Global Edition

THALES
Building a future we can all trust

2022 Thales Data Threat Report

Navigating Data Security in an Era of Hybrid Work, Ransomware and Accelerated Cloud Transformation

#2022DataThreatReport

cpl.thalesgroup.com

Introduction

As the pandemic continues to affect both business and personal lives, expectations of a 'return' to pre-pandemic conditions have faded from most plans. Underlying trends that have always driven information security, such as new technologies, greater compliance mandates and more severe security incidents, continue to be significant change agents. The 2022 Thales Data Threat Report, based on data from a survey of almost 2,800 respondents from 17 countries across the globe, illustrates these trends and changes. This report examines the implications of the survey responses and explores their meaning to security strategies and how organizations should plan for the year ahead.

451 Research

S&P Global
Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

56%

of global respondents ranked malware as the leading source of security attacks.

21%

of all respondents said they had experienced a ransomware attack.

Contents

COVID-19 (Continues) to Change Everything

The COVID-19 pandemic, with its waves of infection from variants, is shifting mindsets from taking urgent action to handling a chronic condition. The impacts continue to cause lasting changes within enterprises with ripple effects throughout the security community. The durable shift to remote work continues to alter mindsets – enterprises are realizing that what seemed to be a singular event may extend indefinitely. Despite another full year of remote work and newer technology adoption, 79% of respondents indicated they are still 'somewhat' or 'very concerned' about the security risks and threats that a greatly increased remote workforce poses. 40% said they are not confident that their current security systems could effectively secure remote work.

New technologies and increased cloud consumption continued to grow at the same rapid rates as last year. In the 2021 report, 16% of respondents used more than 50 software-as-a-service (SaaS) apps. In the 2022 report, 34% of respondents said they used more than 50 SaaS apps and more than 16% said they used more than 100 SaaS apps. Some progress has been made despite market disruptions. Last year, only 17% of respondents said that more than 50% of their sensitive cloud data was protected with encryption. This year, 22% said that more than 60% of their sensitive cloud data is encrypted. The financial services sector is also a bright spot for cloud data protection and encryption; 19% of financial enterprise respondents said that more than 80% of their sensitive cloud data is encrypted. However, there remains work to be done in data identification, classification and protection in the context of the shifting threat and risk landscape.

Respondents agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than in on-premises networks within their organization."

79%

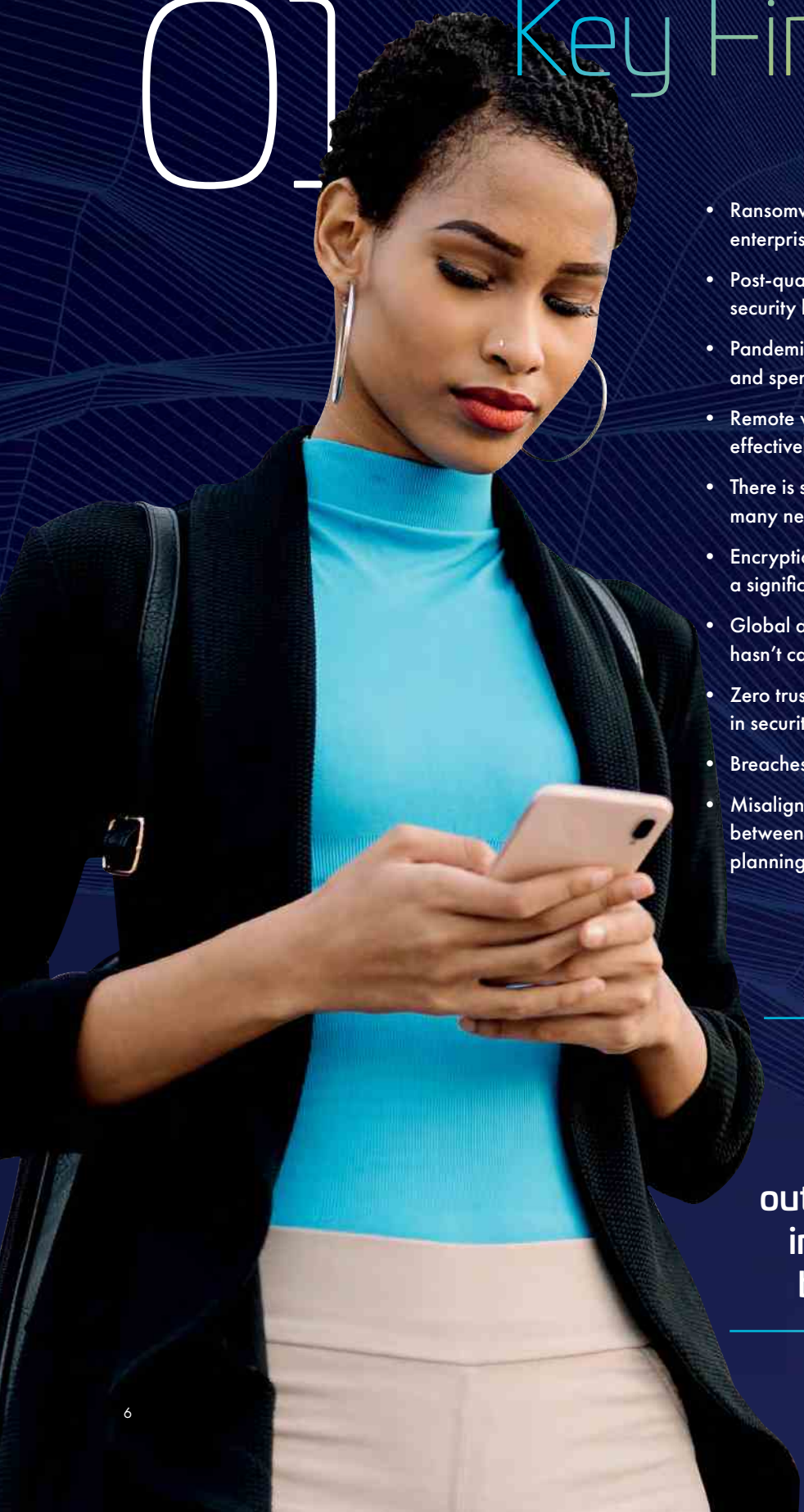
of businesses remain concerned about the security risks of an increasingly remote workforce.

