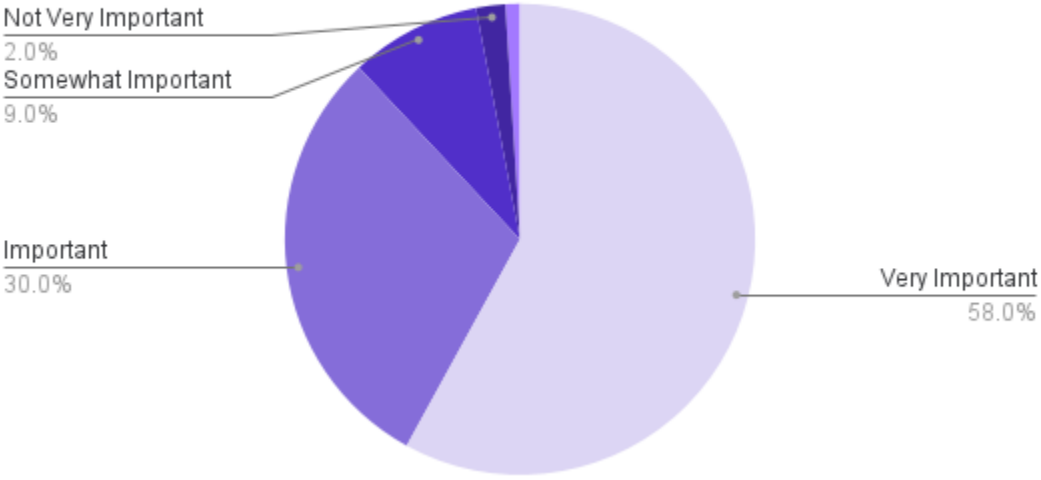




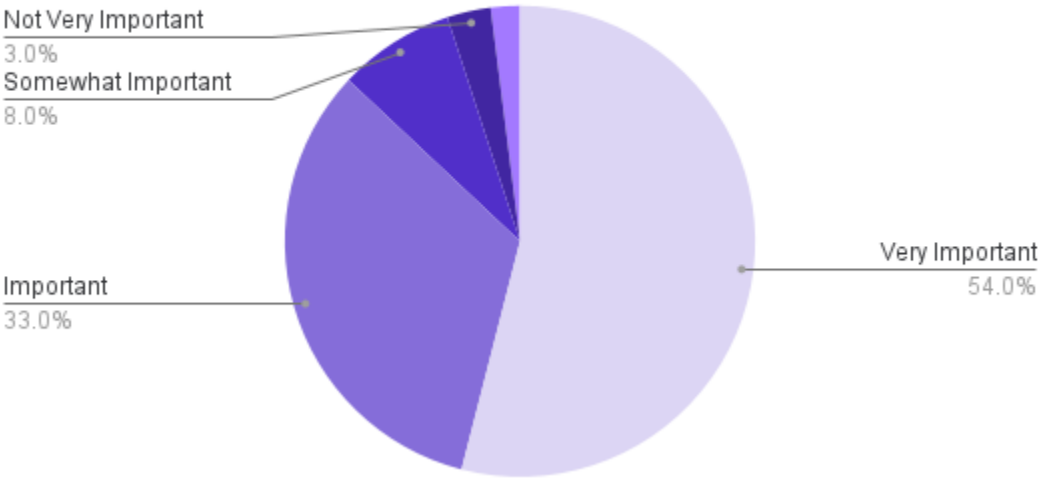
How important to your organization is moving towards just-in-time infrastructure access?



