GLOBAL EDITION

THALES
Building a future we can all trust

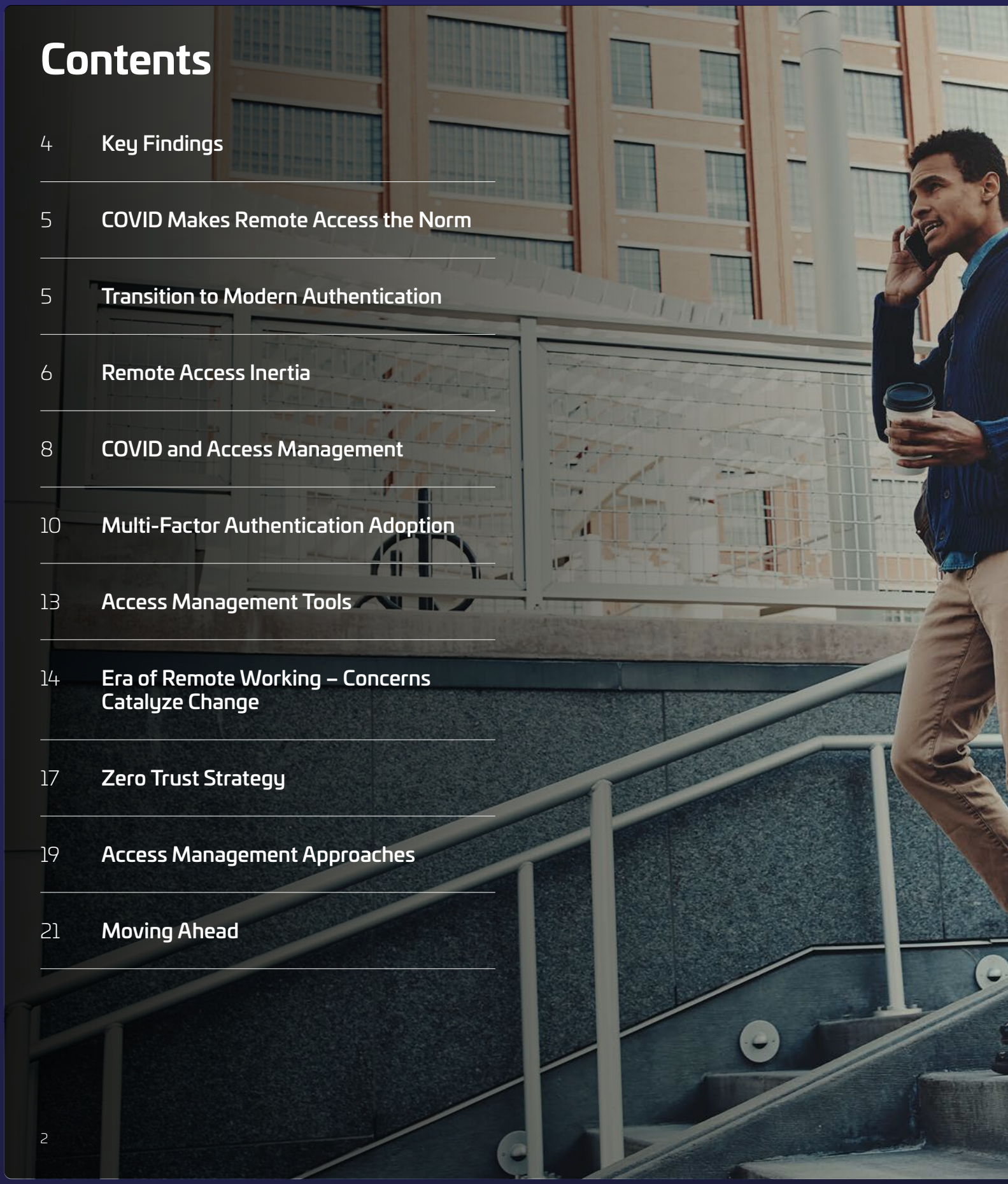
2021 Thales Access Management Index

The Challenges of Trusted Access in a Cloud-First World

#2021AMI

cpl.thalesgroup.com

Contents



About this study

The changes that the last year has wrought upon organizations' technology teams have been most acute in access management. Seemingly overnight, remote access went from being an exception to the default working model for a large swath of employees. The 2021 Thales Access Management Index, based on data from a survey of more than 2,600 respondents in more than 10 countries across the globe, looks to identify the depth of that change, as well as the current state of and plans for access management across a range of industries. The insights in this report were gleaned from the survey data, and it explores the impacts for security strategy and planning.

451 Research

S&P Global
Market Intelligence

Source: 2021 Access Management custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Our sponsors are:

