Global Edition

THALES
Building a future we can all trust

2022 Thales Access Management Index

Building Zero Trust with Modern Access Security

#2022AccessManagementIndex

cpl.thalesgroup.com

Contents

Introduction

The impact of remote work throughout the COVID-19 pandemic has caused both security professionals and the average technology user to be more aware of security concerns and how to address them. The 2022 Thales Access Management Index, based on data from a survey of nearly 2,800 respondents in more than 15 countries across the globe, looks to identify the extent of that change, as well as the current state of access management and plans for access security across a range of industries. The insights in this report were gleaned from the survey data, and this report explores the impacts on identity and access management (IAM) security strategy and planning.

For brevity, we will define all forms of authentication stronger than a password as MFA for the remainder of this report.

Key Findings

- Overall, worldwide multi-factor authentication (MFA) deployments remained relatively unchanged, with pockets of strength and weakness.
- On the plus side, India, Singapore and the UAE revealed significant increases over the past year in terms of overall MFA adoption levels. Additionally, organizations have increased their use of MFA (those that involve using more than just a password), particularly for cloud and SaaS applications, but also for legacy, on-premises applications.
- On the negative side, the majority of firms still have less than 50% of employees using MFA methods and still rely on passwords to an alarming degree. The heaviest users of MFA, for example, remain remote and privileged employees.
- MFA is still the most widely deployed form of authentication technology (chosen by 56% of global respondents), ahead of the increasingly popular passwordless authentication (48%).
- Pandemic impacts have lowered concerns about remote working as work-from-home strategies have become more common. Virtual private networks (VPNs) continue to lead the way as the primary method for employees to access applications remotely. The planned use of zero-trust network access (ZTNA) and software-defined perimeter (SDP) fell slightly, though nearly half of respondents plan to keep their existing VPNs while adding new technology such as ZTNA.

Firms still have less than 50% of employees using MFA methods."

56%

of companies chose MFA as their authentication technology of choice over passwordless authentication (48%).

MFA Adoption a Mixed Bag, but India, Singapore and UAE Stand Out

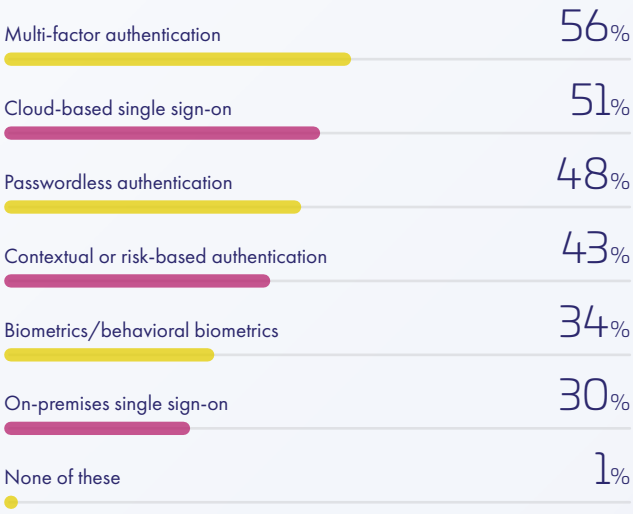
56% of global respondents have adopted two-factor authentication in their organizations.

Globally, the use of multi-factor authentication (MFA) has remained essentially the same year-over-year, at 56% in 2022 (versus 55% last year), with pockets of strength offset by areas for improvement. In terms of highlights, Singapore, India and the United Arab Emirates (UAE) all saw notable increases in MFA adoption in 2022. India obtained both the highest percentage increase of MFA adoption and highest overall percentage of MFA usage, up 19 percentage points to 66% this year. Singapore saw a 17-percentage-point increase in adoption to 64%, while UAE saw a 10-percentage-point increase, to 65%.

In comparison with last year's report, however, MFA adoption in the UK and USA experienced reductions of 14 percentage points and five percentage points, respectively, to 50% and 57%. While these countries are still above average in their overall MFA adoption, the results run counter to recent positive momentum for MFA adoption, and thus should perhaps be viewed in the broader context of ongoing challenges with MFA adoption relative to other security technologies. Another plausible explanation is simply that some organizations have reevaluated and reconsidered security spending plans as employees return to the office and the initial surge from work-from-home mandates subsides.