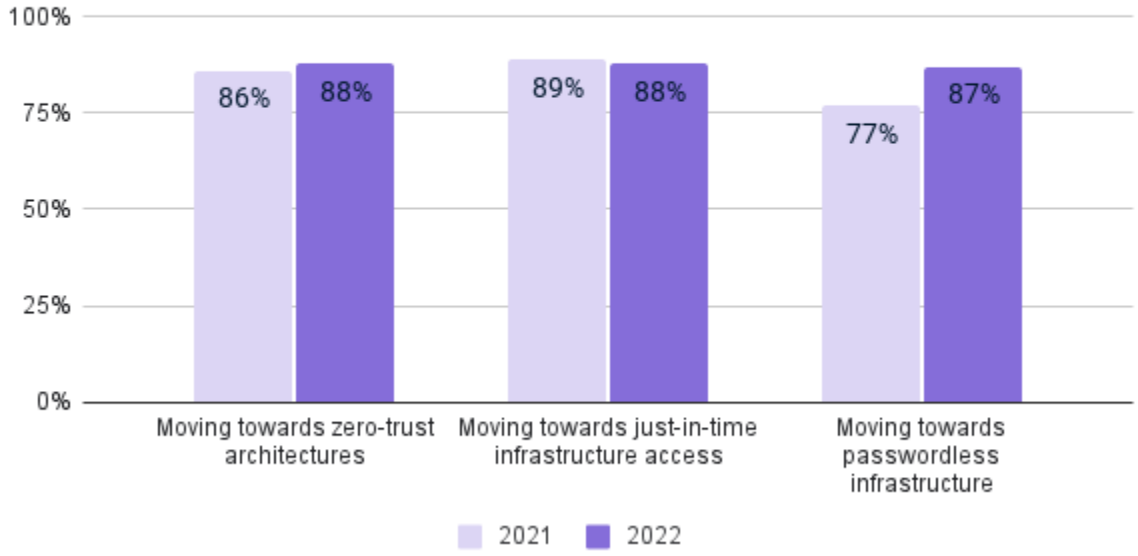
How important to your organization is moving towards zero-trust architectures?