22%

of respondents disclosed that more than 60% of their sensitive data has been encrypted.

"The high percentage of recent breaches could be an indication that organizations face challenges meeting improved attacker techniques."

01 Key Findings



- Ransomware has changed breach economics; enterprises must refine their responses.
- Post-quantum security should further accelerate data security hygiene.
- Pandemic pressures are impacting security approaches and spending.
- Remote work is a risk that needs to be managed more effectively.
- There is significant momentum in cloud migration, but many necessary controls are lagging.
- Encryption use to protect sensitive data in cloud is low – a significant risk.
- Global awareness of changing risks is high, but this hasn't catalyzed organizations to address them.
- Zero trust architectures need to show more improvement in security outcomes.
- Breaches and their impacts weigh on security planning.
- Misalignment in understanding security impacts between management and practitioners could affect planning and budgeting.

> **There is a correlation between investment in compliance and breach outcomes. It seems efforts to improve compliance lead to better security outcomes."**

Small Improvements, Increasing Risks and Changing Security Mindsets

Despite the general security concerns regarding remote work, survey results show slight improvements in the security posture of organizations. Implementation of security technologies such as encryption and multi-factor authentication (MFA) have slightly increased but have not yet reached saturation levels such that the majority of applications and data are fully protected. Last year, we reported that 83% of respondents had less than 50% of their sensitive cloud data encrypted. This year, there was a slight improvement to 78% of respondents having less than 60% of their sensitive data encrypted. Other controls like MFA adoption remained flat.

Heading into 2022, there have been no shortage of vulnerabilities and threats severely affecting enterprises. 'Hafnium,' Conti RaaS and Log4J highlight the increased risk landscape as workers remain distributed and their workloads further dispersed to multiple clouds and SaaS solutions. The attack surface, asset management and supply chain challenges can only increase this year.

Encouragingly, our research does reflect changing and improving data security mindsets. Last year, we reported disparities in the perception of attack frequency and severity among individual contributors, mid-level managers and senior leaders. This year, the perceptions were much more unified. For example, 43% of senior leaders, 46% of mid-level managers and 45% of individual practitioners reported an increase in attacks from the prior year. Furthermore, enterprises' confidence in their security capabilities remained relatively high. 79% of all respondents said they would entrust their personal data to their organization. This confidence remained high among senior leaders (72%) and individual practitioners (71%). Despite talent and personnel shortages in regions such as North America, optimism was consistently high. The 'can do' attitude was a refreshing vote of confidence considering the increasing volume of attacks faced by practitioners.

The report explores the results in more detail and looks at the impacts on organizations as they navigate the complex security environment that they find themselves in today.

43%

of senior leaders reported an increase in attacks from the prior year.

28%

of senior leaders said they would not entrust their personal data to their organization.

Security Threats

Breaches are a trailing indicator of security effectiveness. The research also examined forward-looking metrics, including perceptions about security threats. We asked the panel to identify levels of attack activity and understanding about attack risks. Almost half (45%) of respondents reported seeing an increase in the volume, severity and/or scope of cyberattacks in the past 12 months. These perceptions were consistent across all geographies.

To gauge overall risk levels, enterprises need to better understand the locations and classes of data. In 2022, only 56% of respondents were very confident or had complete knowledge of where their data was being stored, down from 64% in 2021.

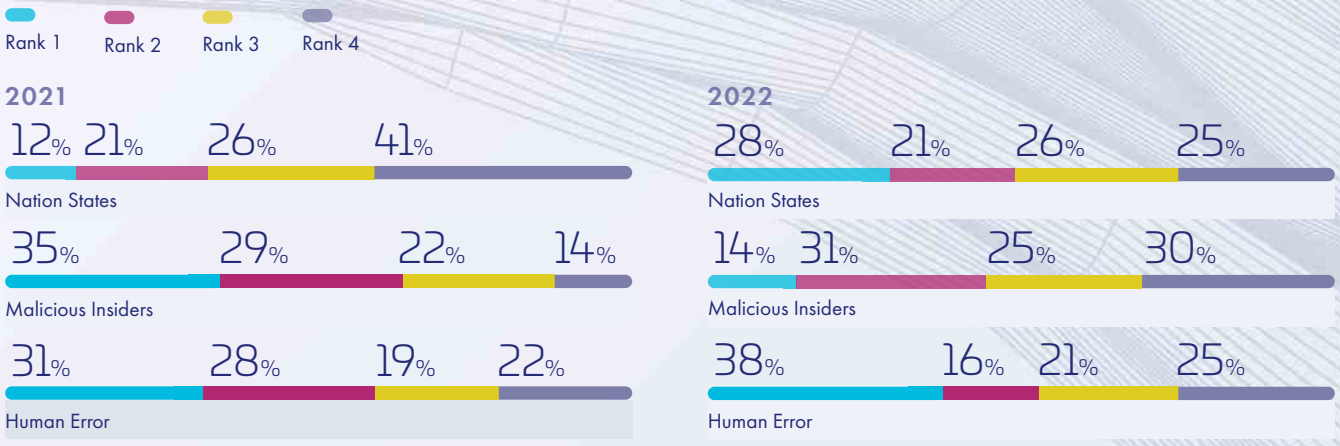
Only 25% of all respondents said they could classify all their data and 53% said they could classify at least half of their data in 2022, compared to 2021, when 31% of respondents claimed to be able to classify all data and 54% said they can classify at least 50% of the data. As other parts of this report show, the dynamic nature and growth of the cloud only adds a challenge for organizations to understand their data's risks and sensitivities.