ARROW

SENETAS

versasec

SYNNEX WESTCON

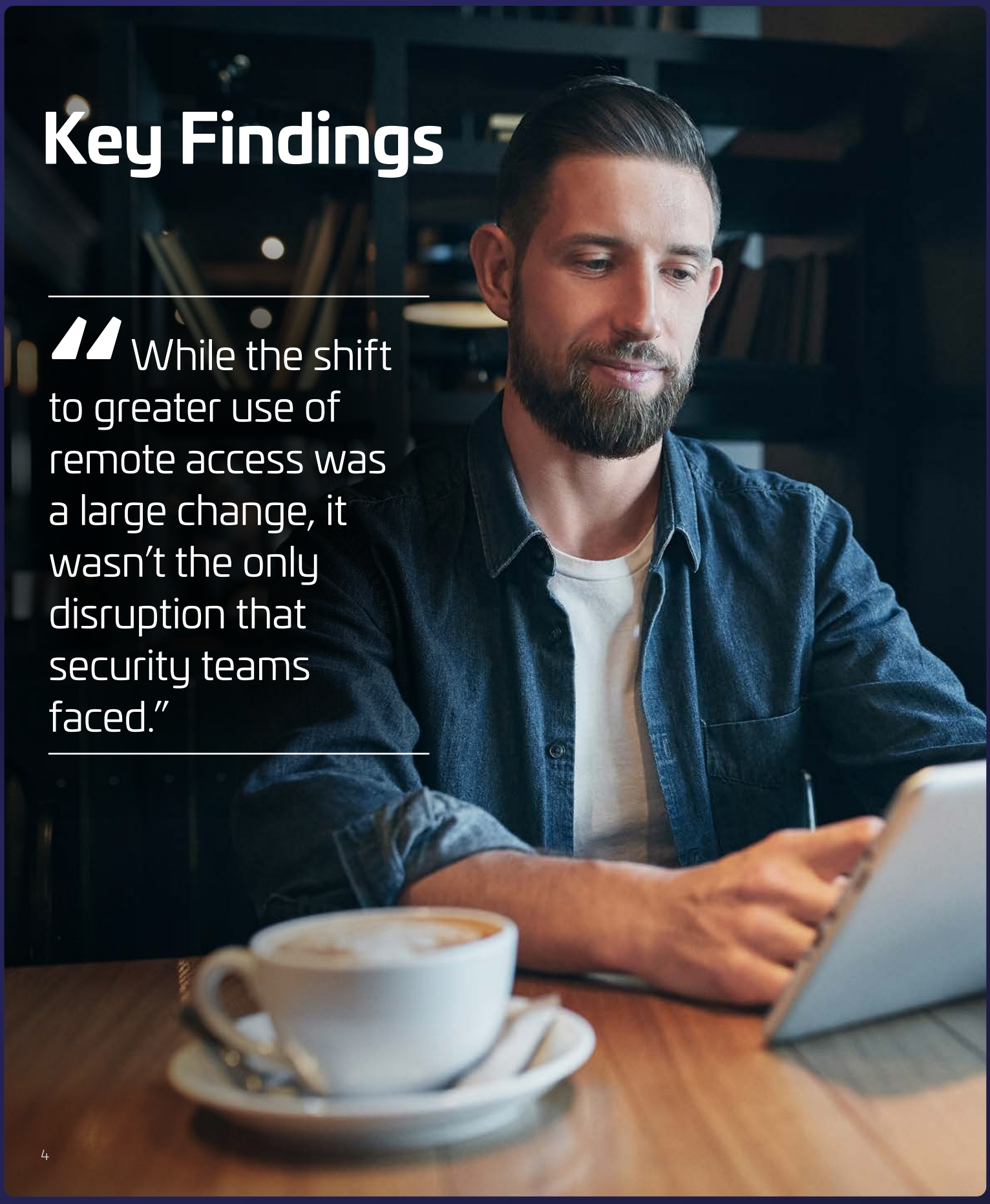
NTT DATA
NTT DATA INTELLILINK Corporation

F9C
Walking Together

FIRST TECH

Adistec

Key Findings



"While the shift to greater use of remote access was a large change, it wasn't the only disruption that security teams faced."

COVID Makes Remote Access the Norm

The COVID-19 pandemic has changed the expectations and reality of information security and its management. While the shift to greater use of remote access was a large change, it wasn't the only disruption that security teams faced. A dramatic increase in the use of cloud-based services strained identity and access management infrastructure at the same time. Not only were employees suddenly scattered to the four winds, but workloads, applications and business functions also took flight. Security infrastructures were stressed by this shift, with just a fifth of respondents (20%) indicating that their environments were "very prepared" to deal with the disruption. The shift to remote work was a large contributor to that disruption. Almost 82% of respondents said they are "somewhat" or "very" concerned about the security risks and threats that a greatly increased remote workforce poses. Almost half (44%) are not confident that their access security systems can effectively secure remote work. That's a significant level of concern across these environments. The survey looked to explore expectations about access management and respondents' plans.

Transition to Modern Authentication

The changes that occurred in the last year have pushed organizations to evaluate the state of authentication environments, and many are looking to adopt modern authentication approaches. Beyond the strain that remote work created, organizations faced the limitations of their current implementations and considered how they could improve their situation. The study found that more than half have adopted two-factor or multi-factor authentication (MFA), but there is still a lack of investment in access management controls compared to perimeter-focused tools like network firewalls and endpoint security (for brevity, we use MFA to refer to both 2FA and MFA for the remainder of this report). That's an indication that there is still a lack of maturity in understanding security approaches that are more effective in a world where there is no longer a defined perimeter. Access management is a key element on which these other technologies rely to be effective. Underinvestment in this foundational element may be a symptom of outdated, perimeter-based strategies and can leave significant gaps in security protections.

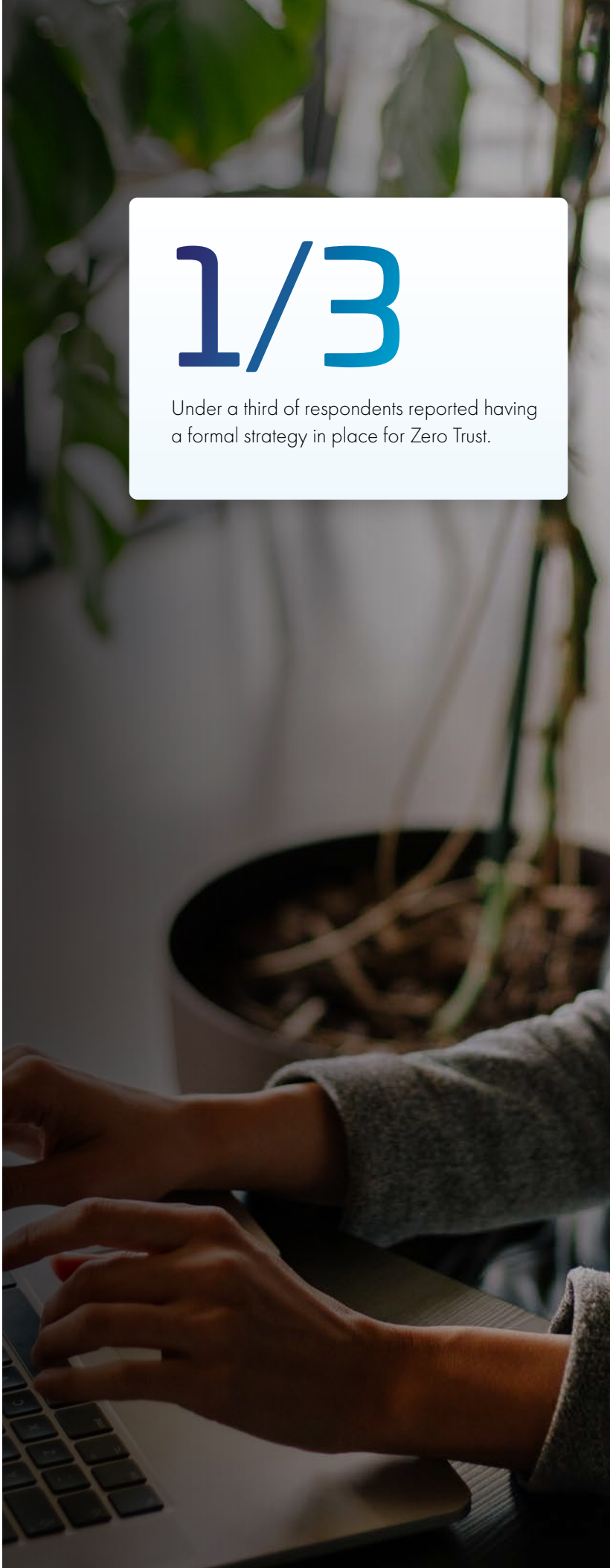
The more sophisticated technologies that make up a modern authentication approach have most often been put to work in remote access. It's seen as a higher-risk environment and, presumably, is the place where it is worth the cost of deployment and use. But respondents indicated a desire to get to greater levels of control through Zero Trust strategies. The challenge is that only about a third said they have an integrated access management system deployed. The majority that don't likely face operational burdens on their teams as they coordinate across systems. About a third of respondents said that they have three or more systems. That level of operational complexity can slow responses and increase the chance for errors.

