Teleport

2024 State of Secure Infrastructure Access

Survey Report

Since the password was first introduced into computing in the early 1960s, it has had the singular goal of holding back the hordes: hackers, criminals, hostile nation-states, insiders, and countless other malicious black hats.

It has been a lonely vigil, and the headlines show it has been a losing battle. Amazon, Apple, Microsoft, Marriott, and Uber have all experienced high-profile data breaches in recent years. Why is it that some of the world's most technically advanced, highly funded companies failed to secure their computing systems? And if they failed, what hope do the rest of us have?

It was precisely these questions that motivated Teleport to commission our **2024 State of Secure Infrastructure Access survey**. We wanted to learn how large enterprises sought to secure their valuable computing infrastructure, and how their efforts were going. And ultimately, we hoped to learn the best practices that would allow enterprises to gain the upper hand.

What we found was very interesting ...

Contents

Secure Infrastructure Access Matters

Securing access to computing infrastructure is extremely important to the enterprises we spoke to. But infrastructure access security isn't easy. Three of four say it is getting somewhat hard to extremely harder each year. Why?

- **Cloud computing** complicates securing access to computing infrastructure due to its distributed nature, which increases potential entry points and requires robust, scalable security measures across diverse environments.
- **An increase in identity attacks** complicates securing access to computing infrastructure by making it challenging to distinguish between legitimate users and malicious actors, thereby undermining access control and security measures.
- As **infrastructure becomes more complex**, securing access to computing systems becomes more challenging due to the increased number of potential vulnerabilities and entry points that need to be managed and protected.
- **Remote work** makes it harder to secure access to computing infrastructure, because it often involves diverse and unsecured home networks, increasing the risk of unauthorized access and data breaches.
- **Malicious actors are using AI** to craft attacks. This makes attacks cheaper to execute and more effective.

As to what, exactly, is more challenging, enterprises cite five big challenges:

- **Massive scope of what they're protecting** complicates securing access due to the increased scale, complexity, and diversity of components that need to be managed and protected.
- **The proliferation of credentials and secrets** from emerging silos such as cloud, edge, and IoT significantly complicates securing access to computing infrastructure by introducing a multitude of diverse and numerous access points that require meticulous management and constant vigilance.
- **An expanding attack surface** (cloud, microservice architectures, containers, etc.) increases complexity and potential vulnerabilities, making it more challenging to secure access to computing infrastructure.
- **Regulatory compliance** adds complexity to securing access to computing infrastructure by imposing stringent requirements and controls that must be meticulously followed to protect sensitive data and ensure legal adherence.
- **Support of DevOps methodologies** complicates securing access to computing infrastructure due to the dynamic and collaborative nature of continuous integration and delivery, which demands frequent changes and broad access permissions.

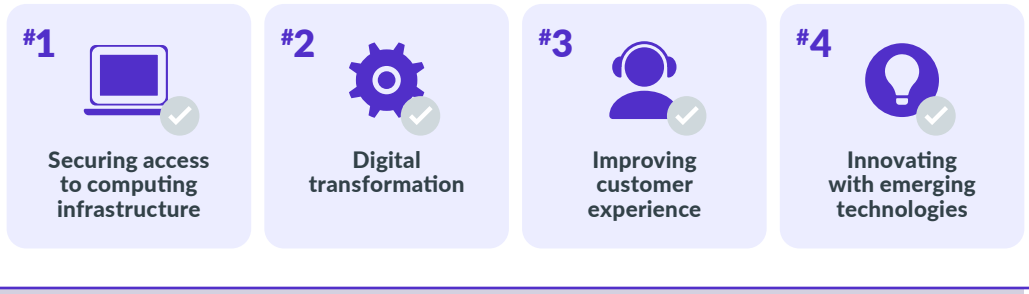
We asked enterprises to tell us what are the most difficult attacks to protect against. They responded with five attack vectors:

- **AI impersonation by threat actors** is difficult to defend against because it can mimic legitimate user behavior with high accuracy, making it challenging to distinguish between genuine and malicious access attempts.
- **Social engineering attacks**, like phishing, are difficult to defend against because they exploit human psychology and trust, often bypassing technical security measures by manipulating individuals into revealing sensitive information.
- **Compromised privileged credentials and secrets** are difficult to defend against because they provide attackers with elevated access, making it challenging to detect unauthorized activities and secure the computing infrastructure effectively.
- **Breach and pivot attacks** are challenging to defend against in securing access to computing infrastructure due to their complex nature and the stealth tactics employed, allowing attackers to move laterally within a network undetected.
- **MFA resets** are challenging to defend against because attackers can exploit social engineering tactics to manipulate support staff or users into bypassing security protocols, thereby compromising access to computing infrastructure.

In summary, we found that securing access to computing infrastructure was important, but getting more difficult by the day. How important? We asked respondents to rank their IT initiatives by importance. It turns out that **infrastructure access security is more important than any of the leading IT initiatives** enterprises are commonly working on, such as digital transformation, improving the customer experience, or driving innovation with emerging technologies.

With this level of importance, we were curious about what enterprises are doing to secure infrastructure access.

Secure Infrastructure Access: Top Technology Initiative



State of Secure Infrastructure Access Practices

Enterprises employ a wide range of security safeguards designed to secure infrastructure access. The most common cited tactics are listed here, in order of adoption:

- **Multi-factor authentication:** MFA enhances security by requiring multiple forms of verification, making unauthorized access to computing infrastructure significantly harder.
- **VPN:** Crucial for securing access to computing infrastructure by encrypting data and protecting it from unauthorized access.
- **Identity Provider (IdP):** Secures access to computing infrastructure by centralizing authentication and ensuring only authorized users can access sensitive resources.
- **SSO:** Enhances security by centralizing authentication, reducing password fatigue, and minimizing potential attack vectors.
- **Using AI to make safeguards more accurate and effective:** Analyzes patterns and detects anomalies.
- **Phishing-resistant password-less authentication:** Enhances security by effectively preventing unauthorized access to computing infrastructure.
- **Zero Trust Networking:** Minimizes security risks by continuously verifying every access request.
- **Use of cryptographically authenticated identities for systems or resources:** Prevents guessing of passwords (or obtaining them through phishing).
- **A unified store for all identities (people, machines, services):** Streamlines authentication and authorization, enhancing security by providing centralized control and monitoring of access to computing infrastructure.
- **Use of cryptographically authenticated identities for users:** Makes it more difficult to guess passwords (or obtain them through phishing).
- **PAM:** Privileged Access Management (PAM) enhances security by controlling and monitoring privileged access to critical computing infrastructure.
- **IGA/ITDR:** Identity Governance and Administration (IGA) and Identity Threat Detection and Response (ITDR) solutions provide enhanced security by controlling access and detecting threats to computing infrastructure.
- **CIEM:** Cloud Infrastructure Entitlement Management (CIEM) ensures only authorized users have access to specific cloud resources, reducing the risk of unauthorized access.

Clearly, enterprises implement safeguards on a wide range of fronts. How effective are these efforts?

How is Secure Infrastructure Access Faring?

Enterprises are mostly doing well when it comes to securing access to their computing infrastructure. For example, here are the outcomes where enterprises say they are doing well:

- **Protecting sensitive data**
- **Ensuring systems availability**
- **Preventing unauthorized access**
- **Complying with regulations**
- **Maintain systems integrity**
- **Passing compliance audits**

At least four out of five say they are doing "somewhat to extremely well" in each area. But, the costs of even one failure can be catastrophic: millions of dollars, key people fired, loss of reputation, and so on. This makes securing infrastructure access seem a bit like shooting an arrow through an apple on someone's head — getting close just isn't enough; only perfection will do.

So, what areas were enterprises most likely to say they were doing poorly?

- **Complying with regulations**
- **Passing compliance audits**
- **Preventing unauthorized access**
- **Protecting sensitive data**
- **Maintain systems integrity**
- **Ensuring systems availability**

The astute reader will notice this is the same list. How can that be?

How can companies be doing well while simultaneously doing poorly?

Actually, they aren't. The truth hidden in the averages: some enterprises have done quite well, while others are doing poorly. In fact, those doing poorly had more bad news:

- **14%** say they cannot react quickly to security incidents.
- **19%** cannot quickly determine who has access to infrastructure resources.
- **18%** say their efforts at preventing security incidents are less than effective.

Ensuring Compliance

We asked enterprises how they ensured that the rank-and-file properly adhered to corporate standards for infrastructure access security.

The respondents were flat. About half of enterprises enforce infrastructure access through code, whereas 41% publish their standards and ask for compliance.

Secure Infrastructure Access Lessons from Leaders

To find the differences between enterprises that excel at infrastructure access security, and those that struggle, we divided them into three buckets:

- **Leaders:** Enterprises that reported the best outcomes
- **Average:** Enterprises that reported neither the best nor the worst outcomes
- **Novices:** Enterprises that reported the worst outcomes

How we defined “Leaders” and “Novices”

There were 10 questions in the survey that pertained to how well (or how poorly) an enterprise had performed in their infrastructure access security efforts:

- **Rate how well you are performing in specific areas.**
- **How have your organization’s security initiatives affected development in terms of agility and time-to-market?**
- **How many security incidents have you experienced in the past 3 years?**
- **Which consequences have you experienced as a result of these incidents?**
- **Estimate the total cost of these consequences.**
- **How has the threat of security incidents changed over time?**
- **How would you characterize the efforts your organization is making toward preventing security incidents?**
- **How quickly can you determine who has access to various infrastructures?**
- **How quickly can you react to security incidents?**
- **Rate the importance of the following technology initiatives.**

These performance-based responses were graded on a five-point scale: -2 for the worst performances through +2 for the best.

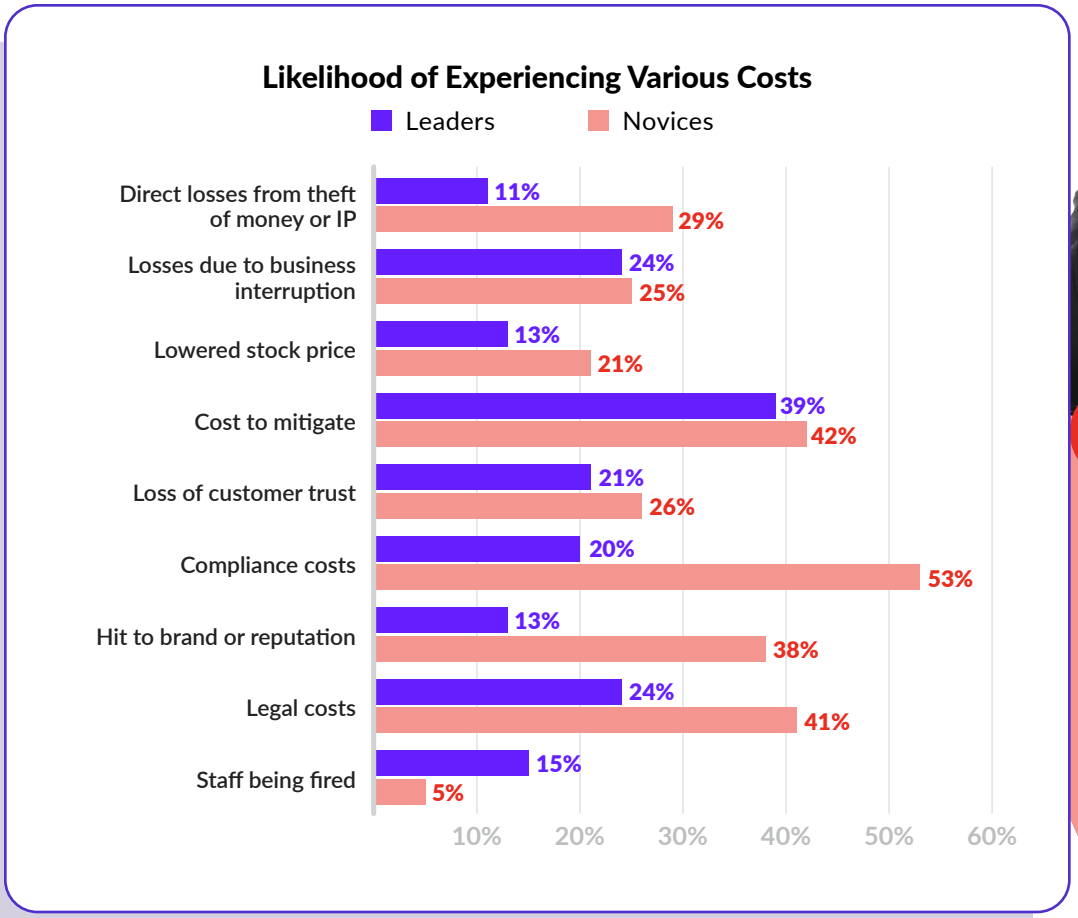
The sum of each respondent’s answers gave a total score for their infrastructure access security efforts, which allowed them to be sorted into the following 3 tiers:

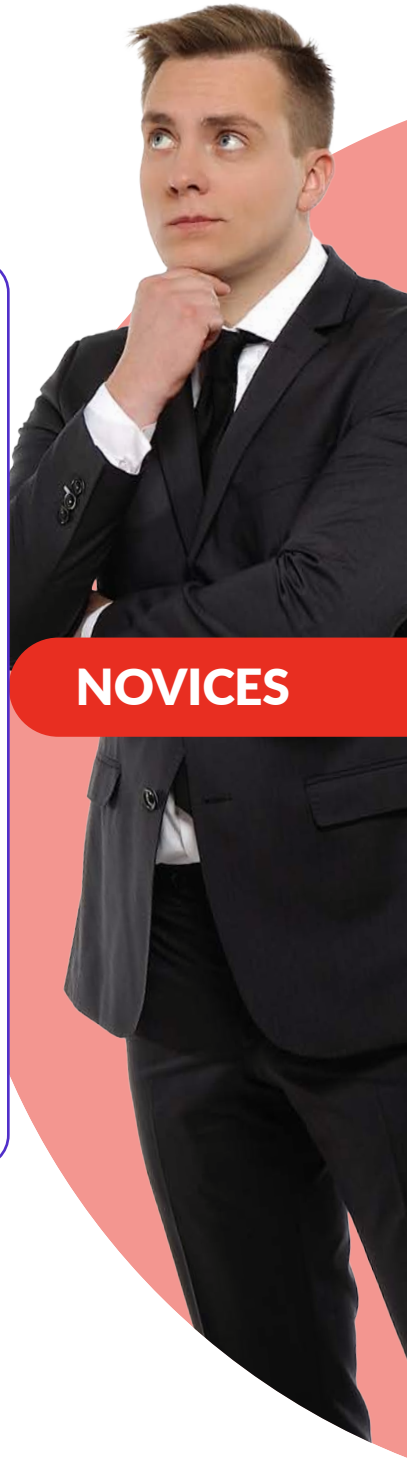
- **Leaders:** Enterprises that scored in the top third of all respondents
- **Average:** Enterprises that scored in the middle third of all respondents
- **Novices:** Enterprises that scored in the bottom third of all respondents

By definition, Leaders are better performers than the Novices. But how much better? The chasm between them was dramatic, especially when it came to security incidents (such as data breaches, ransomware, unauthorized access, etc.).

While Novices experienced an average of 12 security incidents over the past 3 years, Leaders on average experienced just 2 incidents.

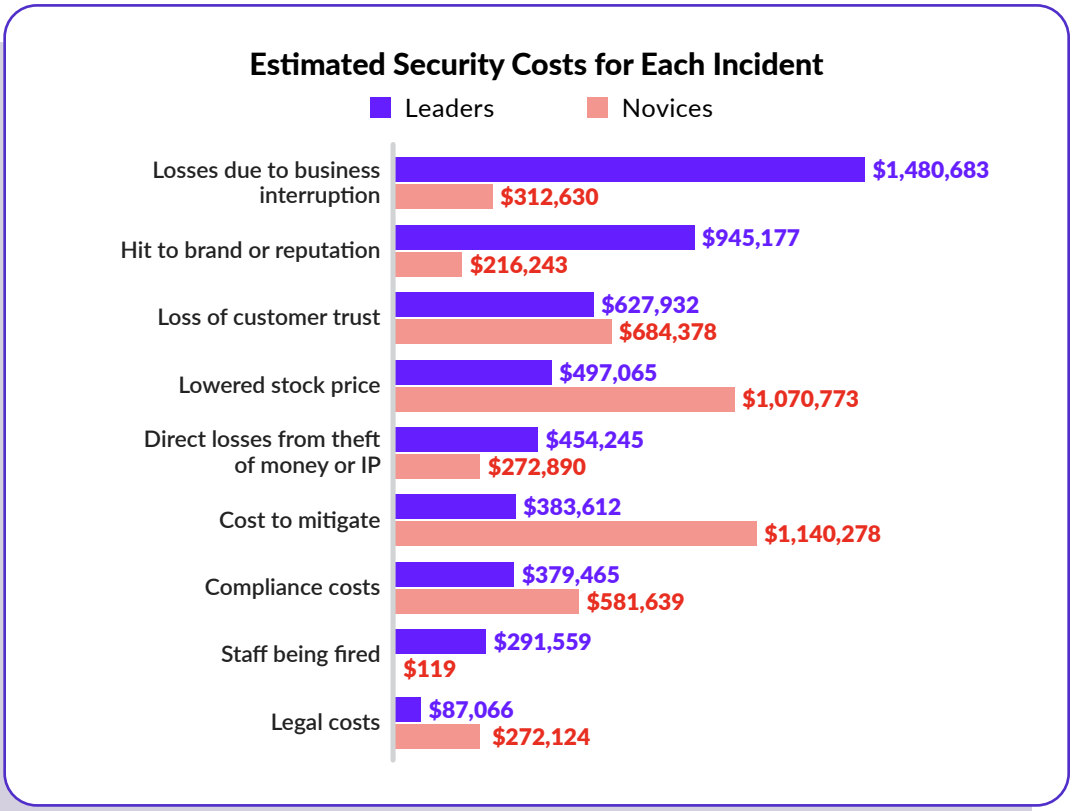
Still, there is more to the story. We looked at the types of costs respondents experienced, and while both groups identified the costs shown in the figure below, **the Novices were 50% more likely, on average, to have experienced these costs.**





We also measured the difference in the magnitude of these costs.

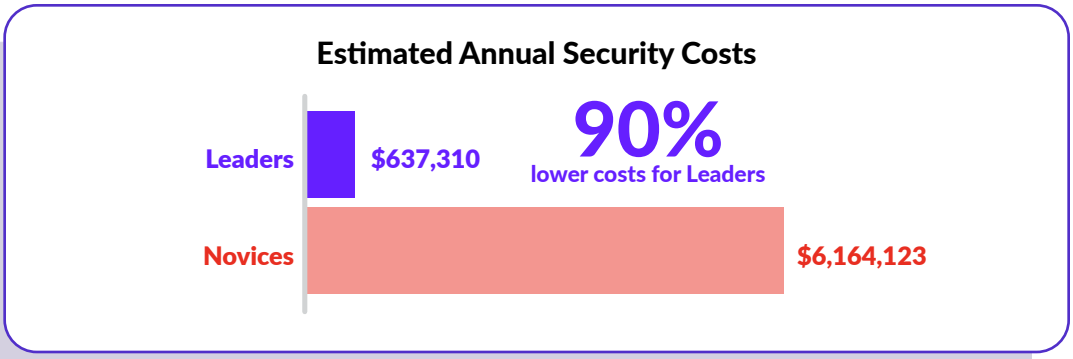
For roughly half of the cost types, Leaders incurred higher costs per security incident, while Novices incurred higher costs for the other half.



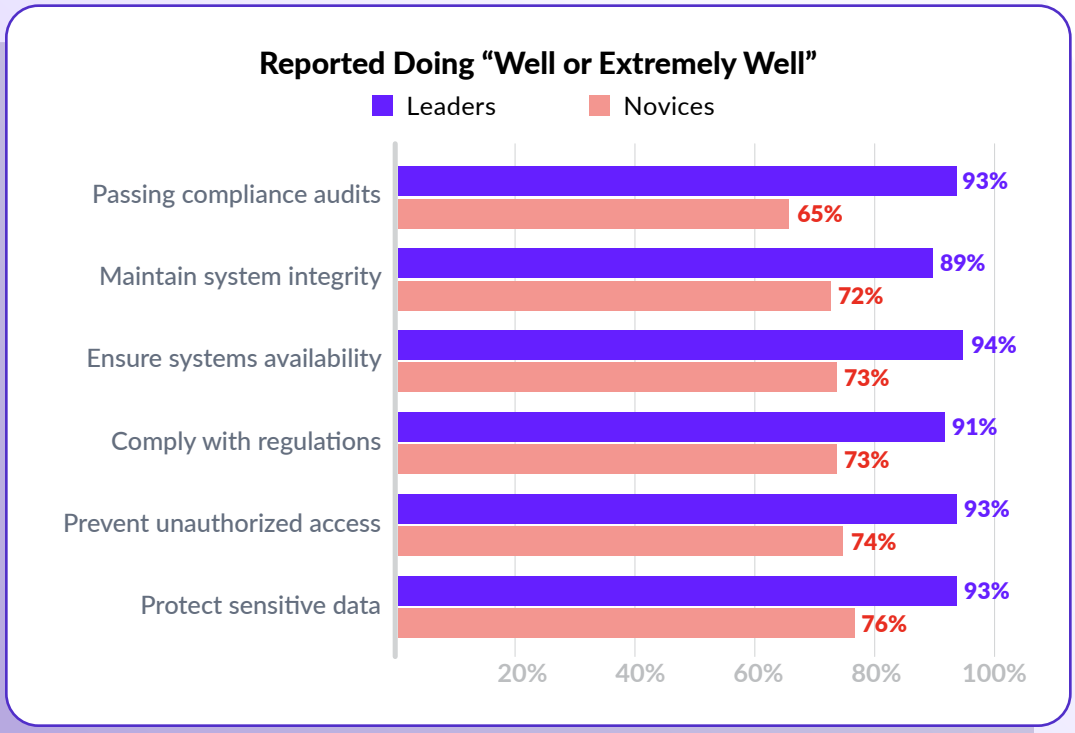
But the most important measure was the annualized cost of security incidents.

We calculated the total costs per security incident by factoring the likelihood each cost was incurred for the Leader and Novice, multiplied by the cost per incident, and summed for the total incidents over three years. This was then normalized as an annualized cost.

The infrastructure access security Leader incurred **90 percent less cost per year** than Novices.



These differences in outcomes persisted throughout the results. For example, **Leaders were 20% more likely on average to report doing somewhat well to extremely well** in a wide variety of infrastructure access security outcomes.

