Teleport State of Infrastructure Access and Security Report

2021

Teleport

2021 State of Infrastructure Access and Security Report

Executive summary

On March 11th, 2020, the World Health Organization declared COVID-19 a global pandemic. In the months that followed, enterprises faced unprecedented, transformational change to the ways in which they work and communicate. Accustomed to protecting sensitive information on-premises or with limited remote access, IT and security organizations were given the overnight task of creating and securing a completely new set of hybrid work environments.

While enterprises have tried to adapt to the new normal in network access and security, the overall situation has only become more complicated over the last two years. Companies are simultaneously embracing long-term work-from-home along with cloud-native tools such as containers, Kubernetes, and new database types that add new layers to the already existing IT stack. This dramatic increase in complexity has made the challenge of securing the network perimeter go from difficult to nearly impossible. Meanwhile, the massive employee turnover now known as the "Great Resignation" has dramatically increased the risk of former employees maintaining access to company infrastructure.

The *2021 State of Infrastructure Access and Security Report* conducted by Schlesinger Group, an independent research company, seeks to better understand the challenges facing IT, DevOps and security professionals. Featuring survey data from 1,000 respondents, the Report offers a representative sample of the common beliefs held by industry professionals, as well as the actions being taken to maintain security in an era of unparalleled complexity. More on the survey methodology below.

Key findings

The Report reveals strong opinions on some of the most pressing issues facing engineering and security professionals today:

- **The "Great Resignation" causes security concerns for enterprises -** More than half (58%) of IT, DevOps and Security professionals are "concerned" or "very concerned" about ex-employees leaving with secrets and/or knowledge into how their organization accesses infrastructure. 83% of respondents cannot guarantee that ex-employees can no longer access their infrastructure.
- **Managing infrastructure access is a shared responsibility -** 54% of respondents said three or more departments are responsible for infrastructure access in their organization.
- **Industry professionals recognize an urgent need for new access methods -** 95% of respondents "somewhat" or "strongly" agree that greater visibility is critical to their business's success.
- **Majority of respondents rely on outdated security methods -** 70% of those surveyed still use passwords to grant infrastructure access, while 53% still use VPNs.
- **Organizations are challenged to make sense of complex architectures -** 61% of organizations currently use three or more databases; 60% of organizations are running applications in virtual machines, containers and Kubernetes; 94% of organizations run the Windows operating systems for servers, and 43% also run Linux.
- **Decision-makers prioritize developer productivity when considering infrastructure access technology -** 84% of respondents view developer productivity as a "big" or "major" factor when considering implementing infrastructure access technology.

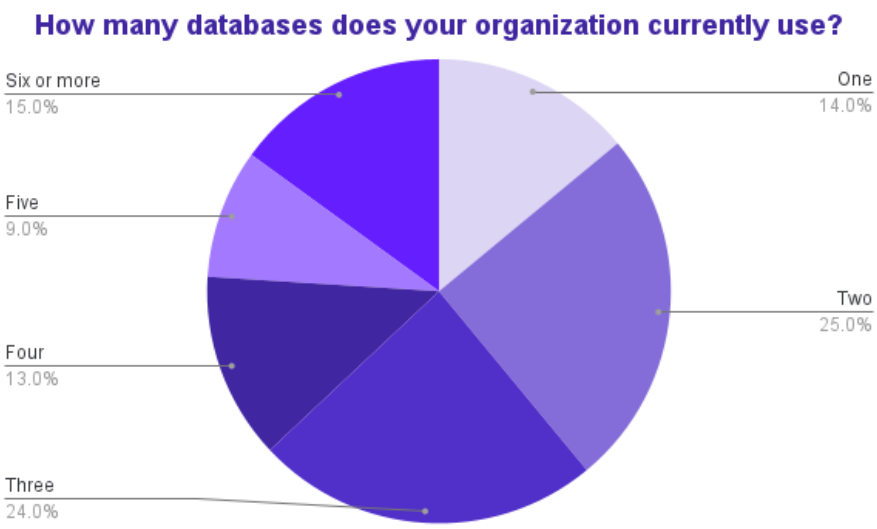
Analysis of key findings

The stakes for IT, DevOps and security professionals have never been higher. The past two years have seen unprecedented hacks and breaches, resulting in millions of dollars in losses, penalties and even ransom payments to bad actors. But while organizations work to secure their networks and sensitive assets, they must balance their security approaches with the need to maintain operational agility.

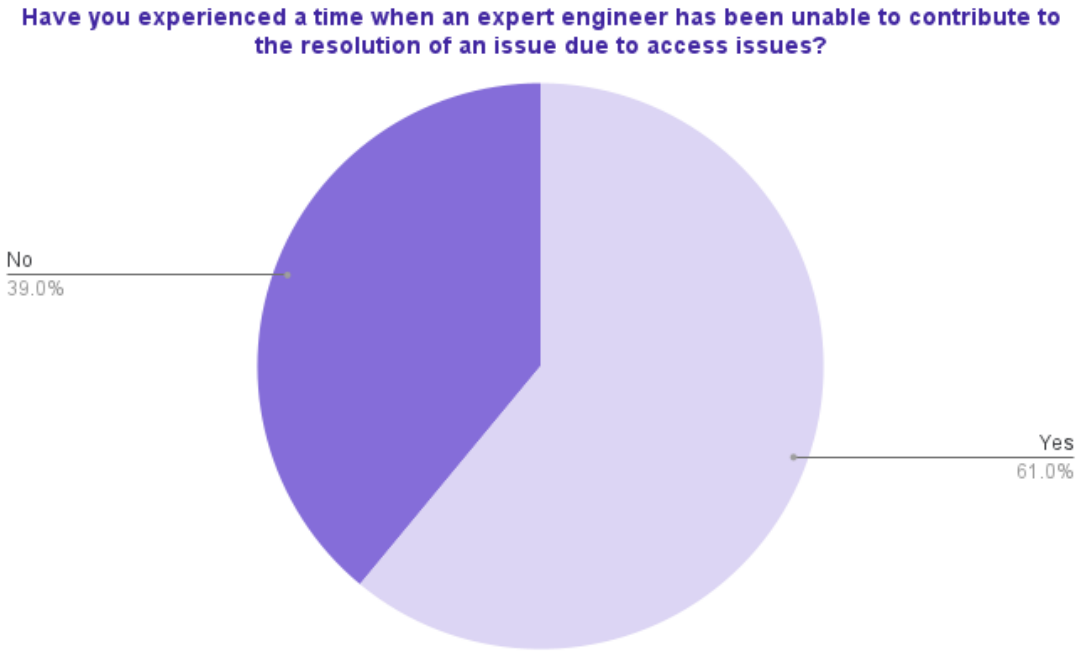
The *2021 State of Infrastructure Access and Security Report* finds industry professionals divided in how they choose to manage these tradeoffs, in some cases with discord between high-level executives and the practitioners responsible for everyday operations.

Infrastructure complexity introduces security vulnerabilities

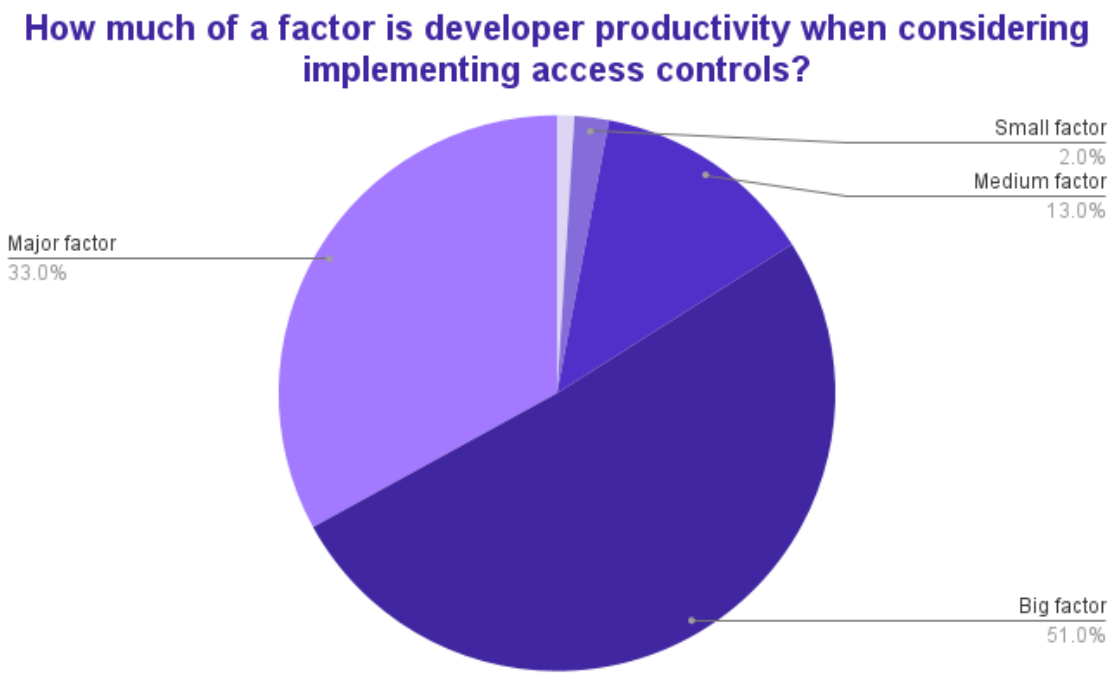
Today's architectures are remarkable in their complexity. According to survey respondents, 60% of organizations are running applications in virtual machines, containers and Kubernetes. Similarly, 61% of organizations currently use three or more databases, and 15% of organizations use a whopping six or more databases. 94% of organizations run the Windows operating systems for servers, and 43% also run Linux. Compliance adds an additional layer of complexity, with nearly half (46%) of respondents reporting that they must adhere to three or more compliance regimes such as SOC2, PCI, HIPAA, and FedRAMP.



The impact of this increased complexity is not abstract or theoretical. When issues arise, organizations find it hard to achieve the necessary access to their systems to investigate and make fixes. During an outage or other crisis, 61% of enterprises have experienced a time when an expert engineer couldn't help solve the problem due to access issues.