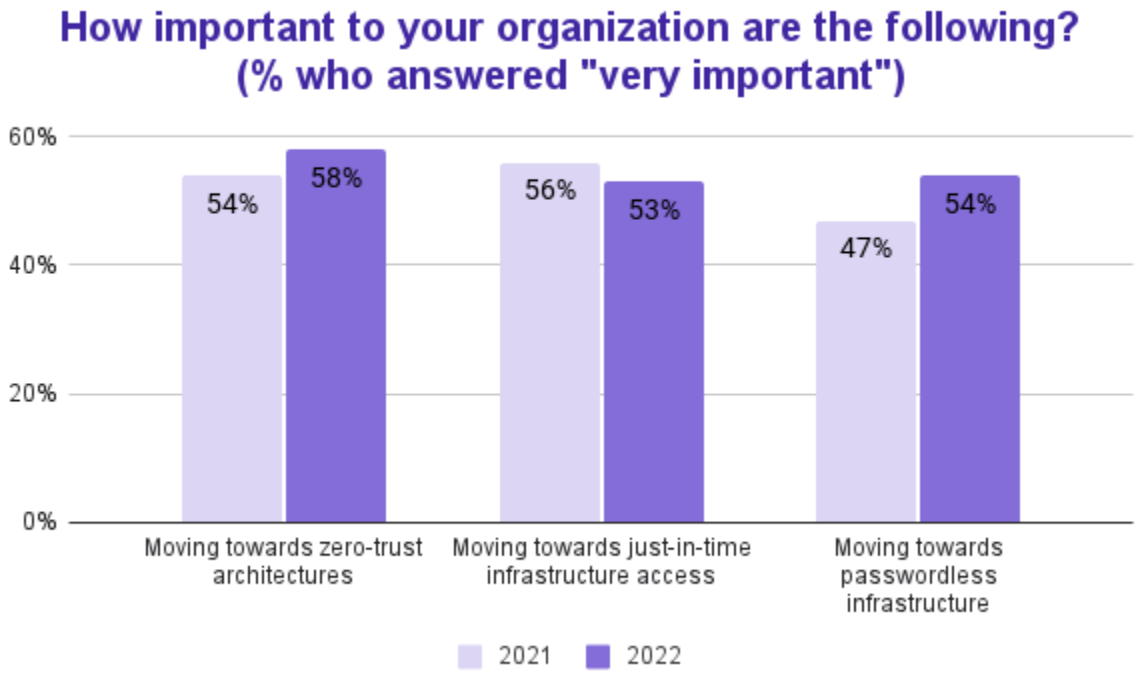


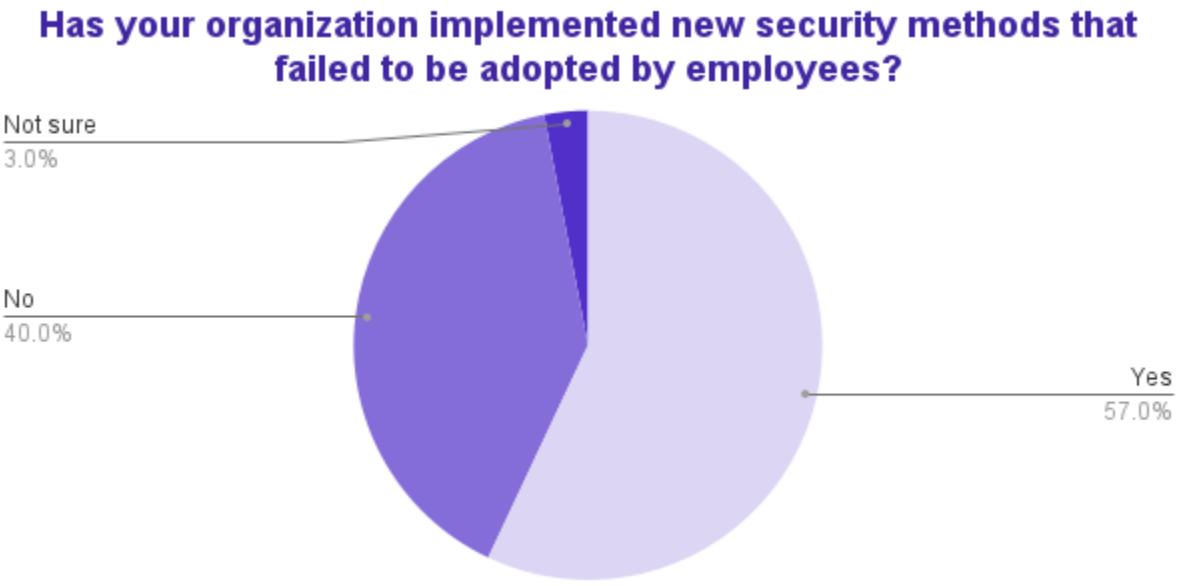
How important to your organization is moving towards passwordless infrastructure?



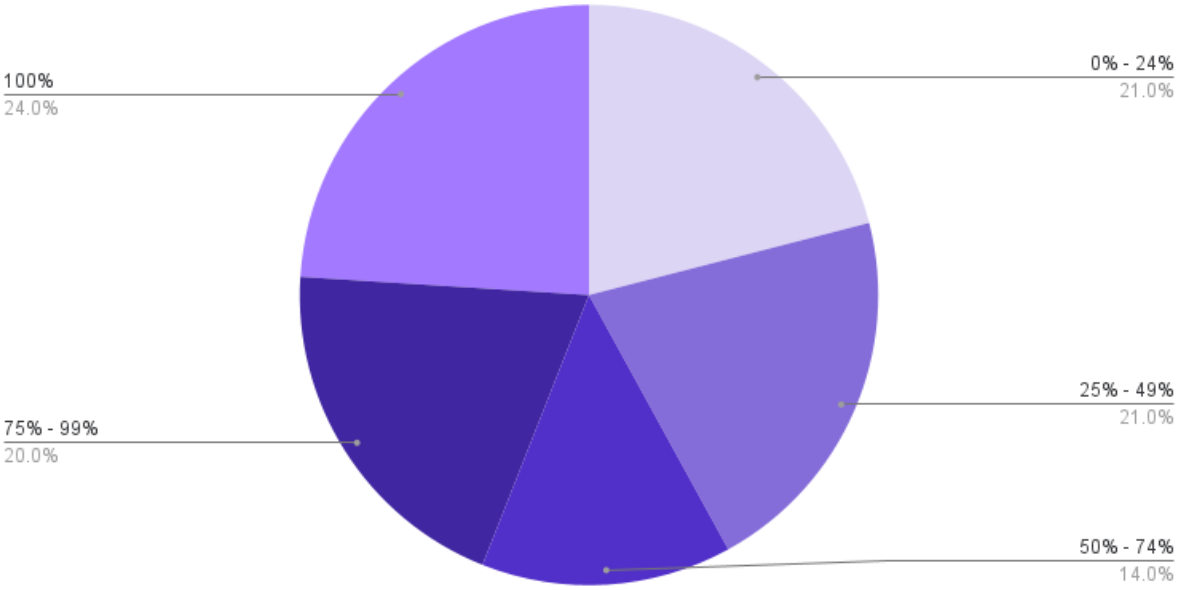
How important to your organization are the following? (% who answered "very important" or "important")