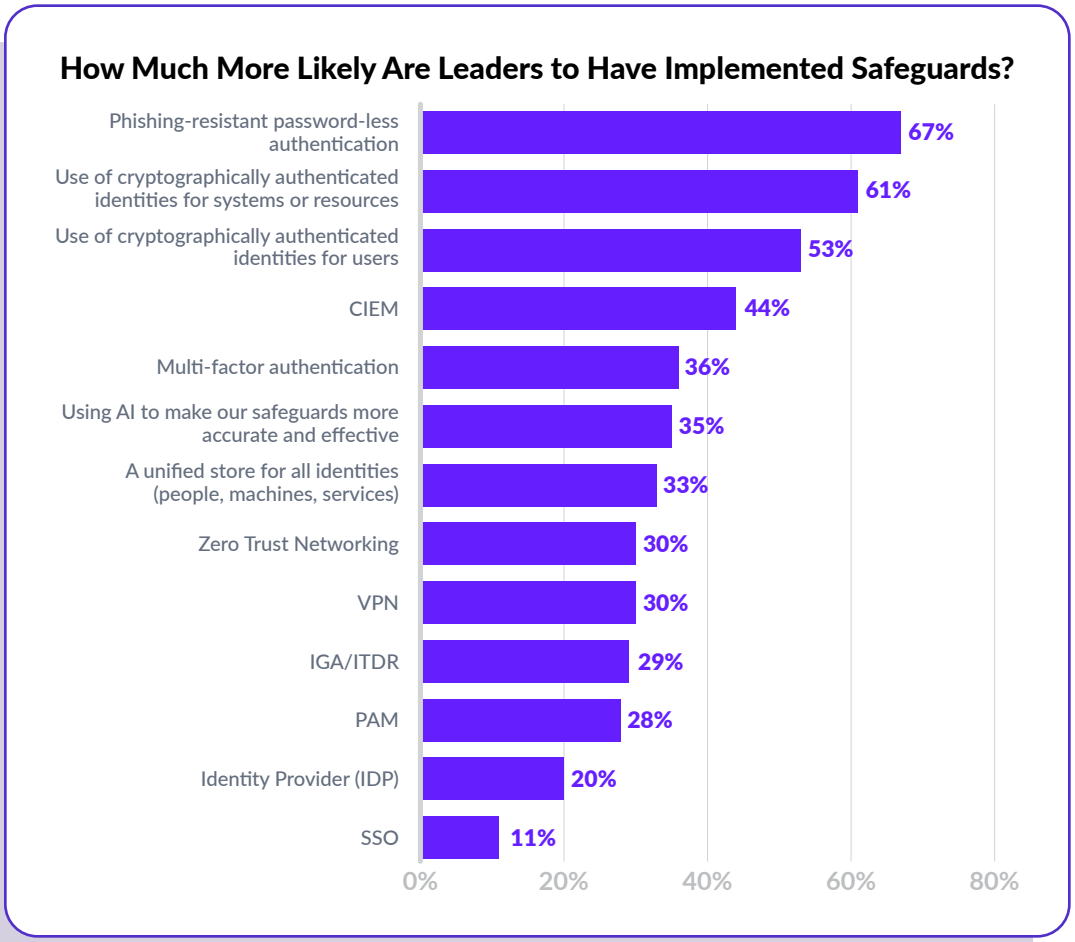


The question, of course, is why?

What are the Leaders doing differently that drives such superior outcomes?

It turns out that across a wide range of secure infrastructure access initiatives, Leaders are far more likely to have implemented safeguards.

For example, the Leaders are 67% more likely to have implemented phishing-resistant passwordless authentication than Novices. This is important because this practice eliminates the vulnerabilities associated with traditional passwords, such as phishing attacks and credential theft. Additionally, it improves the user experience by providing a seamless and hassle-free login process, reducing the need for frequent password resets and complex password management.



Leaders were also 62% and 55% more likely to be using cryptographically authenticated identities for systems and resources or for users. This matters because it ensures that only verified users or systems can access resources, thereby reducing the risk of unauthorized access. This method provides a robust layer of security by leveraging encryption to confirm identities, making it significantly harder for malicious actors to impersonate legitimate users.

We ultimately found 13 key safeguards that the Leaders were more likely to have deployed than Novices, leading to the stark differences in their outcomes. One tangible indication of the impact of a more aggressive pursuit of these safeguards was that Leaders were up to 60% less likely to say protecting against common attack vectors like AI impersonation or compromised privileged credentials was difficult.

Teleport's Advice

As a global provider of modern access to infrastructure, Teleport has a unique vantage point on how to secure infrastructure access. Here is our advice on how to embrace the lessons of infrastructure access security Leaders and improve your outcomes today:

1. **Consolidate identities.** Consolidating identities across humans, endpoints, workloads and machines reduces the complexity and overhead of securing modern environments. This removes the need for silos of access control focused on different access paths, which in turns reduces the attack surface area and simplifies policy management.

2. **Unify your access control.** Providing engineers (or other company employees) with a dynamically generated dashboard of their resources eliminates the need for users to remember a myriad of access paths and siloed security methods and improves productivity. This helps prevent backdoors, which can be identified and eliminated. Unifying user and machine access policy further hardens security across the organization.

3. **Eliminate passwords and standing privileges.** Adopting ephemeral privileges and identity security grounded in cryptographic identity, rather than a credential such as a password that can be stolen, reduces the attack surface that can be targeted by threat actors and thwarts social engineering efforts.

4. **Implement infrastructure defense in depth.** Configuring your environment with appropriate identity verification redundancies and safeguards, such as MFA for administrative actions or dual authorization, helps prevent threat actors from executing breach and pivot strategies to sensitive data. This ensures that if privileged (or unprivileged) identities are compromised, your systems and data remain secure.

5. **Unify policy.** Consider consolidating policy for all computing resources in a single access control system. This minimizes the misconfiguration risk, reduces operational overhead of synchronizing policy across different workloads, and shortens the time to respond to incidents, make policy changes, or achieve compliance.

The data is in. Leaders experience fewer annual security incidents (2 vs 12) and significant cost savings compared to Novices. Clearly, upfront investment in secure infrastructure access pays off — Leaders can reduce compliance costs, and even if incidents do occur, they can protect their brand reputation and continue to support the business outcomes their infrastructures are designed to enable.

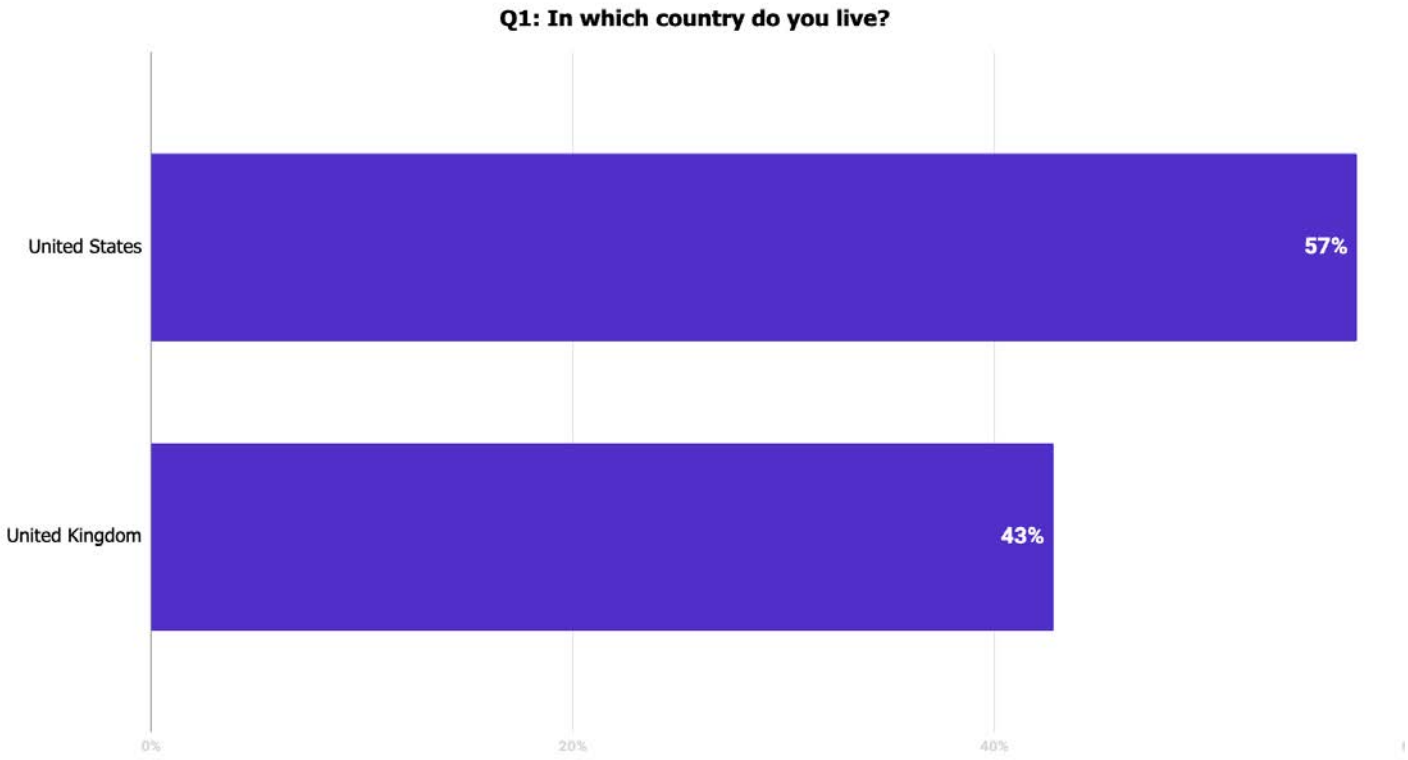
Demographics & Survey Data

This survey was conducted in July of 2024, and includes data from 125 respondents in North America and 125 in the United Kingdom.

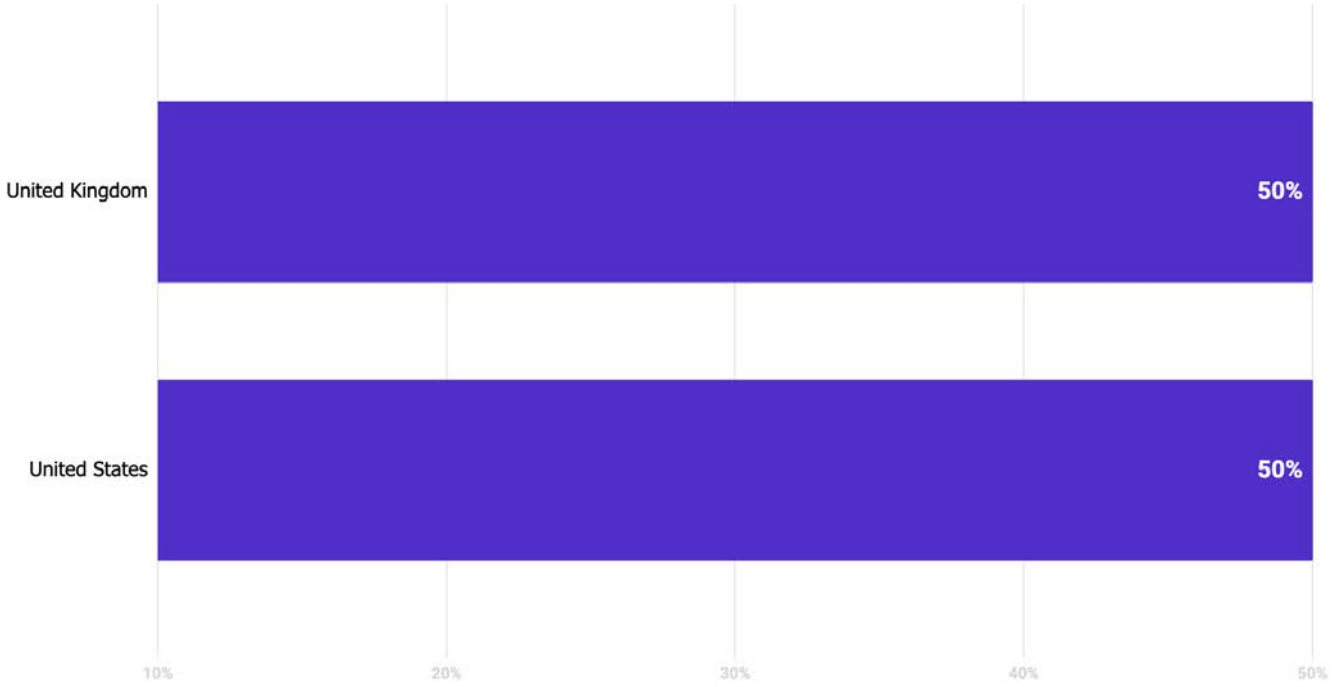
Respondents were senior managers, director/VP, or C-level professionals, where 40% or more of their time includes responsibility for one or more of the following:

- access control (managing privileged user permissions defining access workflows, and/or onboarding or offboarding privileged users)
- compliance (implementing access controls for SOC 2, FedRAMP, HIPAA or other similar industry or technology regulations)
- audit (supporting audit activities to prove adherence to compliance requirements)
- architecture (defining security architecture or policy related to access control or identity security)

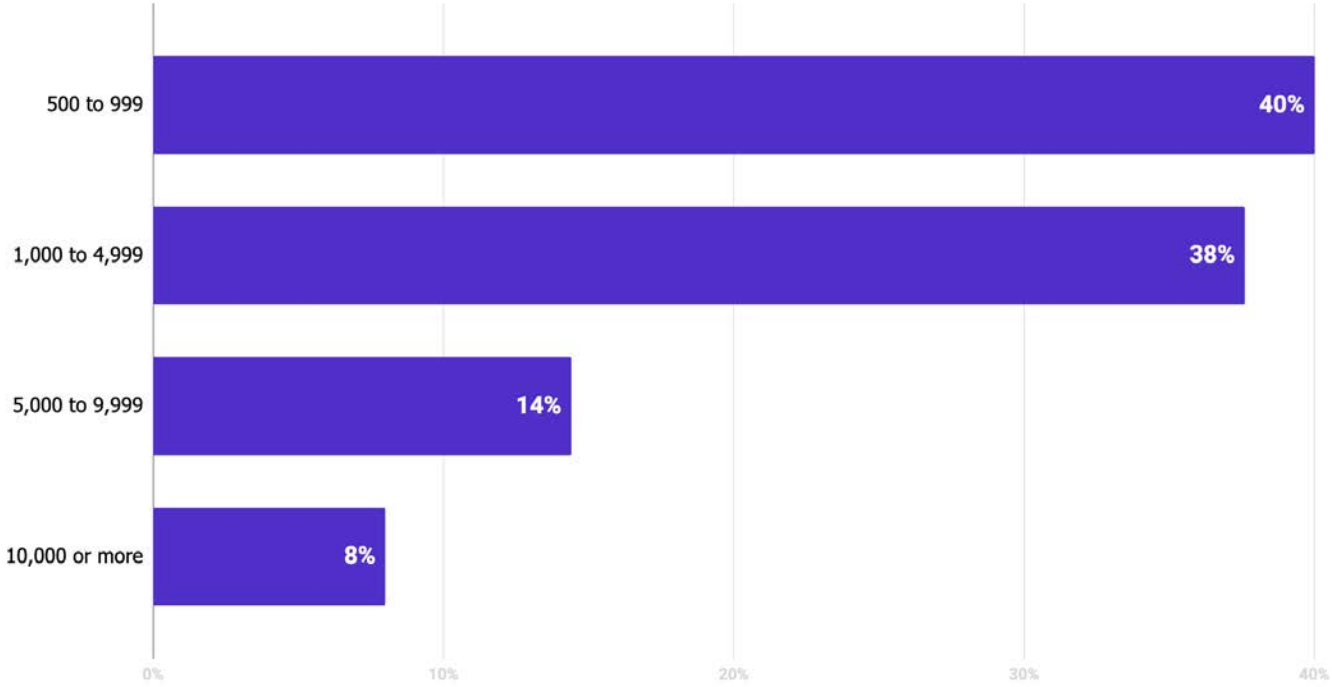
The survey focused on respondents working in the financial services, technology and software, and healthcare industries.



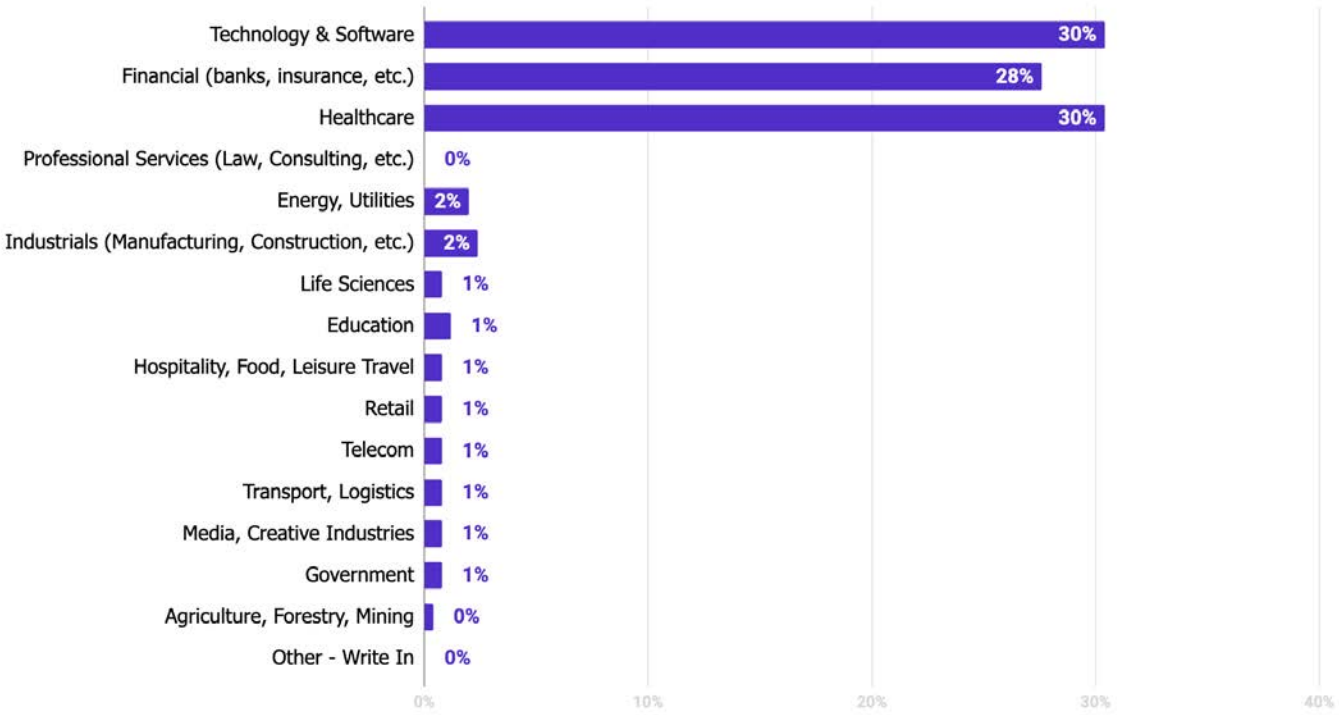
Q2: In which country is your organization headquartered?



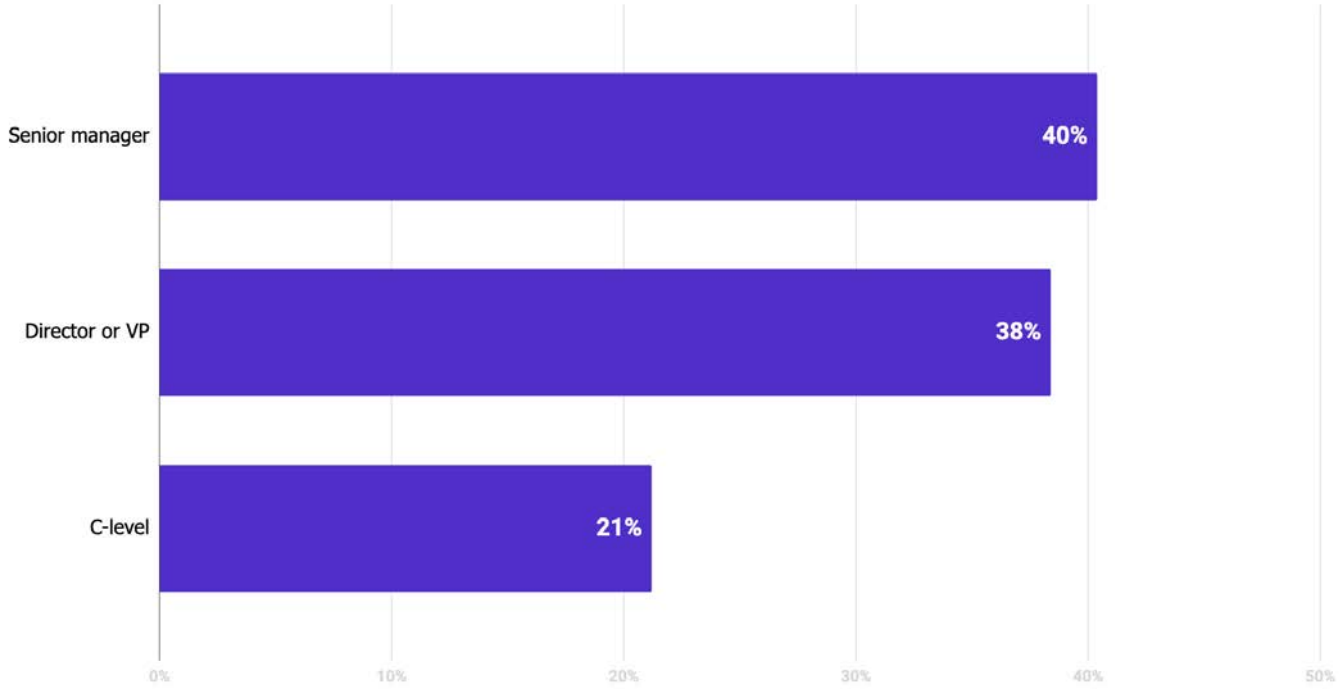
Q3: How many employees work at your organization worldwide?



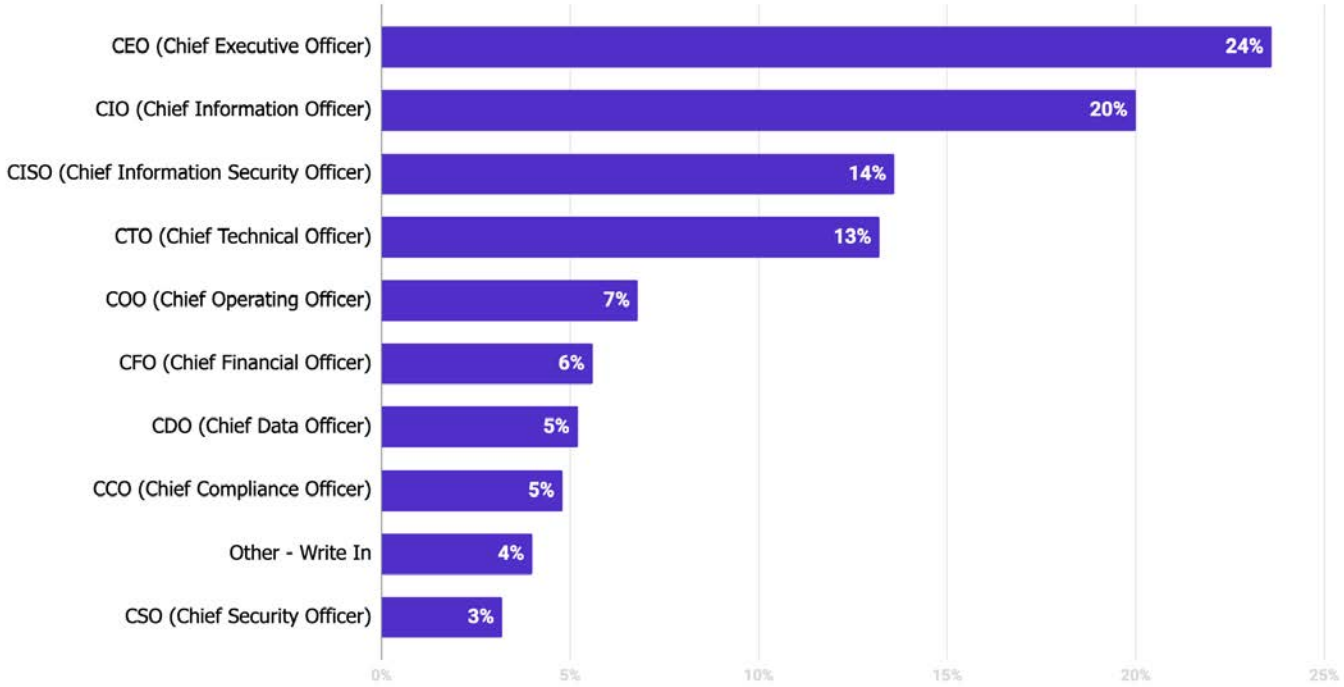
Q4: In which industry does your organization work?