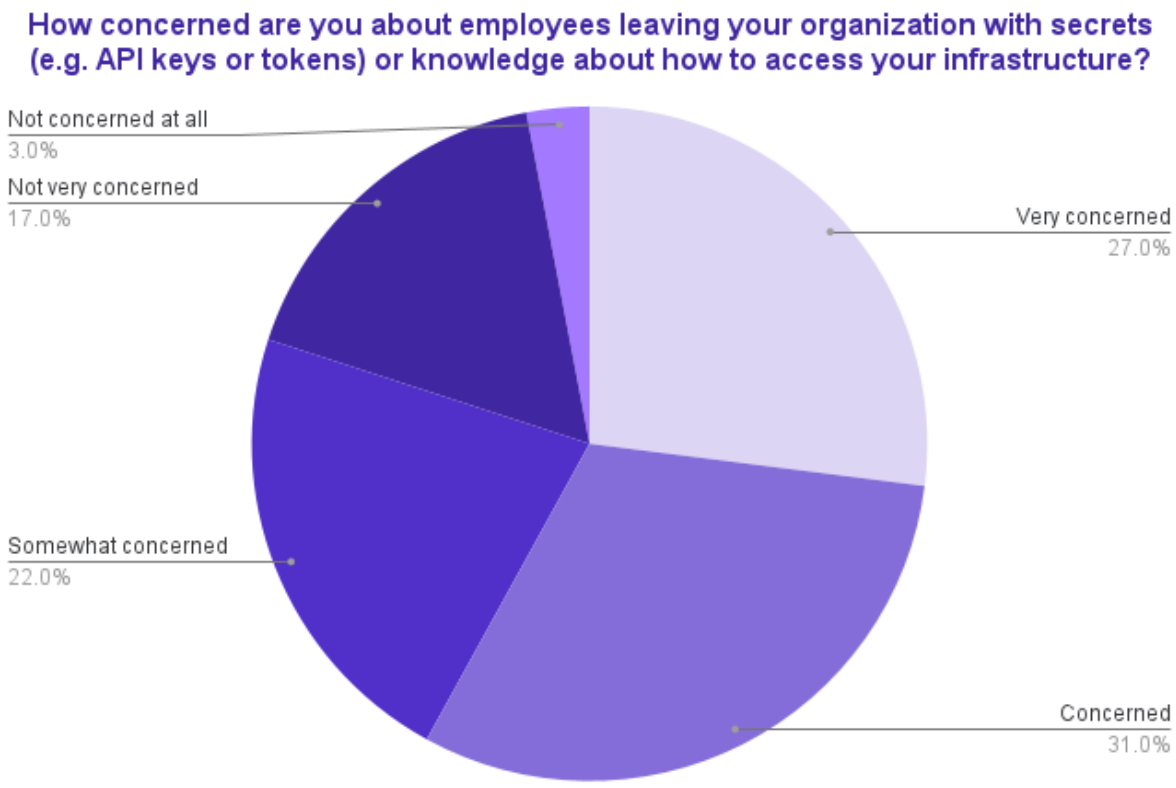
While IT, DevOps and security professionals recognize the need for new infrastructure access technology to address these challenges, they are hesitant to adopt any solution that may hinder productivity. The vast majority (84%) of respondents view developer productivity as a "big" or "major" factor when considering implementing infrastructure access technology. In particular, high-level executives are laser-focused on efficiency: 43% of those with VP titles or higher view developer productivity as a "major" factor, the strongest possible response.



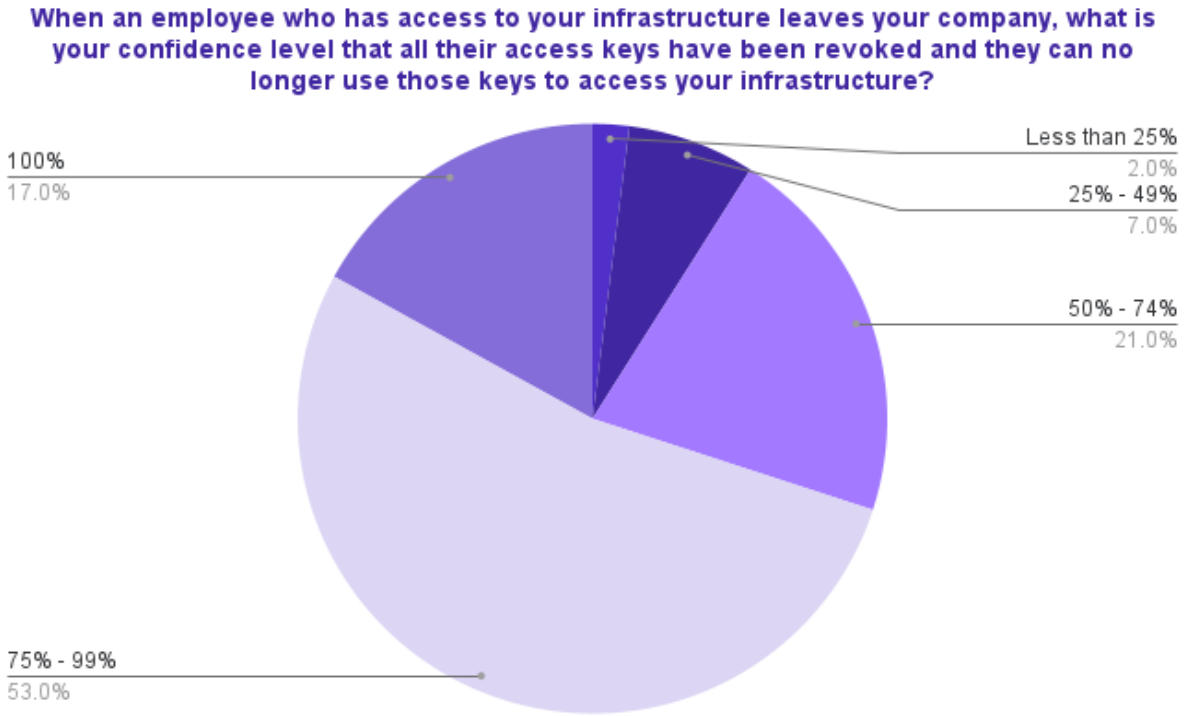
The Great Resignation leaves organizations vulnerable to attacks

Infrastructure access and security challenges are dynamic, requiring constant vigilance and technological superiority to protect an enterprise's most valuable and sensitive assets. But what happens when the employees tasked with deploying and managing applications and infrastructure leave the organization and take their knowledge with them? As highly skilled employees leave their companies in droves as part of the Great Resignation, the organizations they leave behind must ensure that access is only granted to current employees.

The effects of the Great Resignation are top-of-mind for industry leaders. More than half (58%) of IT, DevOps and security professionals are "concerned" or "very concerned" about former employees leaving with secrets or knowledge into how their organization accesses infrastructure. More than a quarter (27%) are very concerned, demonstrating the urgent need for a reliable solution.



These industry decision-makers are aware of the problem at hand, yet they haven't made the necessary adjustments to protect their infrastructure. Despite the obvious risks, 83% of respondents cannot guarantee that ex-employees can no longer access their infrastructure.



The problem is not awareness, but execution. Of the respondents who are "very concerned" about ex-employees leaving with knowledge about how their organization accesses infrastructure, more than three-quarters (77%) said their organization implemented new security methods that failed to be adopted by current employees.

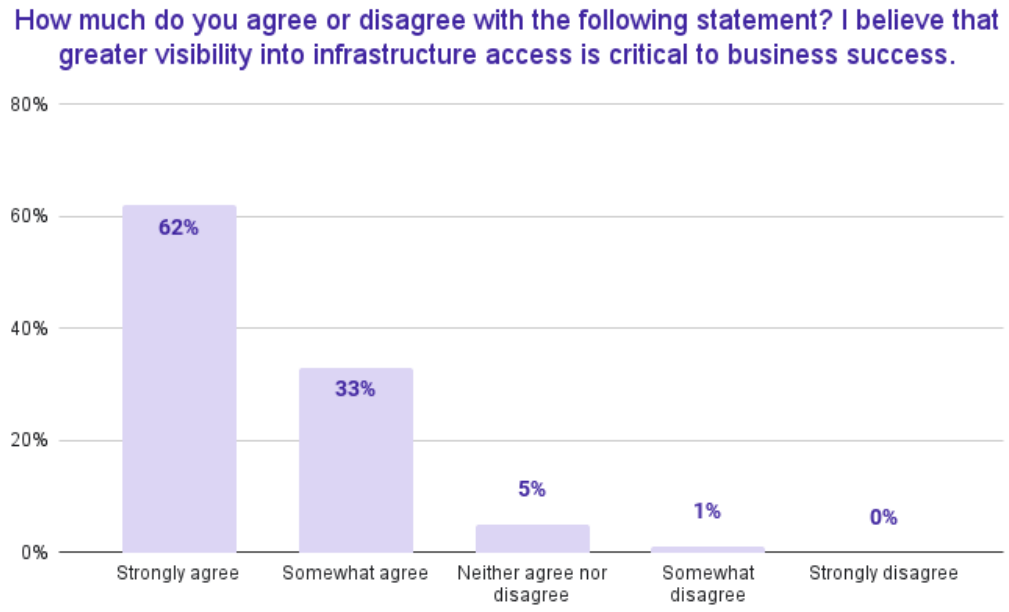
Due to the complex nature of modern applications and infrastructure, and the need to secure all levels of the stack, infrastructure access is a shared responsibility between different stakeholders. 54% of respondents said three or more departments are responsible for infrastructure access in

their organization. For 11% of respondents, five or more departments are responsible for infrastructure access.

Industry professionals are divided on what role should be most responsible for infrastructure access in their organization. 40% of respondents said the responsibility lies with security employees, while 33% said DevOps and engineering. Rather than pursuing a one-size-fits-all solution that ignores the needs of individual teams, an infrastructure access system must allow decentralized, protocol-specific enforcement of centralized access policies.

Battles with obsolescence and complacency

It's obvious that IT, DevOps and security teams are wrestling with a growing list of challenges, and these professionals are nearly unanimous in their desire for new solutions. Asked which strategies and technologies could make a difference for their organization, 95% of respondents "somewhat agreed" or "strongly agreed" that greater visibility is critical to their business success.

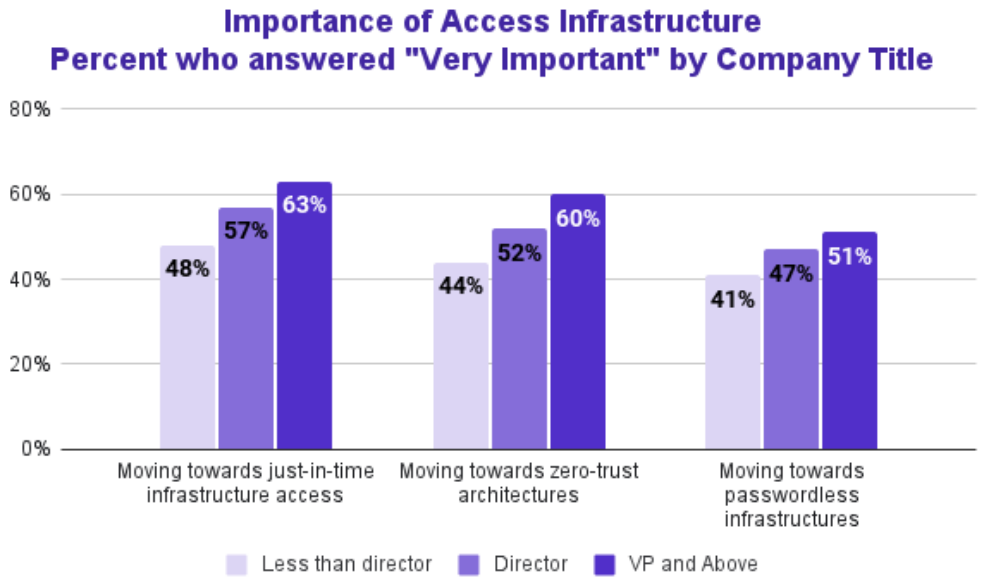


These organizations are willing to invest in making improvements: 86% of those surveyed expect their budget for infrastructure access technology to increase over the next 12 months, and more than one-third (36%) expect this to be a big increase.