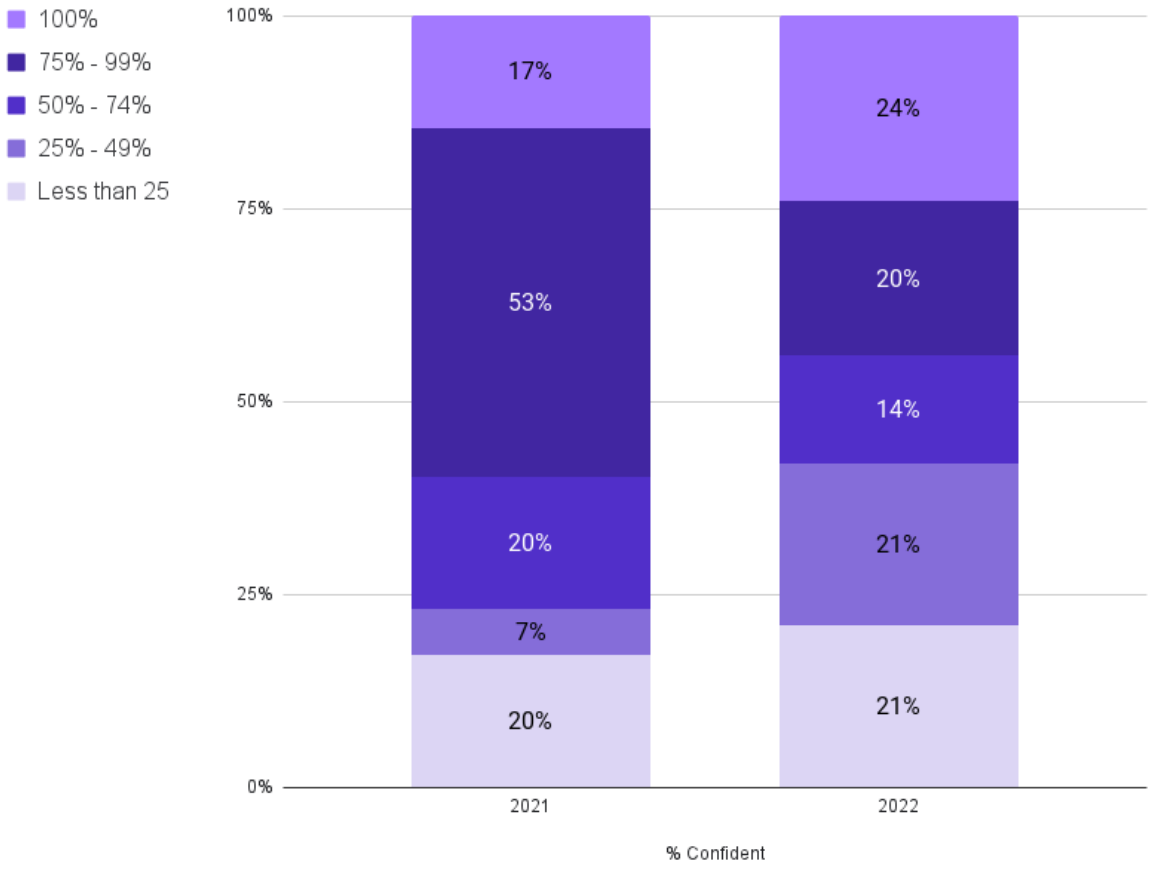




When an employee who has access to your infrastructure leaves your company, approximately what percent can you guarantee that their access have been revoked and they can no longer use those secrets to access your infrastructure?