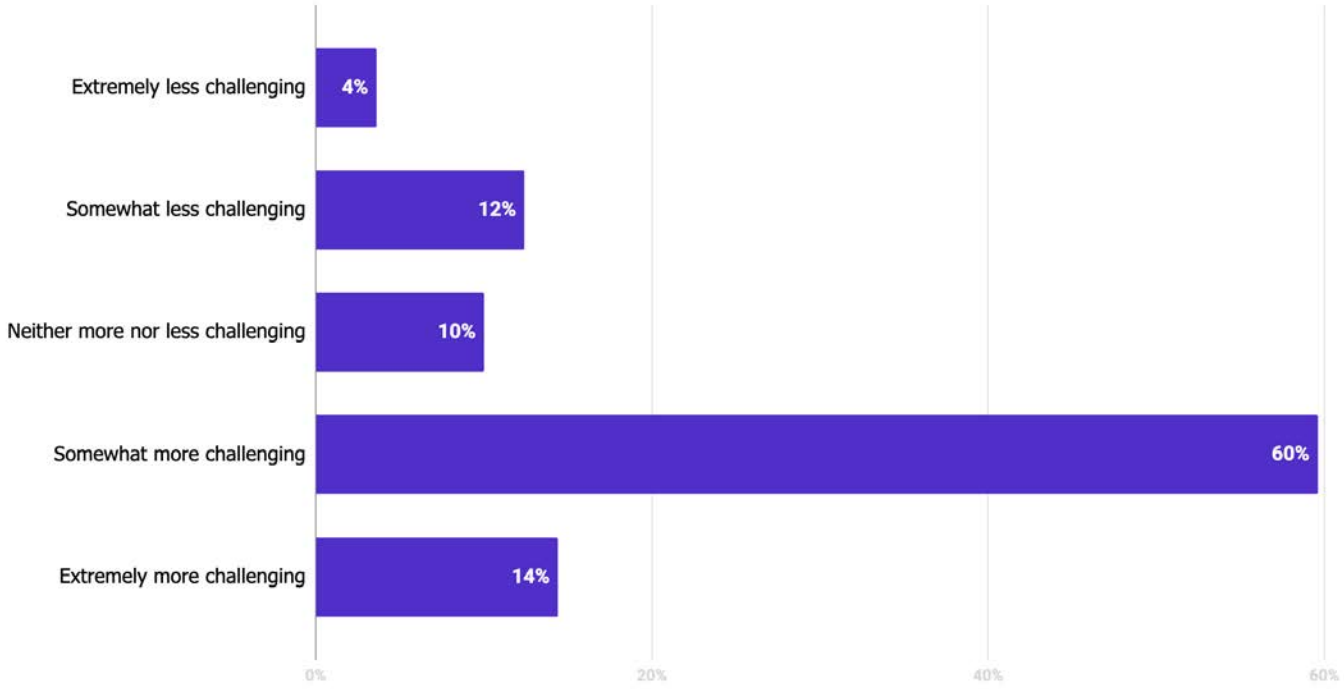
Q6: What is your level of seniority?



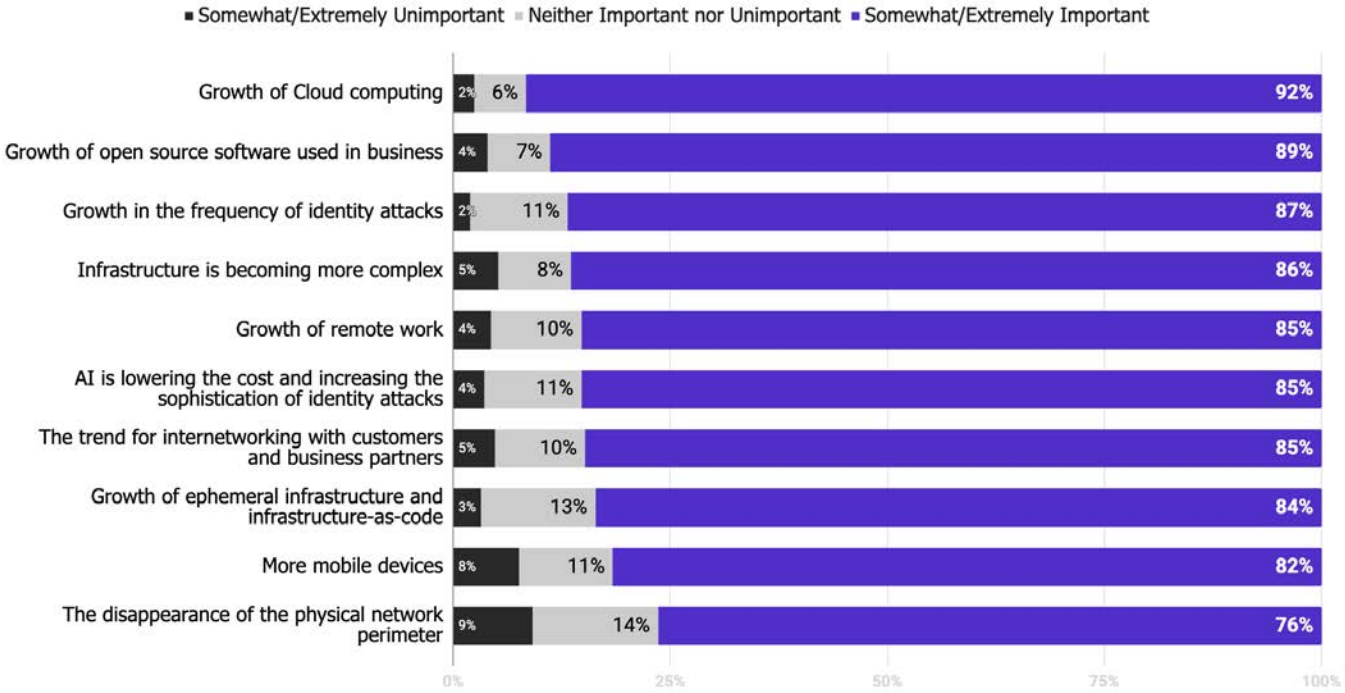
Q8: Which C-level executive is over your department?



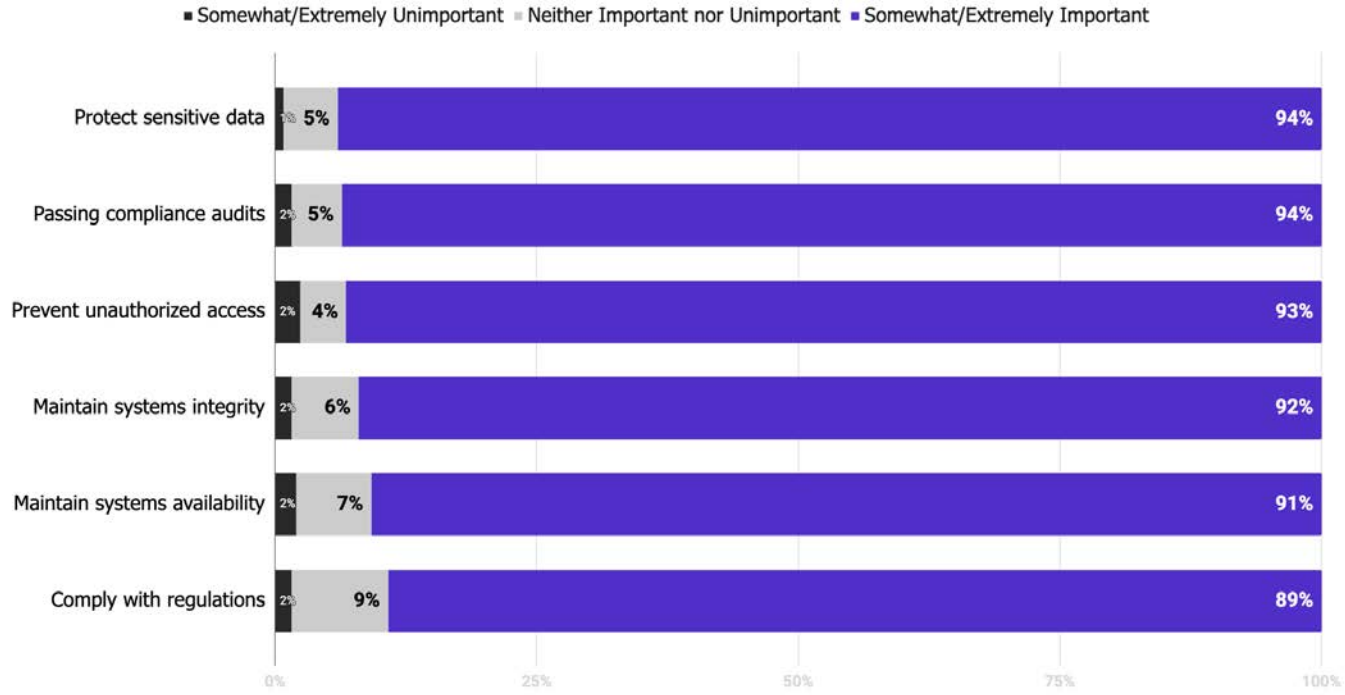
Q9: How are the challenges of infrastructure access security changing?



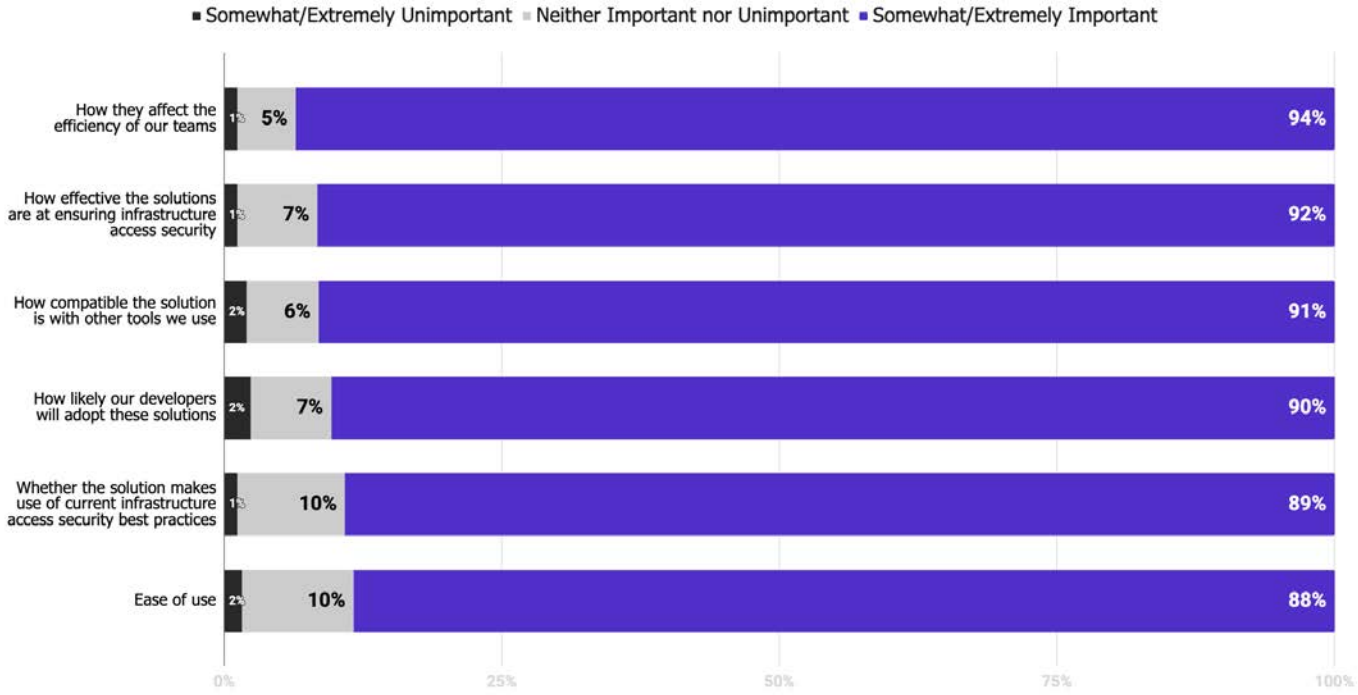
Q10: Rate the importance of the following factors in terms of making infrastructure access security more challenging over time



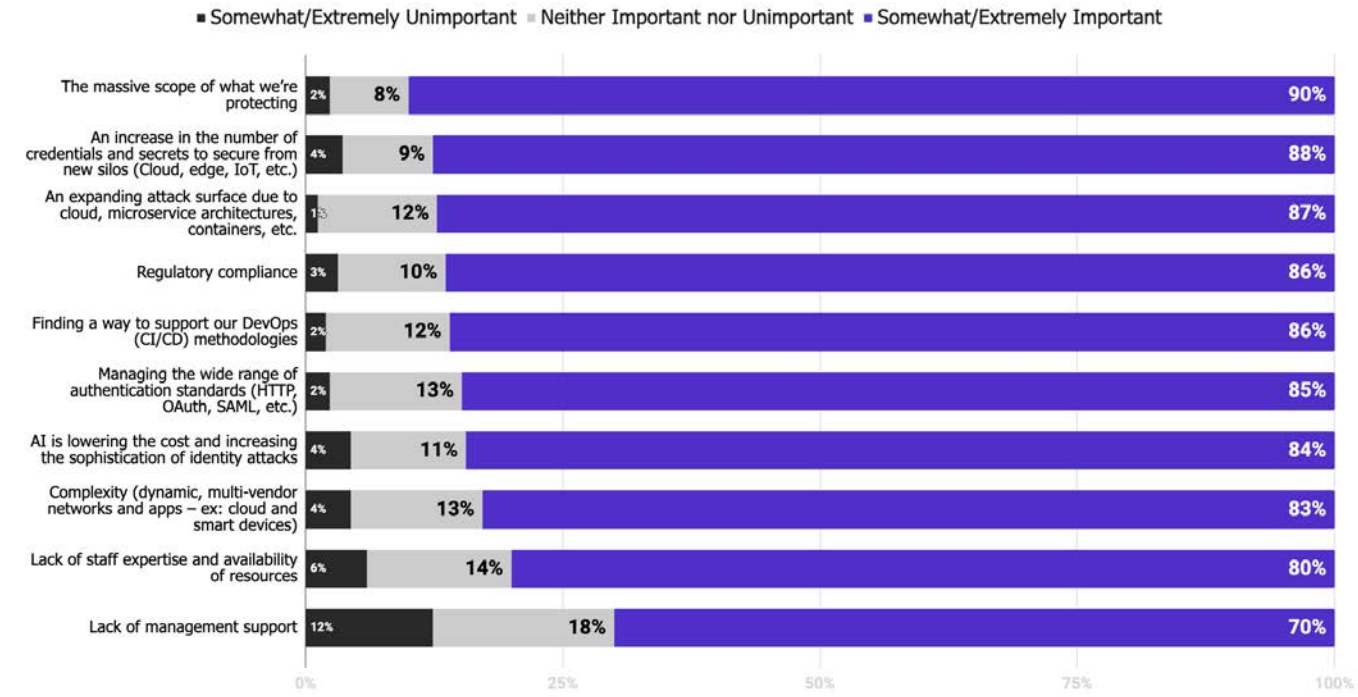
Q11: How important are each of these goals in infrastructure access security?



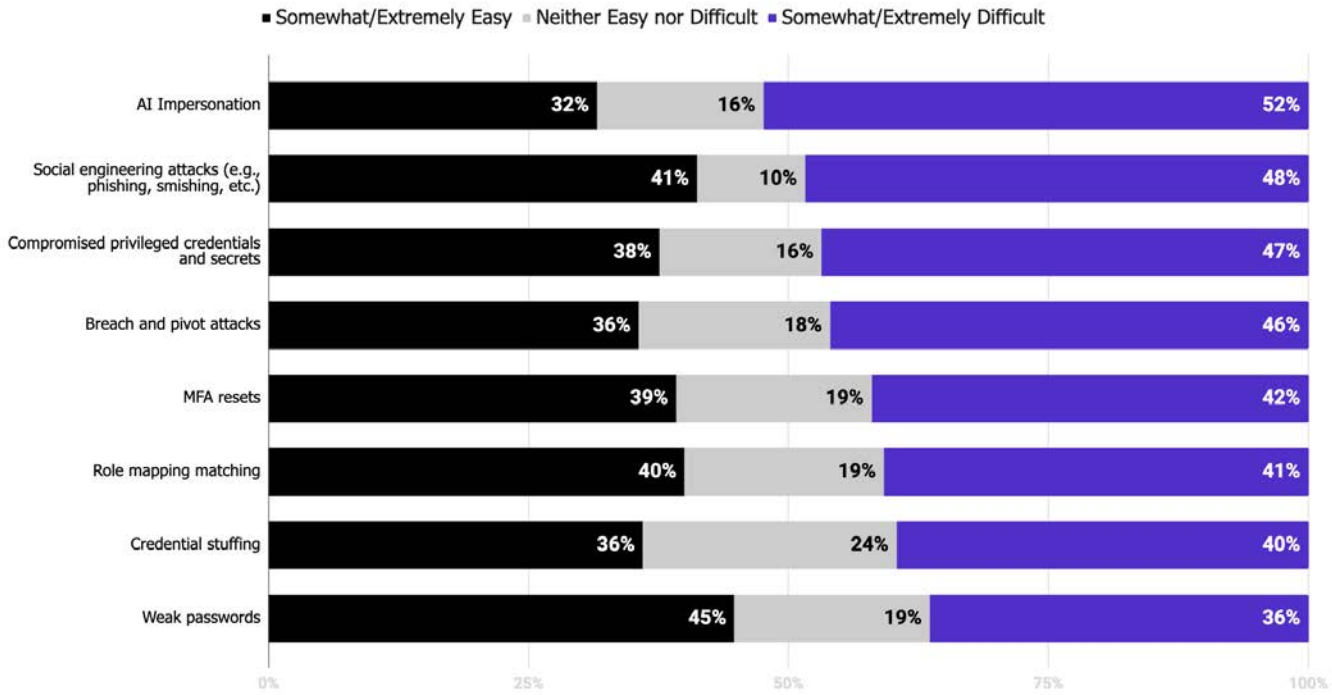
Q12: How important are the following factors when choosing infrastructure access security solutions?



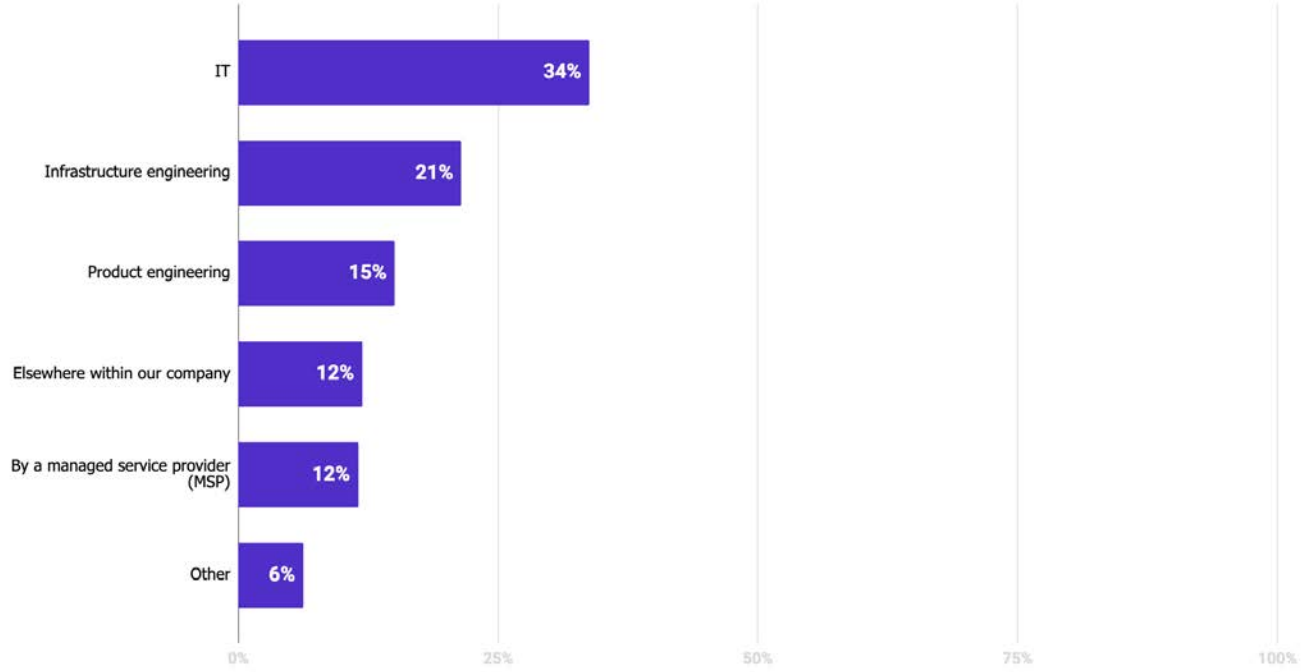
Q13: Rate the importance of the following challenges you face in implementing your infrastructure access security