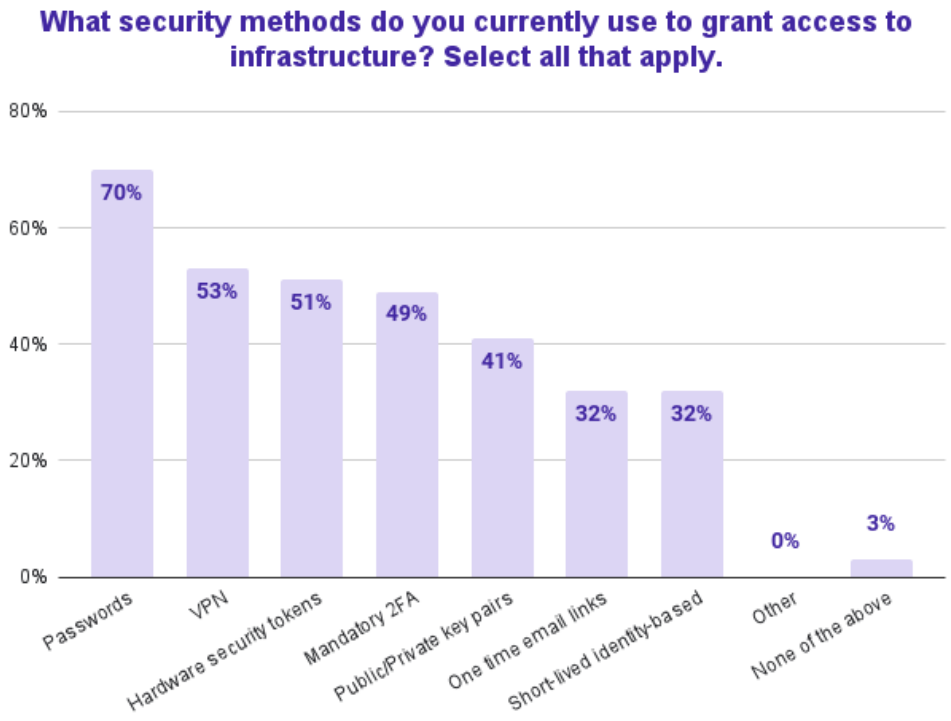
Survey respondents identified several key technologies to improve their security practices. Organizations ranked moving to the following access methods as important or very important: Just-in-time access (89%), Zero-trust architectures (86%), Passwordless access (77%).

How important is moving towards:	Very Important	Important	Somewhat Important	Not Very Important	Not Important at All
Just-in-time infrastructure access	56%	33%	8%	2%	1%
Zero-trust architectures	54%	32%	12%	2%	1%
Passwordless infrastructure	47%	30%	15%	6%	2%

For those who ranked these technologies as “very important”, the more senior a respondent was in the survey, the more likely they were to support these architectures, most likely because they have the most accountability when things go wrong.



Despite the steady drumbeat of news stories on security breaches caused by compromised passwords, 70% of survey respondents reported that they still use passwords to grant infrastructure access. More than half of those surveyed (53%) say they still use VPNs to grant infrastructure access, even though weak VPN protocols have led to damaging data breaches.



According to the survey, only one-third (32%) of IT, DevOps and security professionals currently use short-lived identity-based certificates to grant infrastructure access, one of the most effective solutions for preventing unauthorized access to enterprise infrastructure and information. When asked why they've chosen to implement these certificates, 44% cited greater security than other types of credentials, and 34% said greater functionality than other types of credentials.

Conclusion

Security is a primary concern for today's enterprises, with vulnerabilities or failures leading to significant economic, legal and reputational costs. The *2021 Infrastructure Access and Security Report* finds that IT, DevOps and security professionals are fully aware of the threats to modern tech stacks. However, this awareness is not always matched by a sense of urgency, particularly among those at the highest echelons of decision-making. As architectures become more complex — and as bad actors become more sophisticated — industry leaders must move from concern to action, implementing the passwordless, identity-based solutions that can effectively safeguard their most important assets.

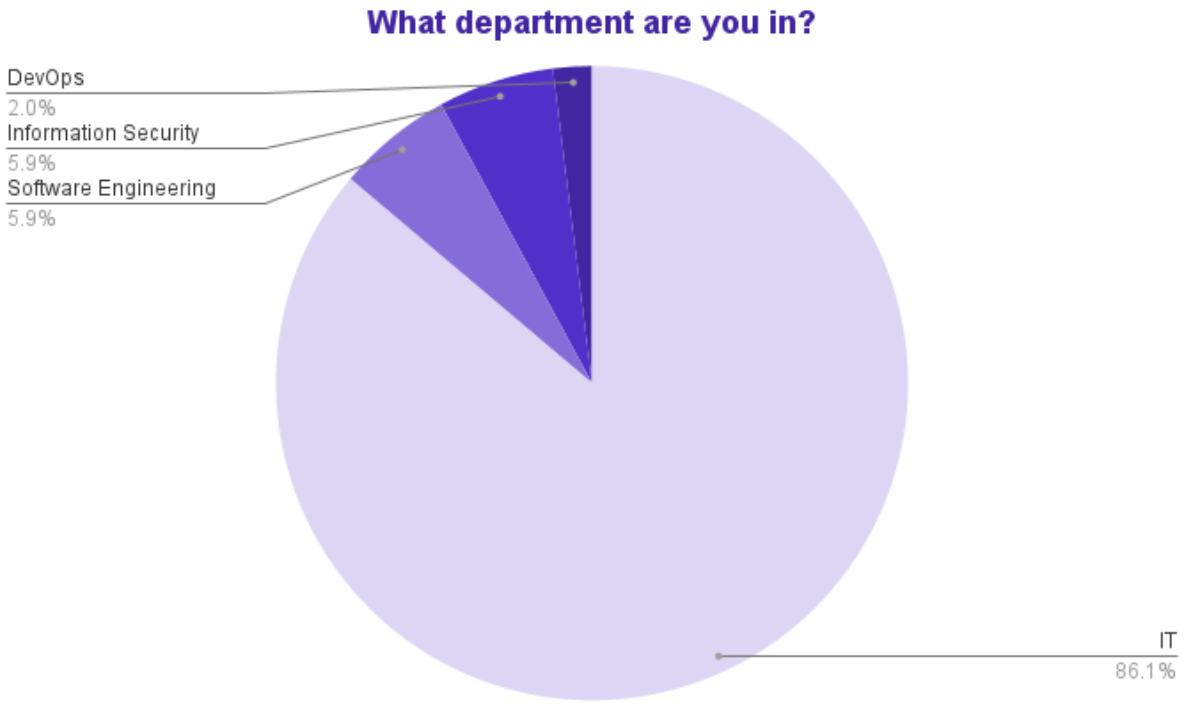
Methodology

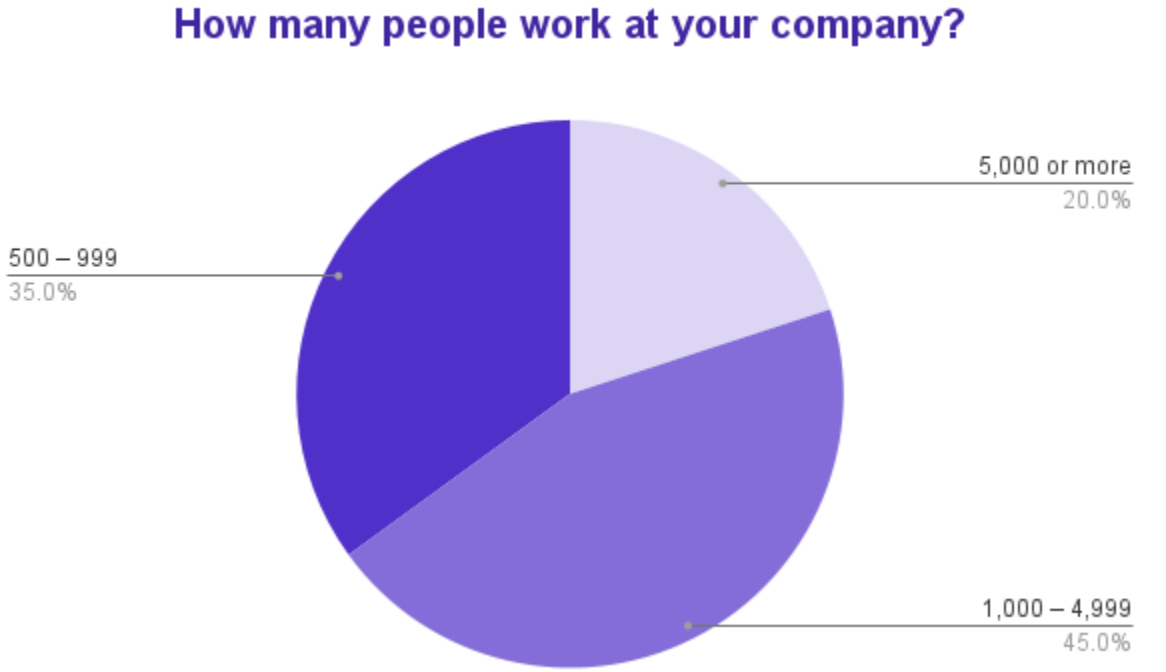
The *2021 Infrastructure Access and Security Report* survey collected a representative sample of IT, DevOps and Security professionals with knowledge about how their company manages access. A total of 1,000 respondents completed the survey, which was conducted by Schlesinger Group, an independent research company.

About Teleport

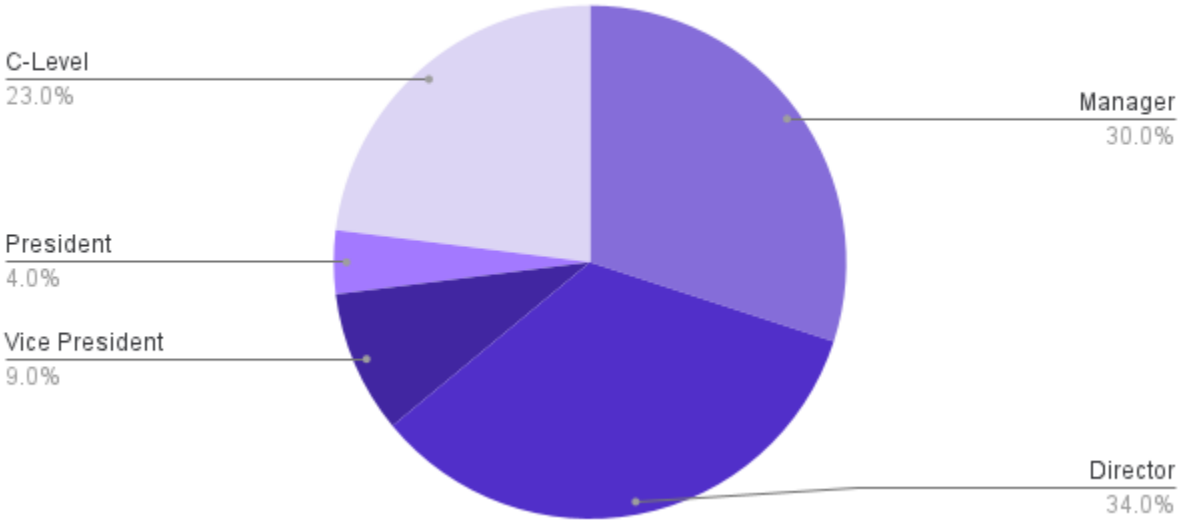
Teleport is the easiest, most secure way to access all a company's infrastructure. The open-source Teleport Access Plane consolidates the four essential infrastructure access capabilities every security-conscious organization needs: connectivity, authentication, authorization, and audit. Teleport's unique approach is not only more secure but also improves developer productivity. Teleport is used by leading companies, including Elastic, Samsung, NASDAQ, and IBM. The company is backed by Kleiner Perkins, Y Combinator and S28 Capital. Headquartered in Oakland, California, the company embraces a remote-first work culture.