Authentication Technologies in Use

WHICH OF THE FOLLOWING AUTHENTICATION TECHNOLOGIES HAS YOUR ORGANIZATION DEPLOYED IN PRODUCTION?



Source: 451 Research's 2022 Access Management custom survey

MFA Still Leads Other Forms of Authentication

MFA remains the most widely deployed form of IAM technology (chosen by 56% of global respondents), followed by cloud-based single sign-on (SSO) at 51%. Passwordless authentication, which attempts to reduce or eliminate the use of passwords or other shared secrets to help improve both the user experience and security, is gaining in popularity, and only trails MFA by eight percentage points at 48%. Biometric authentication, however, was chosen by just over one-third (34%) of respondents, despite considerable attention in the mainstream media in recent years.

Another positive sign is that more firms are using MFA for cloud and SaaS apps. More than a third (37%) of global respondents have 40% or more of their employees using MFA specifically for cloud and SaaS apps in 2022, a sharp increase from only 12% last year. Additionally, 21% of respondents reported having over 40% of employees using MFA for on-premises and legacy apps, which is also a notable jump from just 4% last year.

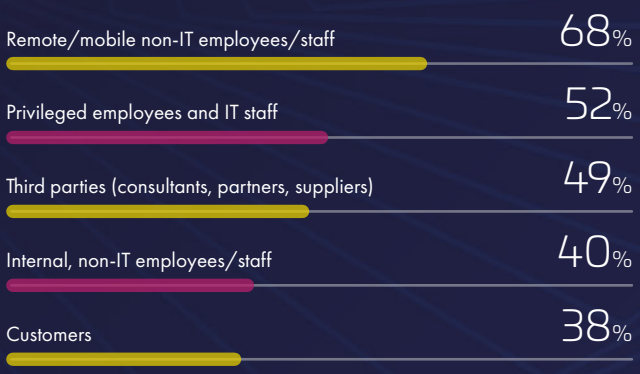
37% of respondents have more than 40% of their employees using MFA for cloud and SaaS apps."

MFA Still Mainly for Remote and Privileged Users

Remote access is still the main use case for MFA – in 2022, 68% of remote/mobile non-IT employees/staff used MFA (a slight dip from 71% last year), followed by privileged employees (52%, up from 48% in 2021) and third parties (consultants, partners, suppliers) at 49% (compared to 50% in 2021). In contrast, the majority of firms have less than half of their general employees using MFA, though deployments for internal employees and staff have also increased by six percentage points over the last year – to 40% – while MFA deployments for customers edged higher (38% vs. 36% in 2021).

User Groups With MFA Deployed

FOR WHICH USER GROUPS HAVE YOU DEPLOYED MFA?



Source: 451 Research's 2022 Access Management custom survey

The use of MFA for privileged employees and IT staff increased by 4% in 2022."

Firms Gaining Comfort with Remote Work

After two years of a global pandemic and a permanently altered remote work environment, changes in security have been both necessary and notable. Overall, the survey results suggest that firms remain concerned about the security risks of remote work, but those concerns seem to be less severe. At the same time, firms are also growing more confident in the ability of access management systems to manage those risks. Most respondents fell into the category of either "very" or "somewhat" concerned, which, combined, constitute 79% of the response base, down slightly from 82% in 2021. However, only 31% reported having "very high" concerns about the security risks and threats of remote work in 2022, down from 39% in 2021, while those who said they were "somewhat concerned" – the most popular response – increased from 43% to 48% in 2022.

Level of Concern About Remote Work Risks

HOW CONCERNED ARE YOU ABOUT THE SECURITY RISKS/THREATS OF EMPLOYEES WORKING REMOTELY?

- Very concerned 31%
- Somewhat concerned 48%
- Somewhat unconcerned 18%
- Not at all concerned 3%

Source: 451 Research's 2022 Access Management custom survey

Firms are also expressing increased confidence in their ability to handle the security challenges that remote work presents. More than 8 in 10 respondents (84%) expressed some degree of confidence in current access security systems to enable remote work securely and easily, and 60% were either "highly" or "significantly" confident.

Level of Confidence in Access Security Solutions

HOW CONFIDENT ARE YOU THAT YOUR CURRENT ACCESS SECURITY SOLUTIONS CAN EFFECTIVELY ENABLE EMPLOYEES TO WORK REMOTELY IN A SECURE AND EASY MANNER?