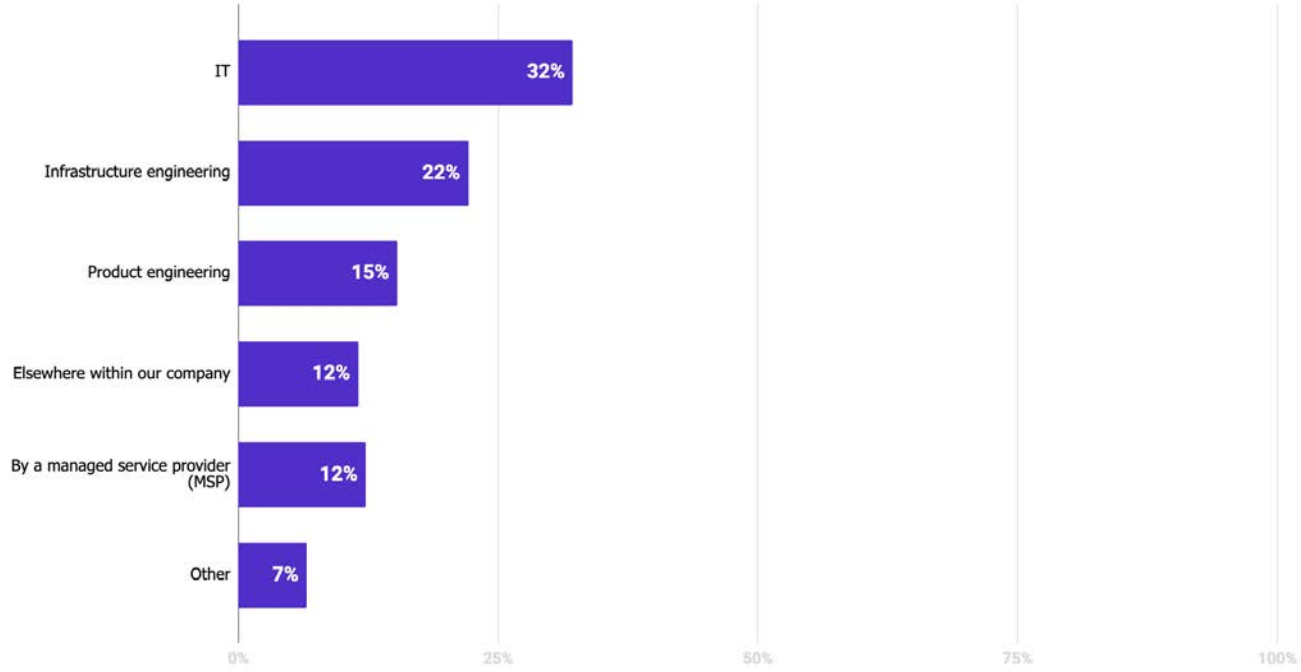
Q14: Rate how easy or difficult it is to protect against each of these attack vectors:



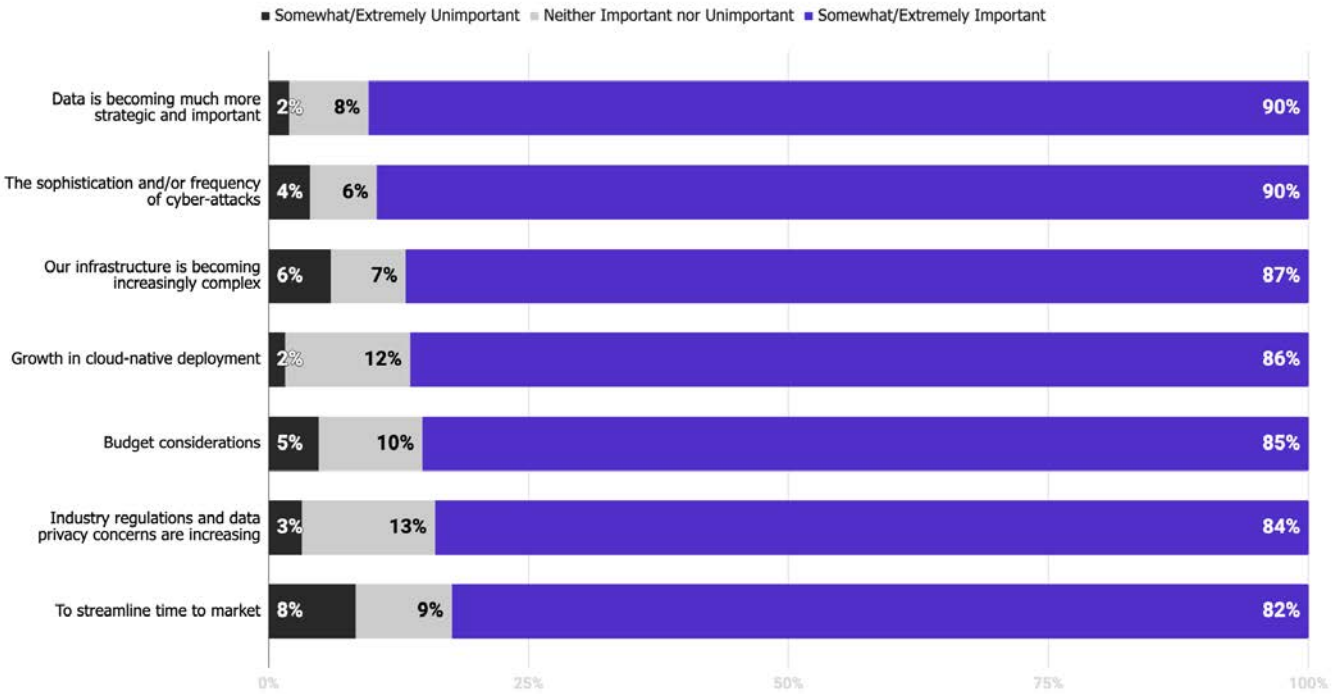
Q15: We first want to explore where infrastructure access security is managed today. What percentage of your infrastructure access security is managed in each of these areas?



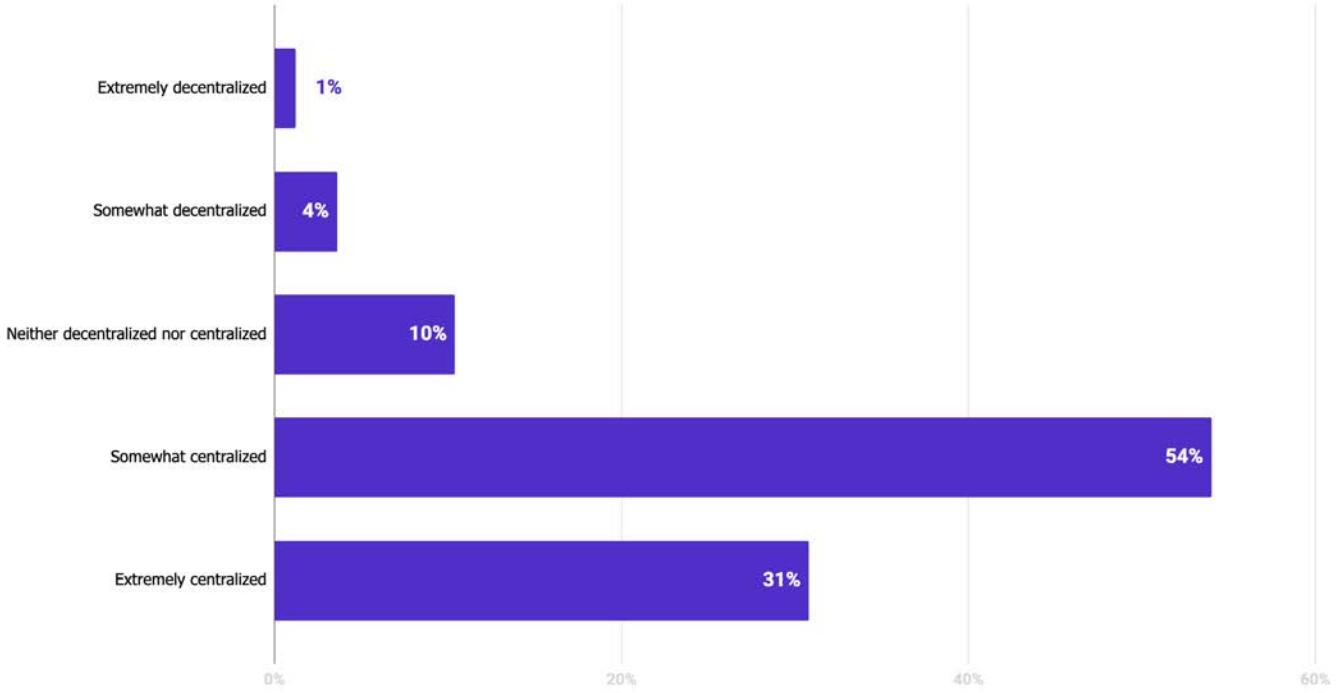
Q16: Next, where will infrastructure access security be managed in three years? What percentage of your infrastructure access security is managed in each of these areas?



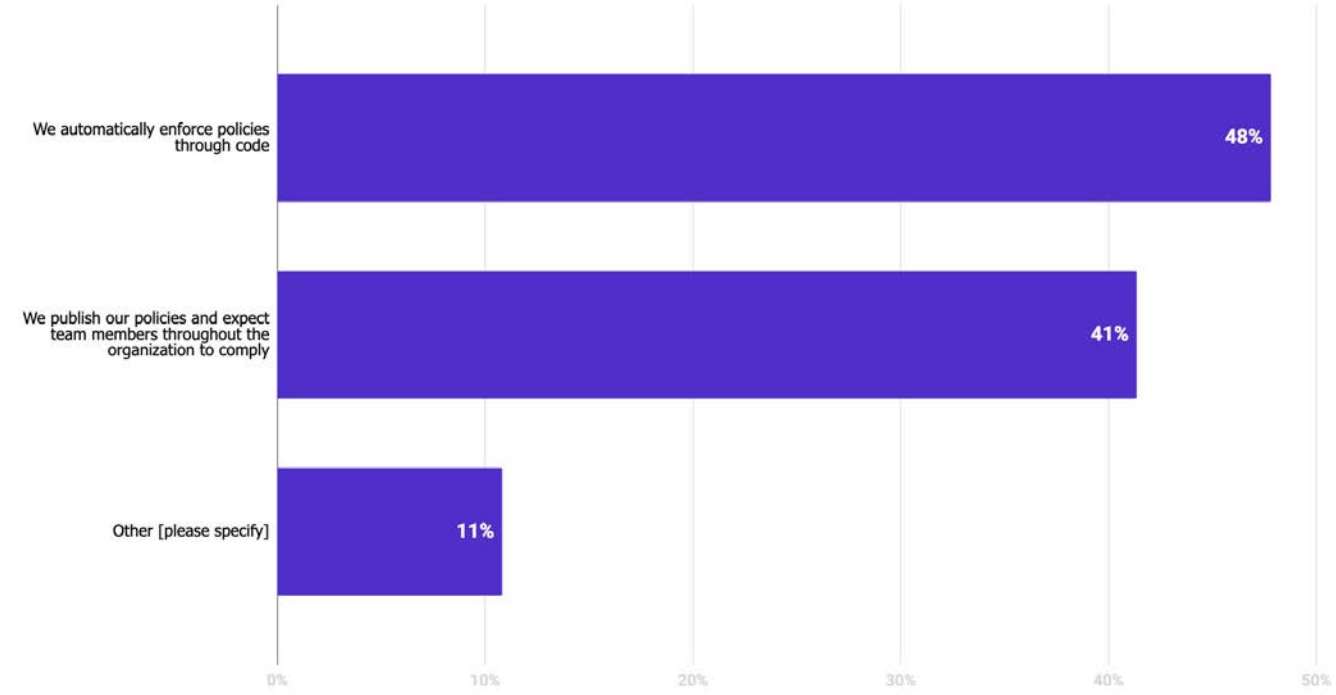
Q17: How important are the following factors in determining where you manage infrastructure access security?

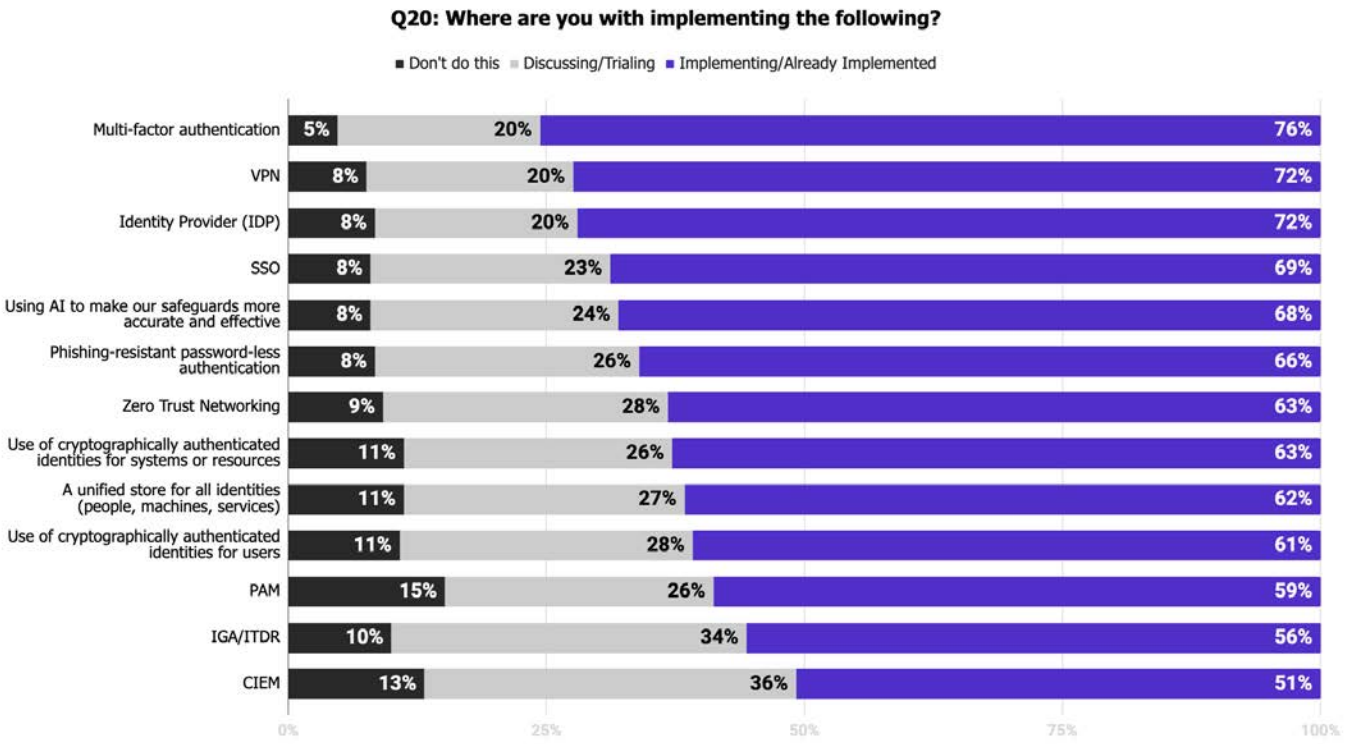


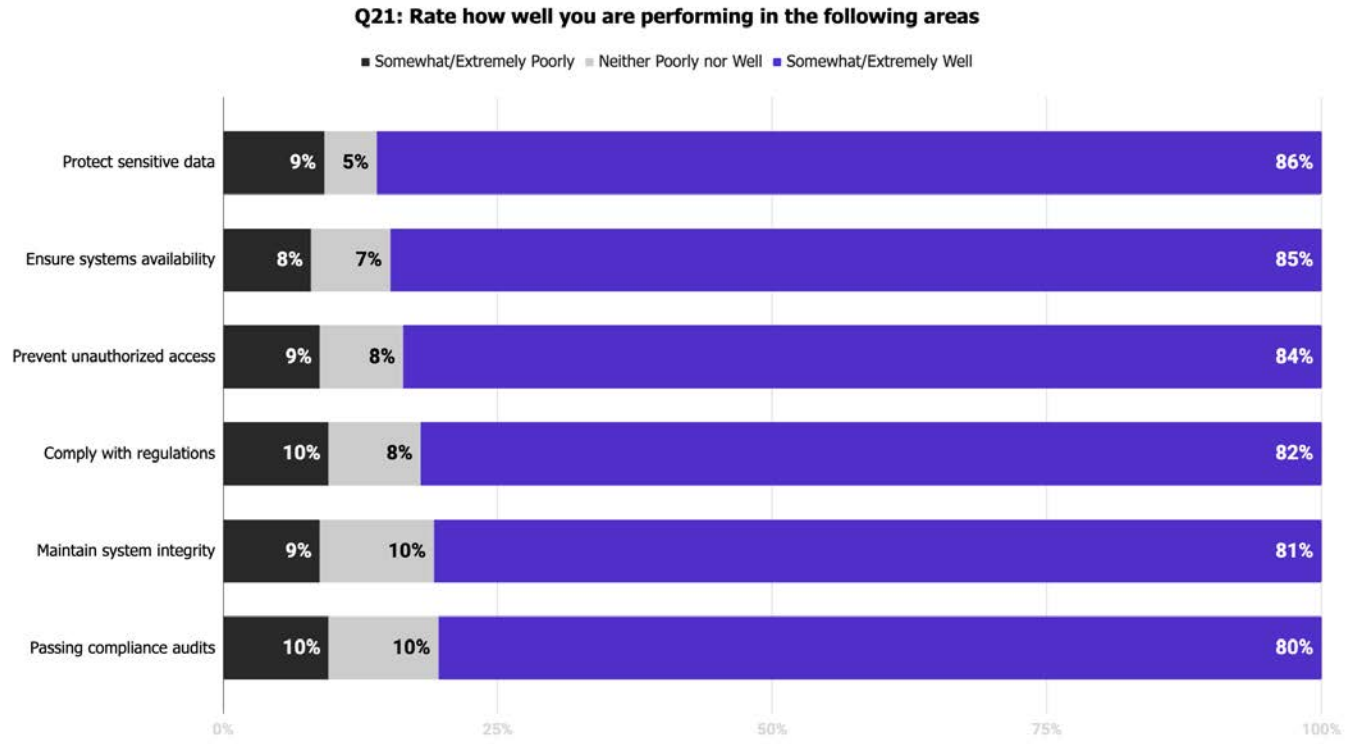
Q18: How centralized is infrastructure access security responsibility in your organization?



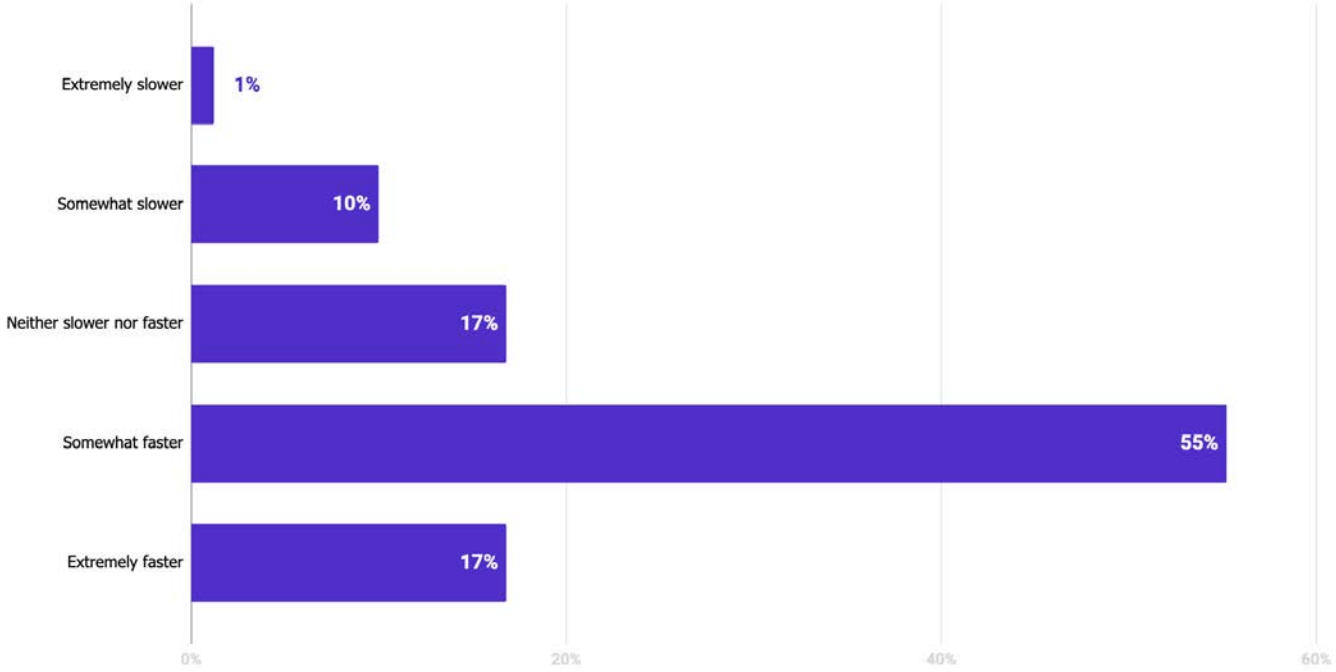
Q19: What percentage of each method do you use to enforce security policies organization-wide?