We asked respondents reporting an increase in cyberattacks to identify the type of attack in which they'd seen the greatest increase in activity, and 56% of global respondents ranked malware as the leading source of security attacks. Ransomware ranked second (53%) and phishing/whaling rounded out the top three (40%). Last year, respondents chose malware at 54%, ransomware at 48% and phishing/whaling at 40%.

Looking forward, we asked the panel to rank their expectations for the greatest risks to their environments from a set of choices. This year, 29% of respondents ranked 'accidental human error' as the top threat, with 78% of respondents ranking accidental or human error in their top four threats. 19% of respondents cited attackers with geopolitical goals (i.e., 'nation-state actors') as the top threat, followed by 17% who cited external attackers with financial motivations. Curiously, only 9% of respondents chose malicious insiders with financial motivations as the top threat, with 62% of all respondents ranking this threat in their top four. Last year, 35% of respondents identified malicious insiders as the top threat.

Prioritization and Perceptions of Greatest Threats

WHICH TYPES OF THREATS DO YOU SEE AS THE GREATEST?



Source: 451 Research's 2021 and 2022 Data Threat custom surveys

At the time last year's study was published, the attribution of the SolarWinds breach to state-sponsored attackers was not completely known. Curiously, respondents have not given more importance to these serious attacks, even with the greater impact of nation-state actors pursuing intellectual property and the collateral damage to those who were not the primary target.

One interesting aspect of this year's data is the similarity in perceptions of attack rates by organizational role. In last year's study, 56% of practitioners reported an increase in attacks, but only 46% of managers and 40% of senior managers reported an increase. In this year's study, practitioners, managers and senior managers were much more closely aligned, with 46%, 46% and 43%, respectively, reporting an increase in attacks.

The investigation also asked respondents to identify what they felt were the biggest targets for cyberattacks. Last year, perhaps in response to the SolarWinds breach and the general topic of software supply chain security, 38% of respondents ranked third-party networks as the high-priority target. Curiously, this year, only 25% of respondents prioritized third-party networks. This year, cloud storage (33%), cloud databases (32%) and cloud-delivered hosted applications (28%) round out the priorities. The continued high ranking of cloud as a target illuminates the inconsistency between identifying the threat and mitigating it with solutions such as encryption and MFA. Intriguingly, respondents indicated they believe on-premises environments to be significantly less of a target: internal networks (23%), on-premises networks (23%) and on-premises databases (27%).

> **"There is a lack of maturity in cloud data security with limited use of encryption, perceived or experienced multicloud complexity and rapid growth of enterprise data."**

Ransomware Alters Breach Economics

Ransomware's severity, frequency and impact altered breach economics. Unlike other 'low and slow' data breaches that occur over days and months, ransomware immediately takes data captive and by definition demands action. About one fifth (21%) of all respondents said they had experienced a ransomware attack. Of those attacked, 43% were significantly impacted, and 3% of those impacted had been mentioned publicly in the media. Enterprises still prioritize based on harder and then softer ransomware costs. 23% of enterprises surveyed said that hard financial losses from penalties, fines and legal expenses have been or would be the greatest impact from ransomware. Lost productivity, recovery costs and breach notification were behind at 19%, 18% and 16%, respectively. Softer, long-term costs such as brand reputation and customer loss were further behind at 11% and 7%, respectively.

Respondents were also uncertain about their ransomware plans, with only 48% having a formal ransomware plan in place. 50% of companies with annual revenue greater than $1bn said they do not have a formal ransomware plan. Perhaps the reason so many enterprises do not have specific and formal ransomware plans is because ransomware response has so far been most closely associated with disaster recovery. According to 451 Research's Voice of The Enterprise: Storage, Data Management & Disaster Recovery – Advisory Report, 62% of enterprise respondents said they feel 'very confident' or 'extremely confident' in their organization's ability to recover from ransomware. Despite receiving notable attention, only 56% of healthcare companies and 44% of energy companies have formal ransomware response plans.

An alternative explanation is that the ransomware threat landscape changes quickly, which may make planning difficult to measure. In 2021, the industry saw the rise and demise of the Avaddon ransomware-as-a-service provider.

Curiously, 22% of respondents worldwide said they have paid or would pay a ransom for their data. Within the US, 24% of respondents said they have paid or would pay. Enterprises may not have a good understanding of the effects of all the parties involved, such as cyber insurance underwriters, incident response firms, government regulations and ransomware attribution. For example, the NotPetya ransomware was considered an 'Act of War' by NATO, causing some cyber insurance vendors not to pay claims. The US Department of Treasury Office of Foreign Assets Control (OFAC) issued guidance stating that facilitating ransomware payments to attackers on behalf of victims could risk violating OFAC regulations. Despite ransomware's additional impacts on data integrity and availability, the changing and unknown landscape may cause new plans to stall. 41% of all respondents said they have no plans to change security spending, even with greater ransomware impacts.

It is interesting that of the attacked respondents, 3% had media coverage. While it is easy to recall major incidents affecting some very large organizations, we found that most of the attention affected medium-sized enterprises with annual revenue of $500m-1.5bn. Perhaps it is because medium-sized companies can still be large enough to be regionally noteworthy yet small enough to be significantly affected.

50%

of companies with annual revenue greater than $1bn said they do not have a formal ransomware plan.

22%

of respondents worldwide said they have paid or would pay a ransom for their data.