Remote Access Inertia

The pandemic created an urgent need for organizations to scale up their remote access capacity, and most needed to improve the security effectiveness, too. Only about a fifth of those surveyed indicated that they have no plans to change from existing VPN environments. The greatest number were looking to Zero Trust network access and software-defined perimeter (ZTNA/SDP) options. Interestingly, just under a third indicated that MFA requirements were driving a change. That could be caused by concerns about existing authentication mechanisms in their VPN deployments.

Zero Trust is an area of great interest but still has low adoption. Under a third of respondents reported having a formal strategy in place for Zero Trust. However, ZTNA/SDP was the leading answer to the question of which new access technologies were going to be put in place as a result of the pandemic. Zero Trust is already guiding security strategies in cloud environments, with three-quarters of respondents saying they rely on it. With the high level of interest expressed, Zero Trust concepts should be integrated into broader access management applications in short order. That's one more change that information security teams will be handling in the year ahead.

> **"Zero Trust is an area of great interest but still has low adoption."**



1/3

Under a third of respondents reported having a formal strategy in place for Zero Trust.

Key Findings

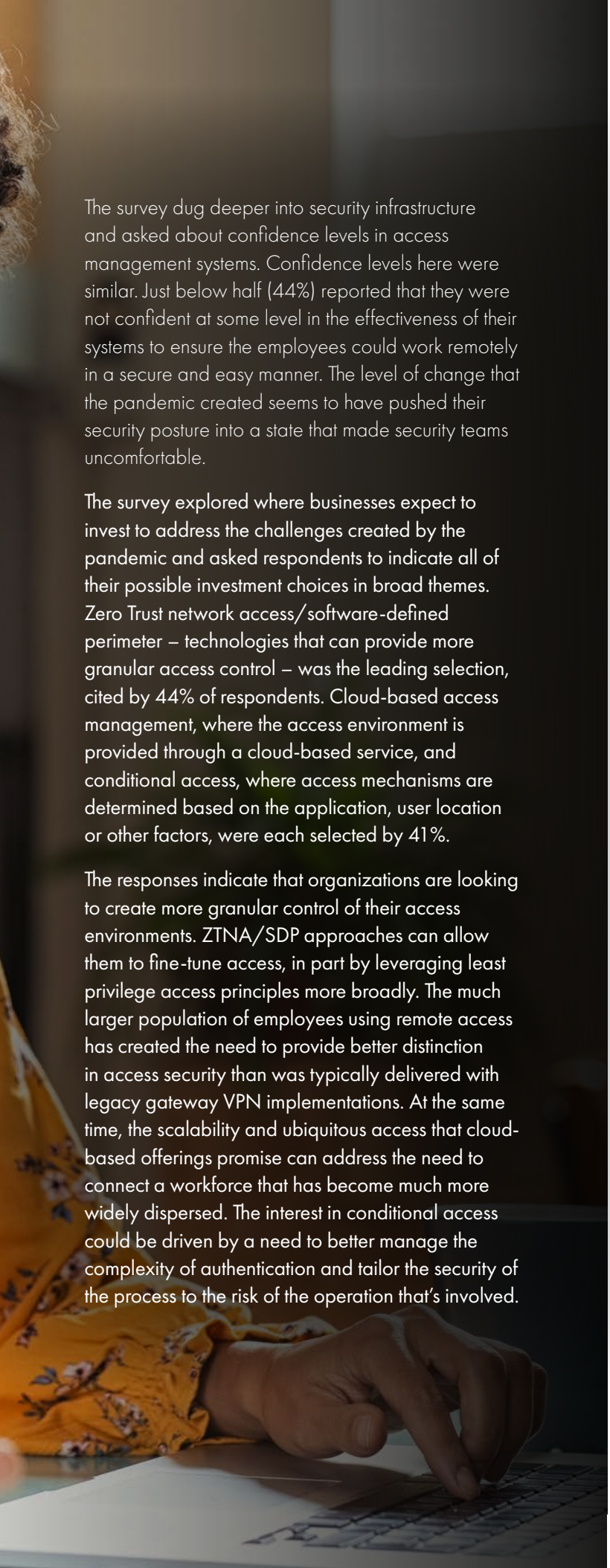
- The COVID-19 pandemic has put considerable strain on information security environments, with only a minority (20%) indicating that they were prepared.
- The much larger population of employees using remote access has created the need to provide more granular control in access security than was typically delivered with legacy gateway VPN implementations.
- Respondents cited spanning on-premises and cloud-based environments as the greatest challenge in access management.
- Organizations indicated that they're moving to more modern authentication technologies, and that's prompting changes in remote access.
- There's significant interest in Zero Trust strategies, but it's still early days, with low levels of reported adoption balanced by high levels of interest and plans for deployment.