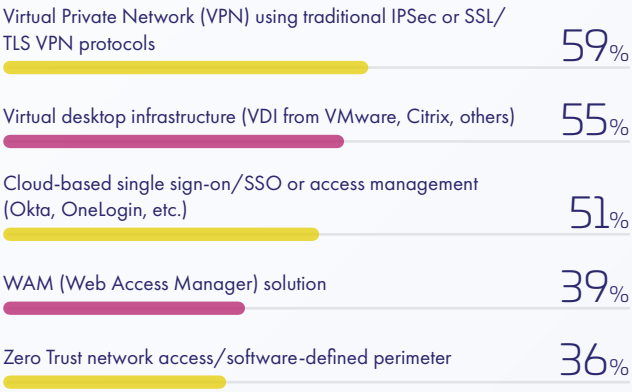
- Highly confident 26%
- Significantly confident 34%
- Slightly confident 24%
- Not at all confident 16%

Source: 451 Research's 2022 Access Management custom survey

VPNs Still the Leading Remote Access Technology

Means of Remote Application Access

HOW DO EMPLOYEES CURRENTLY ACCESS THEIR APPLICATIONS REMOTELY?



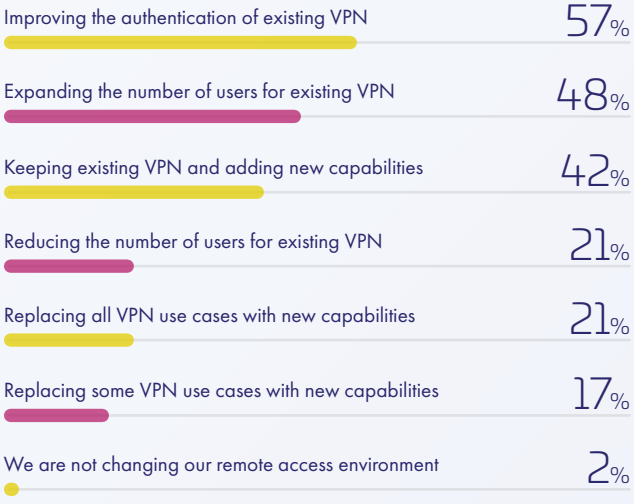
Source: 451 Research's 2022 Access Management custom survey

Overall, attitudes toward remote working technologies were relatively unchanged from the previous year. VPNs continue to lead the way: This year, 59% of global respondents selected VPNs as the primary method for employees accessing applications remotely, which is about the same as 2021 (60%). It is worth noting that all surveyed regions selected VPN as the number one response. Virtual desktop infrastructure (VDI), from providers such as VMware and Citrix, took second place (55%), followed by cloud-based SSO (51%). Furthermore, just 21% plan to reduce the number of VPN users, while more than twice as many (48%) have plans to expand the number of users for existing VPNs. On an encouraging note, more than half (57%) of respondents plan to strengthen the authentication methods of existing VPN deployments.

Planned usage of zero-trust network access and software-defined perimeter fell slightly, though almost half of respondents said they are planning to keep their existing VPNs while adding new technology such as ZTNA. It is also worth pointing out that the current usage of ZTNA/SDP to access remote applications fell from 53% in 2021 to 36% in 2022. That said, there is a considerable amount of confusion in the market regarding the precise definitions of zero trust, ZTNA, secure access service edge (SASE) and SDP, which could play a role in the divergent results. It is also very early in the maturity cycle of ZTNA, and most firms are still grappling with how to deploy ZTNA alongside existing investments such as VPNs and VDI. It is also important to keep in mind that VPNs, ZTNA and SDP are not necessarily mutually exclusive and can coexist, particularly for specific use cases. To illustrate, 42% of respondents plan to keep their existing VPNs but still plan to add new technology such as ZTNA, SASE or SDP.

Plans for the Remote Environment

WHICH OF THE FOLLOWING ARE YOU PLANNING ON DOING WITH YOUR REMOTE ACCESS ENVIRONMENT?