Breaches and Their Impact

Arguably, the ultimate strength of an organization's security protection is preventing breaches. We saw some improvement, but there remains a lot of work to be done. This year, 52% identified a breach in their operational history, and 35% of those experienced a breach in the last 12 months, compared to 56% and 41%, respectively, last year. In absolute terms, 18% of all respondents have experienced a breach in the last 12 months. The high percentage of recent breaches could be an indication that organizations face challenges meeting improved attacker techniques.

This year's survey data allowed us to compare compliance audit success to breach history. While 43% of respondents failed a compliance audit, some regions significantly improved their audit success. For example, in the previous year's report, 59% of UK respondents reported a failed compliance audit within the previous 12 months. In this year's report, only 42% of UK respondents reported a compliance audit failure.

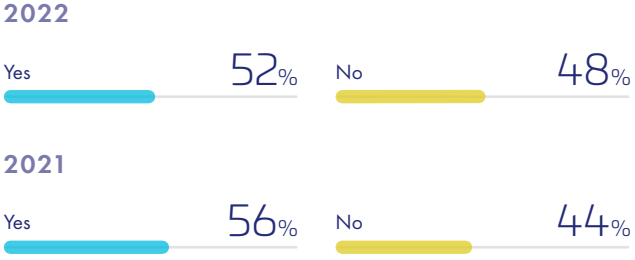
57% of respondents said that their companies have successfully passed their compliance audits. Of those that have passed, 40% have had a breach. Yet only 12% of companies that have passed compliance audits have experienced a breach in the last 12 months. There is a correlation between investment in compliance and breach outcomes. It seems efforts to improve compliance lead to better security outcomes.

Of note, 'safe harbors' for breach notification came down in 2022. In 2021, 46% of respondents said they had avoided a breach notification because underlying data was encrypted or tokenized. In 2022, only 40% of respondents avoided a breach notification because data was protected and covered by safe harbors. In general, there was also a slight decline in breach notifications, with 32% of respondents issuing a breach notification compared to 36% the prior year.

The use of cloud-based infrastructure exposes new risks as an organization's data footprint expands. The research also looked at breaches tied to cloud; 44% reported that they had experienced a breach or failed an audit in their cloud environments, a slight step back from the 40% of last year's respondents. The report found that there is a lack of maturity in cloud data security with limited use of encryption, perceived or experienced multicloud complexity and rapid growth of enterprise data.

Prevalence of Breaches at Organizations

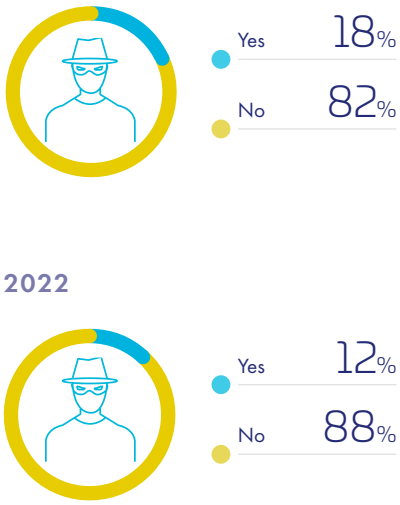
HAS YOUR ORGANIZATION EVER BEEN BREACHED?



Source: 451 Research's 2021 and 2022 Data Threat custom survey

Prevalence of Recent Breaches, Compliance Success

HAVE YOU EXPERIENCED A BREACH IN THE LAST 12 MONTHS?



Source: 451 Research's 2021 and 2022 Data Threat custom surveys

Avoiding Breach Notification Process Due to Encrypted Data

HAVE YOU EVER AVOIDED A BREACH NOTIFICATION PROCESS (E.G., ENCRYPTION SAFE HARBOR) BECAUSE THE STOLEN OR LEAKED DATA WAS ENCRYPTED OR TOKENIZED?