> **"Respondents cited spanning on-premises and cloud-based environments as the greatest challenge in access management."**

COVID and Access Management

The global pandemic has forced lasting changes across the information technology landscape. The 2021 Thales Access Management Index looks to characterize the nature of the change in access management through a far-reaching, global survey of over 2,600 information security professionals. The survey explored experiences in the past year and their expectations for the year ahead. The results bring together the thoughts and opinions of professionals in senior management, implementation and strategic roles from 16 countries.

The changes driven by the pandemic were most acute in access management. The rapid shift to remote work meant that the normal priorities for access were upended as large numbers of employees shifted out of traditional office environments. When respondents were asked about the preparedness of their information security infrastructure to deal with the challenges that the pandemic presented, just 20% indicated that the infrastructure was "very prepared." Almost half (46%) felt that it was "somewhat unprepared" or "not at all" prepared for the risks that the pandemic shifts created.



The survey dug deeper into security infrastructure and asked about confidence levels in access management systems. Confidence levels here were similar. Just below half (44%) reported that they were not confident at some level in the effectiveness of their systems to ensure the employees could work remotely in a secure and easy manner. The level of change that the pandemic created seems to have pushed their security posture into a state that made security teams uncomfortable.

The survey explored where businesses expect to invest to address the challenges created by the pandemic and asked respondents to indicate all of their possible investment choices in broad themes. Zero Trust network access/software-defined perimeter – technologies that can provide more granular access control – was the leading selection, cited by 44% of respondents. Cloud-based access management, where the access environment is provided through a cloud-based service, and conditional access, where access mechanisms are determined based on the application, user location or other factors, were each selected by 41%.

The responses indicate that organizations are looking to create more granular control of their access environments. ZTNA/SDP approaches can allow them to fine-tune access, in part by leveraging least privilege access principles more broadly. The much larger population of employees using remote access has created the need to provide better distinction in access security than was typically delivered with legacy gateway VPN implementations. At the same time, the scalability and ubiquitous access that cloud-based offerings promise can address the need to connect a workforce that has become much more widely dispersed. The interest in conditional access could be driven by a need to better manage the complexity of authentication and tailor the security of the process to the risk of the operation that's involved.

FIGURE 1

Access Management Confidence

Q: How confident are you that your current access security solutions can effectively enable employees to work remotely in a secure and easy manner?

- **22%** Very confident
- **34%** Somewhat confident
- **28%** Somewhat not confident
- **16%** Not at all confident

Source: 451 Research's 2021 Access Management custom survey

> **"44% reported that they were not confident at some level in the effectiveness of their systems to ensure the employees could work remotely in a secure and easy manner."**

Multi-Factor Authentication Adoption

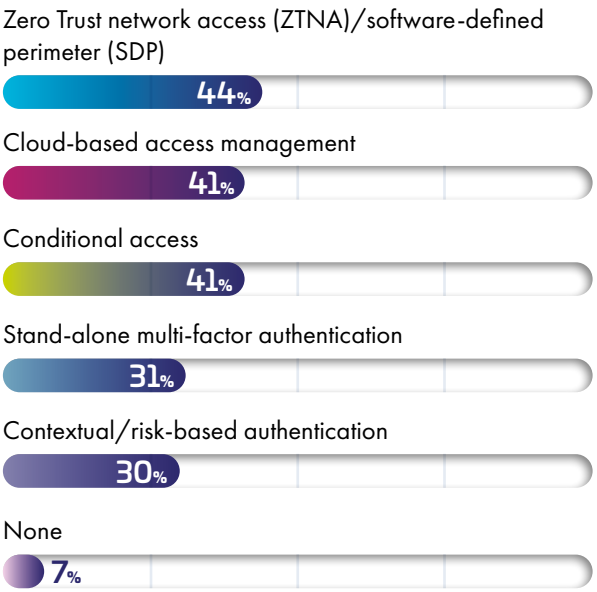
The survey found that organizations have a strong desire to improve the security of their authentication processes in a number of areas. We wanted to understand where they were on their journey to more sophisticated and modern authentication capabilities. We looked first at the current level of MFA adoption. While the global average was 55% having adopted MFA, there was notable variation among geographies: the UK led at 64%, followed by the US at 62%, the APAC region at 52% and LATAM at just 40%. These varying levels of adoption may be due to how organizations prioritize better access management in security investments. The survey asked respondents to rank technologies by their expected effectiveness in protecting sensitive data, and access management was ranked below endpoint protection, encryption, key management and network security. An interesting perspective in the survey data is that those respondents who reported that they were further along in the adoption of Zero Trust, a change that requires more sophisticated access management, were less likely to have reported that they had experienced a data breach. While this correlation cannot be identified as the cause of this outcome, it is an interesting observation.

More sophisticated techniques, such as MFA, are still primarily reserved for use cases that are perceived as risky. Respondents identified remote access users as the most likely to use MFA at 71%. Third parties (consultants, partners, suppliers) were a distant second at 50%. Privileged users followed closely at 48%, and customers and internal users were a step behind at 36% and 34%, respectively. The results indicate that greater concern – and resulting investment – is placed on threats that are expected to come from external sources. This contrasts with the results of another question in the survey in which respondents ranked malicious insiders well ahead of external attackers, human error and nation states as the greatest threats to their environments. Improving the maturity and effectiveness of access management is one of the best ways to counter insider threats. The data seems to show that many organizations would be better served by reevaluating their security investment priorities. Greater use of modern authentication methods in all areas, rather than just in externally facing situations, would better mitigate insider threats.

FIGURE 2

New Access Investments

Q: Which of the following new security technologies are you investing in?