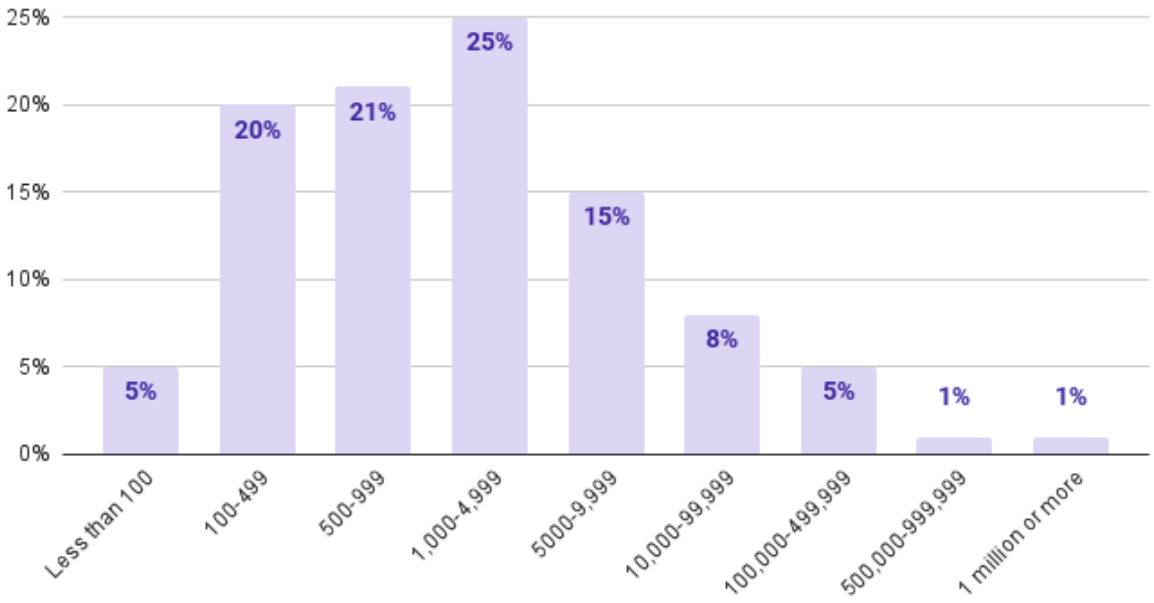


When an employee who has access to your infrastructure leaves your company, approximately what percent can you guarantee that their access have been revoked and they can no longer use those secrets to access your infrastructure?