2022

Yes 40%

No 60%

2021

Yes 46%

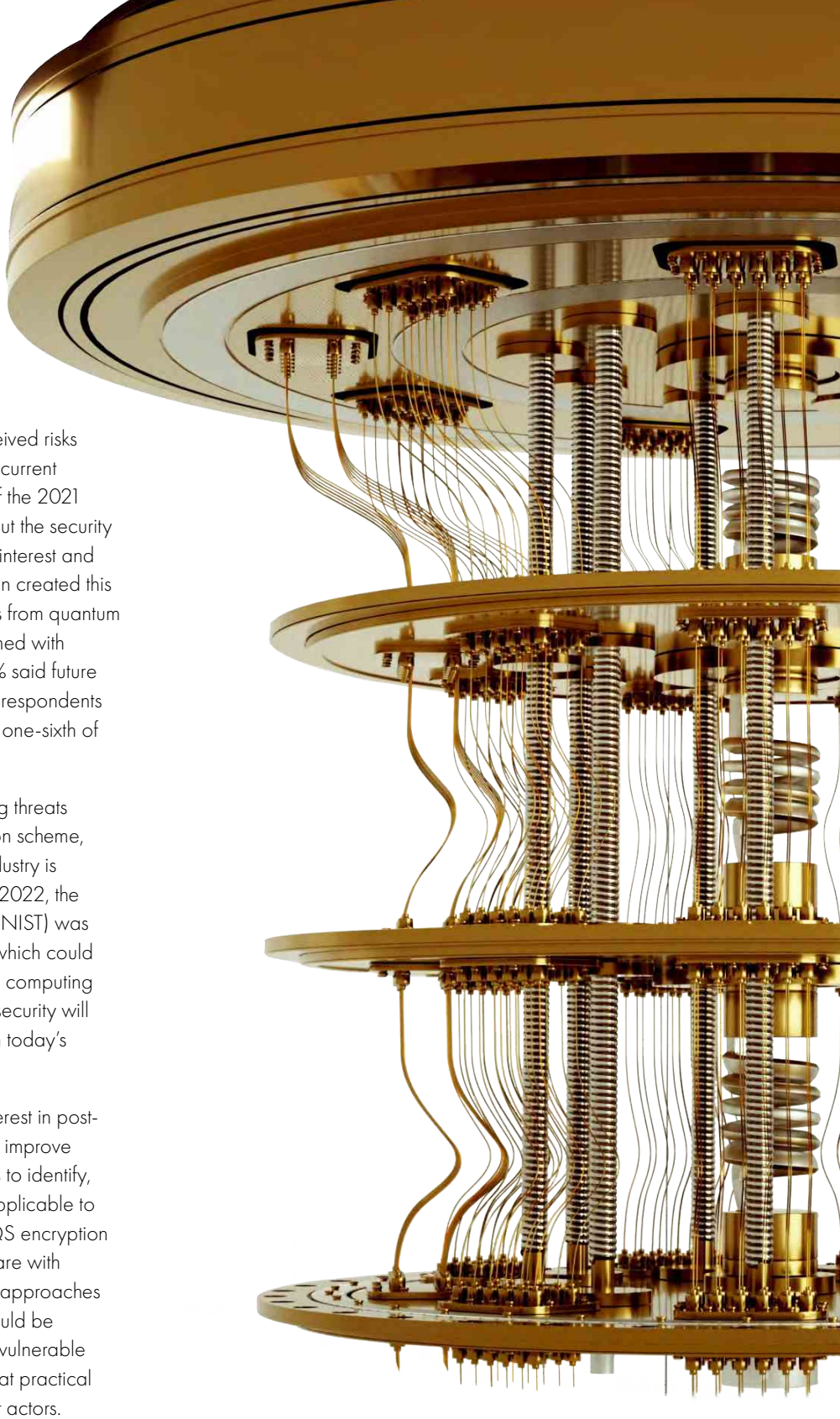
No 54%

Source: 451 Research's 2021 and 2022 Data Threat custom survey

40%

of respondents said they had avoided a breach notification because underlying data was encrypted or tokenized.

Quantum Computing



As part of last year's report, we studied the perceived risks of quantum computing and its potential to break current cryptographic approaches. Nearly half (47%) of the 2021 respondents said they were very concerned about the security threats of quantum computing. More education, interest and activity in post-quantum security (PQS) have been created this past year. When asked to identify security threats from quantum computing this year, 52% said they were concerned with 'tomorrow's decryption of today's data' and 58% said future 'network decryption.' Encouragingly, only 2% of respondents said they are not presently concerned. Last year, one-sixth of respondents were completely unconcerned.

Although there are no current quantum computing threats that can practically affect any classical encryption scheme, the industry proactiveness of government and industry is commendable. At the time of this writing in early 2022, the National Institute of Standards and Technology (NIST) was finalizing and vetting PQS encryption schemes, which could go into effect in 2023 or 2024. Though quantum computing is rapidly developing, post-quantum-computing security will almost certainly be completely implemented with today's classical computing infrastructure.

This level of awareness should be generating interest in post-quantum cryptographic techniques and efforts to improve crypto agility. The continued efforts of enterprises to identify, classify and protect sensitive data are strongly applicable to improving preparations and crypto agility. As PQS encryption schemes are validated, enterprises can still prepare with existing risk management frameworks. These are approaches to quantum computing risk that organizations should be considering today because data protected with vulnerable approaches could still be valuable by the time that practical quantum decryption becomes available to threat actors.

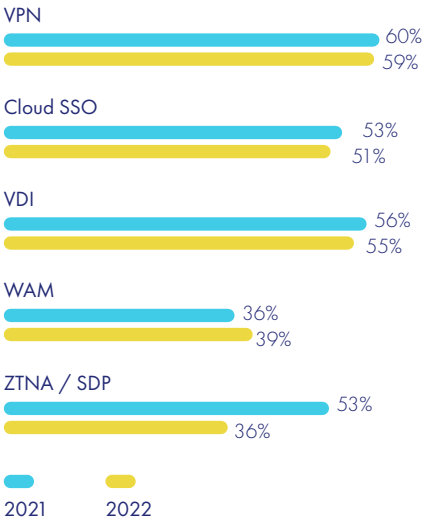
Continued Era of Remote Working

Remote work continues for many regions. Despite another year of adjustment, security professionals overall continue to be uneasy. 79% of respondents expressed some level of concern about the security risks/threats of employees working remotely (31% 'very concerned' and 48% 'concerned'). While overall numbers remain high, a sizable number of respondents work in industries that seem to be most impacted by the pandemic. When looking at respondents from retail, real estate, grocery, restaurant and sports-related industries, only 62% expressed concern about the security risks of remote working (25% 'very concerned' and 37% 'somewhat concerned'). Empirically, it is plausible that these industries have had to make the most severe changes, and that has impacted cultural beliefs about the security risks of remote work. Confidence in access control products significantly increased. Last year, 44% of respondents were not confident at some level that their access security solutions could enable effective and secure remote work. This year, that number dropped to 16%. Last year, only 34% were at least 'somewhat confident'; this year, 60% said they are 'highly' or 'significantly' confident.

We asked organizations about their remote access implementation, and traditional approaches continue to dominate. VPN continues to lead; 59% of respondents selected it as the primary method for remote access. Virtual desktop infrastructure (VDI from VMware, Citrix, others) was second (55%) and cloud-based single sign-on ranked third (51%). Traditional approaches still often lack the granularity of control needed to effectively manage the much more diverse work patterns that the wholesale shift to remote work has required. Most traditional approaches were designed for tactical use in special cases and may not have received the comprehensive reviews needed to secure a much larger user population. It was somewhat noteworthy that zero trust network access (ZTNA)/software-defined perimeter (SDP) solutions fell from 53% to 36%.

Current Remote Access Technologies

HOW DO EMPLOYEES CURRENTLY ACCESS THEIR APPLICATIONS REMOTELY?