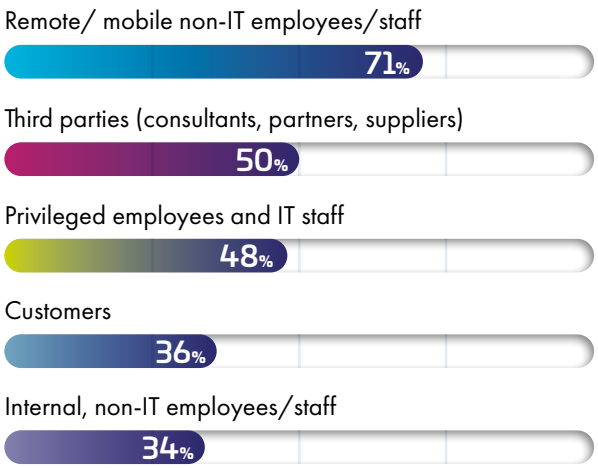


Source: 451 Research's 2021 Access Management custom survey

FIGURE 3

Users of MFA

Q: For which user groups have you deployed multi-factor authentication?



Source: 451 Research's 2021 Access Management custom survey

The trends in MFA user populations extended to application environments where MFA was put in place. Respondents said that MFA was utilized more often by users of cloud applications than those on-premises, and more cloud-based applications were protected by MFA than those that were hosted on-premises. For both sets of questions, greater levels of protection were in place for the off-premises environments. For example, 43% of respondents indicated MFA was in place for over 31% of users of cloud/SaaS applications, but that number dropped to 30% for on-premises applications. For application protection, 36% of respondents said that over 41% of cloud-based applications and services are protected with more modern authentication, but that only 24% were above 41% for on-premises applications and services. That's aligned with historical thinking that prioritized external threats, but it is less effective in addressing the insider threat that the survey respondents and more mature security strategies see as today's greater urgency. Organizations need to shift their security investments to improve their security posture with more modern authentication technologies and approaches.

> **"MFA was utilized more often by users of cloud applications than those on-premises, and more cloud-based applications were protected by MFA than those that were hosted on-premises."**

FIGURE 4

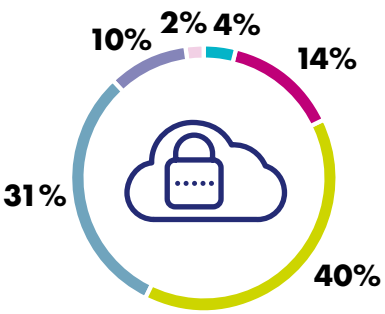
MFA Use – Cloud vs. On-Premises

Q: What percentage of cloud services and on-premises apps in your organization are protected with multi-factor authentication?

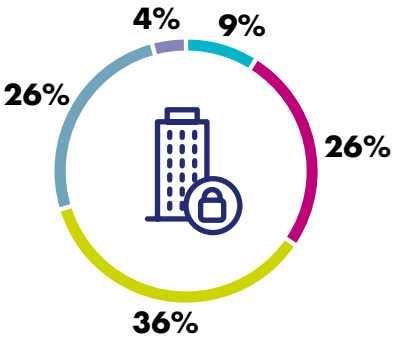
- 0-10%
- 11-20%
- 21-30%
- 31-40%
- 41-50%
- >50%

Source: 451 Research's 2021 Access Management custom survey

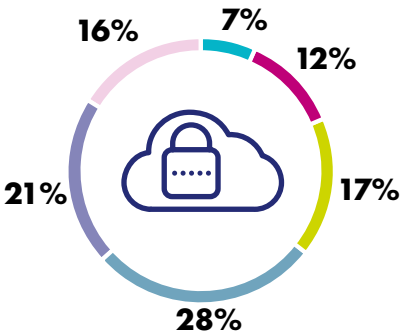
More MFA use in cloud



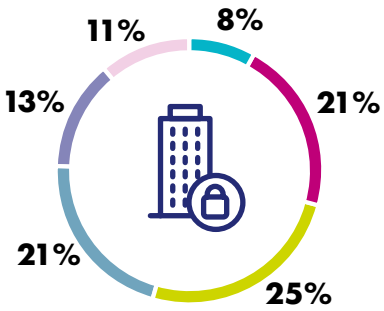
Less MFA use on-premises



Cloud protected by MFA



On-premises protected by MFA



> "Many organizations have grown their access management organically, deploying different tools at different times."

Access Management Tools

Modern access management tools and technologies form a key part an enhanced security infrastructure's foundation. Organizations need to advance their capabilities to keep up with increasingly sophisticated adversaries. Improving access management is a critical element of organizations' progress in moving beyond perimeter-based security models and toward a Zero Trust approach. The survey first looked at what access management tools organizations have in place. Many organizations have grown their access management organically, deploying different tools at different times – 61% of respondents said they haven't deployed an integrated access management platform (an integrated system that provides policy-based access, cloud SSO, authentication). The extent of access management tool sprawl shed more light on this problem. A third (33%) of respondents said they use three or more authentication access management tools. Coordinating that many systems can, at a minimum, create operational complexity, but it can also increase the risk of errors or misconfigurations creating security gaps.

FIGURE 5

Number of Authentication Tools

Q: How many different authentication vendor tools are being deployed?