Source: 451 Research's 2022 Access Management custom survey

Access Management – Critical for Overall Security, Zero Trust

Controlling access to resources, systems and privileges is an increasingly important aspect of securing any environment and protecting it against both internal and external threats. Tools to manage access privileges and rights are, therefore, increasingly seen as an essential piece of securing infrastructure and considered a critical cybersecurity capability by the National Institute of Standards and Technology (NIST). Not surprisingly, then, access management tools were the third most chosen option in terms of security budget priorities, with 25% of respondents identifying it as one of their top three technology spends. Only network security (29%) and container security (26%) ranked higher. However, deploying access management solutions presents several challenges, including the ability to protect both on-premises and cloud-based services, cost and ease of deployment.

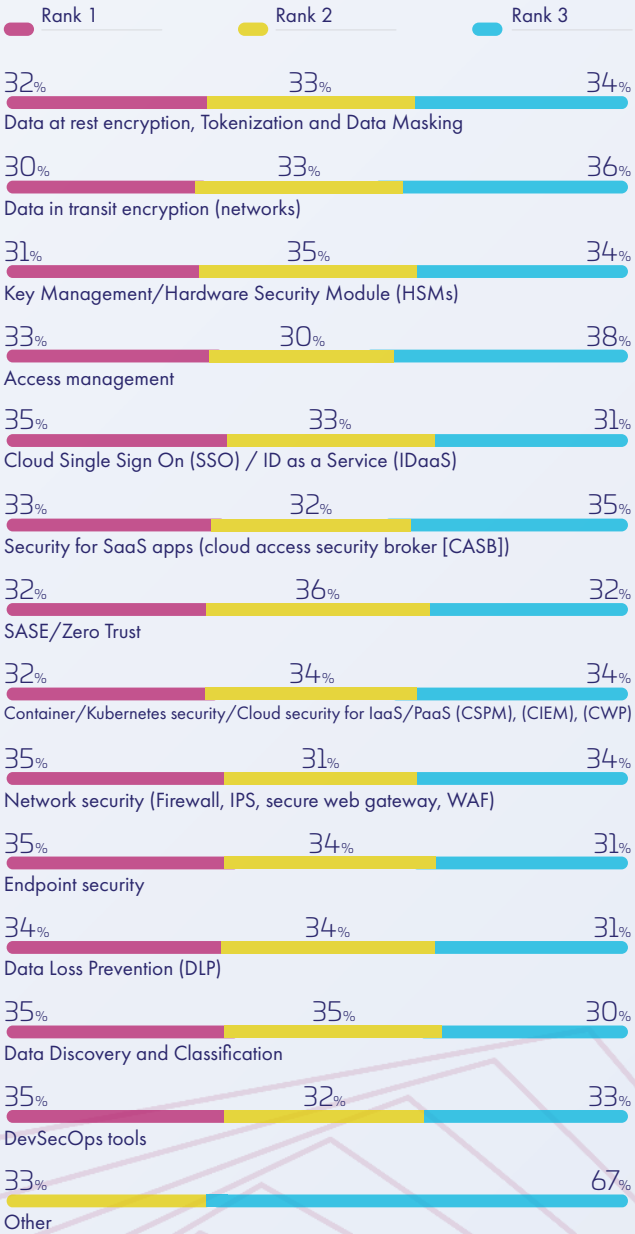
59%

of global respondents selected VPNs as the primary method for employees accessing applications remotely.

More than half (57%) of respondents plan to improve the means of authentication of existing VPNs."

Spending on Security Technologies

WHICH OF THE FOLLOWING SECURITY TECHNOLOGIES ARE YOU SPENDING ON TODAY?