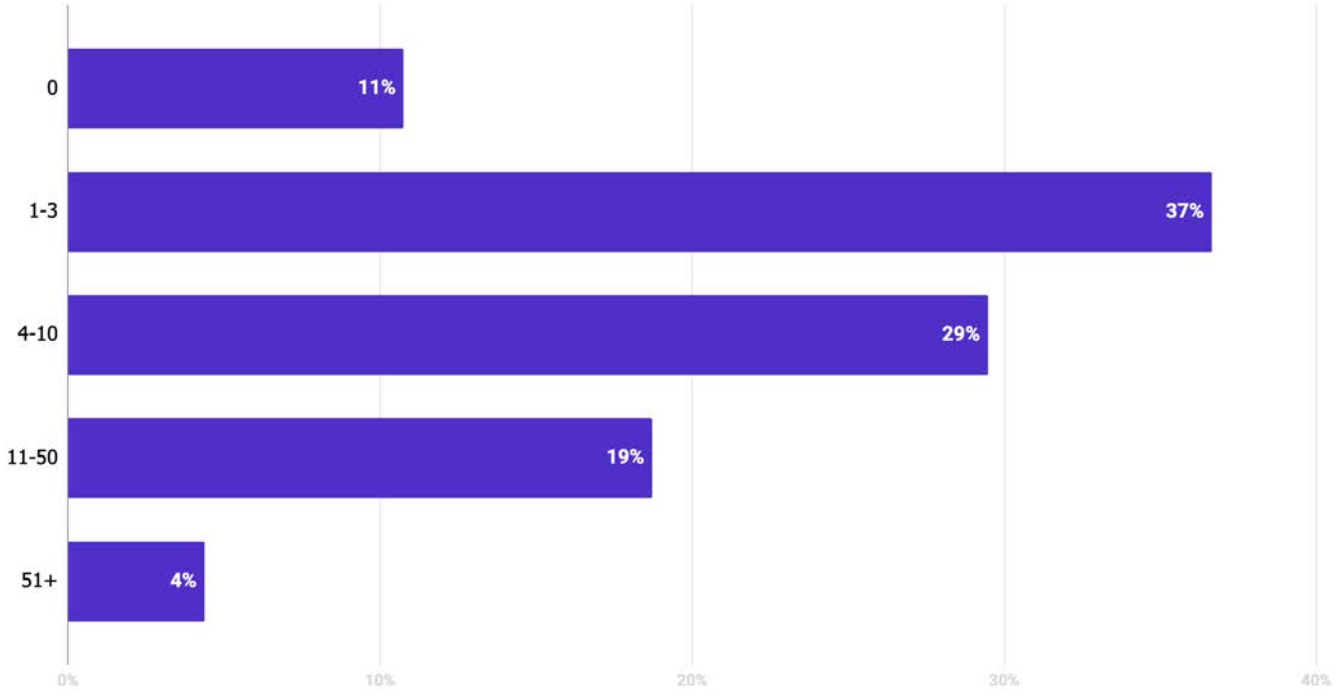




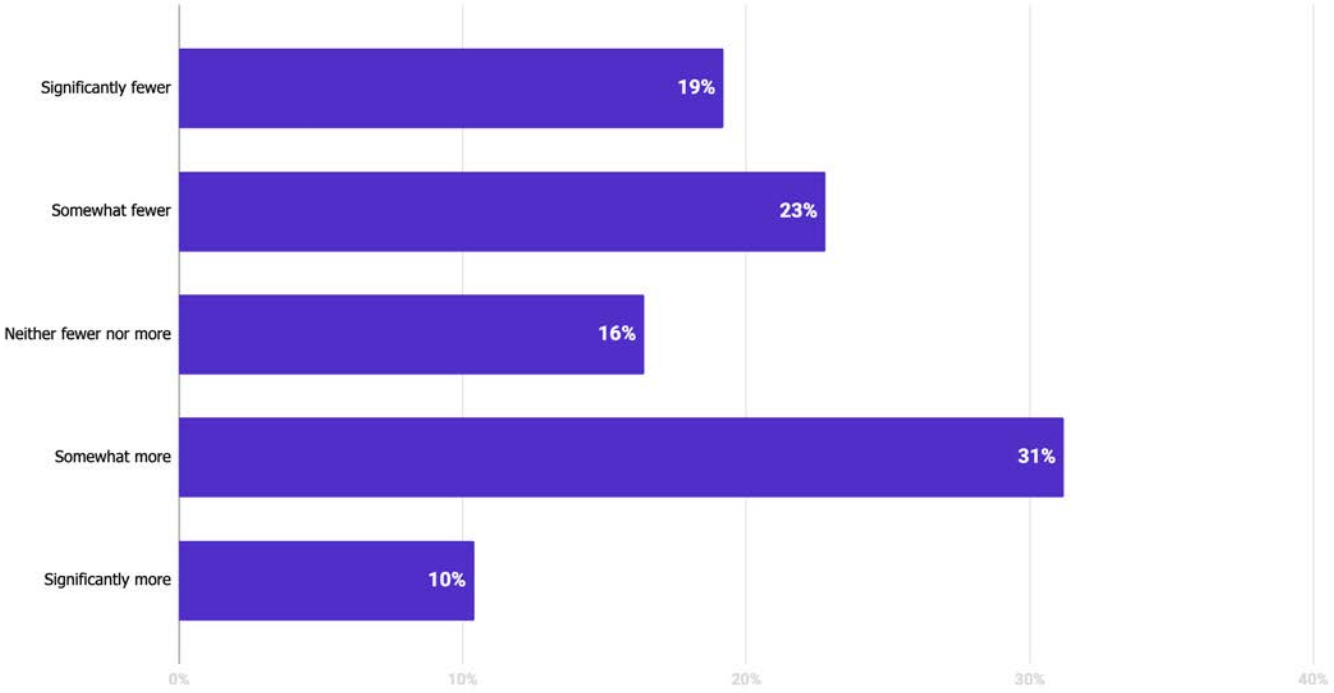
Q22: How have your organization's infrastructure access security initiatives affected software development in terms of agility and time-to-market?



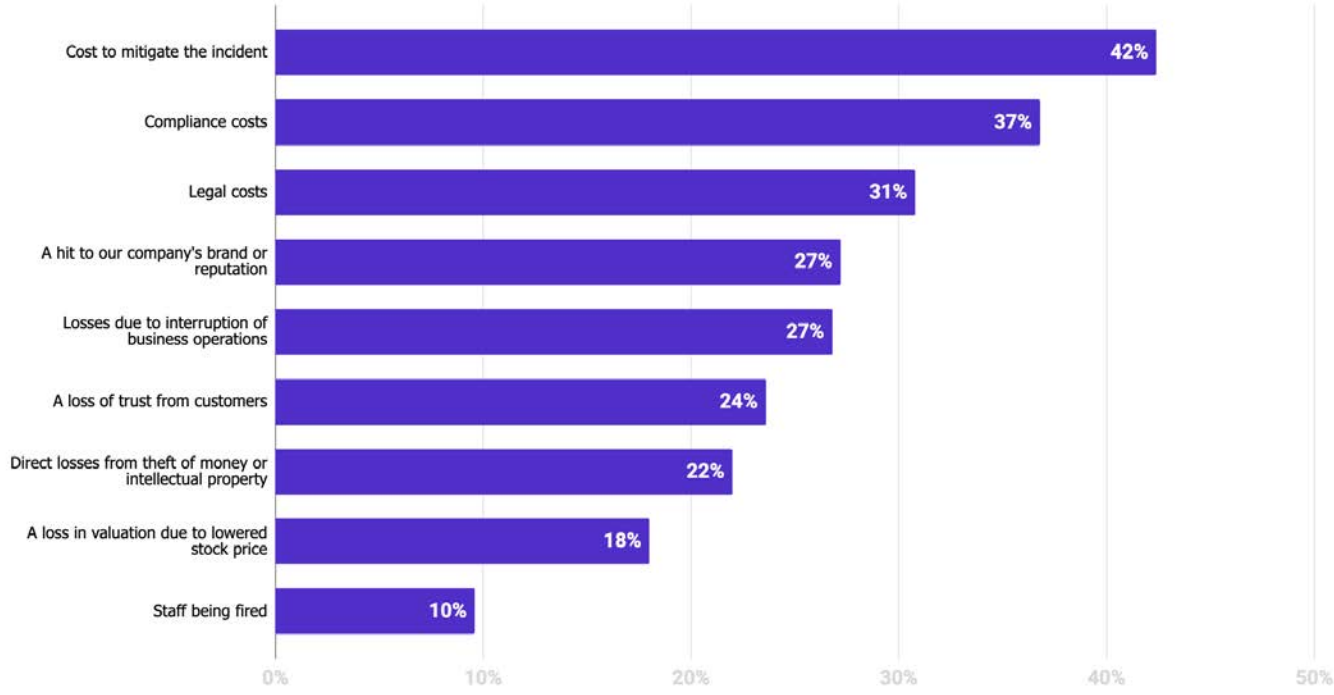
Q23: How many security incidents has your organization experienced during the past THREE years?



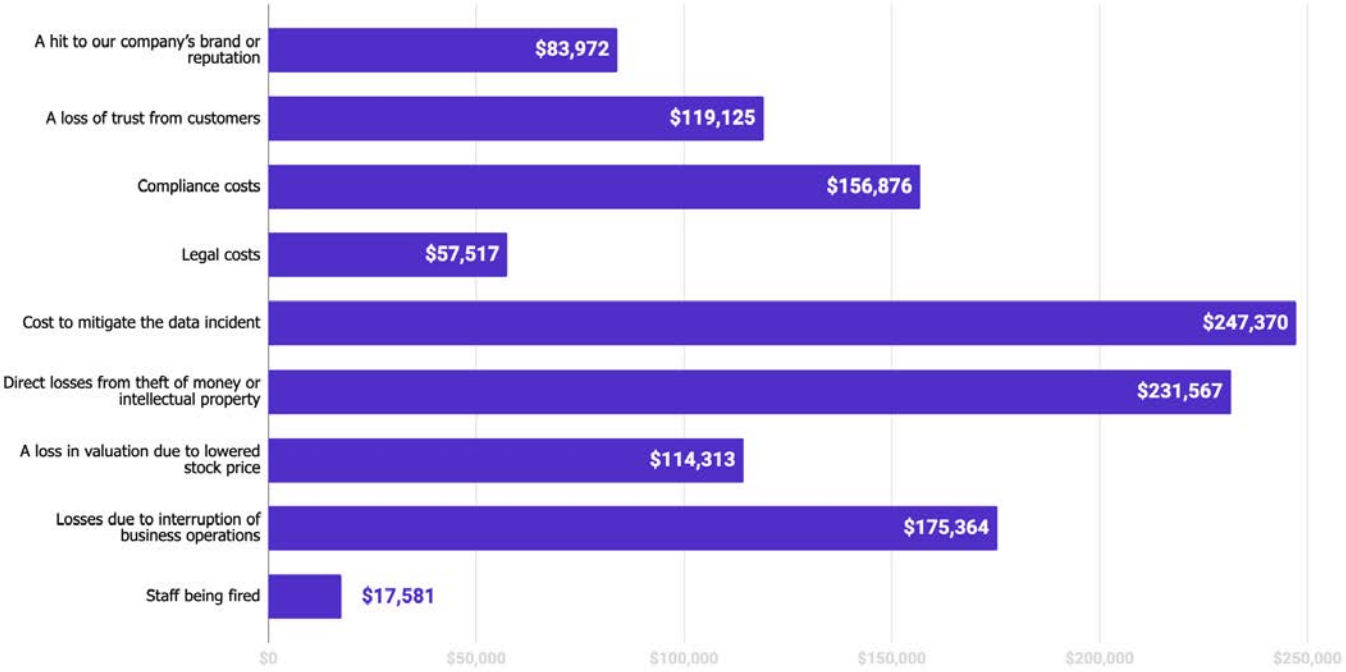
Q24: How has the number of security incidents your organization experiences changed over time?



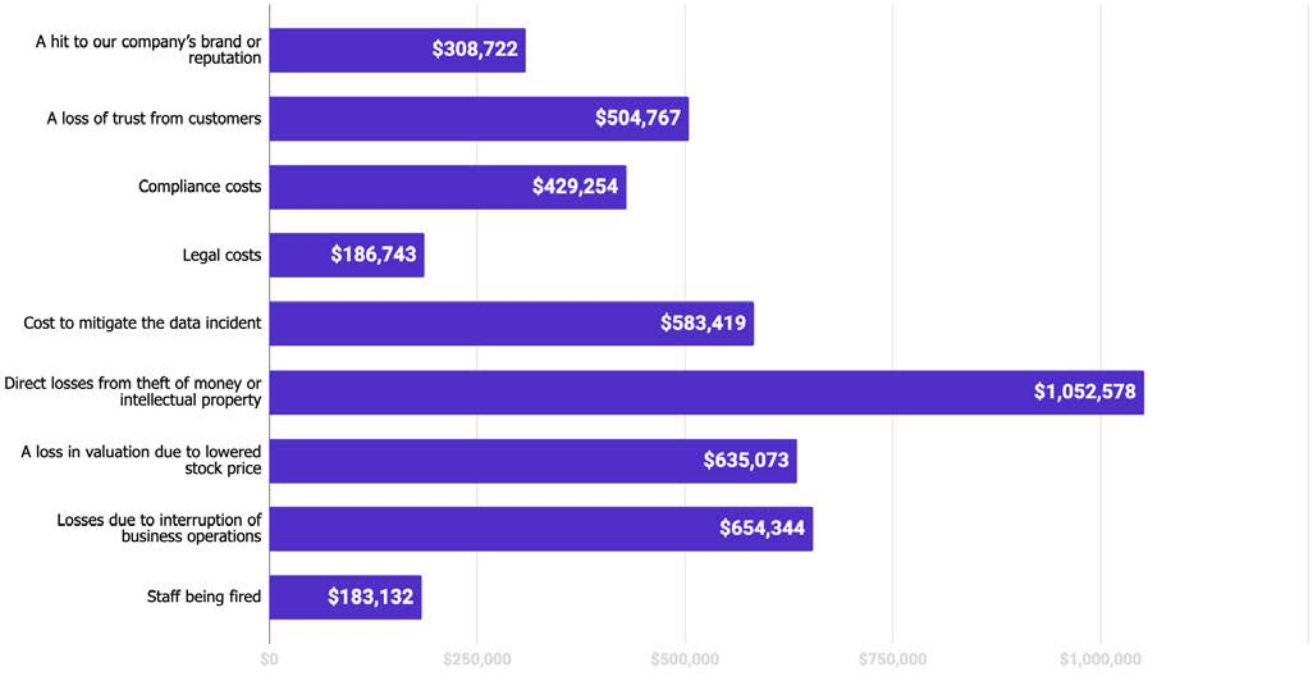
Q25: Which of the following consequences have you experienced as a result of these incidents?



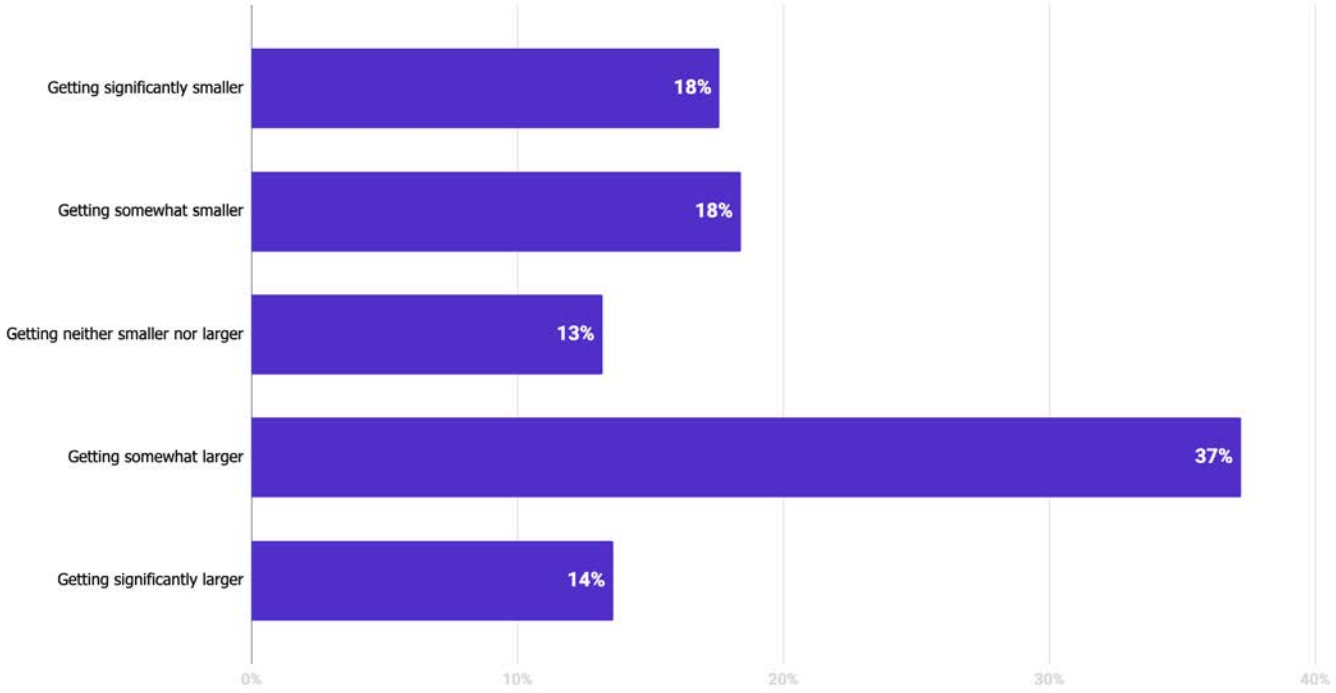
Q26: Estimate the total cost of each of the following consequences on a per-incident basis: (All responses)



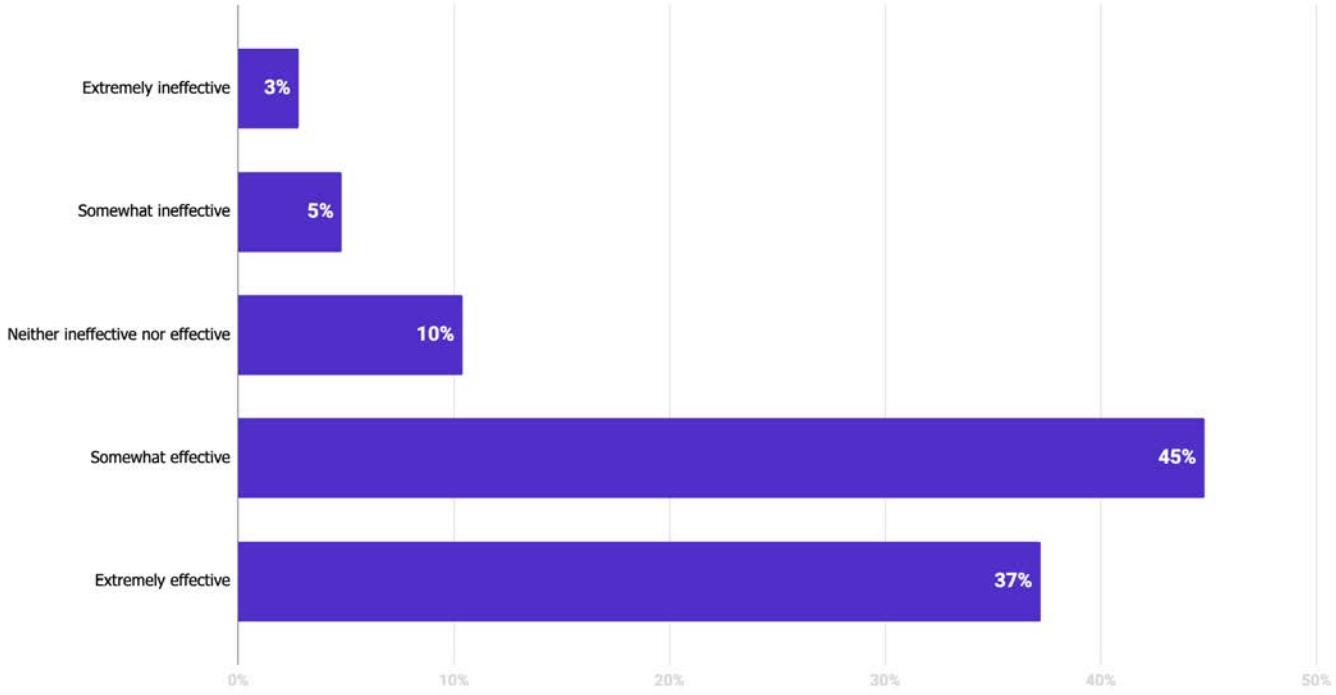
Q26: Estimate the total cost of each of the following consequences on a per-incident basis: (Only those who experienced this consequence)



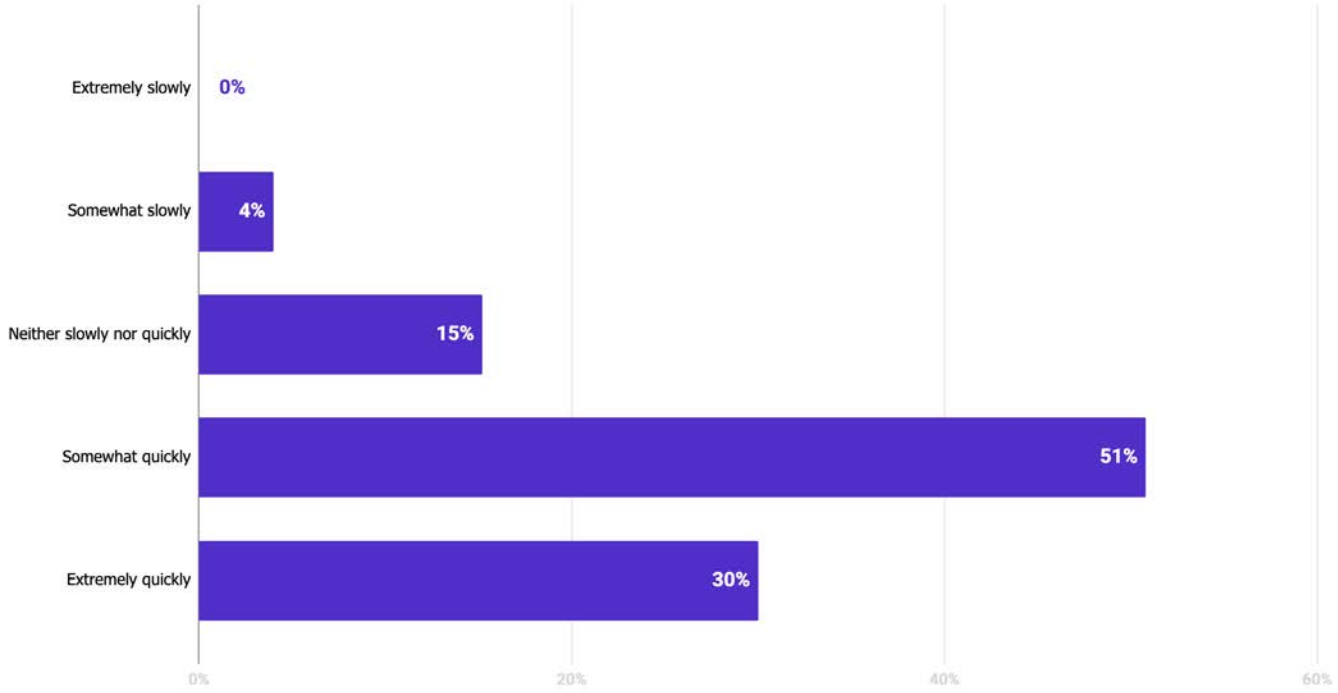
Q27: How is the threat of security incidents changing over time



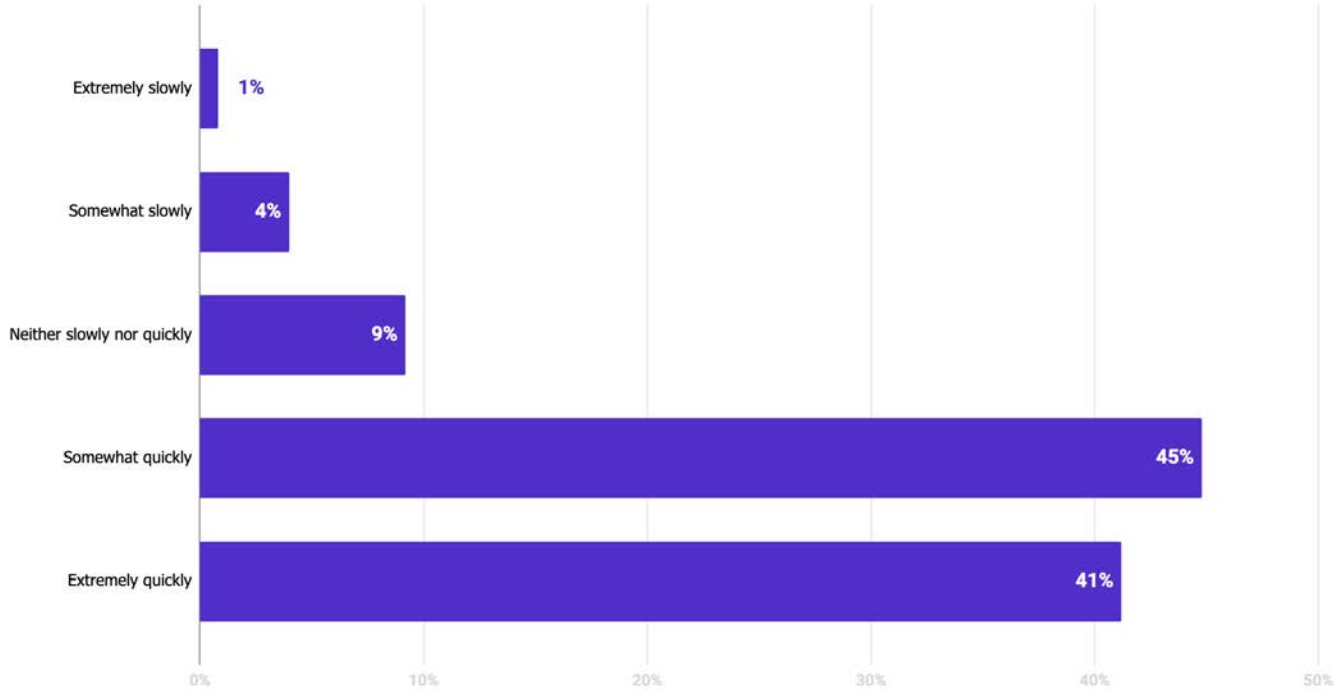
Q28: How would you characterize the efforts your organization is making towards preventing security incidents?