30% 0
37% 1-2
25% 3-5
8% more than 5

Source: 451 Research's 2021 Access Management custom survey

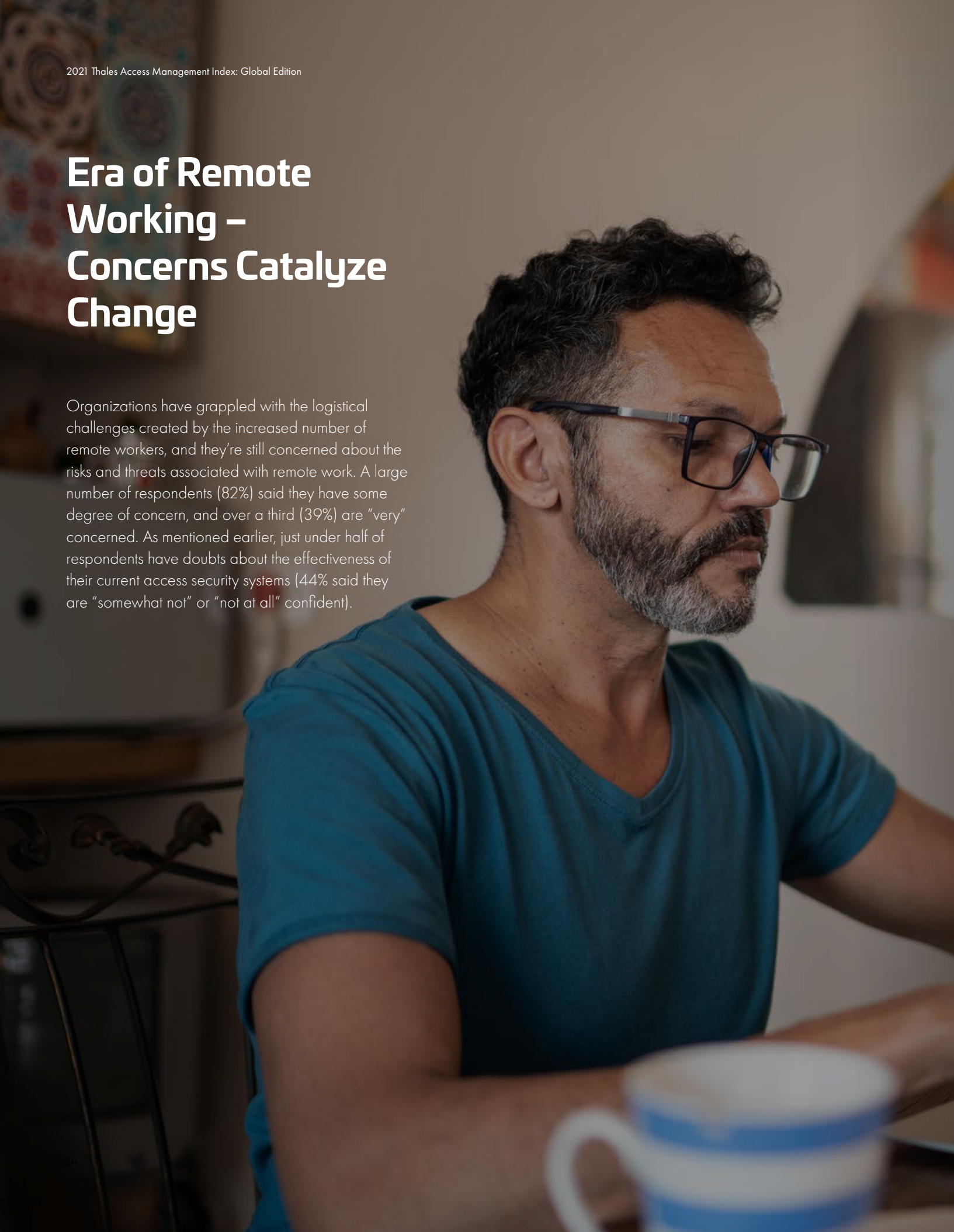
> **"Organizations need to advance their capabilities to keep up with increasingly sophisticated adversaries."**

61%

said they haven't deployed an integrated access management platform.

Era of Remote Working – Concerns Catalyze Change

Organizations have grappled with the logistical challenges created by the increased number of remote workers, and they're still concerned about the risks and threats associated with remote work. A large number of respondents (82%) said they have some degree of concern, and over a third (39%) are "very" concerned. As mentioned earlier, just under half of respondents have doubts about the effectiveness of their current access security systems (44% said they are "somewhat not" or "not at all" confident).



This level of concern coupled with the lack of confidence is motivating organizations to make some changes. Organizations currently have a wide range of remote access systems deployed. VPN is the most common, with 60% globally identifying the capability. Virtual desktop infrastructure (VDI – 56%), cloud-based access (53%) and ZTNA/SDP (53%) followed closely. Regionally, the US was an outlier, placing VDI first (59%) and VPN second (57%). When looking at industry verticals, 62% of financial services respondents indicated VDI, and cloud-based access followed at 60% deployment. Retail followed similar trends with VDI being the leading selection at 61%. While most indicated some level of more advanced access technologies in place, questions about how they expect to change suggest that such deployments may be in the early stages.

When asked about which new access technologies they are planning to deploy because of the pandemic and the increased levels of remote work, ZTNA/SDP narrowly led the set of selections, with MFA coming in second. It is clear that organizations are pursuing a number of options to address the issues that they have identified in their access environments.

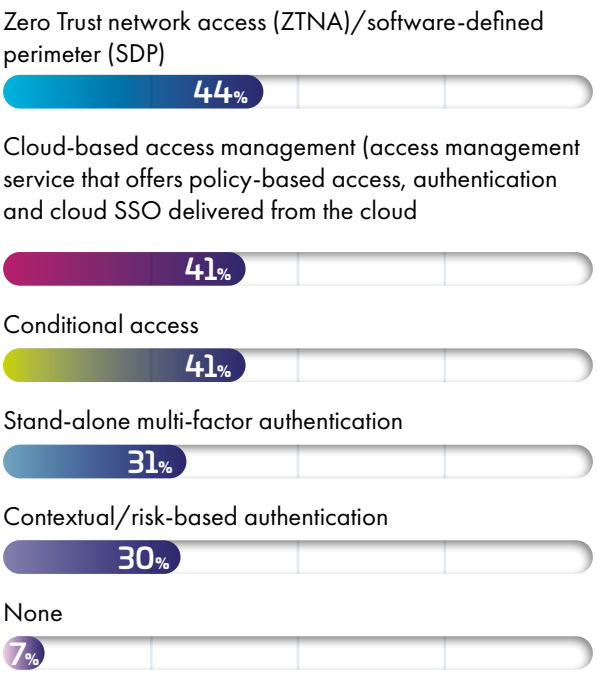
60%

of organizations globally deploy VPN as an access management system.

FIGURE 6

Pandemic-Driven Access Technology

Q: Which of the following new access technologies are you planning to deploy due to the impact of the pandemic and remote work?