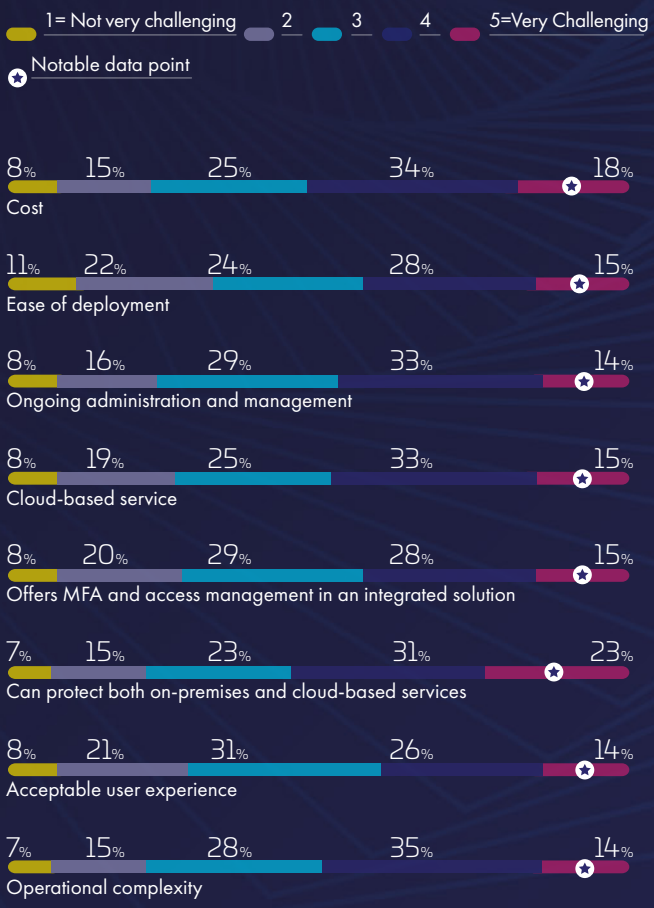


Source: 451 Research's 2022 Access Management custom survey

Access Management – Critical for Overall Security, Zero Trust (continued)

Challenges With Access Management

WHAT ARE THE CHALLENGES YOU HAVE FACED WITH YOUR ACCESS MANAGEMENT SOLUTION?



Source: 451 Research's 2022 Access Management custom survey

Access Management – Critical for Overall Security, Zero Trust (continued)

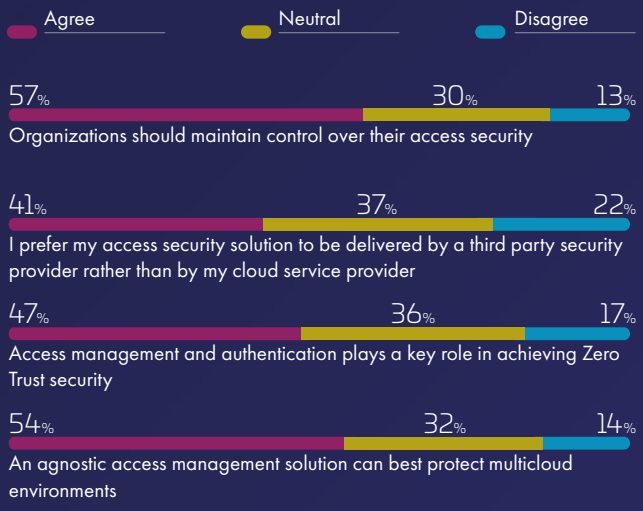
Access management and authentication also play a key role in achieving zero-trust security objectives, which rely critically on identity. Just under half (47%) of respondents support this contention, though there is still work to be done in terms of educating organizations about the importance of effective access controls overall.

To do so, access management solutions need to be capable of protecting both on-premises and cloud-based environments, which remains the most commonly cited challenge for access management systems to address, similar to last year. It is also worth noting that more than two in five respondents (41%) maintain separate access management systems for their on-premises and cloud environments, which can lead to added complexity and operational overhead.

Moreover, access management systems need to be capable of addressing hybrid and multicloud environments. To do so, most respondents (54%) indicated that agnostic access management solutions can best protect multicloud environments, up slightly from 51% in 2021, as opposed to offerings from the cloud providers themselves. Additionally, more than half (57%) of respondents believe their organizations should maintain control over their own access security, while 41% of respondents prefer their access security solution to be delivered by a third-party security provider rather than by a cloud service provider.

Views on Management of Access Security

TO WHAT EXTENT DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENT?



Source: 451 Research's 2022 Access Management custom survey

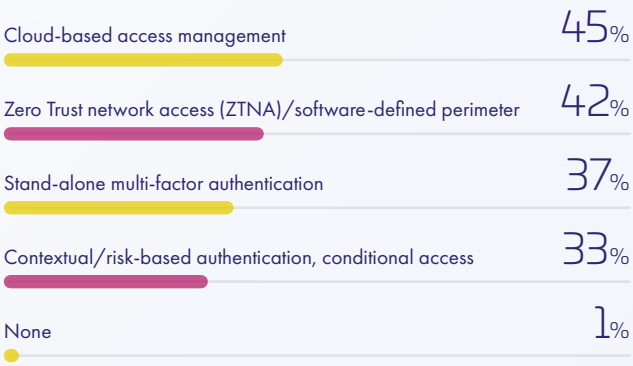
COVID-19 Driving Interest in Access Management, ZTNA and MFA