Appendix: Report Data

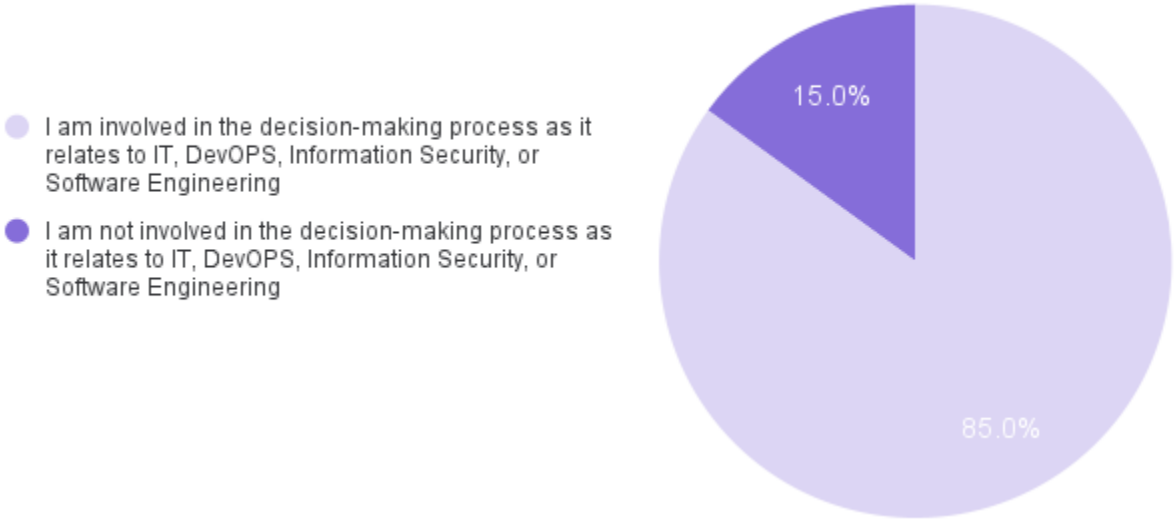


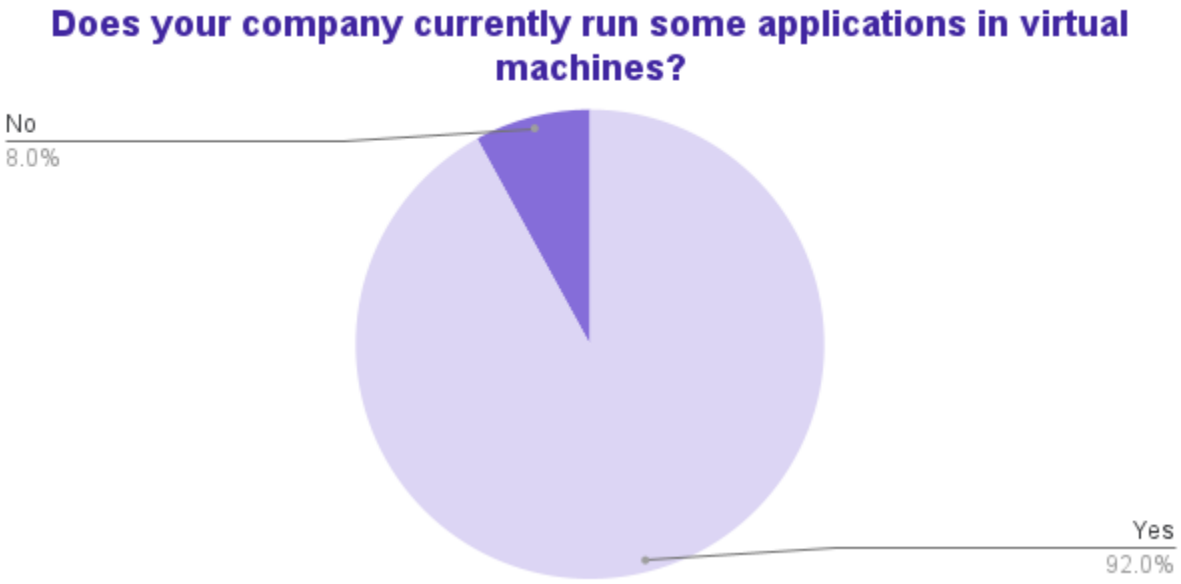


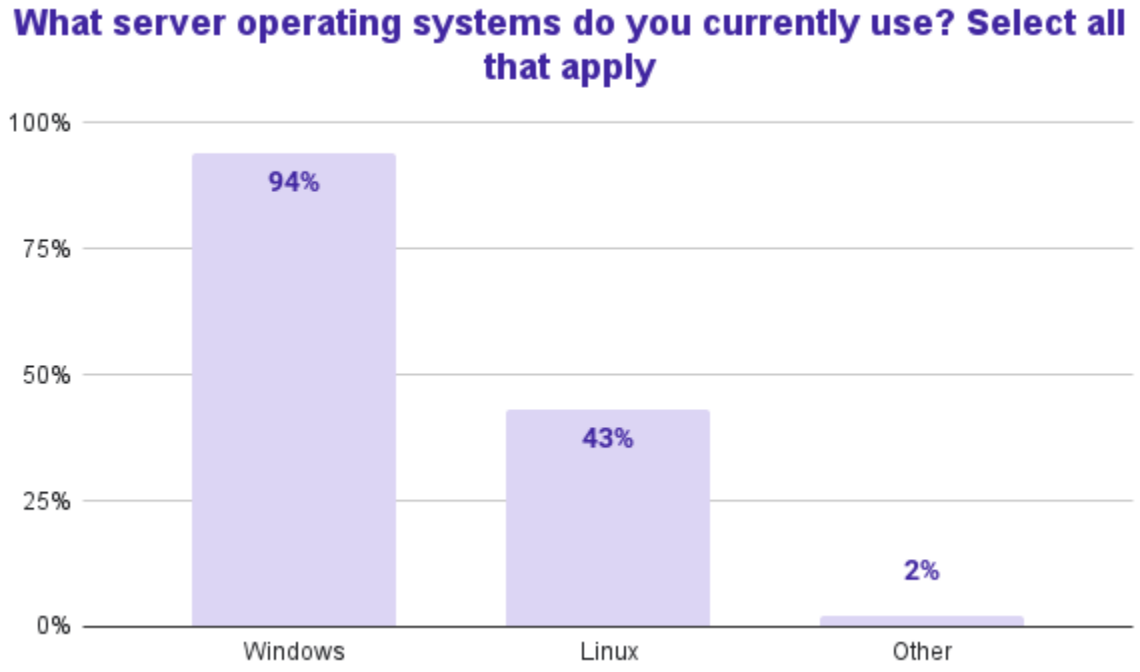
Which of the following best describes your title?

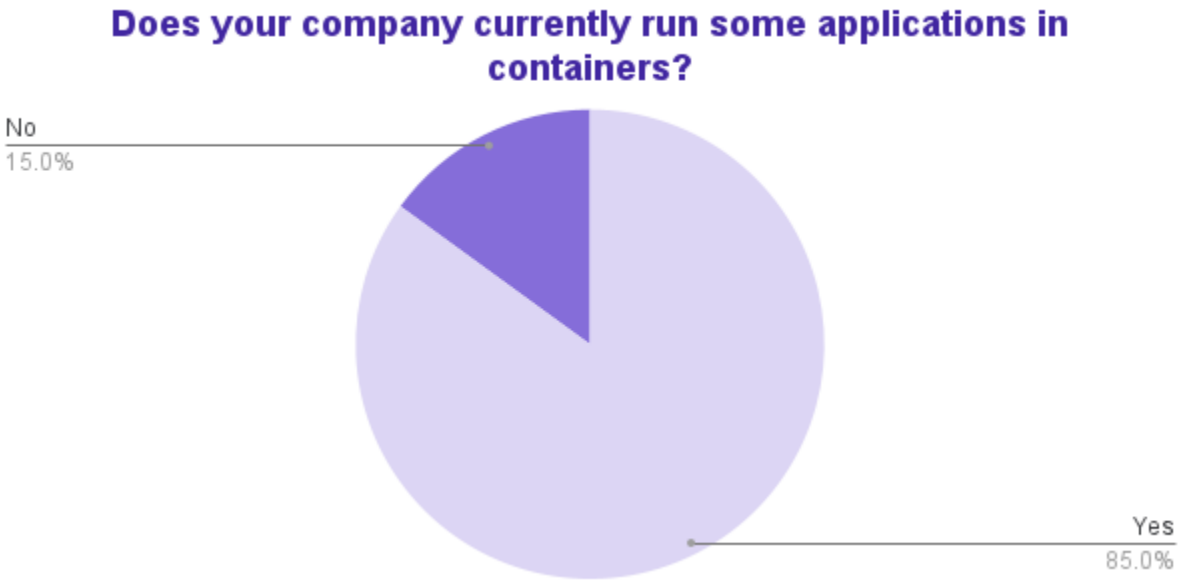


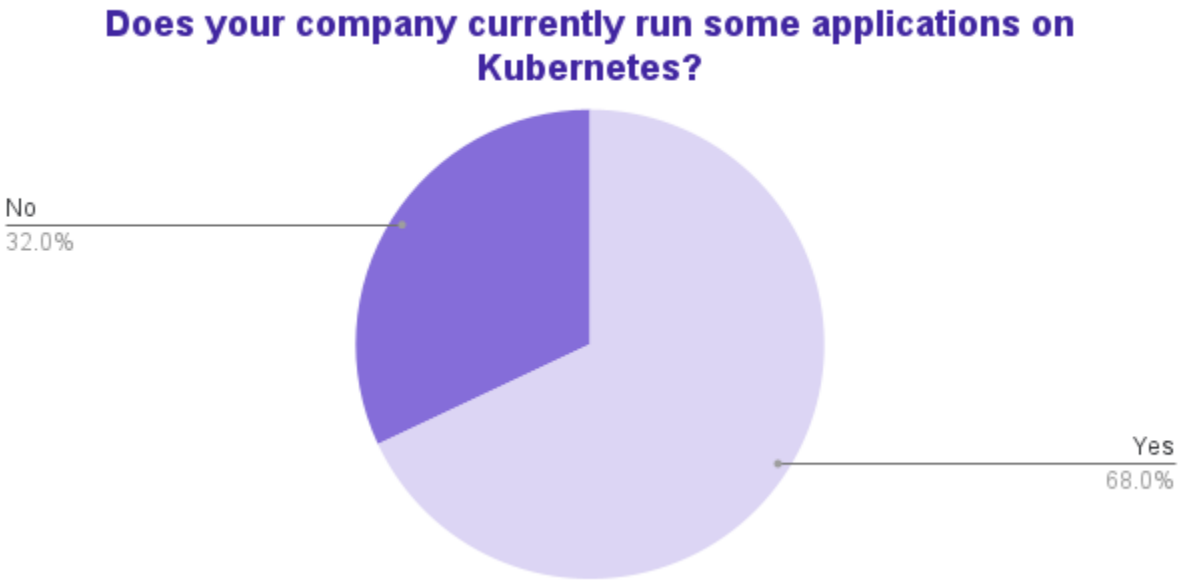
Which of the following best describes you?