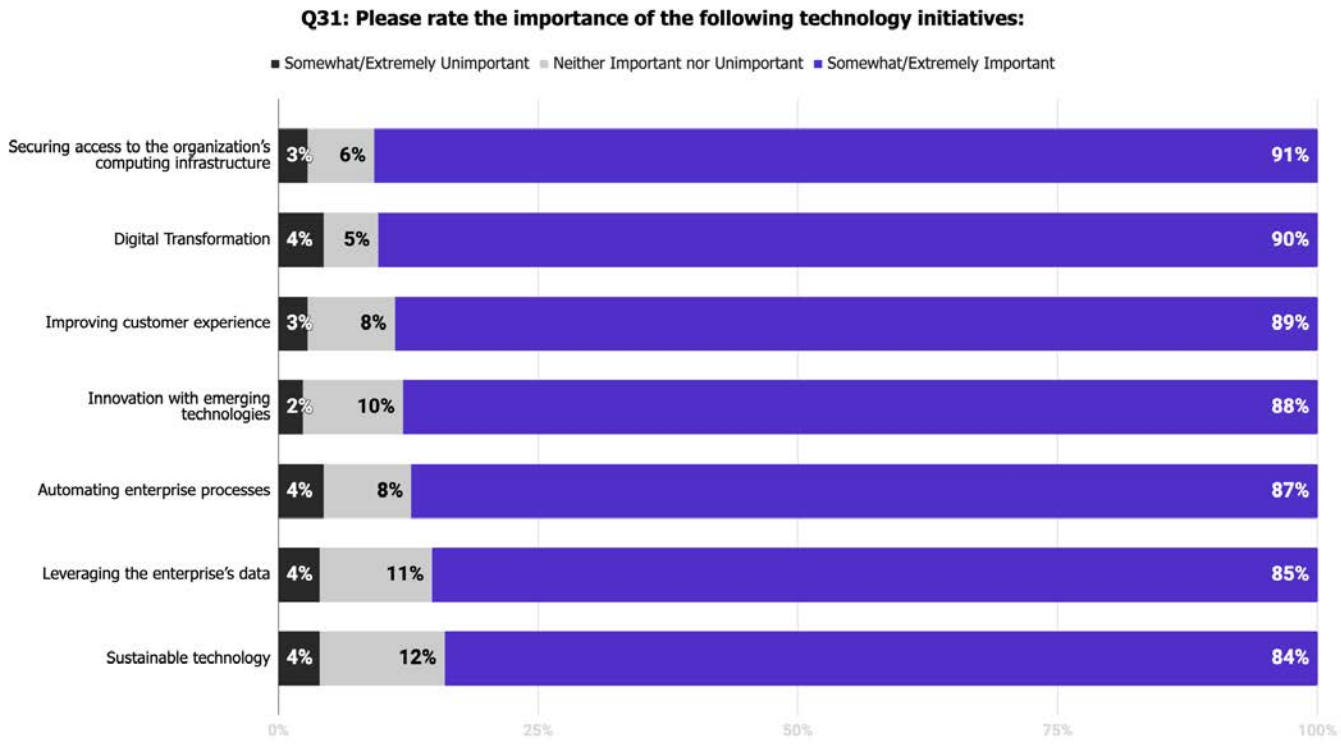


Q29: How quickly can you determine who has access to various infrastructure resources?

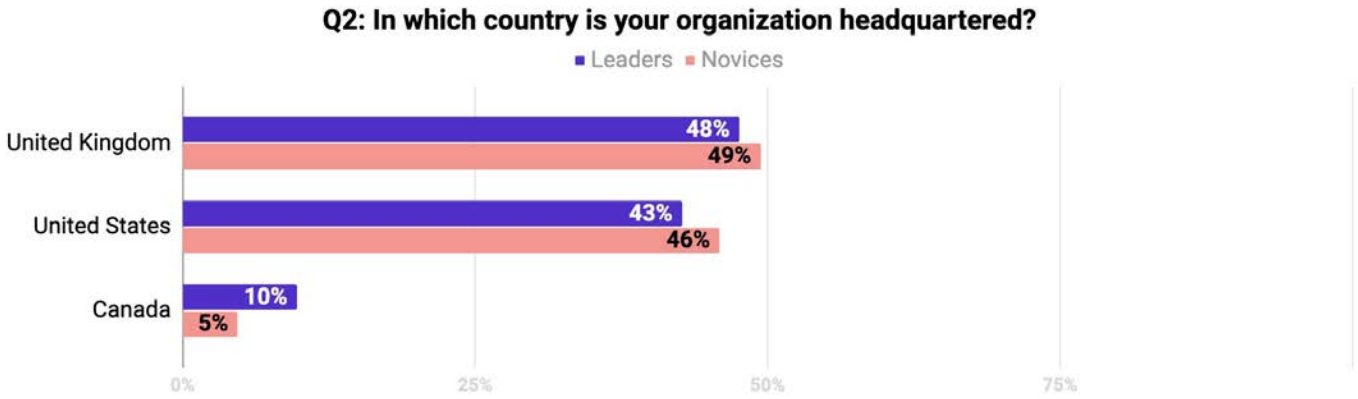


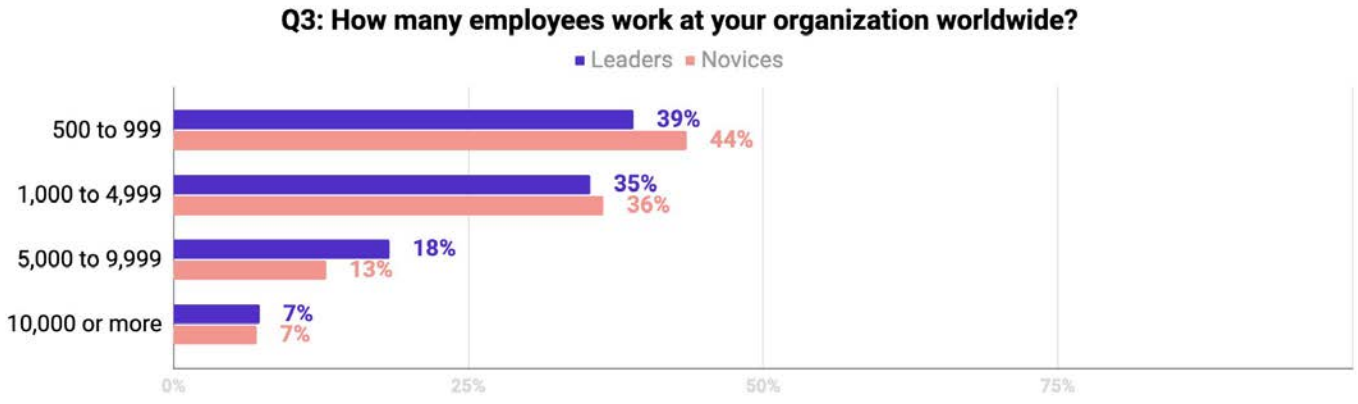
Q30: How quickly can you react to security incidents (e.g., breaches, compromises)?

