cpl.thalesgroup.com

#2020DataThreat

THALES

The Changing Face of Data Security

2020 Thales Data Threat Report

Global Edition

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE

About this study

This report is based on a global IDC web-based survey of 1,723 executives with responsibility for or influence over IT and data security. Respondents were from 16 countries: Australia, Brazil, France, Germany, India, Indonesia, Japan, Malaysia, Mexico, Netherlands, New Zealand, Singapore, South Korea, Sweden, the United Kingdom, and the United States. Organizations represented a range of industries, with a primary emphasis on healthcare, financial services, retail, technology, and federal government. Job titles ranged from C-level executives including CEO,
CFO, Chief Data Officer, CISO, Chief Data Scientist, and Chief Risk Officer, to SVP/VP, IT Administrator, Security Analyst, Security Engineer, and Systems Administrator. Respondents represented a broad range of organizational sizes, with the majority ranging from 500 to 10,000 employees.

The survey was conducted in November 2019.

Contents

Our sponsors are:

SENETAS | KEYFACTOR | Canon Marketing Japan Inc. | OASIS Open standards. Open source. | FIRST TECH | TiSafe | CSA cloud security alliance® | PURESTORAGE® | carahsoft.

Executive Summary

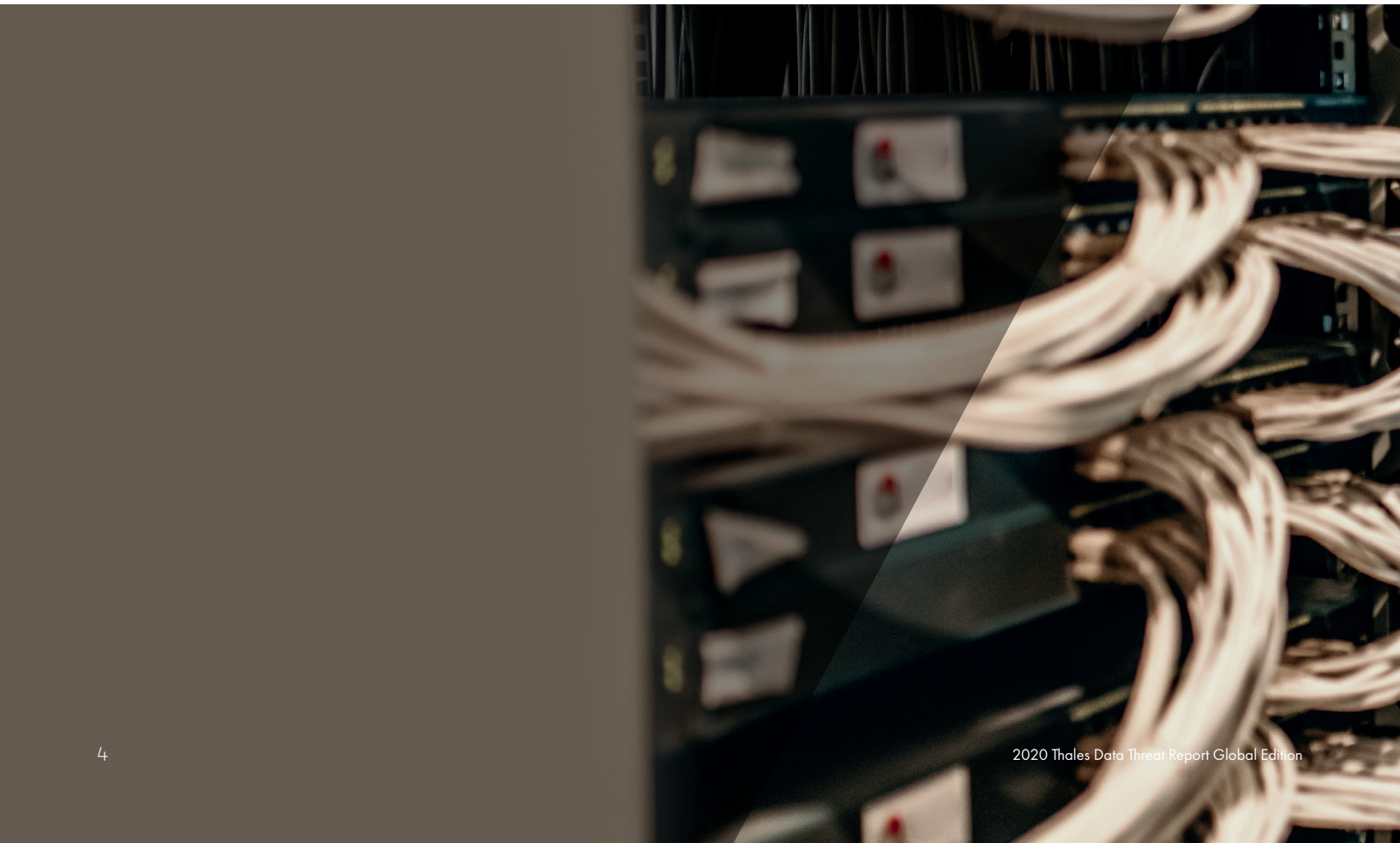
Companies and other organizations are leveraging a wide variety of technologies, including cloud, mobile, and the Internet of Things (IoT) to transform their businesses, improve customer experience, find new sources of value, and reduce costs. IDC research shows that this digital transformation (DX) is well underway, with 43% of companies in our study saying they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