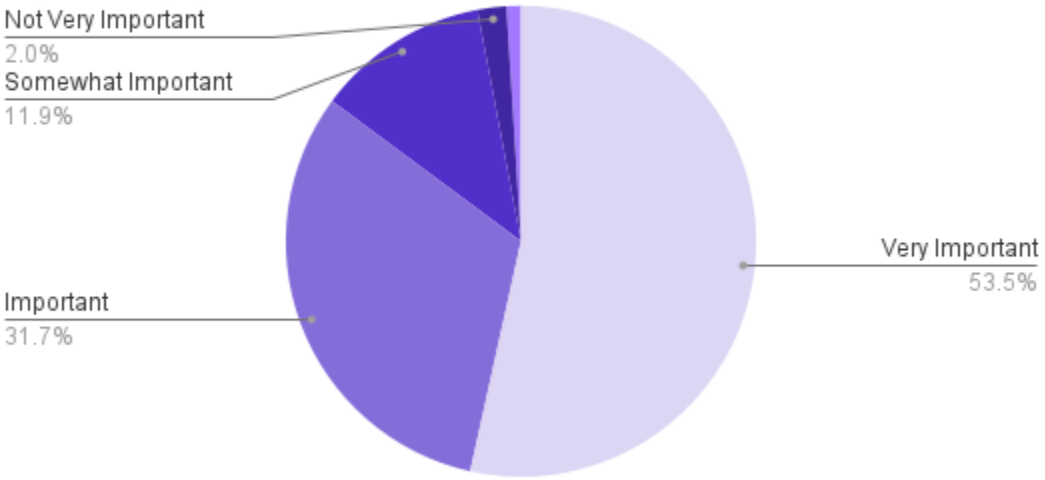




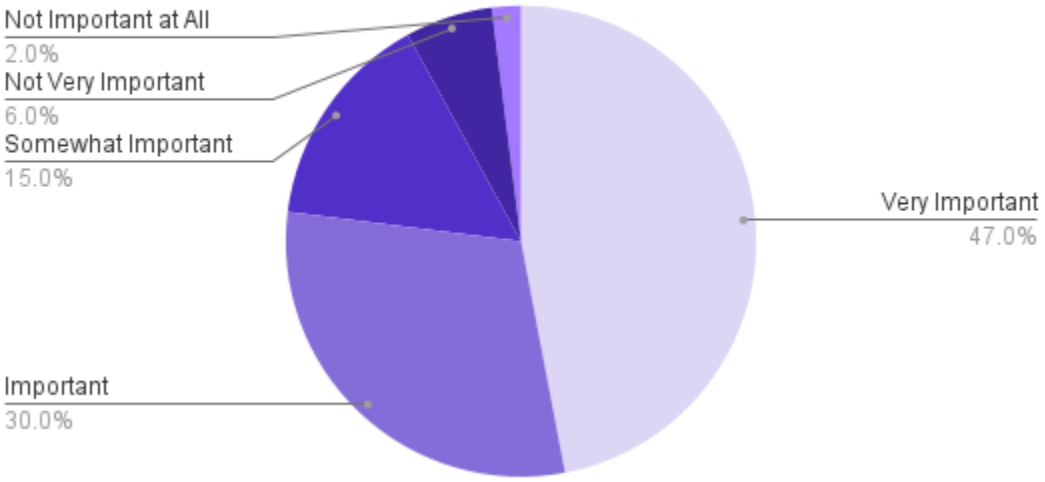


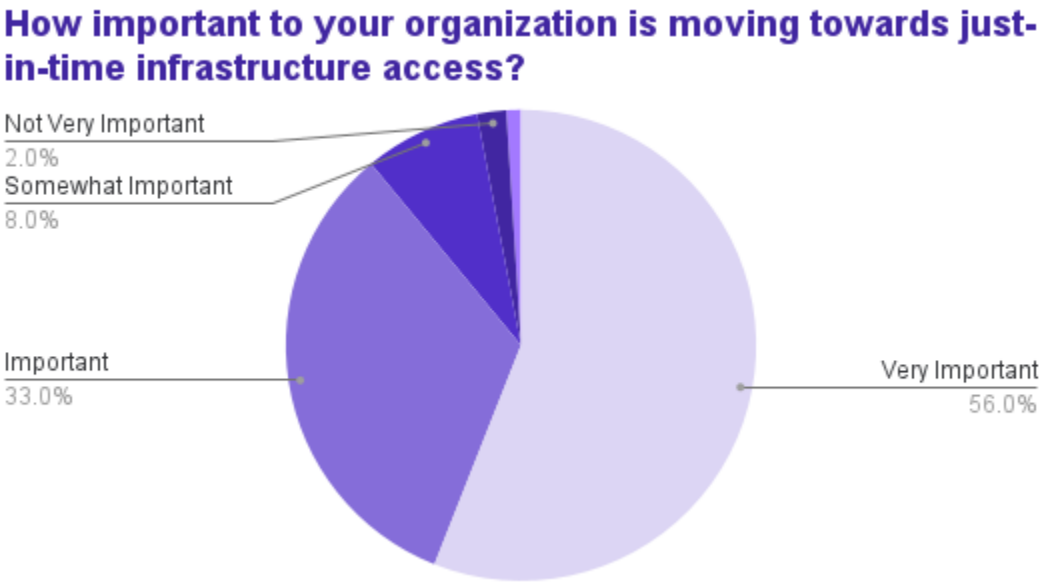
Which databases do your company currently use? Select all that apply.	
Microsoft Azure Database	67%
Microsoft SQL Server	50%
Oracle	41%
Amazon DynamoDB	41%
IBM Db2	34%
MySQL	22%
SAP Hana	17%
MongoDB	11%
Splunk	11%
Snowflake	9%
Cassandra	8%
PostgreSQL	8%
Elasticsearch	8%
CockroachDB	6%
MariaDB	6%
Hive	6%
Teradata	5%
Redis	4%
Other	1%

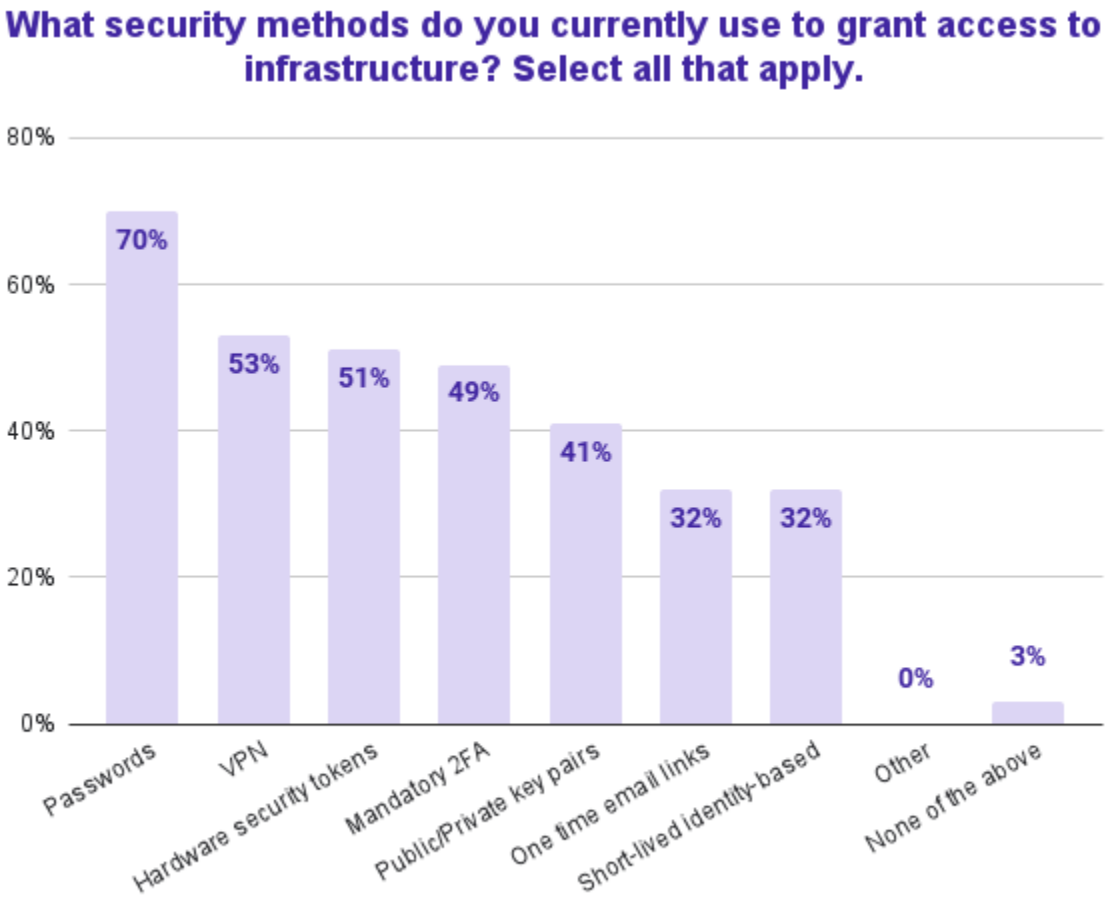
How important to your organization is moving towards zero-trust architectures?



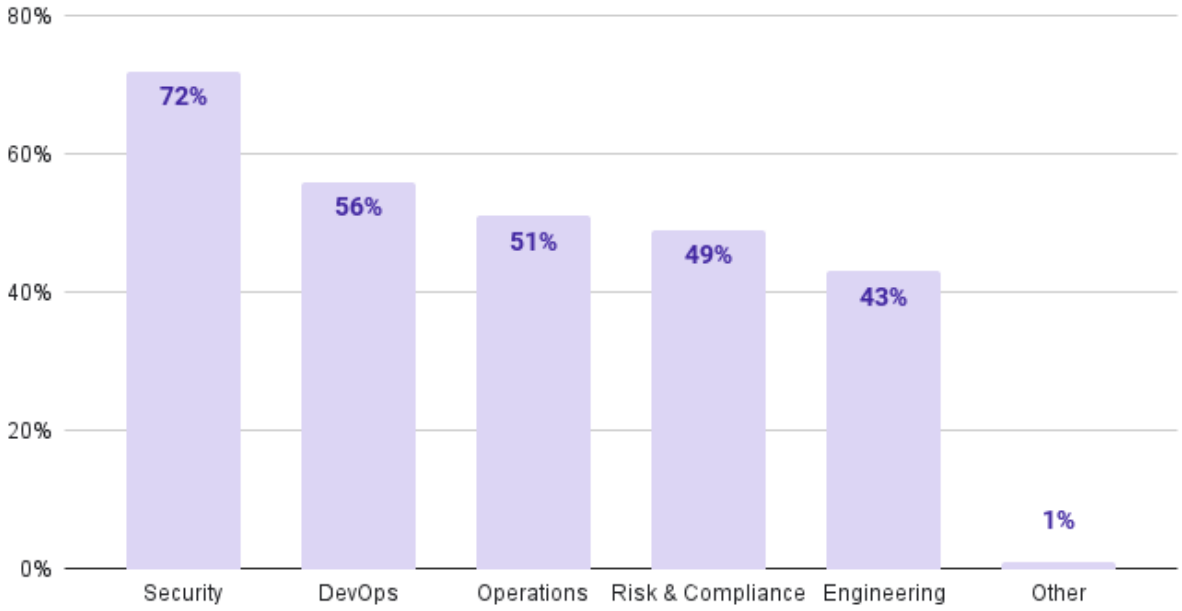
How important to your organization is moving towards passwordless infrastructure?