Source: 451 Research's 2021 and 2022 Data Threat custom surveys

Organizations should expect to invest time and resources to better understand the models of work that they'll be moving toward in the longer term. A separate 451 Research study found that remote work is expected to continue at high levels, and that there's growing acceptance that employees can work effectively in a remote setting. That means that organizations will need security controls and remote access mechanisms that can be effective in the hybrid working environments that organizations have begun to embrace.

Cloud Momentum Continues

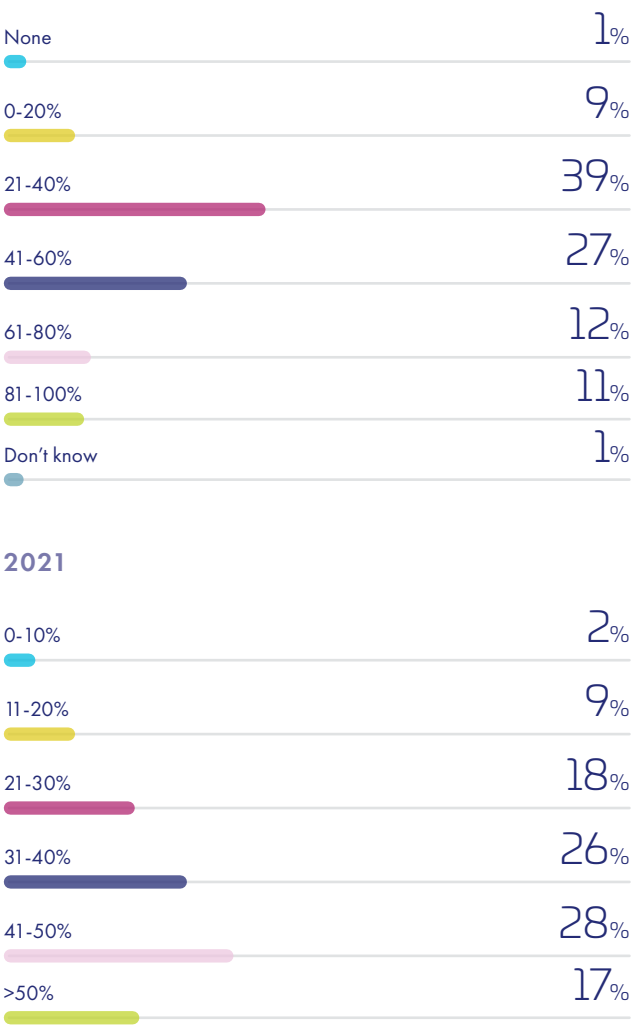
Respondents in the study are showing continued high use of cloud-based infrastructure, and this trend appears to be accelerating in the wake of the pandemic. Just under a third (30%) of respondents stated that 41-60% of their data is stored in external cloud, and 22% indicated more than 60% is stored there. While cloud storage consumption is not increasing relative to on-premises, in absolute terms, data growth remains the largest challenge, according to 451's Voice of the Enterprise (VotE): Storage, Data Management 2021 study. Although the absolute amount of cloud data has been growing significantly, the relative percentage of data encrypted in the cloud remains small. Only 22% of respondents said they have more than 60% of their sensitive data encrypted in the cloud. Survey results indicate that this could be explained by how cloud security policies are defined and implemented: not quite half (48%) have policies that are centrally defined, but technical standards and enforcement are left to individual cloud teams. This likely represents a troubling potential shift in the profile of cloud security stakeholders, making them more aligned with engineering-type concerns over traditional security concerns.

In this year's survey, we offered respondents more ranges to choose from, and we see some step-ups in improvement for sensitive cloud data encryption. Last year, only 17% of respondents stated that more than 50% of their sensitive data stored in cloud was encrypted. In the current year, 22% of respondents said that more than 60% of the sensitive cloud data is encrypted, and 50% of all respondents have at least 40% of their sensitive cloud data encrypted. There was some improvement in regulated industries; for example, 20% of financial services respondents said that 80-100% of cloud data is encrypted. This will certainly be an interesting trend to watch as more industries mature their protection programs.

While there is greater use of cloud infrastructure, 51% of respondents agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than in on-premises networks within their organization (22% strongly agreed and 29% agreed), up from 46% last year. Several factors could be driving this. Persistent skills gaps in both security and cloud infrastructure have strained security teams as they deal with increases in cloud use. In 451 Research's VotE: Information Security, Organizational Dynamics 2021 study, cloud platform expertise was the most-cited security skills gap. The adoption of different cloud service providers and other SaaS/IaaS offerings adds further complexity. Adapting traditional security strategies and teams to cloud operational models is also a complex endeavor.

Encrypted Sensitive Data

WHAT PERCENTAGE OF YOUR SENSITIVE DATA IN THE CLOUD IS ENCRYPTED?



Source: 451 Research's 2021 and 2022 Data Threat custom survey

Most Firms Are Using a Multicloud Strategy

The nature of cloud use is evolving alongside the increase in use. For this Data Threat Report, we explored the extent to which participants are using multiple cloud providers. Organizations are already using multiple providers for infrastructure as a service. This year, 48% of respondents said they employ AWS as their IaaS provider, followed by Microsoft Azure at 47%. Last year, 53% of respondents identified AWS as their IaaS provider, and 41% identified Microsoft Azure, with considerable overlap across Google Cloud, IBM Cloud, Oracle and Alibaba. SaaS usage has diversified significantly. Last year, 27% of respondents said they used at least 50 SaaS apps and 16% said 51-100 SaaS applications. In this year's survey, 34% use at least 50 SaaS apps and 17% use 100 or more SaaS apps. Perhaps because of greater attention to asset management and attack surface area, our survey found 4% of respondents reporting they use at least 500 SaaS apps.