While DX can provide tremendous value, it also makes data security more complex. Organizations are increasingly dependent on and expanding the amount of data stored in the edge, meaning they need to focus on aspects beyond traditional network perimeters. We are at an inflection point with the cloud as half of all data is now stored in cloud environments, and 48% of that data is sensitive. Additionally, most organizations rely on multicloud environments. All of this adds up to today's data environments becoming even more complex; this complexity is a top barrier to data security.

But organizations are cognitively dissonant to data security. Two-thirds believe they are very secure, but organizations are not implementing the processes and investing in the technologies required to appropriately protect their data. More than half have been breached or experienced failed security audits. And when it comes to securing data in the cloud, most companies incorrectly look to their cloud providers for their portion of the shared responsibility model.

43%

of companies in our study saying they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.



As for investment, data security still represents a small share of overall security budget. Forty-six percent of organizations plan to increase data security spending in the next 12 months, a similar amount as last year. But these organizations still focus a disproportionate amount of their spend on network security, as 34% of respondents' focus is on data security and data security averages just 15% of overall IT security budget.

In terms of emerging threats, quantum computing is looming on the horizon and promises to further complicate data security. Cryptography requirements will fundamentally change when quantum computing comes online, and 72% of respondents see quantum cryptography affecting their organization in the next five years.

As organizations face expanding and more complex data security challenges, they need smarter and better ways to approach data security. Companies need to take a multilayered approach to data security, embracing cloud shared security responsibilities and adopting a zero trust model that authenticates and validtes the users and devices accessing applications and networks, while also employing more robust data discovery, hardening, data loss prevention, and encryption solutions.

34%

of respondents' focus is on data security and data security averages just 15% of overall IT security budget.

01 Key Findings

Digital Transformation is Complicating Data Security

Companies and organizations are fundamentally reimagining their businesses and taking advantage of digital technologies like cloud, mobile, and IoT to digitally transform their operations. Even "traditional companies" will drive more revenue from digital products, services, and experiences. Forty-three percent of organizations in our study say they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility (see Figure 1). The U.S. leads all countries surveyed by far, with 59% identifying as either aggressively disrupting their markets
or embedding digital capabilities, followed by the U.K. at 51%.

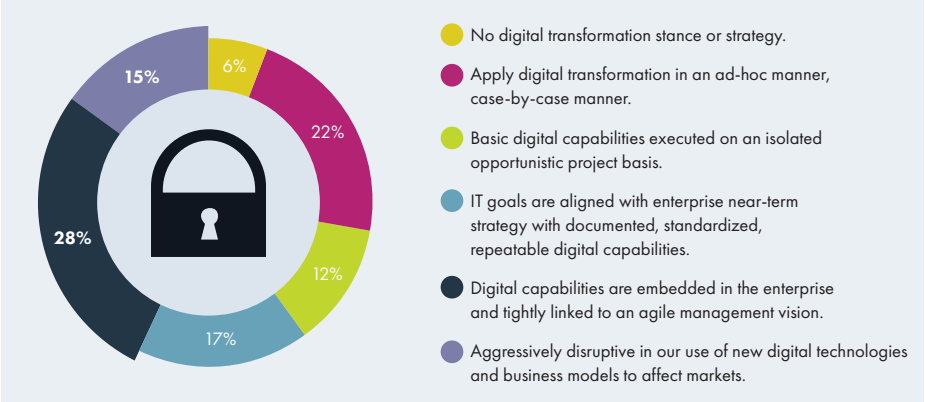


Figure 1 – Digital Transformation Stance
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

No organization is immune from data security threats, with 49% of global respondents experiencing a breach at some point and 26% having been breached in the past year.
And 47% of organizations report that they have been breached or failed a compliance audit in the past year.

"No organization is immune from data security threats, with 49% of global respondents experiencing a data breach at some point."

While organizations that digitally transform are realizing new sources of competitive advantage, these companies face data security challenges that DX presents. The degree of DX transformation positively correlates to data vulnerability: The more digitally transformed an organization, the more likely that it has experienced a data breach. This 2020 Thales Data Threat Report found that 45% of organizations in one of the top two DX categories experienced a data breach this year, significantly higher than the global breach rate. Furthermore, companies that spend more on IT security are more likely to experience breaches. Twenty-nine percent of organizations for which security is more than 10% of their IT budget experienced a breach in the past year, and 52% have been breached at some point, compared to 19% and 40%, respectively, for those companies with an IT spend on security of 10% or less (see Figure 2). Digitally Determined organizations – those organizations making the strategic, organizational, technological, and financial decisions that will set them up to digitally transform in the next several years – may also have greater data threat exposure. Their greater level of sophistication may also mean they are more likely to be aware they are being breached. Less sophisticated companies may have less exposure or are being breached without knowing it.