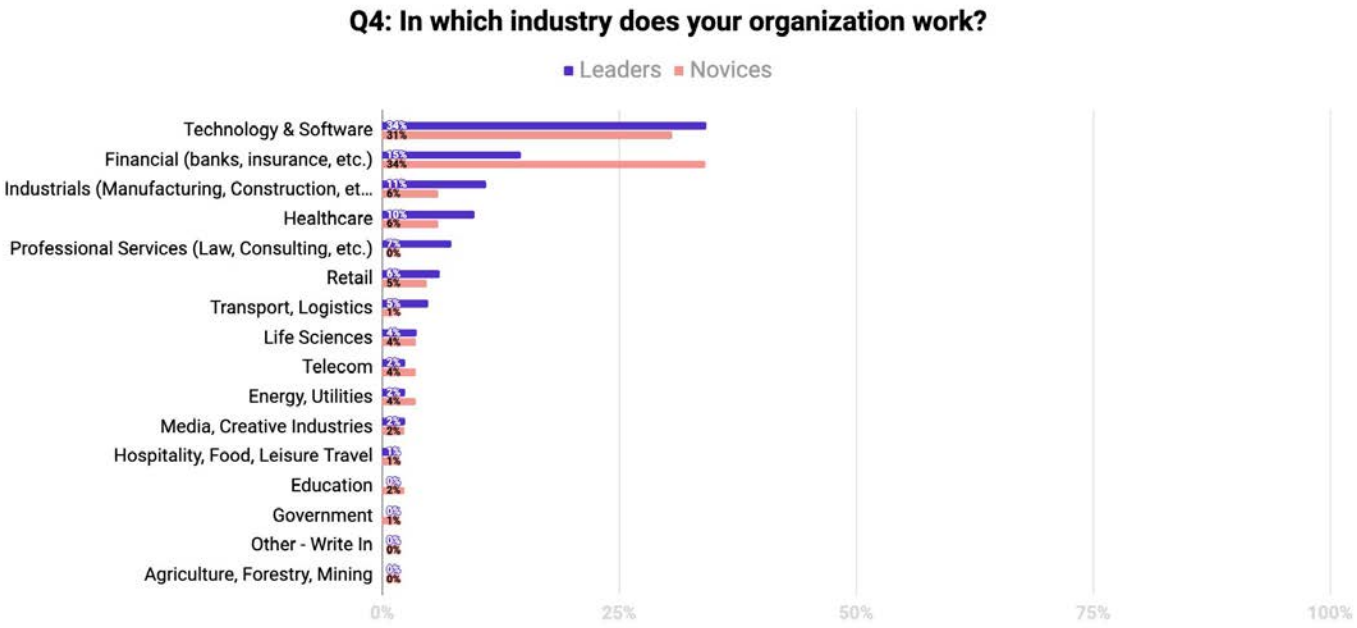


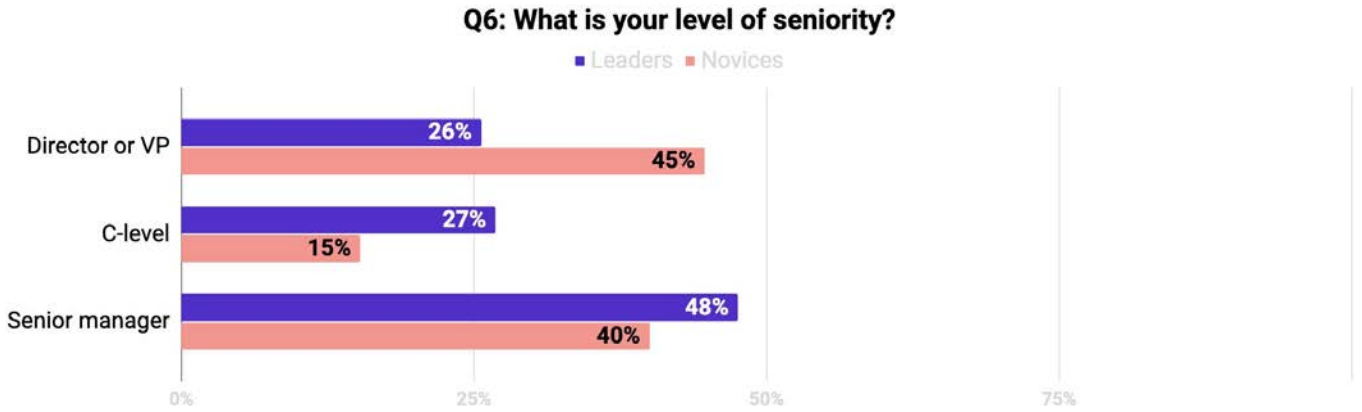


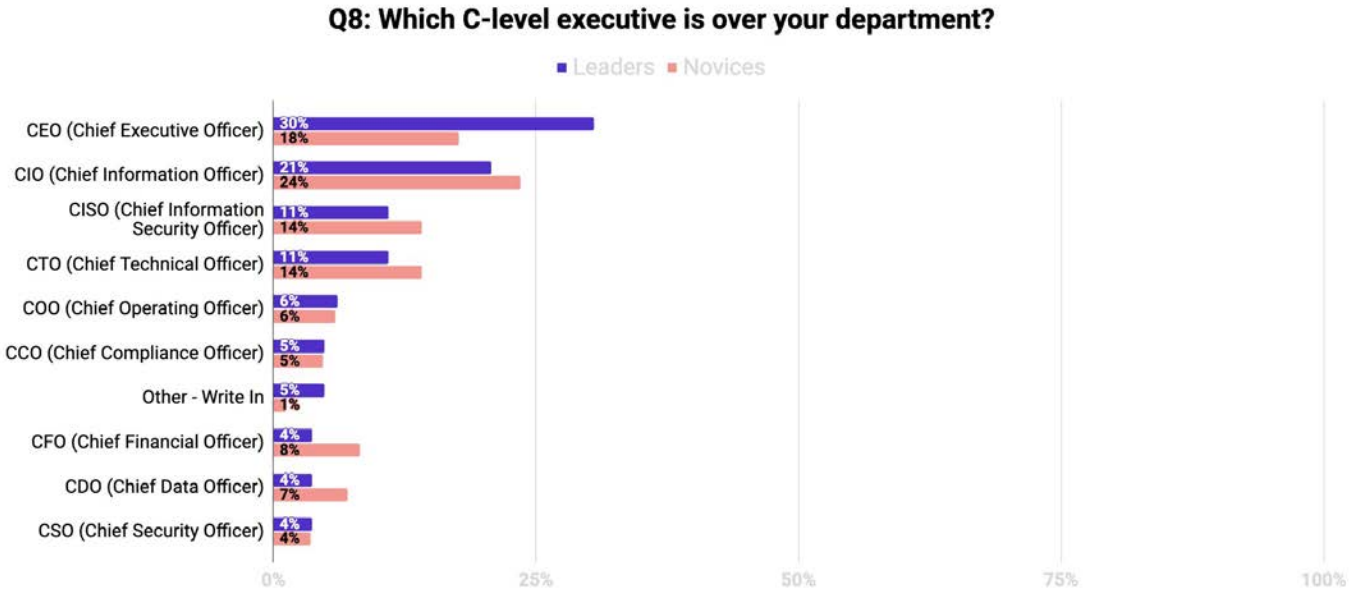
Survey Data:
Leaders vs Novices

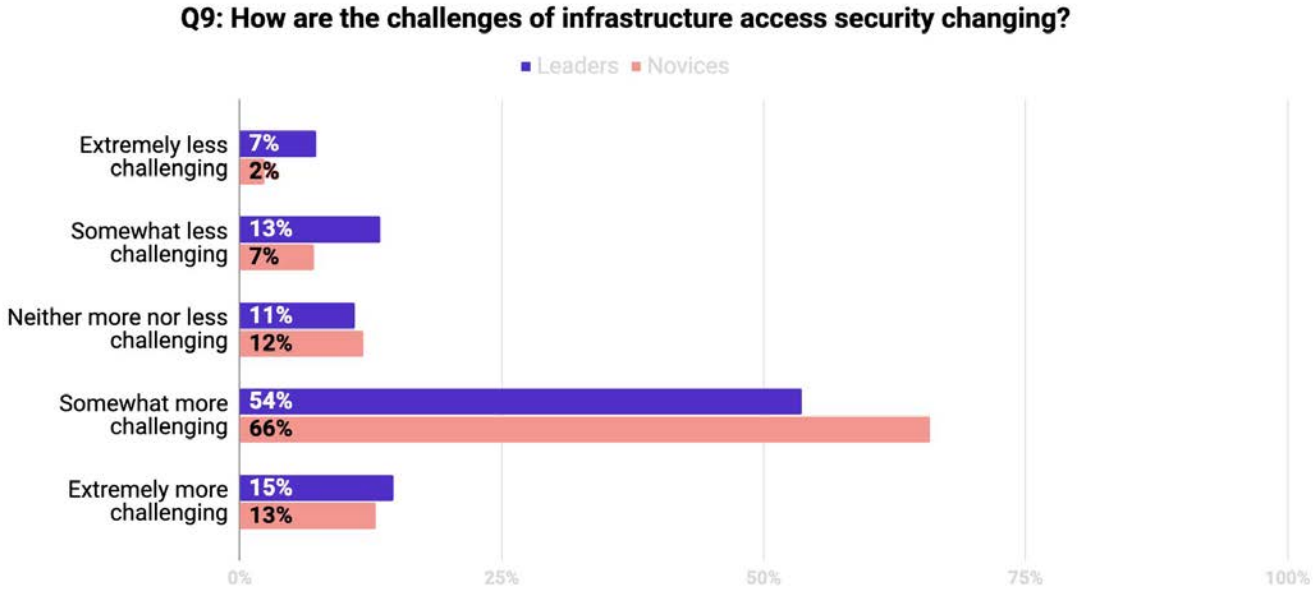


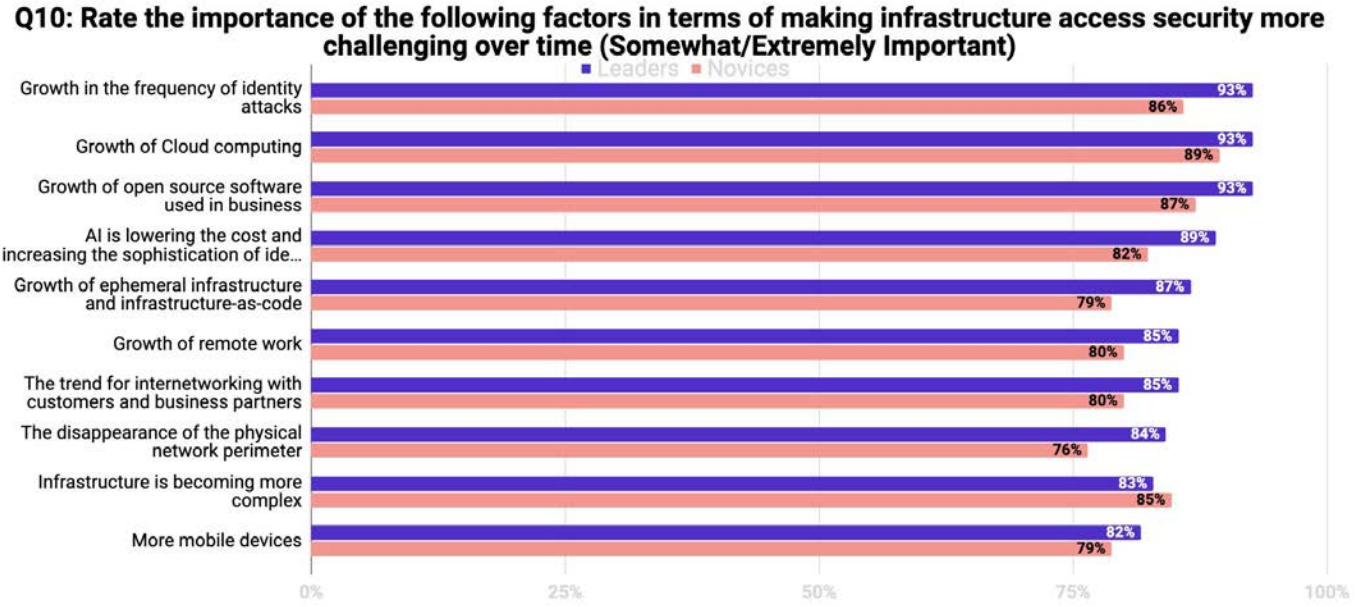


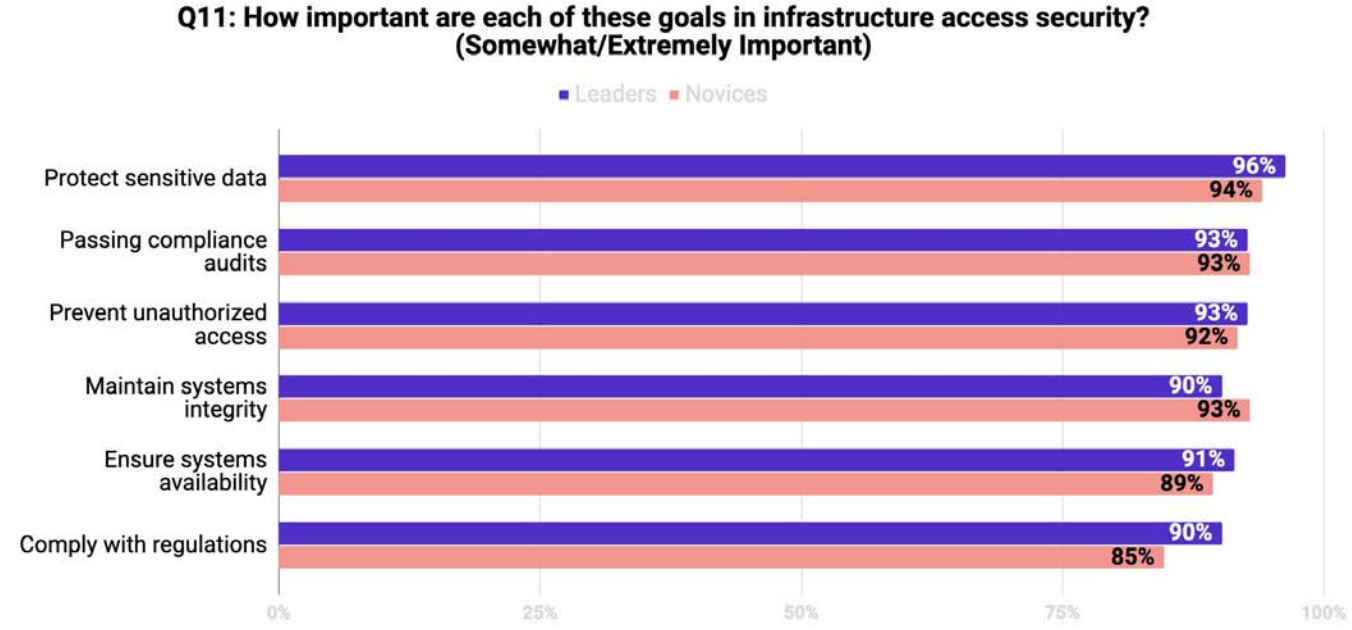




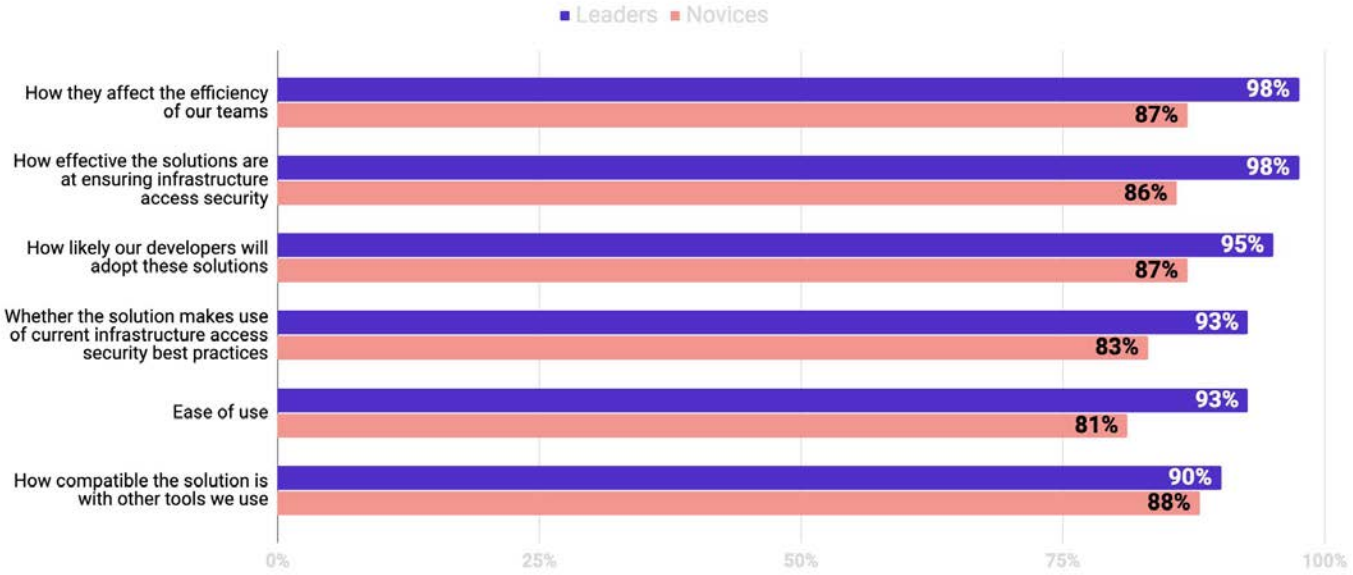




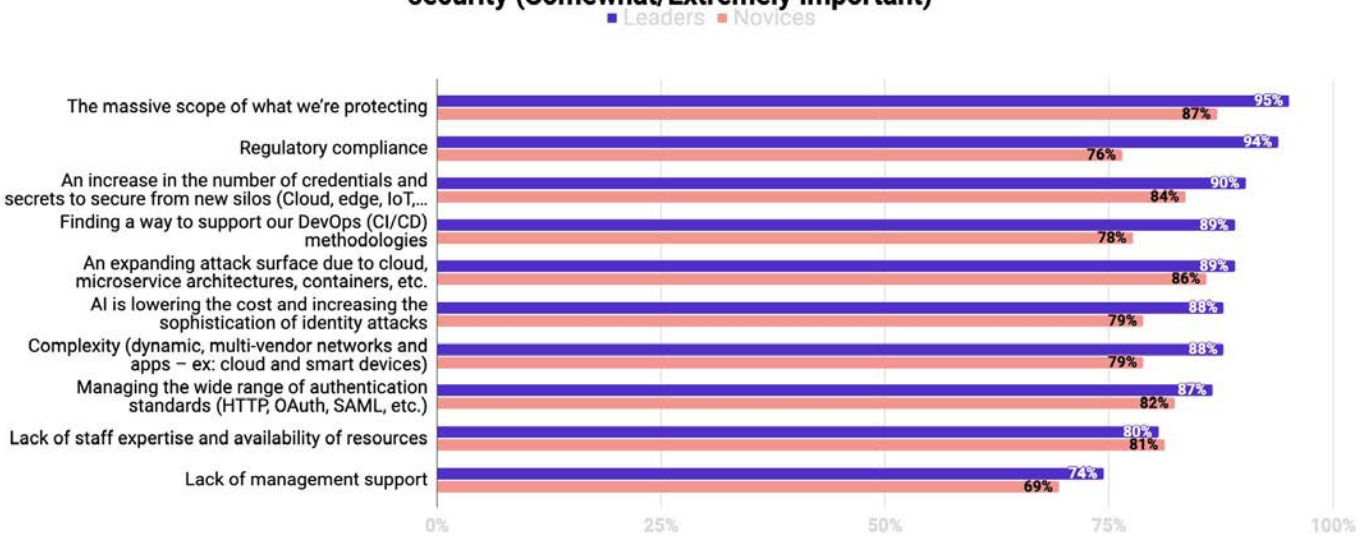




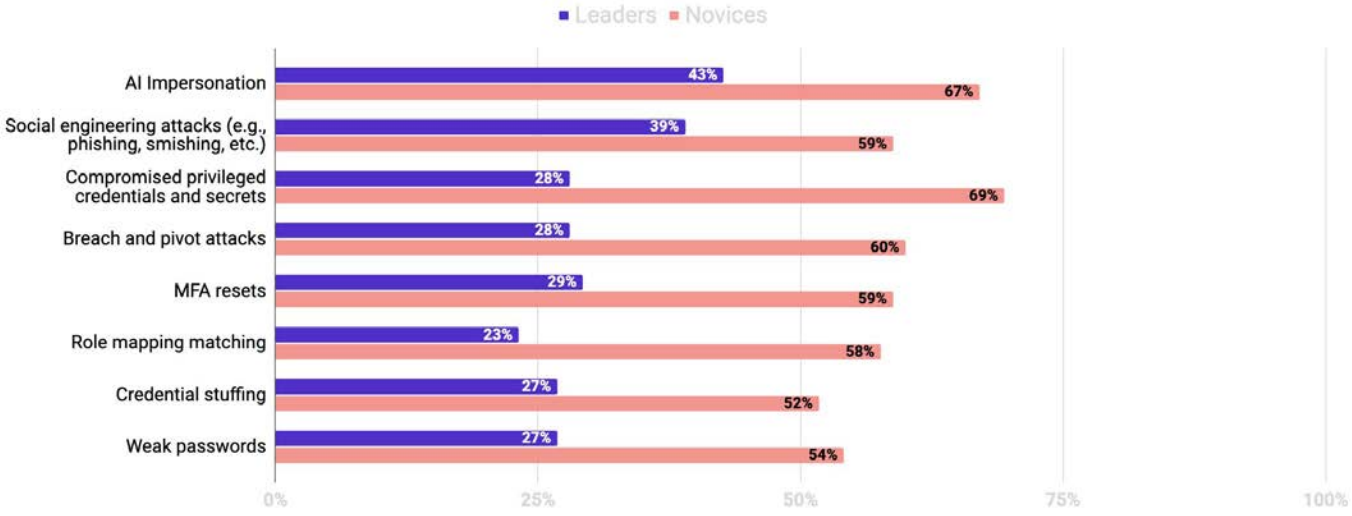
Q12: How important are the following factors when choosing infrastructure access security solutions?



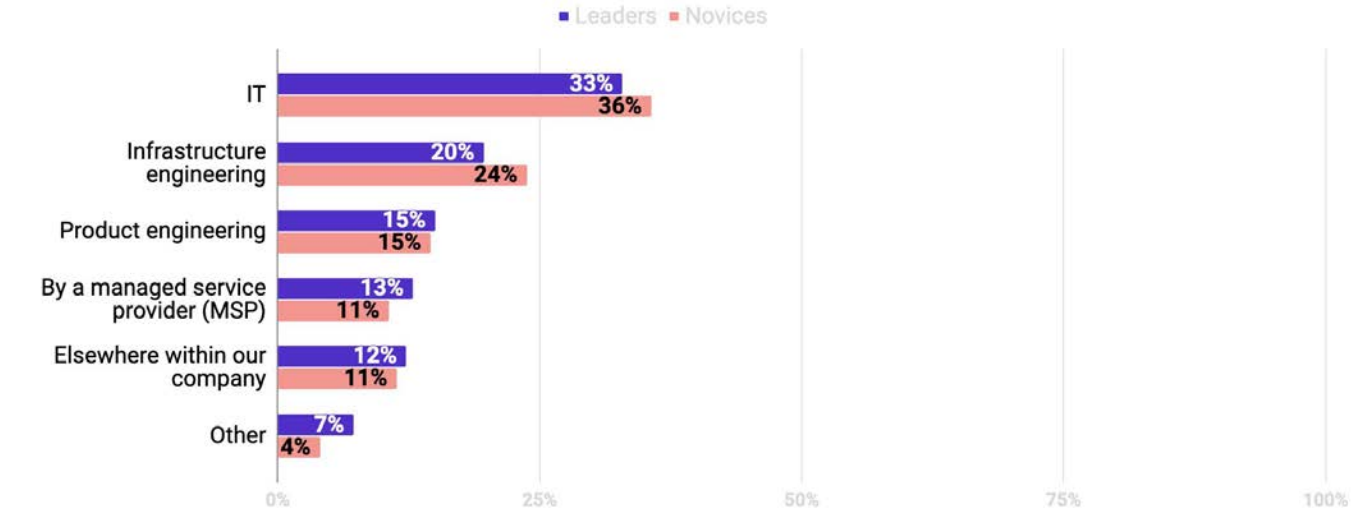
Q13: Rate the importance of the following challenges you face in implementing your infrastructure access security (Somewhat/Extremely Important)



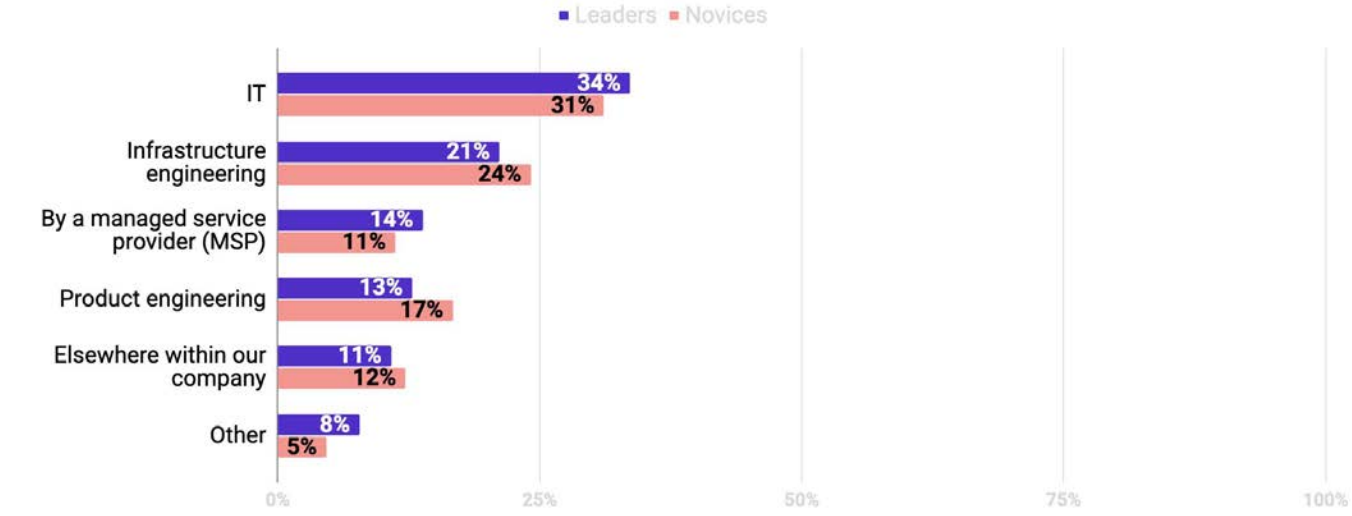
Q14: Rate how easy or difficult it is to protect against each of these attack vectors (Somewhat/Extremely Difficult)



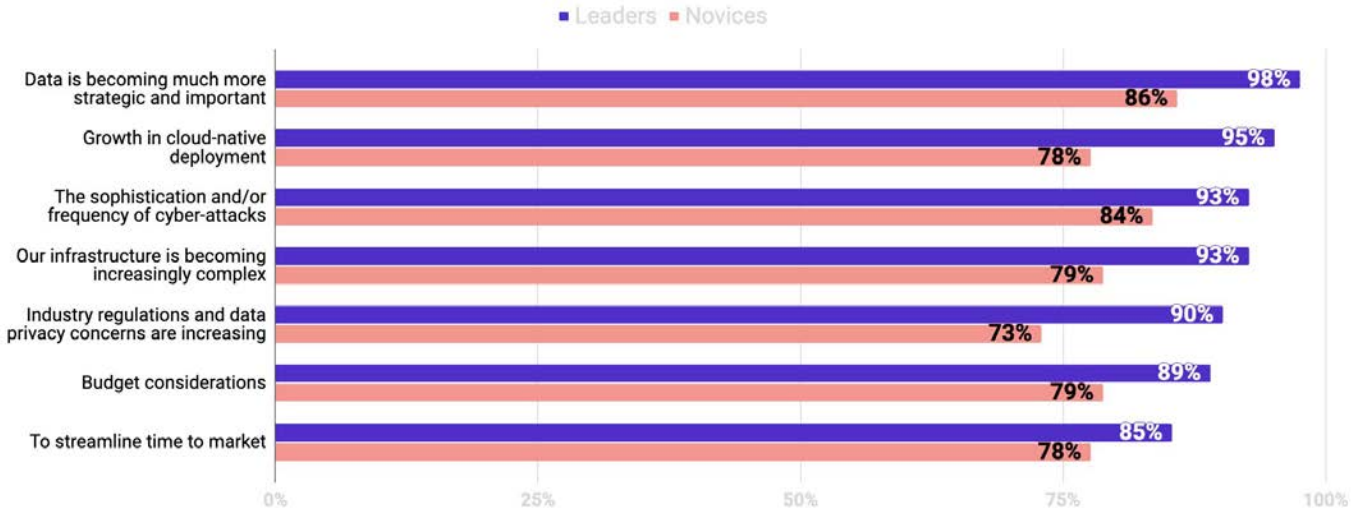
Q15: We first want to explore where infrastructure access security is managed today. What percentage of your infrastructure access security is managed in each of these areas?



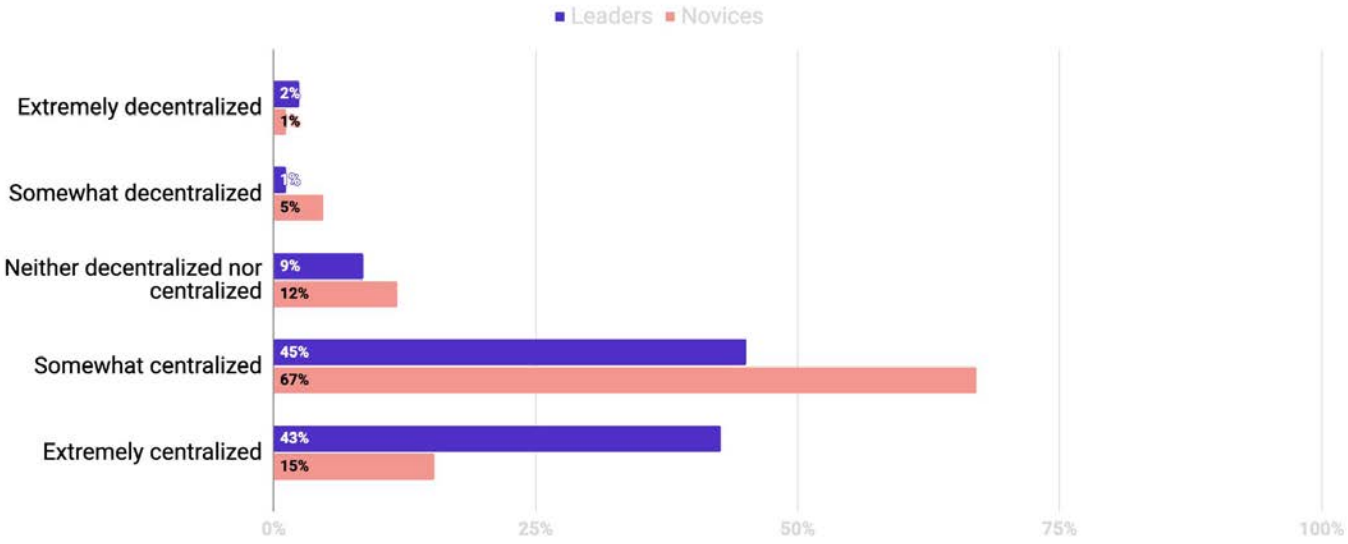
Q16: Next, where will infrastructure access security be managed in three years? What percentage of your infrastructure access security is managed in each of these areas?



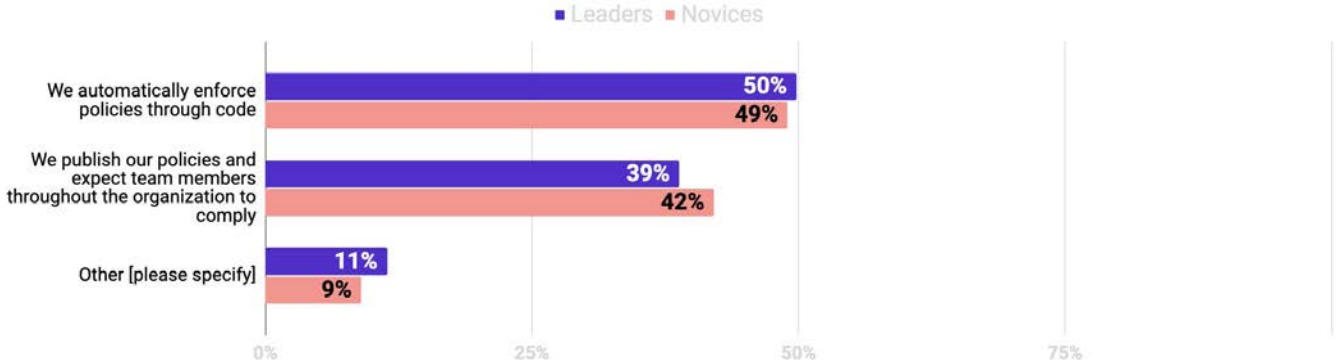
Q17: How important are the following factors in determining where you manage infrastructure access security?

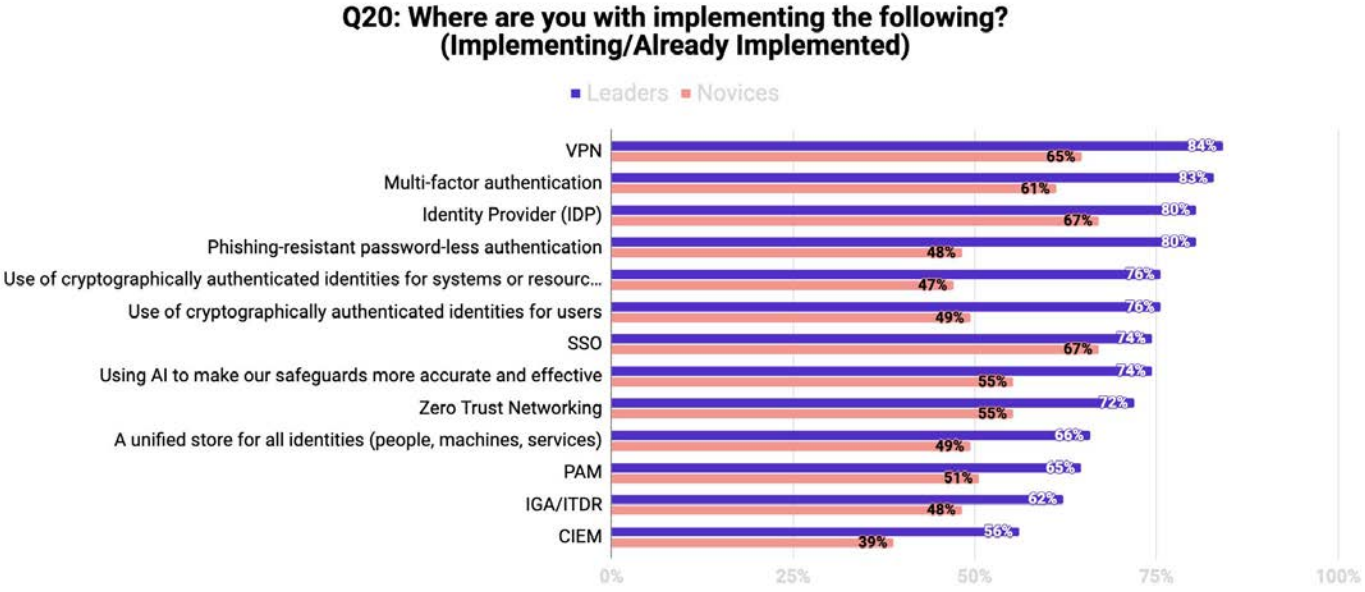


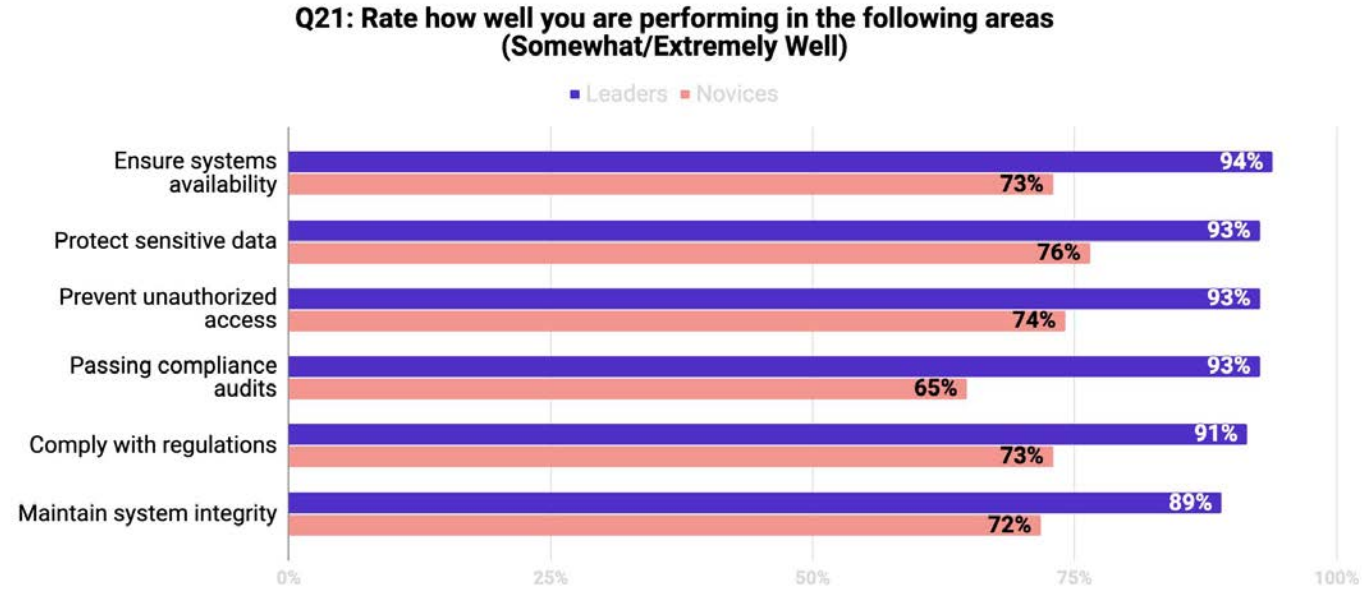
Q18: How centralized is infrastructure access security responsibility in your organization?