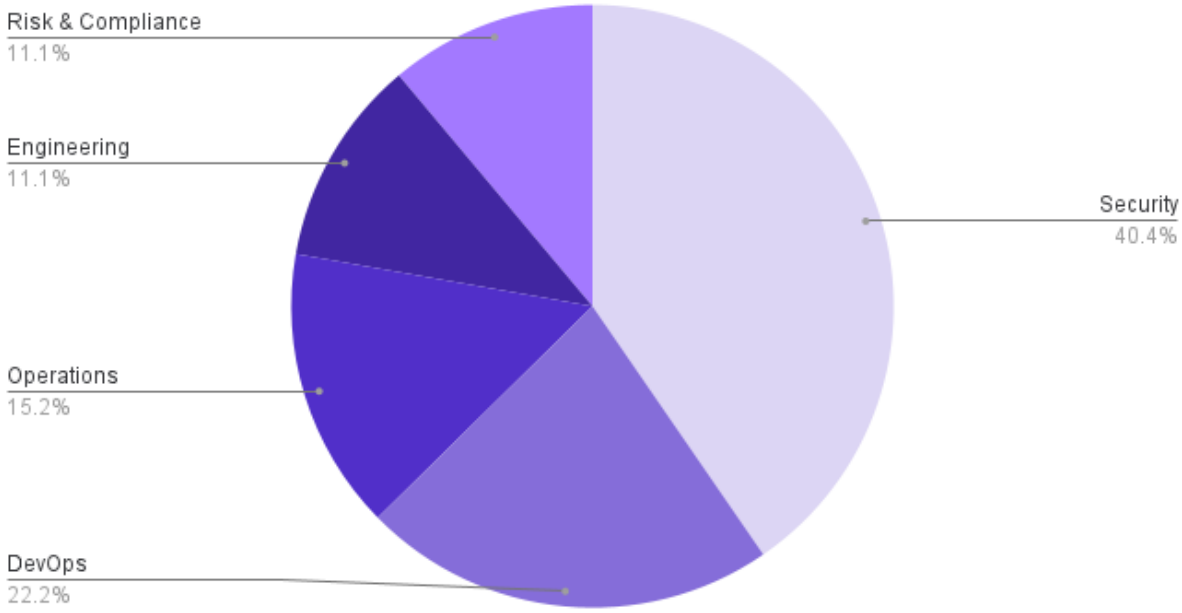




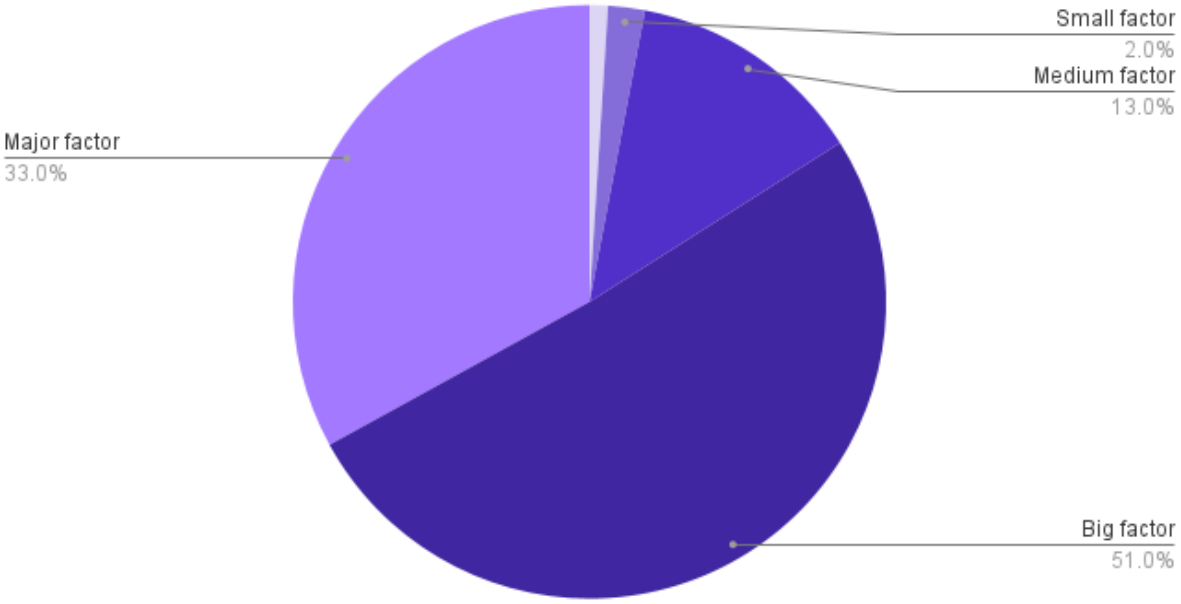
Which roles are responsible for infrastructure access in your organization? Select all that apply.



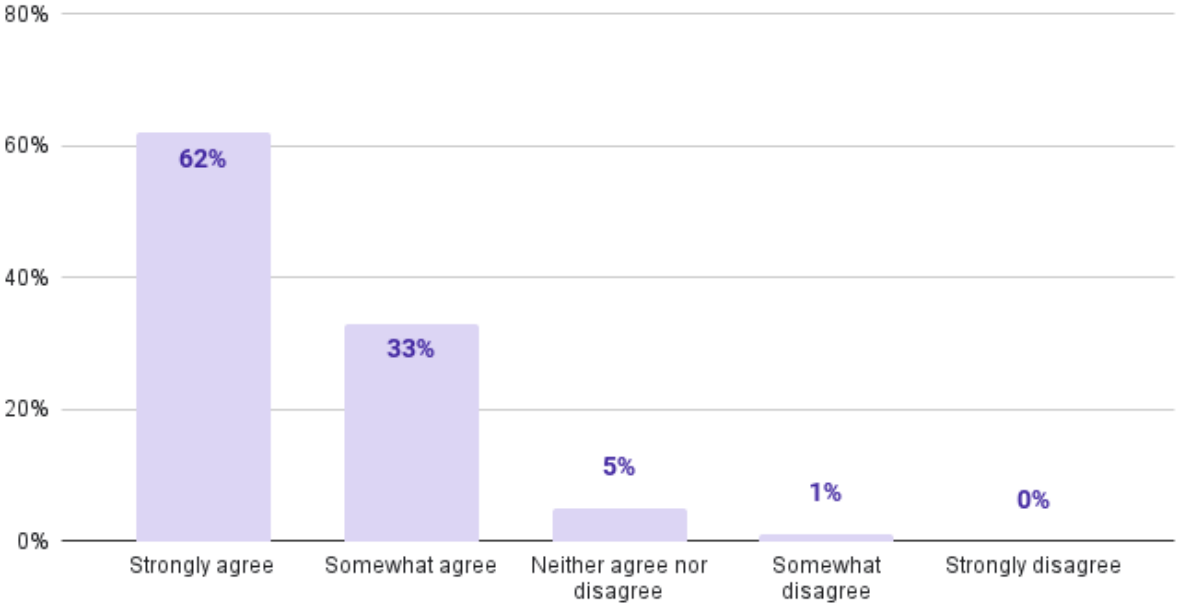
Which role is most responsible for infrastructure access in your organization?



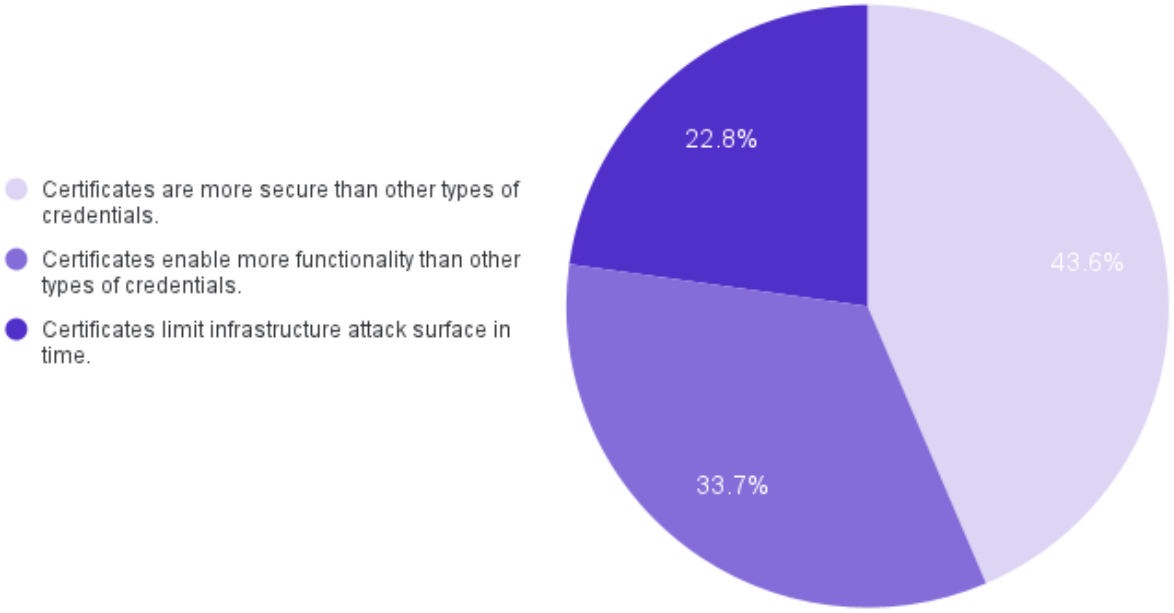
How much of a factor is developer productivity when considering implementing access controls?



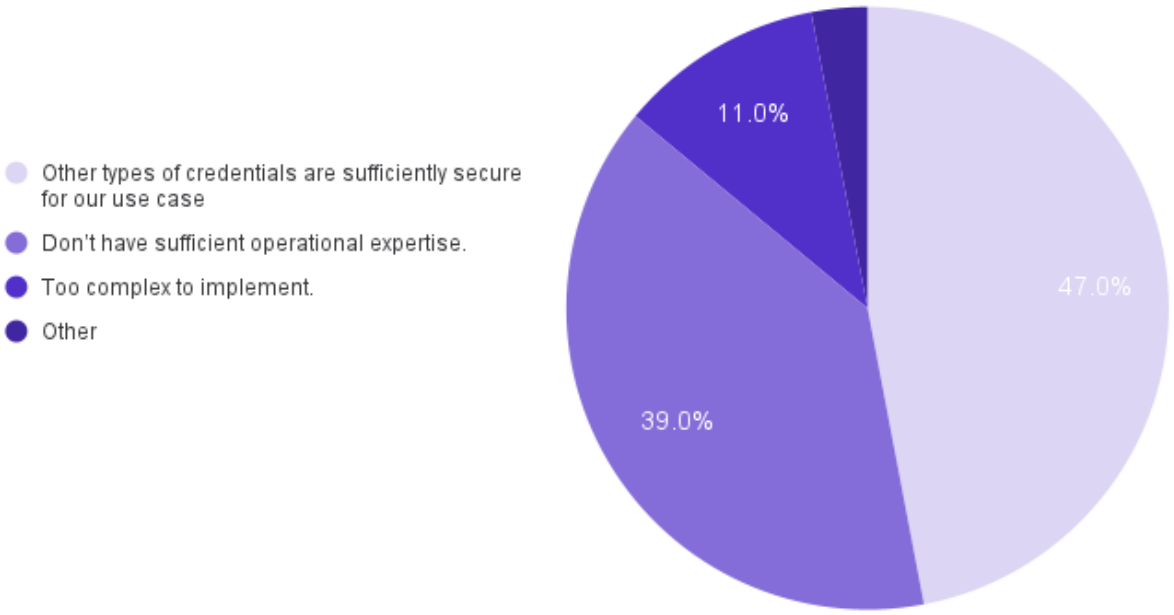
How much do you agree or disagree with the following statement? I believe that greater visibility into infrastructure access is critical to business success.