It is safe to say the pandemic has forever altered the way the world interacts with technology. Remote work is more standard, interconnectivity has become easier, and digitization is more prevalent. Yet such a technologically oriented reality is trailed with legitimate risks and threats – both internal and external – in familiar forms, but with newfound strength. Enterprises around the globe were quick to learn of risks and attacks, such as ransomware and distributed denial-of-service (DDoS) attacks, and adjust their defensive positions, strategies and budgets accordingly.

The survey inquired about direct impacts that the pandemic and remote work had on deployment plans for new access technologies. Responses revealed a six-percentage-point global increase in plans to deploy stand-alone MFA, up from 31% in 2021. The pandemic also impacted plans to deploy cloud-based access management, selected by 45% of respondents worldwide in 2022. These two increases illustrate respondents' growing awareness that threats come from all angles, and that proper authentication and management of access and privileges is necessary for an adequate security foundation. Last year, ZTNA/SDP was the top choice, selected by 44% of respondents. In 2022, ZTNA was the second choice at 42%.

Access Technology Deployment Plans Driven by Pandemic and Remote Work

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 2022 Access Management custom survey

"The top three areas for increased security investment due to COVID-19 include access management, ZTNA and MFA."

Over Half of Ransomware Victims Have Internal Processes Disrupted

Although last year's survey did not address ransomware, almost a quarter (21%) of respondents have experienced a ransomware attack. Of those affected, 55% had internal processes disrupted and 12% had a significant impact on their external/customer-facing operations. Nearly a quarter (23%) of respondents view financial loss as the greatest potential impact from a ransomware attack, closely followed by lost productivity (19%) and cost of recovery (18%). Concerns further down the list include disclosure of sensitive information through exfiltration (16%), reputation damage (11%), loss of customers (7%) and long-term business impacts (4%).

When asked about methods of recovery (or planned recovery in case of an attack), the results were fairly evenly split – Just over half chose internal resources for remediation, while slightly under half chose external resources. In addition, 48% reported having a formal ransomware plan prepared, while nearly a quarter (22%) would actually pay the ransom – though that warrants no guarantee of data being returned to the rightful owner. Only 28% of respondents indicated that they would consult law enforcement.

When asked whether concerns about ransomware have prompted investment in specific security tools or services, only 28% indicated they would tack on additional budget specifically for ransomware tools; 41% reported no change in spending plans, while 29% of respondents indicated they would alter spending but not increase their budgets.

Less than half (48%) of respondents reported having a formal ransomware plan prepared."

21%

of respondents have experienced a ransomware attack.

Moving Ahead

While the COVID-19 pandemic has helped to make remote work and work-from-anywhere a more permanent part of the security landscape, it has also introduced new security risks and challenges. However, growing familiarity with remote work has ultimately broadened enterprise-level awareness of daily business security risks and has strengthened both confidence and ability in security teams and products to handle those risks and threats properly.

Just as the threat landscape has evolved, the tools and methods to navigate that landscape have, too. However, even with innovative tools and boosted confidence levels, security plans and approaches still need to adapt to the ever-changing threat environment. A greater shift toward a zero-trust model would place access management in a central role in corporate security strategies, with a related reliance on MFA as a critical supporting enabler.

Ransomware awareness has grown significantly, and though nearly a quarter of respondents consider financial loss the greatest impact of an attack, more enterprises need to adjust their spending plans and response plans for ransomware attacks.

Growing familiarity with remote work has strengthened both confidence and ability of security teams to handle those risks properly."

About This Study

As organizations step beyond the urgent actions of the last two years, they are grappling with securing the more complex environments in which they now operate. The global edition of the 2022 Thales Access Management Index looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues including access management and access security, multi-factor authentication, zero-trust network access, security spending plans, remote work and VPNs, and ransomware. The 2022 Thales Access Management Study is based on data from a survey of nearly 2,800 security professionals and executive leaders in more than 15 countries across the globe. This research was conducted as an observational study and makes no causal claims.

Industry Sector

Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168

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