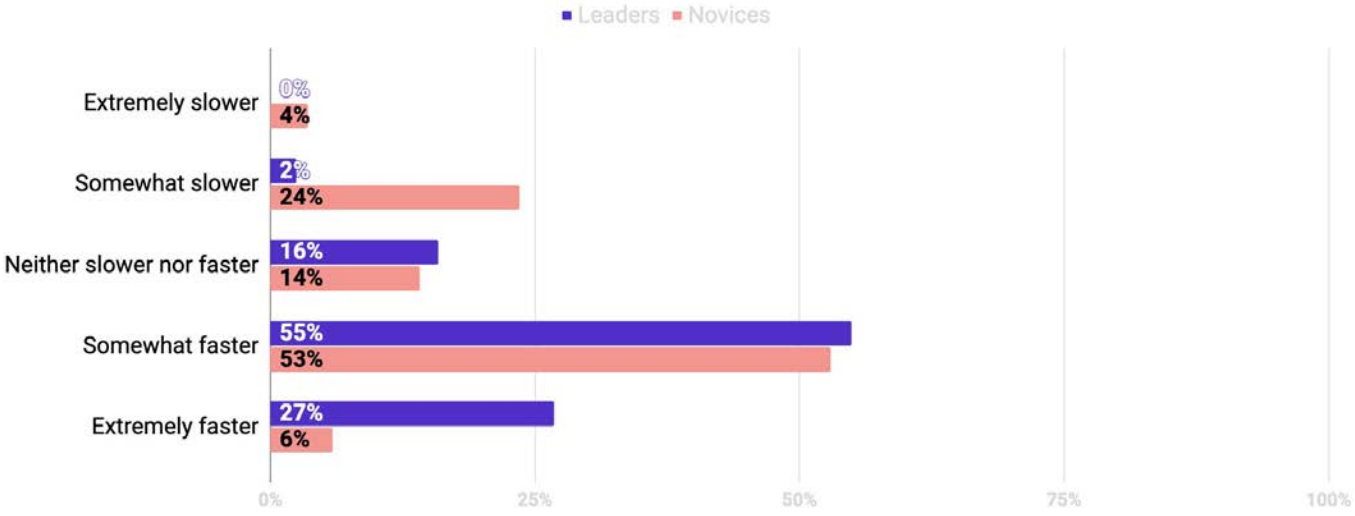
Q19: What percentage of each method do you use to enforce security policies organization-wide?



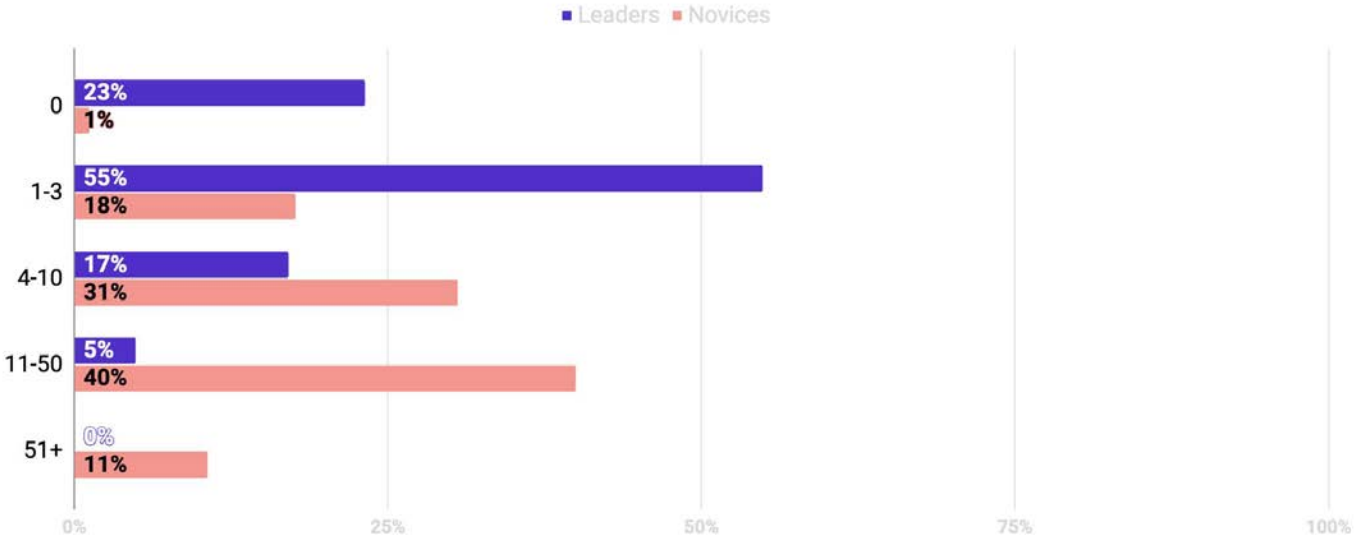




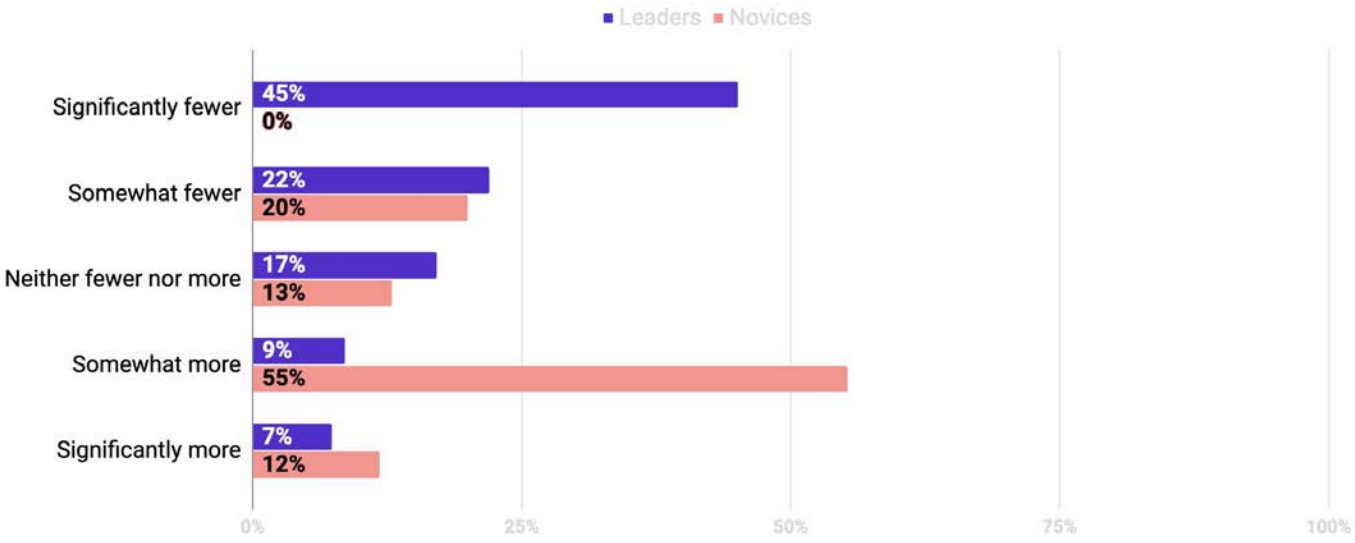
Q22: How have your organization's infrastructure access security initiatives affected software development in terms of agility and time-to-market?



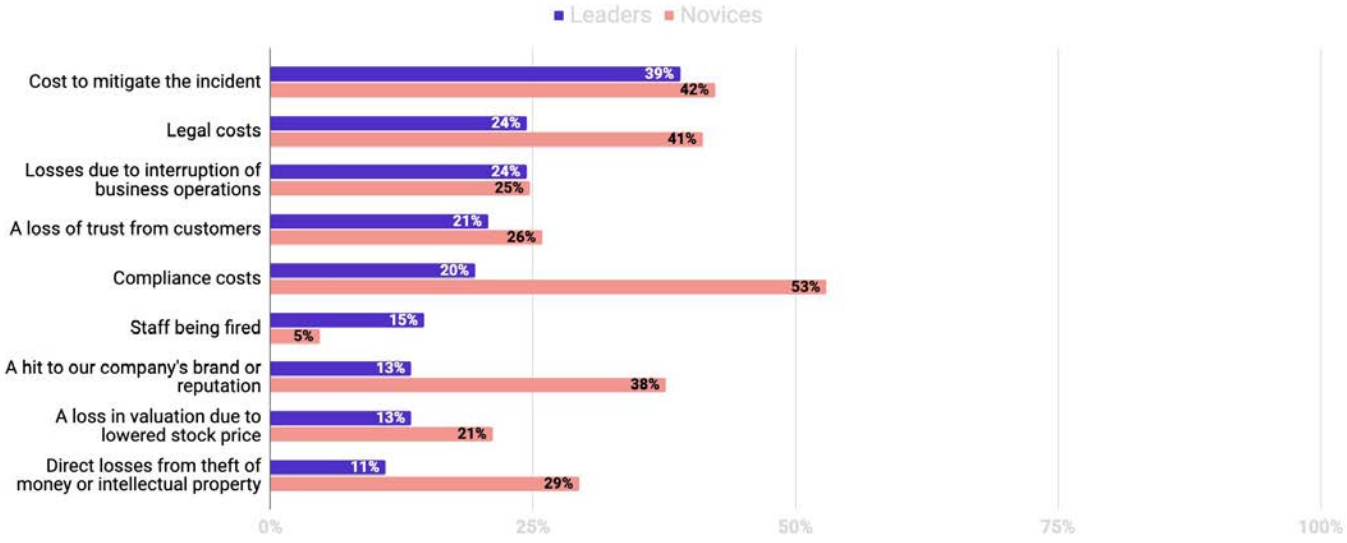
Q23: How many security incidents has your organization experienced during the past THREE years?



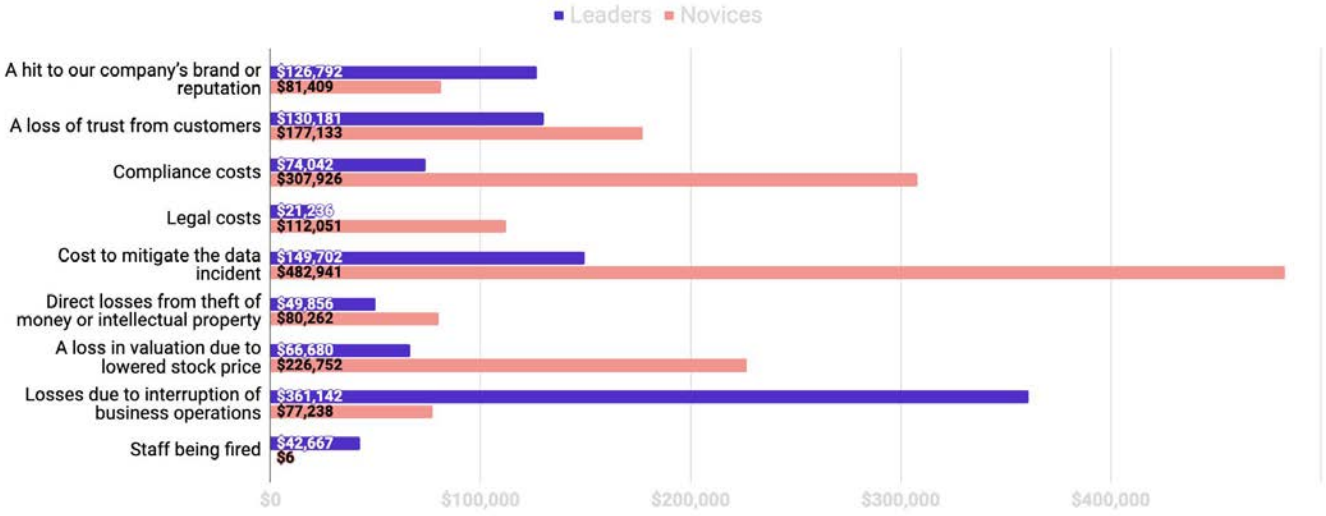
Q24: How has the number of security incidents your organization experiences changed over time?



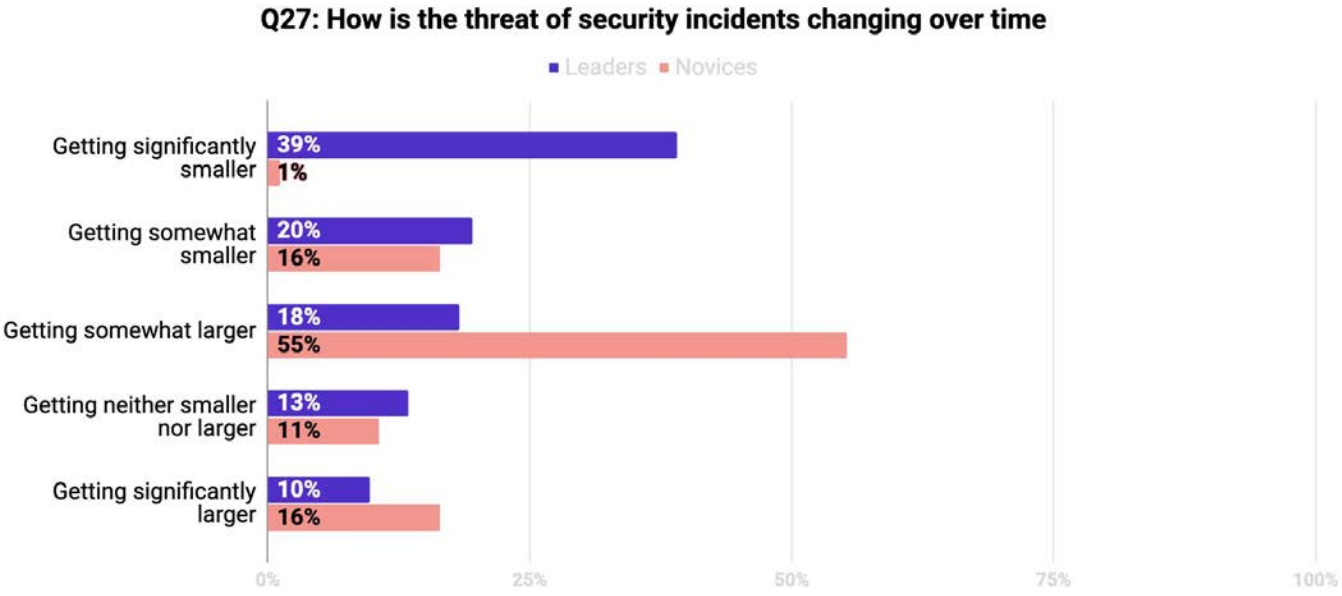
Q25: Which of the following consequences have you experienced as a result of these incidents?



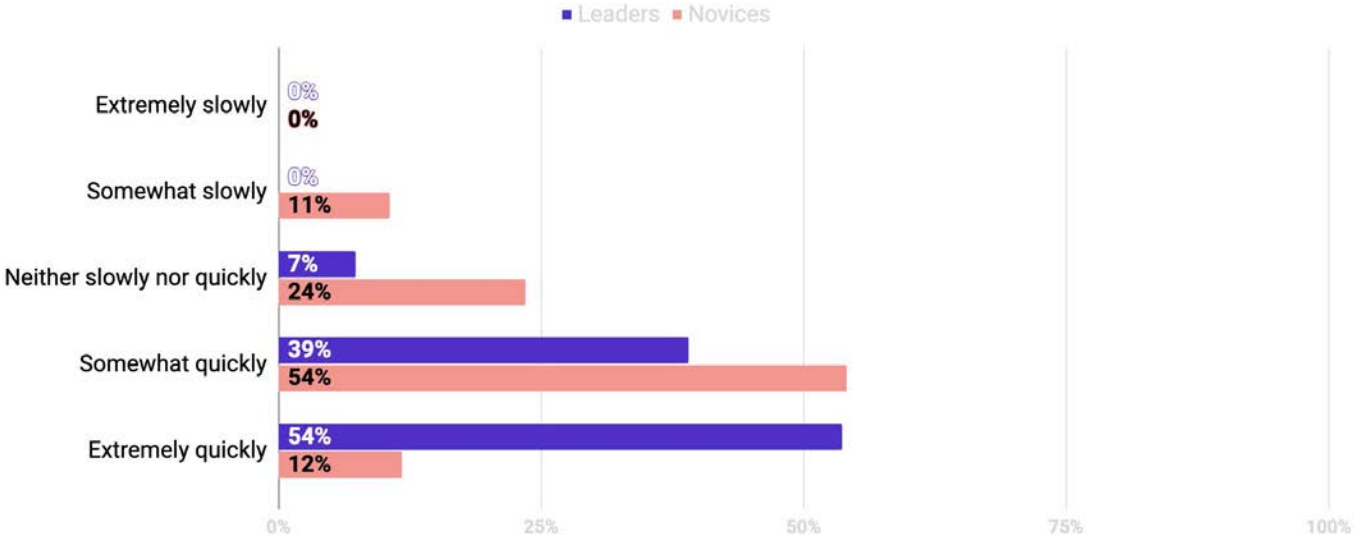
Q26: Estimate the total cost of each of the following consequences on a per-incident basis (Overall)



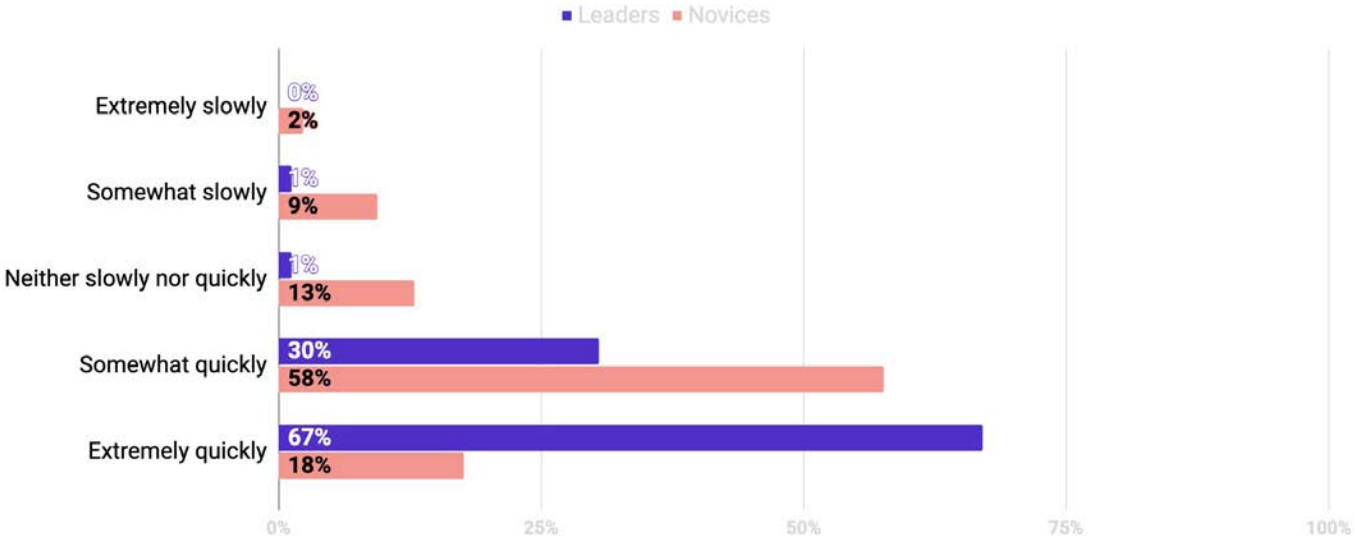
Q26: Estimate the total cost of each of the following consequences on a per-incident basis (Only those who experienced this consequence)

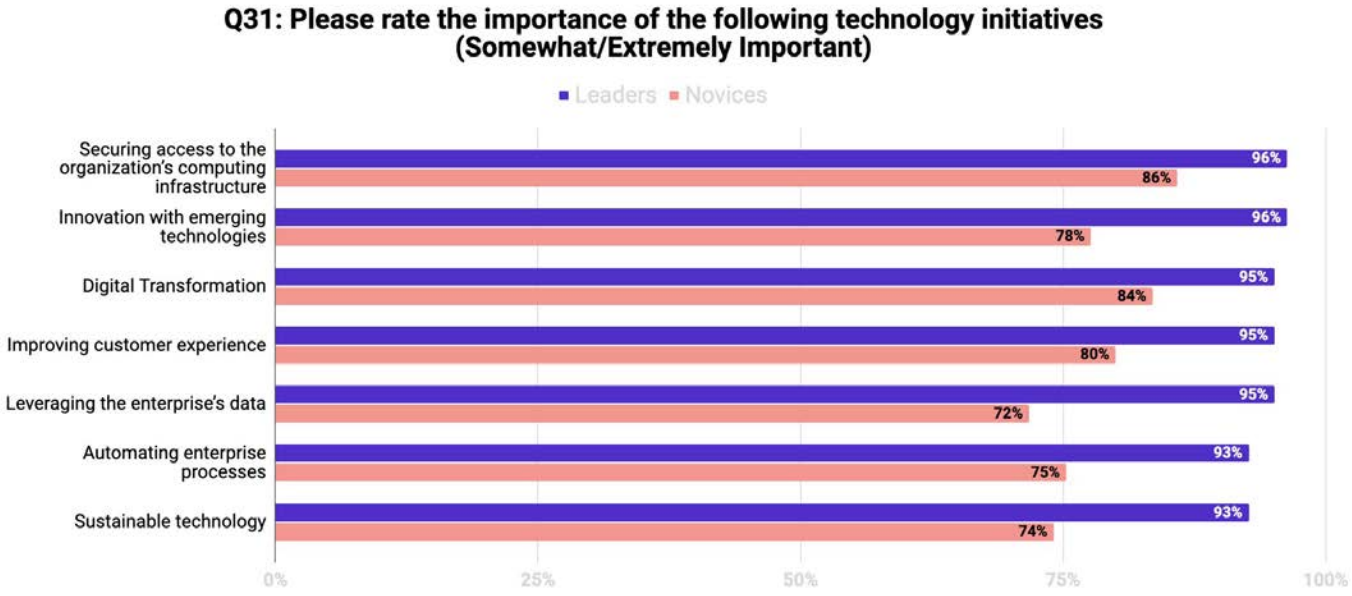


Q29: How quickly can you determine who has access to various infrastructure resources?



Q30: How quickly can you react to security incidents (e.g., breaches, compromises)?





Teleport

Teleport is the global provider of modern access to infrastructure, improving efficiency of engineering teams, fortifying infrastructure against bad actors or error, and simplifying compliance and audit reporting. The Teleport Access Platform delivers on-demand, least privileged access to infrastructure on a foundation of cryptographic identity and zero trust, with built-in identity security and policy governance. Headquartered in Oakland, California, Teleport is backed by Kleiner Perkins, Bessemer Venture Partners, and Insight Partners and serves more than 600 customers around the world.

For more information, visit **www.goteleport.com** or follow **@goteleport**.

Follow us on: