U.S. Federal 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

Two years on, the COVID-19 pandemic continues to dramatically impact IT teams worldwide. The 2022 Thales Global Data Threat Report looked at many aspects of those impacts, drawing insights from topics such as ransomware, zero-trust security strategies and cloud data security trends. This report covers U.S.-based respondents who identified their industry as "federal" or "defense" (n=106 for all U.S. federal respondents). Other "public sector" respondents at the state and local levels are excluded from this executive report.

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

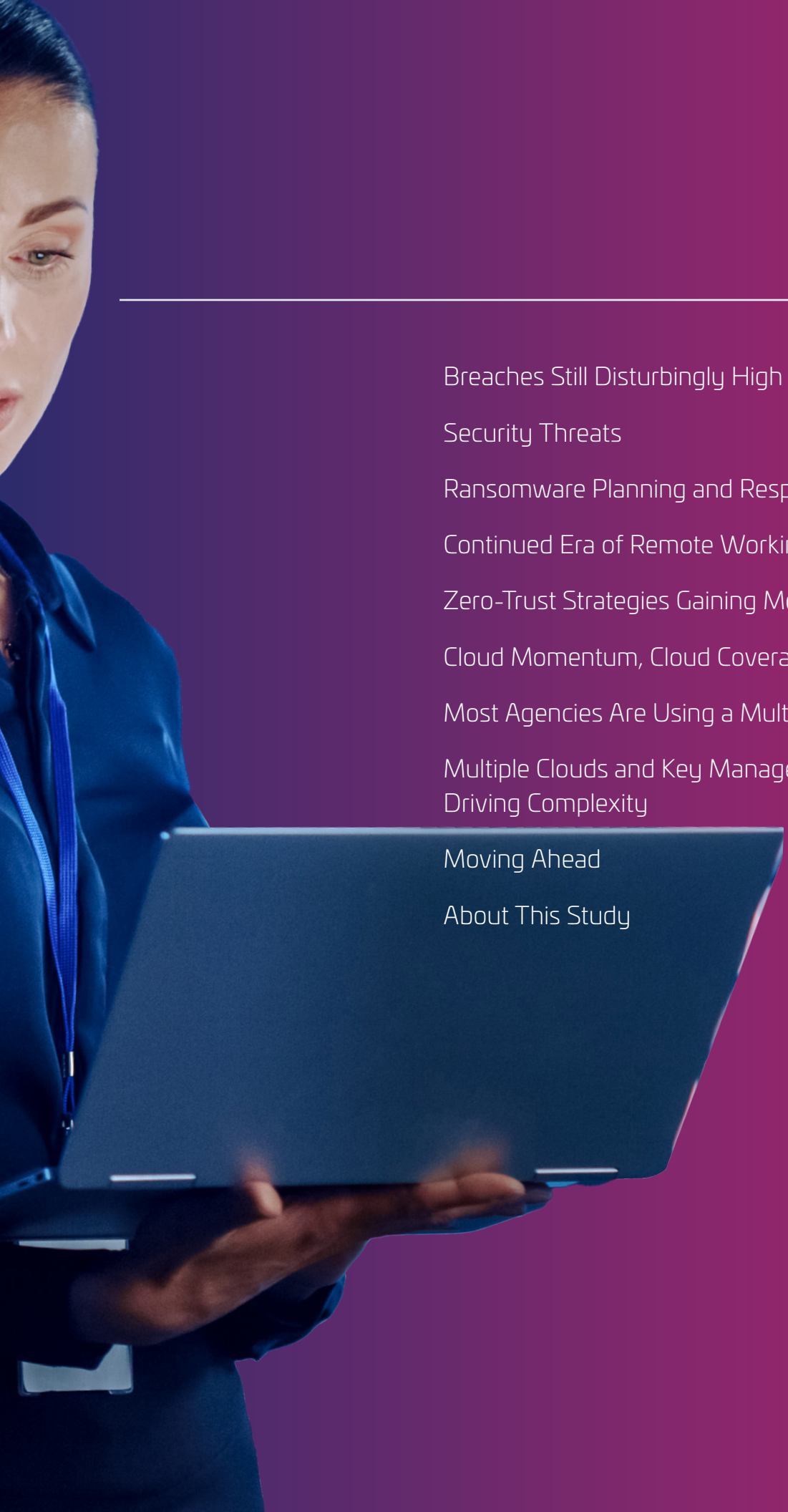
47%

of U.S. federal respondents reported an increase in the number of attacks.

78%

of U.S. federal respondents said they would trust their organization with their own personal data.

Contents



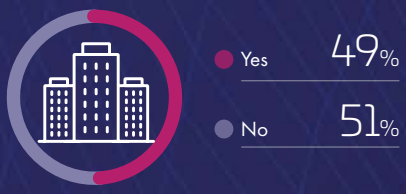
Breaches Still Disturbingly High

Despite substantial annual spending on cybersecurity, breaches are still being reported at a disturbingly high rate: Nearly half (49%) of U.S. federal respondents reported that they had experienced a security breach at some point, and of these, 37% said they had experienced a breach in the last 12 months.

One possible reason breach history remains high is the lack of information on the location and classification of data. In 2022, only 19% of U.S. federal respondents said they had complete knowledge of where their data is stored, with only 27% able to fully classify their data. Safe harbor from breach notification processes also remained elusive: 62% of those breached were not able to obtain it. In comparison, 61% of all U.S. respondents could not obtain safe harbor from encryption or tokenization. Given their breach histories, 30% of federal and 32% of non-federal U.S. enterprises have had to issue breach notifications.

Breaches Reported by U.S. Federal Respondents

HAS YOUR ORGANIZATION EVER BEEN BREACHED?



Source: 451 Research's 2022 Data Threat custom survey

37%

of U.S. federal respondents reported that they had experienced a security breach in the last 12 months.

only

19%

of U.S. federal respondents said they had complete knowledge of where their data is stored.

only

27%

of U.S. federal respondents said they are able to fully classify data.

Security Threats

Almost half (47%) of U.S. federal respondents reported an increase in the number of attacks. Of those who saw an increase, 60% saw increases in ransomware attacks and 56% saw increases in malware attacks. Of last year's respondents, 48% ranked ransomware as the leading source of increased security attacks, with phishing/whaling second at 46%. The speed with which ransomware attacks occur and the increased economic impact will continue to alter the way organizations detect and respond to breaches.

Despite increased attacks, organizations remained confident. Over three-fourths (78%) of U.S. federal respondents said they would trust their organization with their own personal data. For all worldwide respondents, trust in their own organizations remained high at 79% overall.

Among threat actors in ranked choice voting, 76% of U.S. federal respondents prioritized external adversaries motivated by ideology – hacktivists, followed closely by external adversaries with geopolitical goals at 74%. Internal, incidental error was third at 71%. In another ranked choice vote, 37% of federal respondents said their own web applications were the greatest adversarial target. Cloud-hosted (IaaS-based) and cloud-delivered (SaaS-based) applications were prioritized as targets by 32% and 23% of respondents, respectively.

96%

of those attacked by ransomware had some internal or external impact.

Ransomware Planning and Response

In 2022, the study had a new focus on ransomware planning and response. The speed and severity of ransomware compared to "low and slow" data exfiltration of most malware strains not only attacks data confidentiality but also data availability. Among our federal respondents, 23% had suffered a ransomware attack. Of those attacked, 96% had some internal or external impact, with 38% suffering a significant internal or external impact. Of greater concern, only 51% of federal respondents said they have a formal ransomware response plan that they would follow. Given the severity and speed of ransomware attacks, a centralized formal plan that ties together diverse stakeholders such as security operations, legal and senior leadership teams should be primary when coordinating a coherent response.

Only 51% of federal respondents said they have a formal ransomware response plan that they would follow.

Continued Era of Remote Working

For many agencies, the past year has extended remote working for many employees. Concerns about security risks of remote employees continued in 2022, with 27% of U.S. federal respondents "very concerned" and 56% "somewhat concerned." Attitudes improved regarding current remote access security solutions to effectively enable employees to securely work: 33% of respondents said they were "highly confident" and 45% said "significantly" confident in their secure remote access solutions.

When asked about remotely accessing applications, 61% of respondents said they use virtual desktop infrastructure (VDI). VPN fell to number two at 58%, followed by cloud-based single sign-on (SSO) and zero-trust network architecture (ZTNA) at 54% and 36%, respectively. In comparison, the worldwide numbers were 59%, 55%, 51% and 36% for VPN, VDI, cloud-based SSO and ZTNA/SDP, respectively.

48%

ranked ransomware as the leading source of increased security attacks.

Zero-Trust Strategies Gaining Momentum

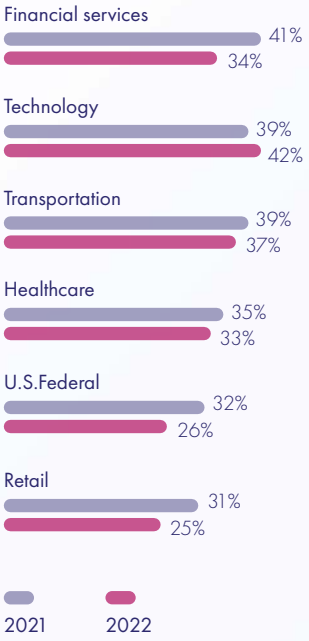
The principle of zero trust is based on the recognition that identities, networks, devices, applications and data are no longer confined within traditional corporate networks. Recently set forth by Office of Management and Budget memo M-22-09, which is complementary to Presidential Executive Order 14028, a federal zero-trust architecture strategy requires agencies to meet specific cybersecurity standards and objectives by September 2024. Perimeter-based approaches to security that rely on outdated notions of "trust" that are largely rooted in physical location (i.e., which network data exists on) have become less effective. In contrast, zero-trust approaches rely primarily on identity as a central means of granting access to resources.

Perhaps because zero-trust security strategies cover so much ground, fewer respondents said they have a formal zero-trust strategy. In 2021, 31% of U.S. federal respondents said they had a formal strategy, while in 2022, only 26% said the same. At the time of this study, another 31% of respondents were still in research and planning to develop a formal ZTNA strategy. Over half (52%) of all U.S. federal respondents said they rely on "some concepts" of zero trust to shape their overall cloud security strategy, and another 32% said that zero trust shapes their cloud security strategy to a great extent.

In 2022, U.S. federal respondents who said they had a formal zero-trust security strategy was down by 5% against 2021."

Formal Zero Trust Strategy/Policy Among U.S. Federal Respondents

WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?



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

Cloud Momentum, Cloud Coverage Gaps

Organizations worldwide place increasing amounts of data in the cloud, and U.S. federal organizations are no exception. In 2021, 29% of U.S. federal respondents stated that 41%-50% of their data was stored in external clouds, while 26% said that over half of their data was stored in external clouds. In 2022, 59% of respondents said they have at least 40% of their data in external clouds, and 27% reported that more than 60% of their data is in the cloud. Worldwide, 55% of respondents said they have at least 40% of their data in the cloud, and 23% said they have at least 60% in the cloud.

Gaps in protection are shrinking. In 2021, only 35% of U.S. federal respondents said that more than 40% of their sensitive data stored in the cloud was encrypted, and only 26% of respondents said that more than 50% of their sensitive cloud data was encrypted. In 2022, 41% of US federal respondents said at least 40% of their sensitive cloud data is encrypted, and 23% said at least 60% of their sensitive cloud data is encrypted. The number of recent breaches remains high but is improving. In 2021, 45% of federal respondents had experienced a breach or failed an audit involving cloud data and applications in the previous 12 months. In 2022, 35% of federal respondents said they experienced a breach or failed an audit for cloud applications or cloud data in the last 12 months.

Despite growth in the cloud and cloud-first strategies, last year 39% of U.S. federal respondents agreed or strongly agreed that it is more complex to manage privacy and data protection regulations in a cloud environment compared to on-premises networks within their organization. In 2022, 52% of federal respondents agreed or strongly agreed that cloud privacy and data protection regulations are more complex to manage than on-premises environments. Worldwide respondents in 2022 reported the same, with 51% agreeing or strongly agreeing. Adding to this complexity, different personas enforce cloud security strategy. In 2022, 46% of U.S. federal respondents said that policies are centrally defined by a security team, but defining technical standards and enforcement is left up to the individual developer or application owner. Another 34% said that policies and standards are centrally defined and enforced by the security team.

Policy Definition and Implementation Stakeholders

HOW DO YOU DECIDE AND ENFORCE POLICIES FOR CLOUD SECURITY?

- Policy defined and enforced by central security team — 34%
- Policy defined by security team, implemented by cloud delivery team — 46%
- Policy defined and implemented by cloud delivery teams — 20%

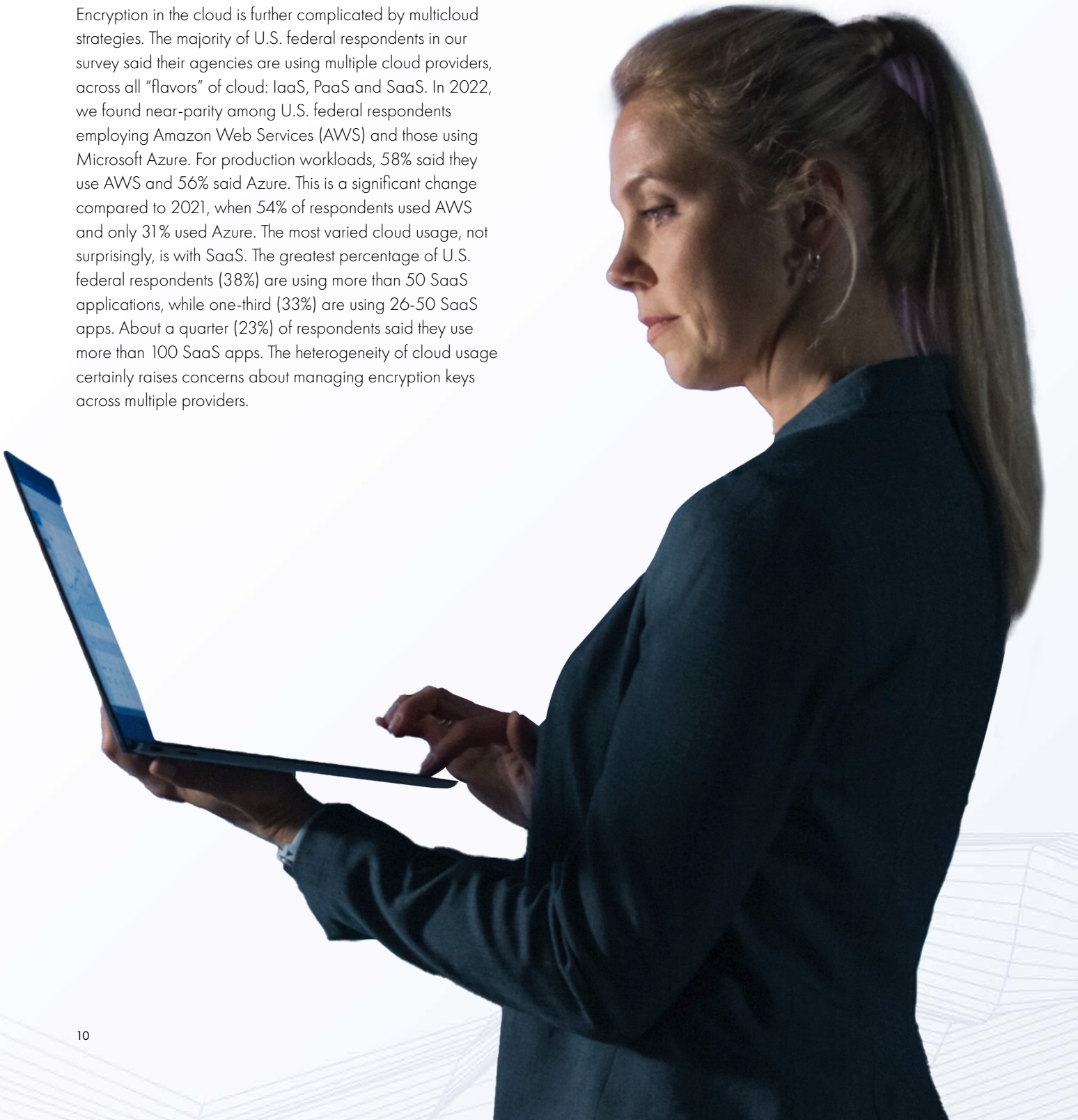
Source: 451 Research's 2022 Data Threat custom survey

35%

of federal respondents said they experienced a breach or failed an audit for cloud applications or cloud data in the last 12 months.

Most Agencies Are Using a Multicloud Strategy

Encryption in the cloud is further complicated by multicloud strategies. The majority of U.S. federal respondents in our survey said their agencies are using multiple cloud providers, across all "flavors" of cloud: IaaS, PaaS and SaaS. In 2022, we found near-parity among U.S. federal respondents employing Amazon Web Services (AWS) and those using Microsoft Azure. For production workloads, 58% said they use AWS and 56% said Azure. This is a significant change compared to 2021, when 54% of respondents used AWS and only 31% used Azure. The most varied cloud usage, not surprisingly, is with SaaS. The greatest percentage of U.S. federal respondents (38%) are using more than 50 SaaS applications, while one-third (33%) are using 26-50 SaaS apps. About a quarter (23%) of respondents said they use more than 100 SaaS apps. The heterogeneity of cloud usage certainly raises concerns about managing encryption keys across multiple providers.



Multiple Clouds and Key Management Options Driving Complexity

Given the diversity of IaaS and SaaS, existing on-premises infrastructures as well as security mandates requiring consistent controls throughout agencies, it is no wonder that organizations have a mixture of encryption and key management solutions. Specifically, our 2022 survey found that the largest percentage (39%) of U.S. federal agencies employ between five and seven separate key management products, while a small number (6%) have as many as 8-10 key management products. These typically include a mix of key management software, hardware security modules, homegrown solutions and spreadsheets or flat files.

Organizations not only have a variety of cloud providers and key management technologies to choose from, but they can also choose the types of controls for encryption and key management from cloud providers. To illustrate, nearly half (49%) of respondents said their cloud provider controls most or all of their encryption keys, and another 49% said their organization controls most or all of the encryption keys deployed for cloud data. Only 2% of federal respondents in 2022 chose a 'shared' key generation/key control arrangement, where the agency controls key generation material, but the cloud provider furnishes key control.

Many cloud services and platforms in general offer data encryption as a feature, yet underlying key management is not as well emphasized or understood, which may further complicate cloud data protection. When asked what security technologies are prioritized for sensitive data in the cloud, 65% of respondents chose data-at-rest encryption, whereas only 55% chose key management. Organizations would be better served taking a holistic look at the different encryption and key management solutions to identify further gaps in implementation and safety.

Cloud Encryption Drivers

WHAT IS THE PRIMARY DRIVER FOR DECISIONS ON WHERE AND HOW ENCRYPTION IS USED IN CLOUD?

Internal security architecture decisions	46%
Regulatory compliance requirements	38%
Customer or partner requirements	12%
Other	4%

Source: 451 Research's 2022 Data Threat custom survey

39%

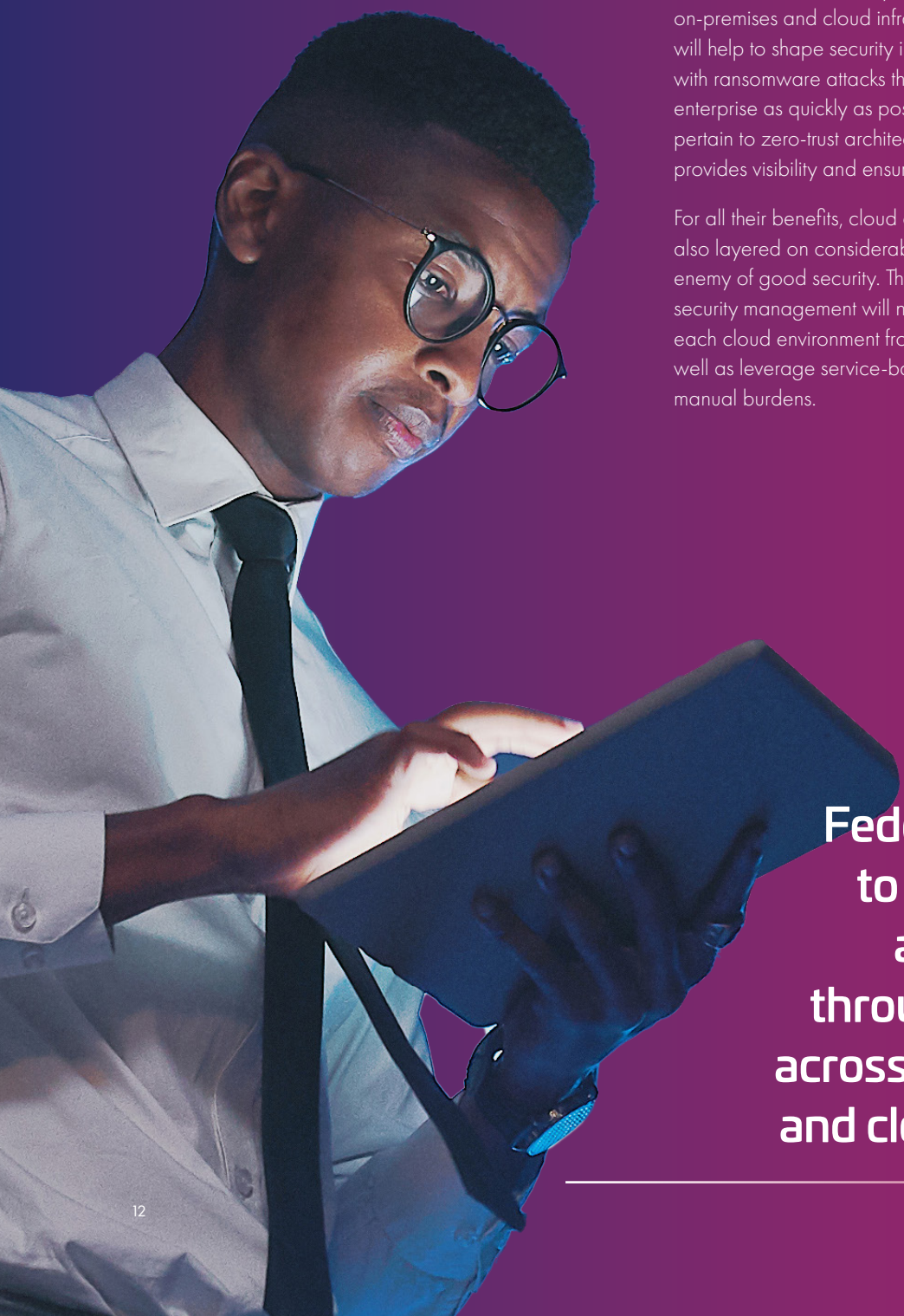
of U.S. federal agencies employ between five and seven separate key management products.

Moving Ahead

This study can serve as an indicator of potential paths U.S. federal agencies may follow on their security journey. One of the key lessons learned from the pandemic was that security strategies must be sufficiently agile to respond to a rapidly changing world, and also flexible enough to deal with the hybrid nature of our infrastructure, applications, data and users as both work-from-home and cloud become permanent fixtures in the security landscape.

The study highlighted the need for federal agencies to better understand and inventory data throughout its lifecycle across both on-premises and cloud infrastructure. A better understanding of the risks will help to shape security incident response and resilience, especially with ransomware attacks that aim to seize and extort as much of the enterprise as quickly as possible. Understanding the risks as they pertain to zero-trust architectures for data, devices and identities provides visibility and ensures governance and regulation.

For all their benefits, cloud computing and hybrid environments have also layered on considerable complexity – and complexity is the enemy of good security. This means that both security controls and security management will need to extend to cloud in ways that keep each cloud environment from being an isolated operational realm, as well as leverage service-based offerings and automation to reduce manual burdens.



Federal agencies need to better understand and inventory data throughout its lifecycle across both on-premises and cloud infrastructure.

About This Study

The COVID-19 pandemic has had an immediate and dramatic impact on IT teams around the globe, and its long-term effects are still evolving. The Federal edition of the 2022 Thales Data Threat Report study looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues ranging from COVID-19 and work-from-home strategies to quantum computing. The 2022 Thales Data Threat Report is based on a survey of nearly 2,800 security professionals and executive leaders, including 106 from U.S. federal agencies.

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-research