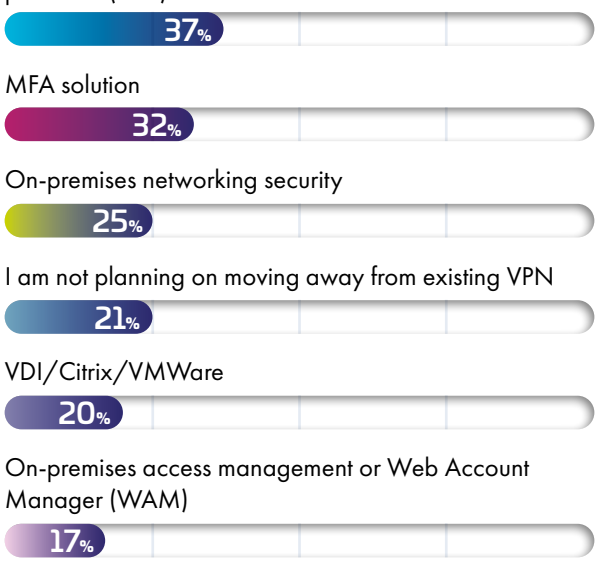
Source: 451 Research's 2021 Access Management custom survey

When we looked in more detail at plans to move beyond traditional VPN environments, ZTNA/SDP again led the way. The second-place choice, MFA, is an indication that a need for more sophisticated authentication capabilities is driving change in some organizations, which could be due to limitations in existing VPN capabilities. Over a fifth of respondents (21%) said that they don't have plans to move away from their existing VPN capabilities, indicating that, for some, the status quo is sufficient.

FIGURE 7

Replacing VPN

Q: Are you planning on moving away from VPN and replacing with any of the following?



Source: 451 Research's 2021 Access Management custom survey

Zero Trust Strategy

For the majority of respondents that are improving their access environments, Zero Trust approaches are the foundation of that shift to modern authentication. Most organizations are in the early stages of the journey, but there is strong interest in deployment. In 451 Research's most recent Voice of the Enterprise: Information Security study, respondents cited Zero Trust as the least implemented (at 13%) of a collection of security technologies, but the technology with the highest level of planned implementation – 49% of respondents said they are either in pilot or expecting to deploy Zero Trust within 24 months. In the custom survey, just under a third (30%) of global respondents said they have a formal strategy and have actively embraced a Zero Trust policy. Interestingly, those with a formal Zero Trust strategy are less likely to have been breached.

We looked at operational adoption of Zero Trust and when asked to what extent Zero Trust security shapes cloud security strategy, 32% of global respondents said, "to a great extent." Regionally, the US reported lower levels at 26%. Japan indicated significantly higher rates at 40% (ahead of the APAC regional average of 35%), and Sweden, Germany and France were slightly above at 38%, 35% and 34%, respectively (above the European regional average of 32%). For industry verticals, financial services firms were again further along in adoption, with 41% of respondents indicating greater Zero Trust involvement.

When taken together (grouping the "great extent" and "some" responses), 76% of respondents' cloud strategies relied to some degree on Zero Trust security strategies. This broader measure captures those that are still early in their journey to more modern access strategies. Once again, financial services firms were further along in industry verticals, with 83% reporting some level of Zero Trust use. The retail segment was close to the average, at 77%. There was less variation in geographic regions, with all close to the average, except for LATAM, which was lower at 71%. However, some individual countries stood out: New Zealand led in Zero Trust influence at 88%, while Mexico lagged with 63%.

30%

of global respondents said they have a formal strategy and have actively embraced a Zero Trust policy.

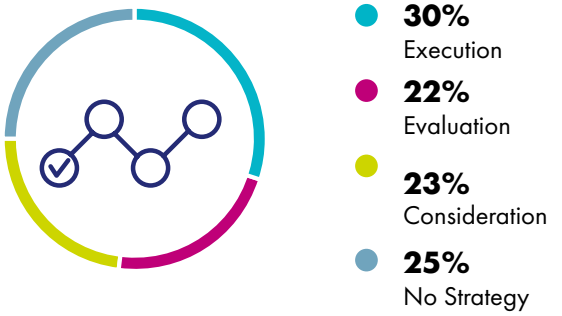
49%

of respondents said they are either in pilot or expecting to deploy Zero Trust within 24 months.

FIGURE 8

Zero Trust journey

Q: Where are you on your Zero Trust journey?



Source: 451 Research's 2021 Access Management custom survey

These results are a clear indication that organizations are expecting Zero Trust approaches in access to play a key role in their strategies. As the previous data has shown, organizations need to ensure that they're building a solid foundation on which to base their Zero Trust aspirations. Modern authentication technologies and granular, policy-based access mechanisms are required to achieve the greater control that Zero Trust promises.

> **"Modern authentication technologies and granular, policy-based access mechanisms are required to achieve the greater control that Zero Trust promises."**

51%

agreed that a cloud-provider-agnostic approach is best.

19%

Almost a fifth (19%) of respondents said they believe getting to MFA integration is challenging.

Access Management Approaches

As organizations cope with the various pressures on their security infrastructure, they're facing challenges in managing their existing access management environments. The survey looked at the nature of those challenges and attitudes toward addressing them.

The leading challenge that respondents identified was the ability to span cloud-based and on-premises services. Organizations are struggling to deal with the extension of their infrastructure with greater use of cloud. As we mentioned above, the number of access management tools many organizations have in place may be contributing to this challenge. Organizations that have to use separate access management systems for different types of infrastructure likely face greater operational complexity. The kind of organic growth that infrastructure often undergoes can lead to project- and resource-specific tools that aren't coordinated.

Cost concerns are always on the minds of information security professionals, and the need for rapid expansion in remote access capacity caused by the pandemic could be adding to this. It was the second highest concern and ranked ahead of challenges with cloud-based services. Almost a fifth (19%) of respondents said they believe getting to MFA integration is challenging, an echo of the importance that MFA has had in respondents' other answers.