Multicloud consumption raises concerns about the operational complexity of successfully managing both encryption and the corresponding keys across multiple providers, each with their own consoles and APIs. As identified above, almost half of respondents see cloud data protection as more complex to manage. Management complexity can be multiplied with each new cloud environment that's added because each brings its own technology implementations, operational models and security tools. Mastering all of them independently can be a huge resource commitment and, even if it is possible for an organization, can leave security gaps if management isn't well coordinated.

Zero Trust Goes Mainstream

Organizations are working to adapt their security strategies to address the changes in the threat models that they face. The study looked at aspects of zero trust and the ways in which it is being incorporated into operational security plans. When asked about their zero trust strategies, 30% of respondents said they have a formal strategy and have actively embraced a zero trust policy. 44% of respondents said they have no formal plans for their zero trust journey. For both the 30% of those that have formal plans and the 44% of those that don't have them, both have significant breach histories at 54% and 53%, respectively. However, looking further into breach history for the last 12 months shows a different story; for the 44% of respondents with no formal plans, 33% had a breach within the last 12 months. For the 30% of respondents with formal plans, 41% had a breach in the last 12 months. While zero trust promises much more granular, automated controls that are pertinent for dynamic remote access and software-defined perimeters, perhaps the complexity or other implementation challenges are impeding the lowering of breach occurrences and frequencies.

We also examined the impact of zero trust approaches on cloud; 34% of global respondents said zero trust security shapes cloud security strategy to a great extent. In comparison, 31% of US respondents reported the same; Germany was at 34%, Sweden at 36% and Japan at 35%. Mexico and Brazil led the way, with 48% of respondents from each saying that ZTNA shapes security strategy to a great extent. Among industry verticals, 34% of financial services respondents said zero trust security shapes cloud security strategy to a great extent, and technology industry respondents led with 40%.

There has also been a modest increase in the proportion of respondents reporting that zero trust is shaping cloud security strategy at least to some extent. Last year, 76% of those said that zero trust was influencing their cloud security strategy to 'some extent' or 'great extent.' This year, 81% of respondents said, 'some extent' or 'great extent.' It's quite a similar story with the industry breakdowns: last year, 83% of financial services and 77% of retail respondents said zero trust was influencing their cloud security strategy. This year, 82% of financial services respondents and 75% of retail said the same. Only 20% of respondents indicated that zero trust does not affect their cloud security strategy, down from 24% last year. Within the Global Access Management Index (AMI) Report, we'll dig deeper into some of the operational challenges with remote access, with some implication for ZTNA approaches.

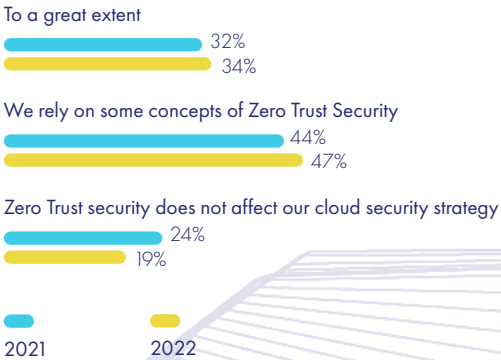
Zero Trust Status

WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?

Source: 451 Research's 2021 and 2022 Data Threat custom surveys

Importance of Zero Trust to Cloud Security Strategy

TO WHAT EXTENT DOES ZERO TRUST SECURITY SHAPE YOUR CLOUD SECURITY STRATEGY?



Source: 451 Research's 2021 and 2022 Data Threat custom surveys

Security Spending Misalignments

This year, our research looked at present and future security technology spending. We found a much greater diversity of technology spending priorities than last year by asking respondents to identify and rank the top three technologies by importance. Last year, the technology categories of data-loss prevention (DLP), encryption/key management, DevSecOps and cloud security all came in above 30%, with DLP the highest at 39% and cloud security at 35%. In 2022, no single category had more than 30%. Network security – firewalls, network access control, etc. – came in at 29%, and DLP fell all the way to 23%.

When asked what solutions would mitigate data loss, 31% of respondents prioritized network security (IPS, gateways, firewalls), and no other technology category scored above 30%, compared to last year, when 38% of respondents selected encryption as the most effective option for protecting sensitive data. In 2021, endpoint security was second (36%) and then tokenization (35%). The only observable alignment was with 'cloud security' categories such as cloud infrastructure entitlement management and cloud security posture management. 27% of respondents prioritized these kinds of cloud security tools to protect sensitive data from attack. The broad 'cloud security' toolset has the greatest future spending priority, with 26% of respondents. Other future spending categories that respondents prioritized in 2022 include key management at 25% and zero trust/secure access service edge/SDP at 23%.

31%

of respondents prioritized network security (IPS, gateways, firewalls), and no other technology category scored above 30%, compared to last year

Data Protection Management Strategies

Given the effectiveness of data encryption and tokenization for data protection, the foundation of data protection then rests on a combination of encryption effectiveness and key management strategies. As we've noted earlier, there is room to expand the use of encryption among the study respondents, but without better key management, usability and simplicity, the overall data security posture will not significantly improve. The study looked at the current state of respondents' environments and how they're managing this important area of security operations. Unsurprisingly, many indicated that they have deployed a number of encryption key management techniques. The organic growth of various approaches and the mashups created through corporate mergers and acquisitions can create a complex operational landscape that can pull together different approaches to key management and hardware security modules alongside homegrown systems, sophisticated vaults and cumbersome static documents or spreadsheets. Well over a third (41%) of respondents indicated that their organization currently deploys five to seven key management products, and 14% of respondents said that they employ eight or more key management products. The larger the number of systems in place, the greater the risk for error and the more work required to manage the combination successfully.