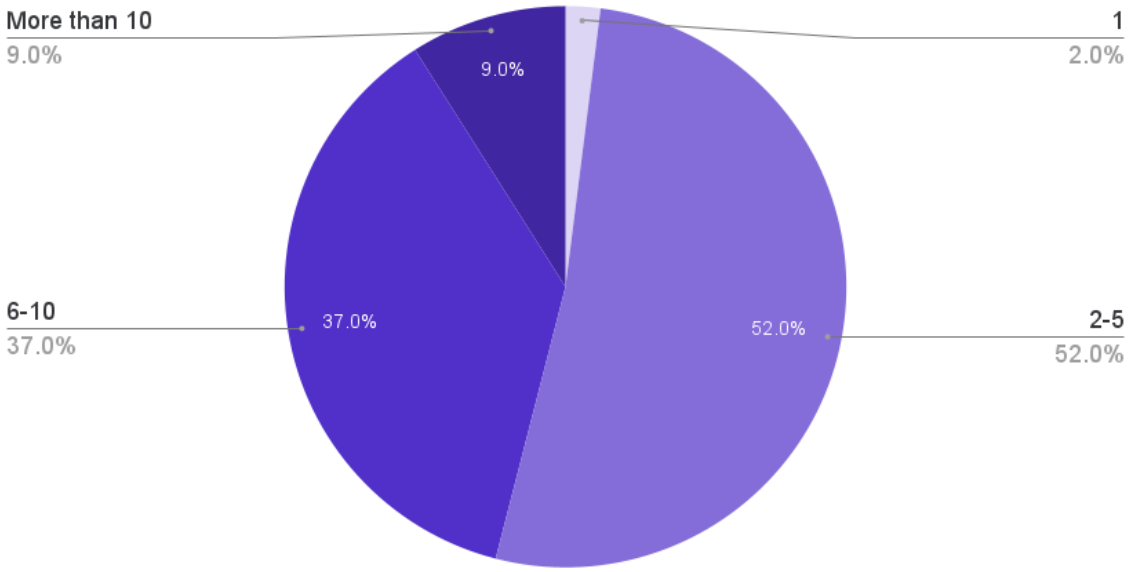


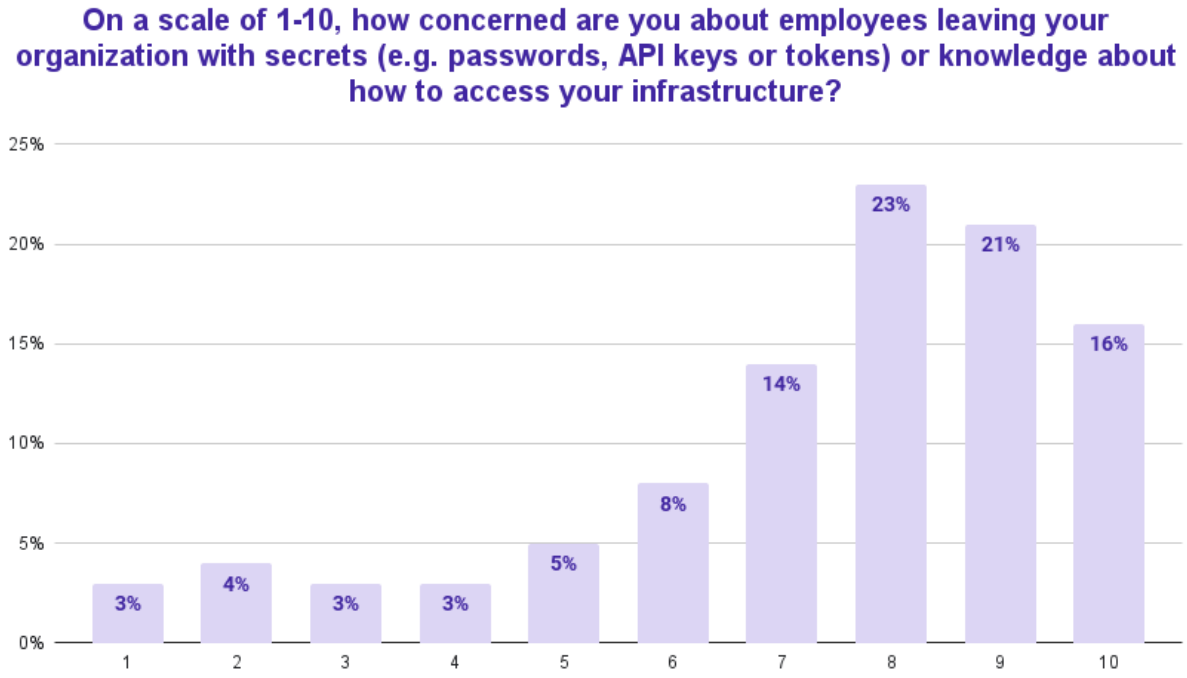
Rank of Challenges When Managing Access to Infrastructure — % Ranked #1