Respondents have strong opinions about how organizations should manage their access environments. These are the precepts that we can expect will guide them as they make investments in improvements. Nearly three-fifths (59%) of respondents said they believe their organizations must maintain control over their access security. In a time where many capabilities are being taken on by service providers, this is an indication that organizations see access as a critical point of control. The need for effective access management in hybrid and multicloud situations led more than half (51%) to agree that a cloud-provider-agnostic approach is best. Thoughts on access management's role in Zero Trust were less definitive, which echoes other responses that seem to be driven by perimeter-based thinking, approaches that are counter to the goals of Zero Trust strategies. While 45% agreed that access management plays a key role, only 17% disagreed, leaving 37% undecided. That may be an indication that there's a lack of complete understanding about the need for modern authentication and granular, policy-based access management as a foundation for Zero Trust initiatives. Those access management controls are what make Zero Trust possible.

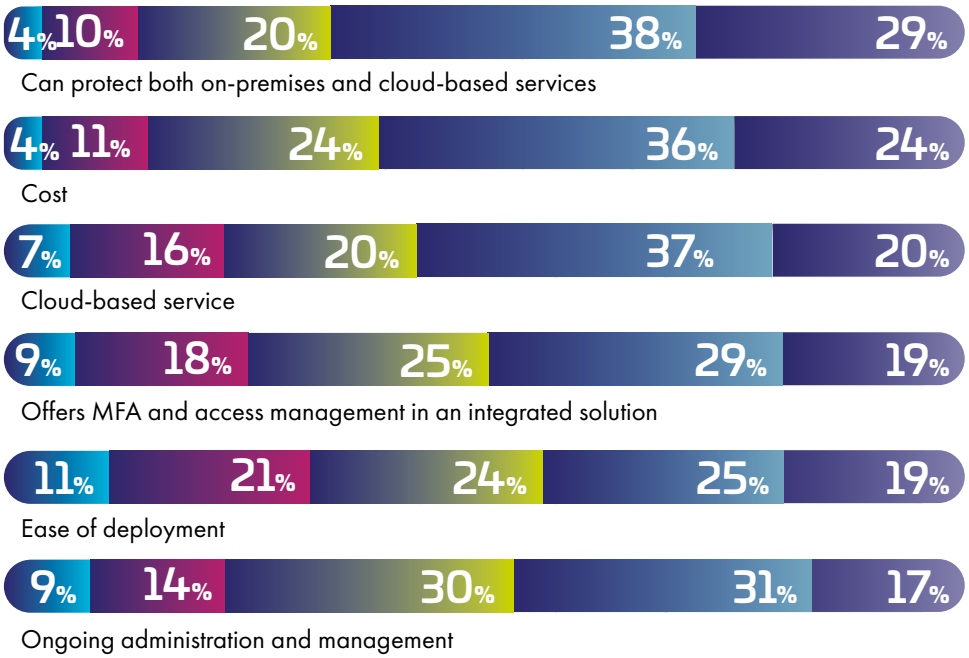
A majority of respondents said they prefer an agnostic access security offering over one hosted by a cloud provider. This is another area where there was a large undecided population (35%). This may also be an indication of a developing level of understanding of the complexities of integrating on-premises and cloud-based capabilities.

FIGURE 9

Access Management Challenges

Q: What are the challenges you have faced with access management solutions?

- **Not very challenging**
- **2**
- **3**
- **4**
- **5 Very challenging**



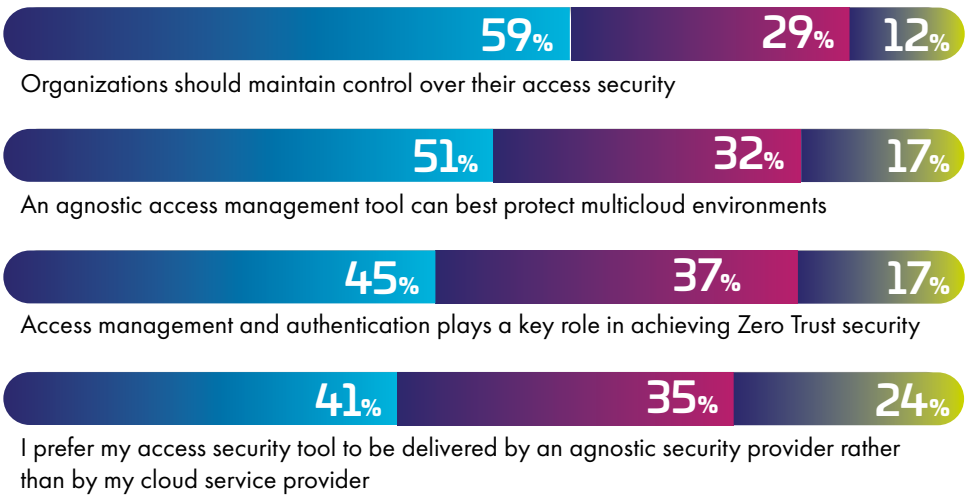
Source: 451 Research's 2021 Access Management custom survey

FIGURE 10

Attitudes Regarding Access Management

Q: To what extent do you agree with the following statements?

- **Agree**
- **Neutral**
- **Disagree**



Source: 451 Research's 2021 Access Management custom survey

Access management is undergoing significant change as security strategies address new business imperatives and work to keep their organizations competitive in challenging and uncertain times.

Moving Ahead

The results of the survey can serve as an indicator of useful paths for organizations to follow as they look to their security journey. One of the overarching takeaways that was driven by lessons learned from the pandemic is that security strategists need to increase the agility of their security controls. Infrastructure will become more hybrid, and security teams must have the capabilities to address this more complex environment efficiently. Controls and security management will have to extend to cloud in ways that keep each cloud environment from being an isolated operational realm.

The native controls and protections available in cloud environments address a set of necessary capabilities, but they're often insufficient to deliver effective protections for sensitive data and workloads, especially when it comes to compliance with regulations such as GDPR and the implications of the Schrems II ruling. Organizations need to increase their use of encryption and ensure they take full advantage of encryption's benefits by controlling the secrets that protect their data through BYOK, HYOK or BYOE approaches.

Organizations also need to make internal changes to ensure that personnel at all levels understand the security challenges and to properly align investment priorities. Senior executives need to ensure that they obtain a more complete understanding of the levels of risk and attack activity that their front-line staff are experiencing. They can't make effective strategy and security investment decisions when perspectives across the organization aren't aligned. This is especially true as regulatory changes and the potential for nation state collateral damage force them to move ever faster.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/access-management-index