When we looked at tactics for data protection in cloud, encryption was the leading choice: 59% of respondents indicated that it is in place. Interestingly, 52% said that they are using key management. Perhaps this discrepancy results from encryption without key management, which would indicate a lack of maturity in data protection implementation and leaves unaddressed risks open. The discrepancy could also be based upon where the feature is implemented and how it is experienced. For example, AWS S3 encryption is a feature that largely abstracts key management, so it is possible for users to be unaware of a key manager. It's important for organizations to understand that simply turning on protections like encryption without managing all the aspects needed to ensure secure use will leave them open to abuse. Encryption needs to be applied with a knowledge of users, processes and applications to be effective against various threats. There needs to be partitioning of identity and techniques to address ransomware attacks or breaches caused by stolen privileged user credentials. Native cloud encryption offerings typically lack these protections. Bring your own encryption (BYOE) is an approach that can offer the controls and protections needed to mitigate these risks.

In looking at industry demographics, the financial services vertical reported high levels of encryption use, at 68%, but lower key management use, at 49%. Financial services respondents indicated greater use of tokenization at 53% and MFA at 50%. Healthcare also led with encryption at 61% and reported key management at 55%.

There is still a significant disconnect between interest and action. Last year, respondents identified encryption as the most important tool for data protection, yet 83% reported that at least half of their sensitive data in the cloud was unencrypted. Still, there are pockets of improvement in encryption implementation, with 20% of financial service customers encrypting 80-100% of their cloud data.

14%

of respondents said that they employ eight or more key management products.

> **Without better key management, usability and simplicity, the overall data security posture will not significantly improve."**

Cloud Data Protection

Given the high rate of multicloud consumption, the responses to survey questions about cloud data protection revealed interesting points. We asked about how respondents were encrypting data in IaaS offerings that they used. A relatively small number (17%) said they rely exclusively on the provider's offerings. The largest number (37%) indicated a blend of their own capabilities and 'mostly' the provider's. That could be an indication that there is a growing understanding of the importance and value that BYOE offers, as mentioned above. Another 13% said they use BYOE exclusively, and 21% use mostly their BYOE, meaning that over a third (43%) are putting BYOE to work today. Another driver of BYOE can be the need to centralize data access policies and encryption key management across multiple clouds and on-premises environments. This is only possible with BYOE.

While there is a positive trend in use, encryption levels are still below what's needed for comprehensive protection."

In looking at cloud key management, the results showed a similar, encouraging situation. While respondents favored the provider's key management systems as the leading situation today at 54%, they also reported strong use of external key management at 38% (23% mostly and 15% use all their own), up from 34% in last year's report. Exploring how users manage keys, more than half said they are managing them in cloud consoles (52%). Multiple options are in use, with some respondents leveraging more than one. 45% are managing keys through their own bring-your-own-key (BYOK) system, and 38% are using a cloud-based service. A hold-your-own-key (HYOK) approach is being used by 29%, while 31% generate their own key material but use the provider management system. The healthcare vertical parallels the average, but financial services, retail and government respondents indicated a much stronger preference for using their own BYOK systems, at 49%, 54% and 48%, respectively.

Despite the early state of cloud data protection in place as mentioned above, a lower number (45%) of respondents reported having experienced a breach or failed audit of cloud data. Retail reported a higher rate of 52% compared to healthcare and financial services (38% and 44%, respectively). Regionally, 50% of respondents in Sweden and 52% of those in the Netherlands said they had experienced a data breach or failed an audit for cloud data. Failed audits or breaches of cloud data often have happened recently. 34% of all respondents experienced a breach or failed an audit involving cloud data or cloud applications this past year. 37% of retailers failed an audit of or experienced a breach of cloud data in the last 12 months. In the US, 37% of respondents had failed an audit of or experienced a breach of cloud data in the past year. In the UK, this number was 36% and in Australia it was 37%.

Moving Ahead

Putting in place systems that use common operational capabilities across on-premises and cloud resources can help tame hybrid complexity

Organizations large and small are reconsidering their security journeys as they recalibrate their expectations for the year ahead. Insights from this year's research can be useful in identifying how to improve those journeys and ensure better outcomes. Any idea that the urgent changes of the previous year were only a temporary disruption should be put aside; the primary goal is to build security capabilities with the flexibility to easily adapt to new realities. Organizations have to:

- Support and scale remote working models effectively.
- Secure data throughout its lifecycle and across applications.
- Span the full breadth of hybrid infrastructure.
- Provide the visibility to support and inform operations while delivering the assurances that governance and regulatory commitments require.

One of the most powerful aspects organizations can focus on is to simplify their operations. Doing so can have a twofold impact: it not only reduces toil but can also reduce risk by minimizing the chance of errors. In an increasingly hybrid infrastructure, putting in place systems that use common operational capabilities across on-premises and cloud resources can help tame hybrid complexity. With over half of respondents indicating that it's more complex to manage security in cloud environments, there's significant benefit to putting tools in place to help security teams perform at a higher level. That means moving beyond the limitations of native cloud controls and protections and ensuring that sensitive data and workloads have the protections they require, no matter where they're hosted.

There continues to be a need to deploy data security measures such as encryption and MFA more widely. While there is a positive trend in use, encryption levels are still below what's needed for comprehensive protection. This is an area that should be driven by regulatory requirements, as well as security common sense. As the research data shows, it may be the complexity of managing at large scale that is holding organizations back. Better security infrastructure can address that issue. Moving to BYOK and HYOK capabilities should be some of the most important projects in the year ahead.

As organizations move forward, they'll need visibility not only across their infrastructure, but throughout their organization. Establishing a common understanding is a key part of effectively setting priorities and executing security projects. When security teams are aligned with the key parts of the business, they can work together to effectively and efficiently address whatever issues the future holds.

About This Study

This research was based on a global survey of 2,767 respondents, fielded in January 2022, via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100m and with US$100-250m in selected countries. 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/data-threat-report