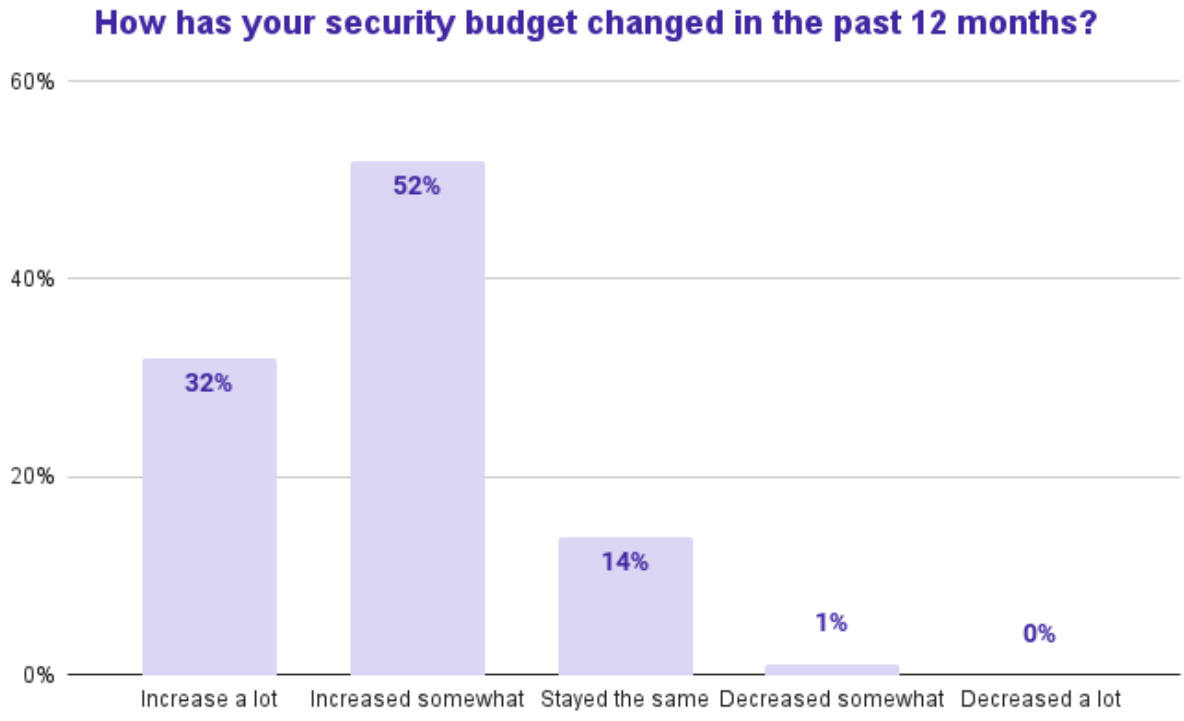
Approximately how many virtual machines, containers, databases and applications does your organization operate?