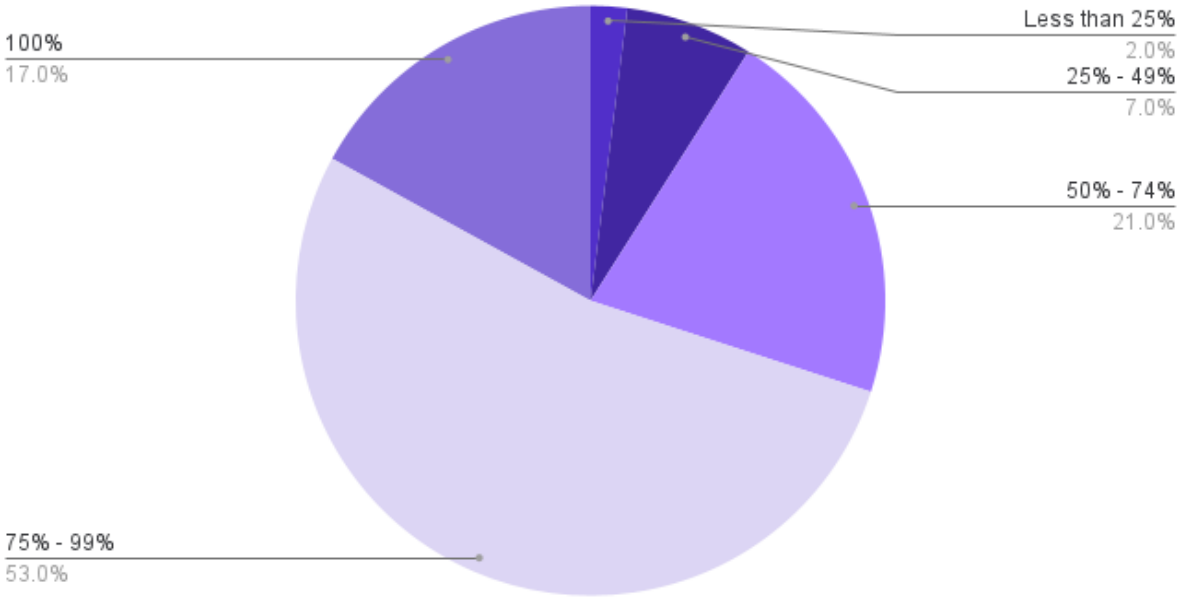
What is the primary reason you have implemented identity-based certificates to manage access to infrastructure?



What is the primary reason you have not implemented identity-based certificates?

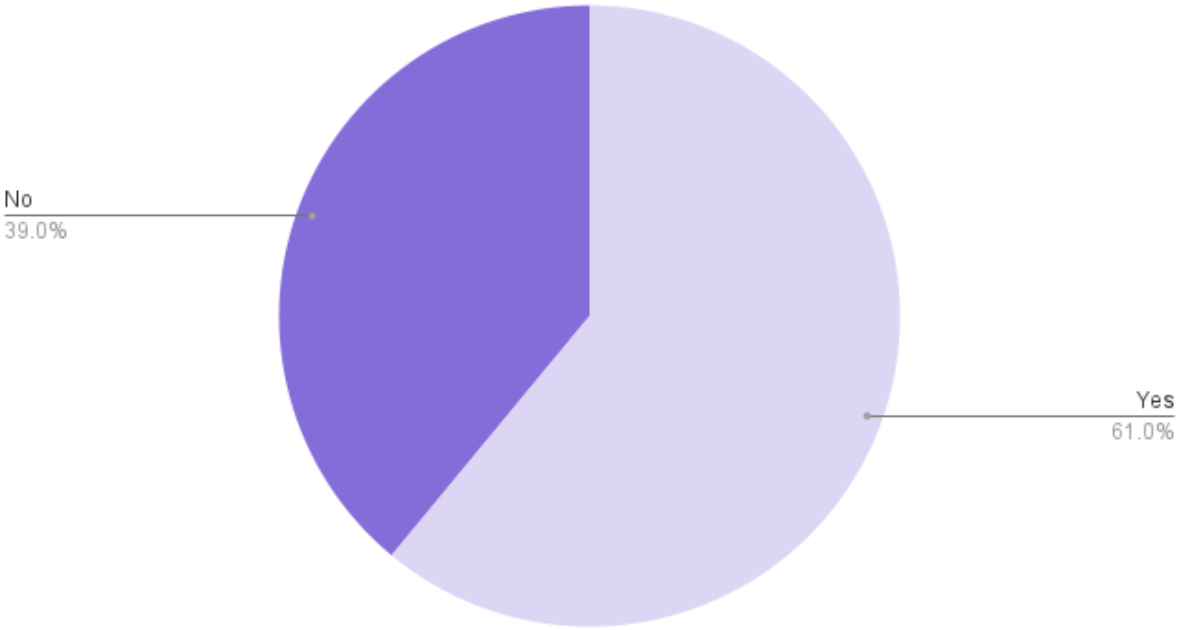


When an employee who has access to your infrastructure leaves your company, what is your confidence level that all their access keys have been revoked and they can no longer use those keys to access your infrastructure?

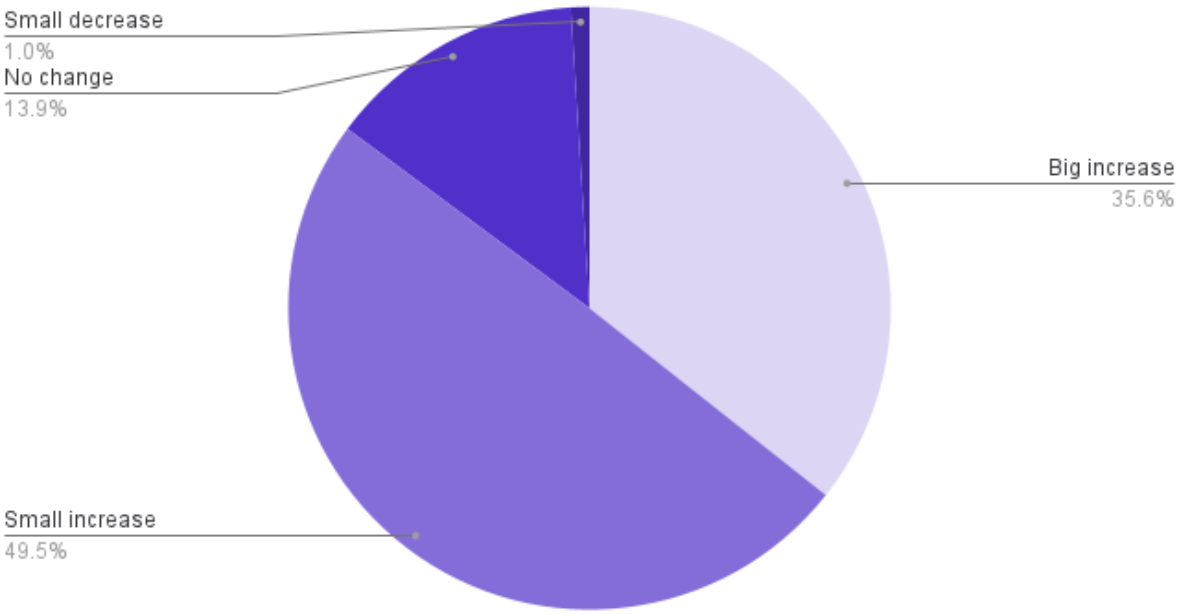


Rank the following challenges you have managing access to your infrastructure (e.g. servers, databases, Kubernetes clusters, internal apps like CI/CD).	Ranked in top 3	Ranked #1	Ranked #10
Implementing zero-trust access	38%	15%	8%
Connecting SSO provider responsible for managing employee identities with infrastructure resources	35%	13%	7%
Managing Key and password rotation	31%	9%	9%
Establishing secure connection to infrastructure resources spread across the globe	31%	9%	9%
Ensuring compliance with governing regulations	30%	12%	9%
Lack of a single solution to manage access in the same way for different resource types such as Linux and Windows servers, databases, Kubernetes clusters, CI/CD environments and more.	28%	9%	11%
Reporting visibility into behavior to fulfill compliance objectives	28%	8%	9%
Implementing passwordless access	28%	10%	11%
Managing VPNs	26%	10%	16%
Fine-grained role-based access control for infrastructure resources	26%	7%	13%

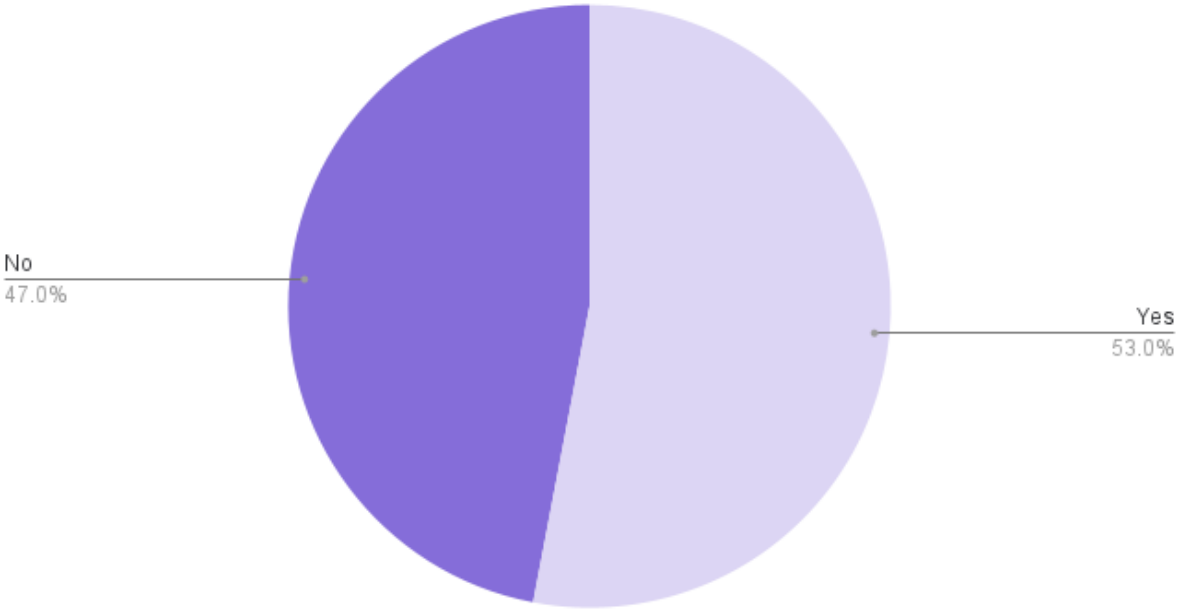
Have you experienced a time when an expert engineer has been unable to contribute to the resolution of an issue due to access issues?



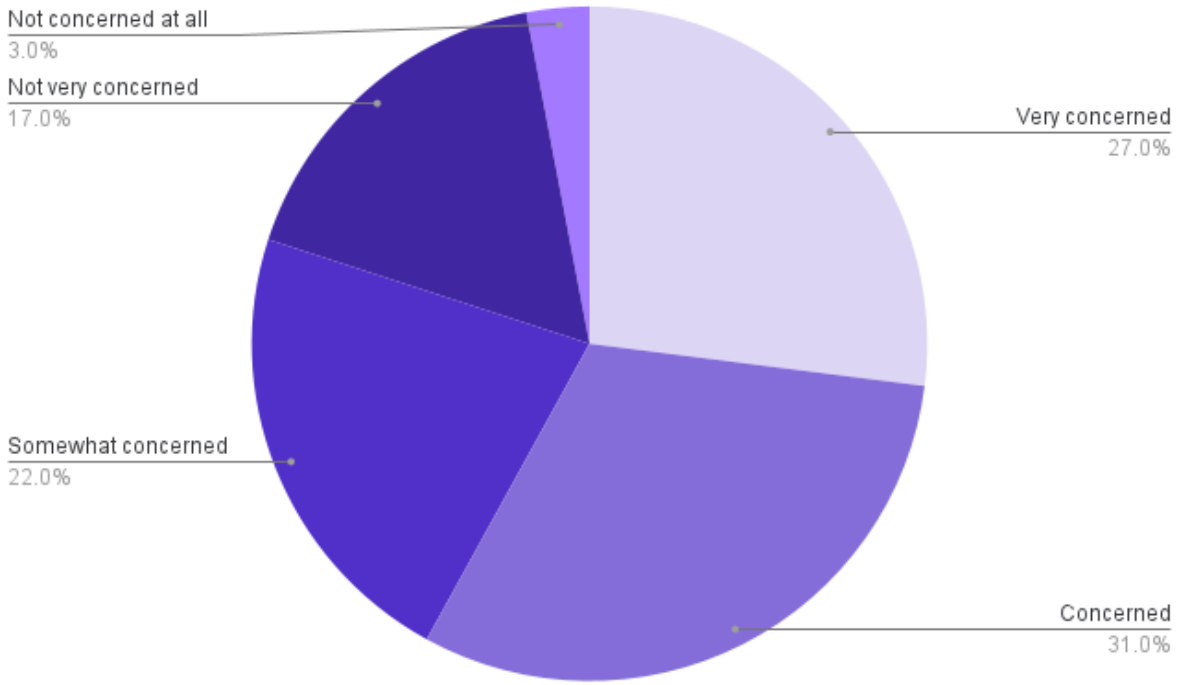
How will the budget for infrastructure access technology change in the next 12 months?



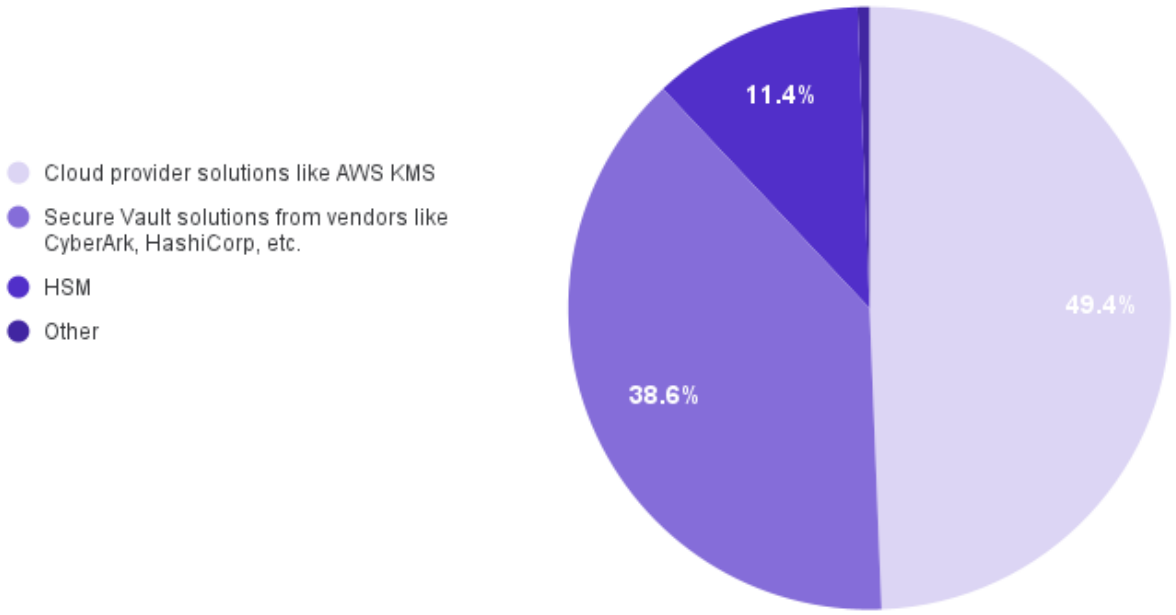
Has your organization implemented new security methods that failed to be adopted by employees?

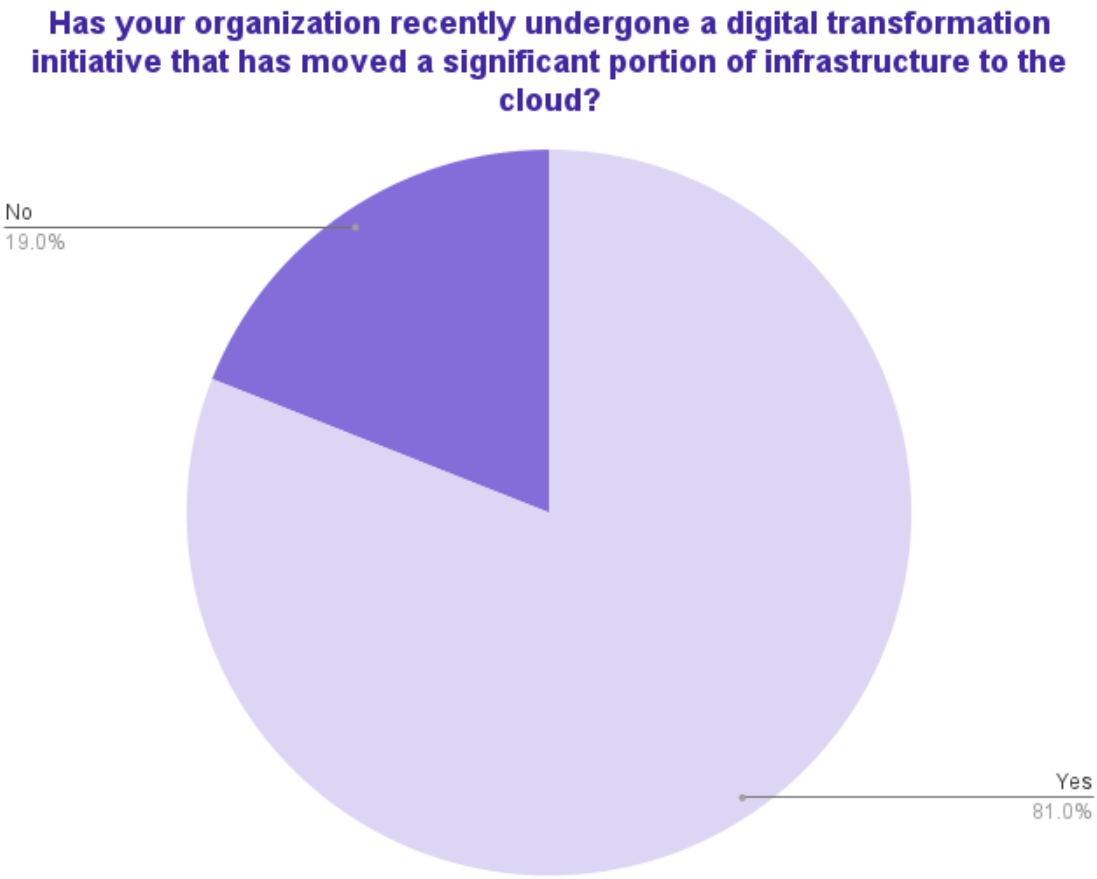


How concerned are you about employees leaving your organization with secrets (e.g. API keys or tokens) or knowledge about how to access your infrastructure?

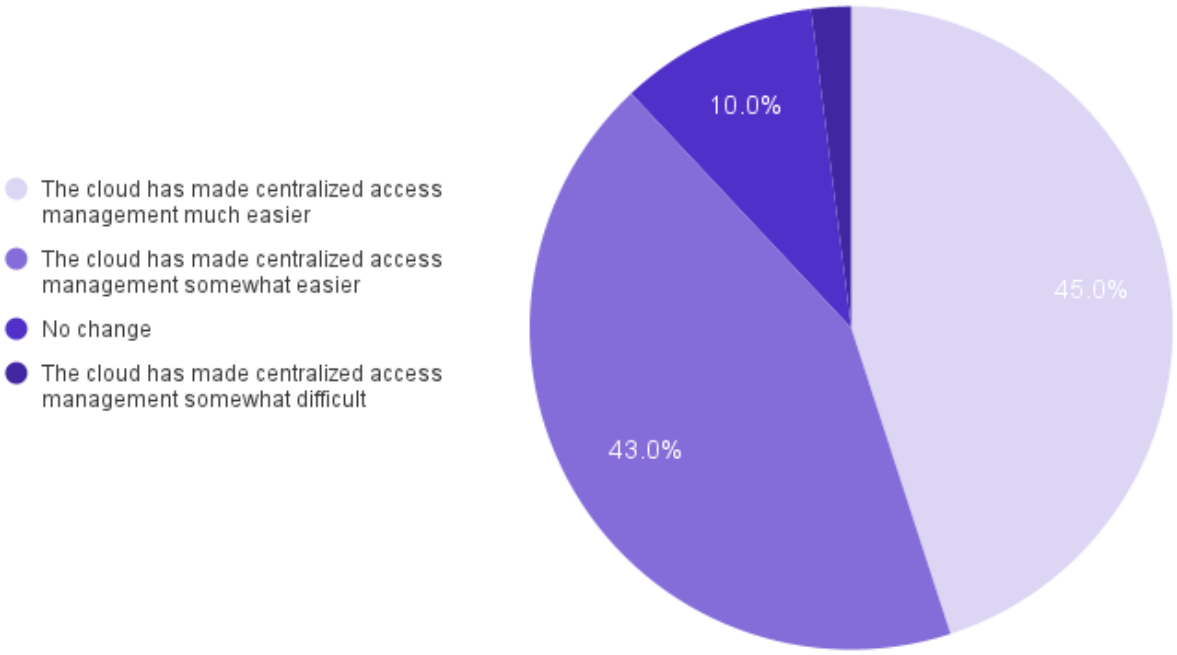


What do you use to securely store private keys, and/or shared credentials? Select all that apply.

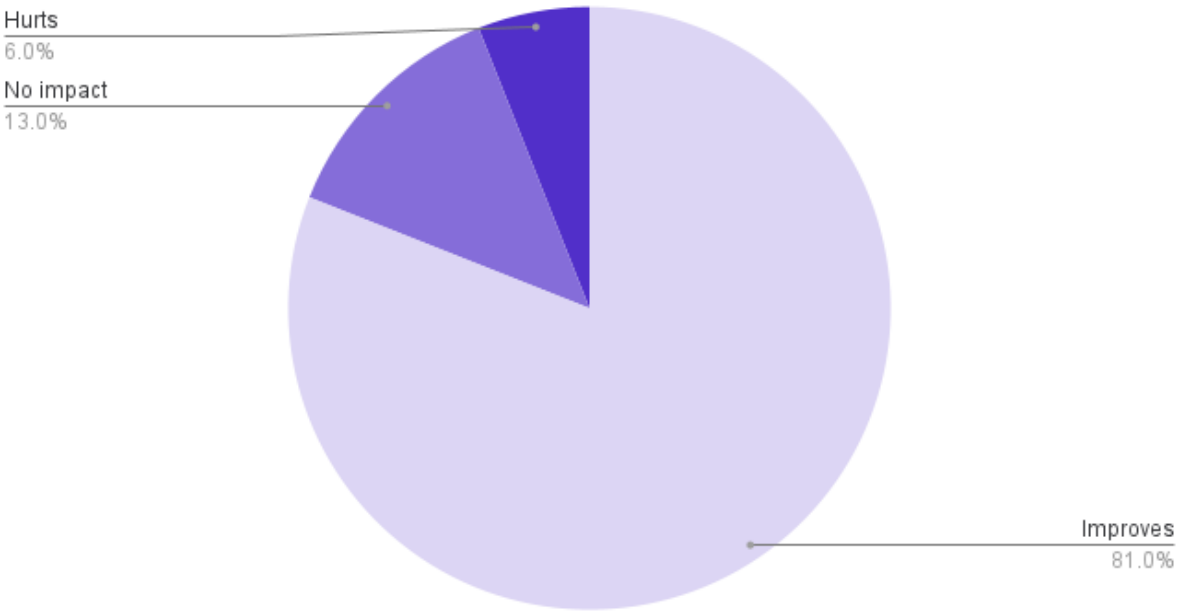




How has the cloud impacted infrastructure access management?



Does your organization's infrastructure access control scheme improve, hurt or have no impact on IT productivity?



In an average month, how many security challenges related to infrastructure access do you have to deal with?