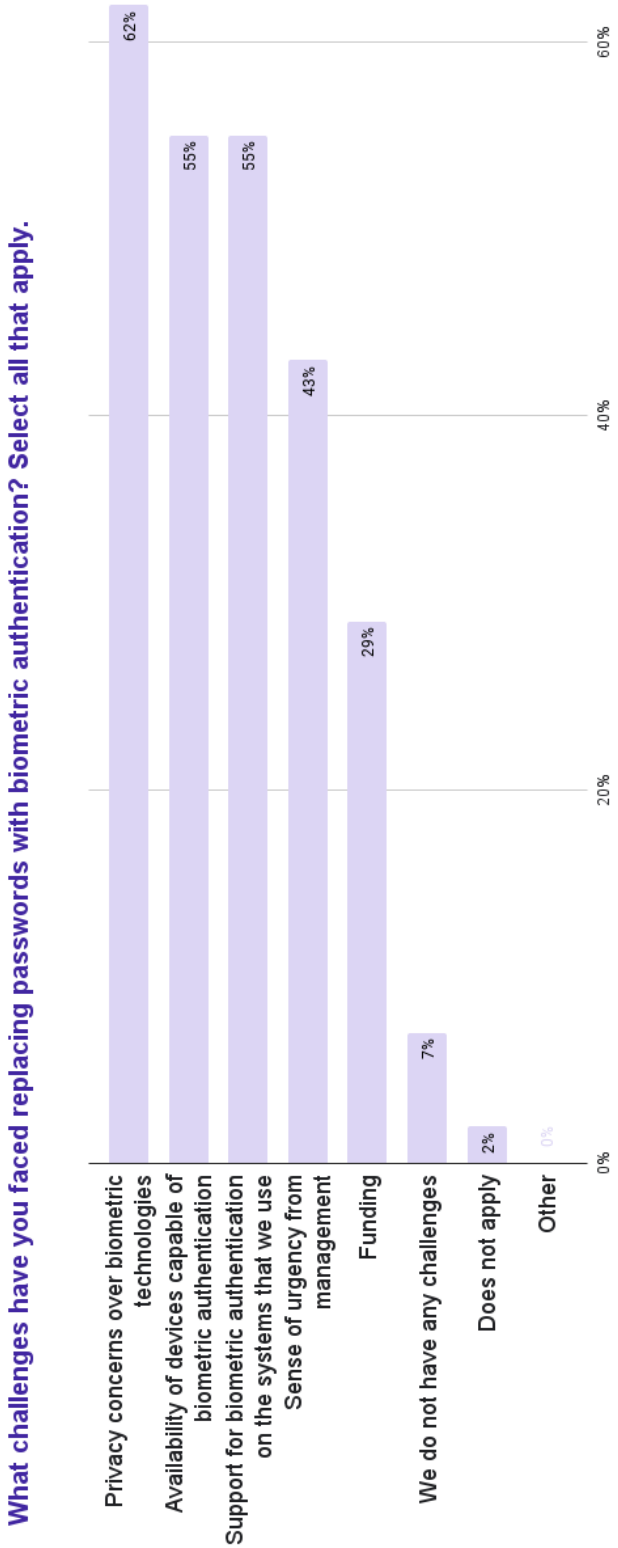


How many different systems do you use to manage access policy & enforcement for engineers and machines connecting to Linux & Windows servers, Kubernetes clusters, databases and internal applications across your company?

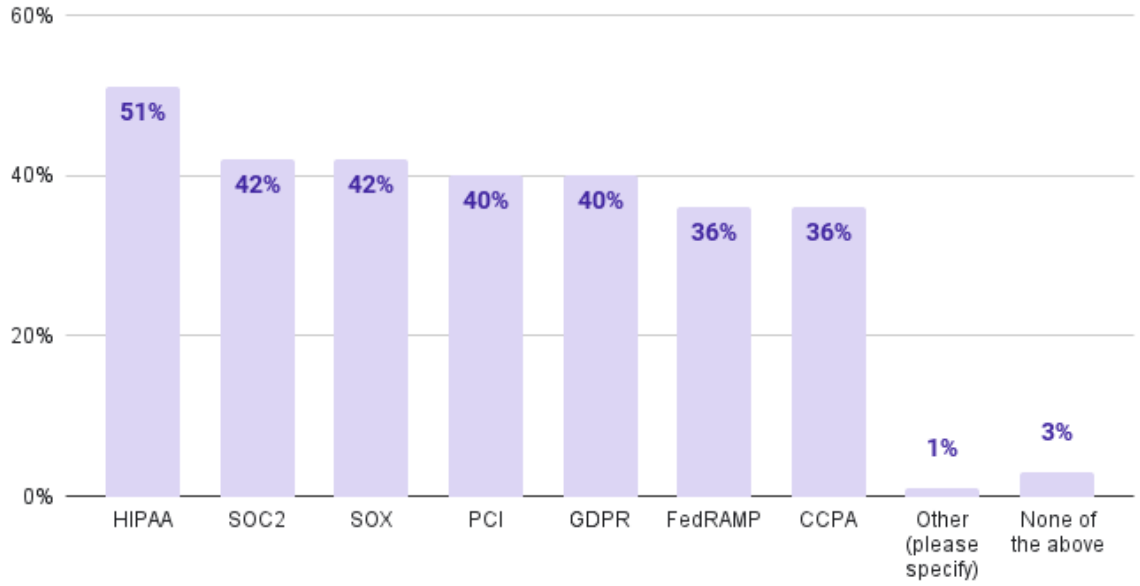








What compliance regimes must your organization adhere to? Select all that apply.



How much do you agree or disagree with the following statement?
I believe that automating infrastructure access is critical to streamlining compliance costs.