> "The more digitally transformed an organization, the more likely that it has experienced a data breach."

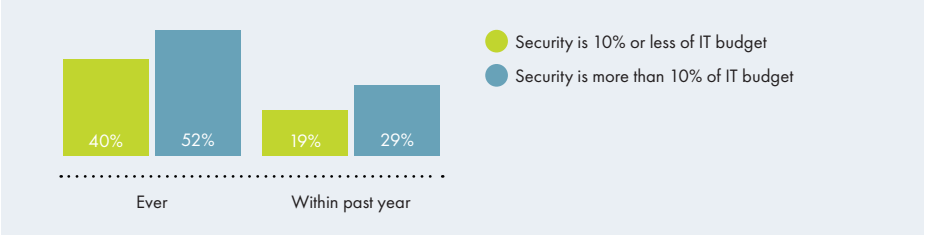


Figure 2 – Breach Incident Rates by Level of Security Spend

Source: 2020 Thales Data Threat Report Survey, IDC , November 2019

Organizations are Housing Sensitive Data Across a Broad Range of Technologies

Organizations are adopting a wide range of 3rd Platform technologies, which include cloud, mobile, social, big data, and IoT. SaaS applications have the widest adoption at 95%, up from 71% in 2018 (see Figure 3). Mobile payments, social media, and IaaS and PaaS cloud environments also lead planned adoption. Note that many of these technologies, such as IoT and mobile, are edge technologies, which reinforce the concept that data exposure is expanding well beyond the traditional network perimeter.

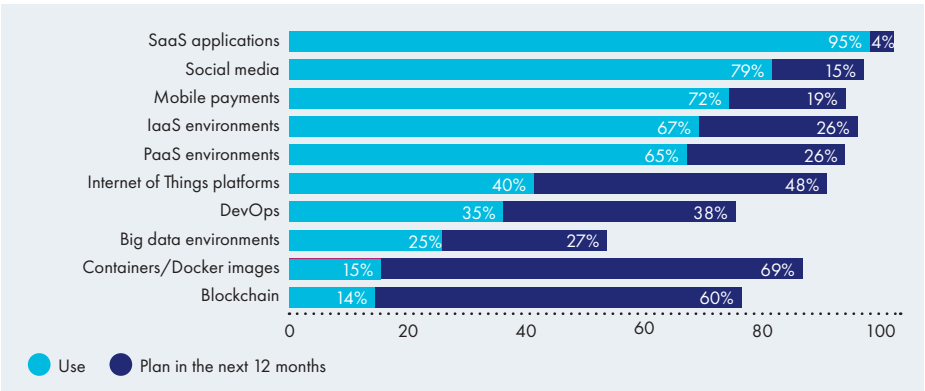
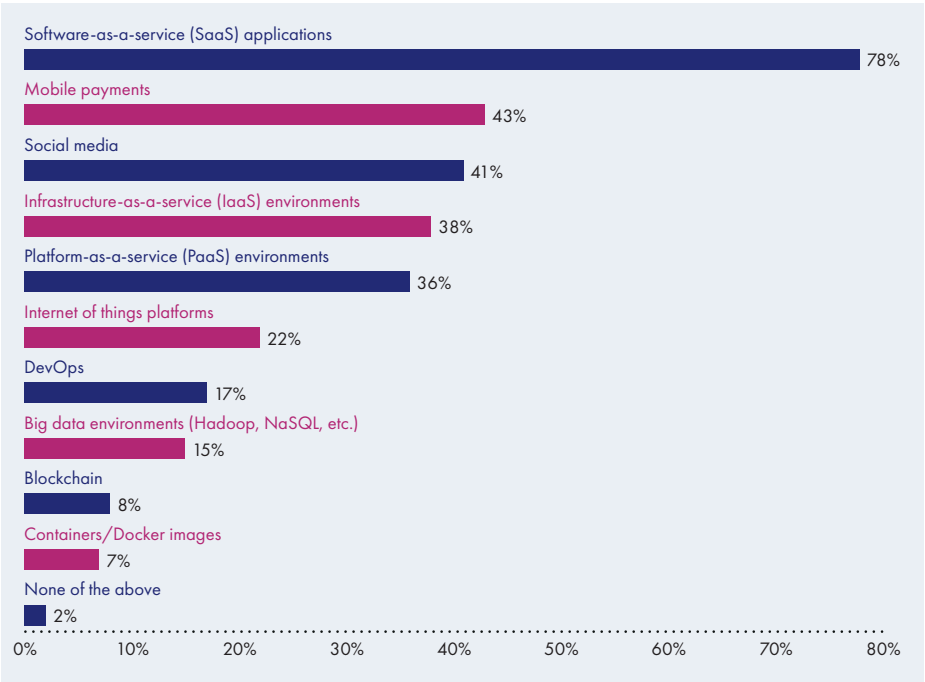


Figure 3 – Technology Adoption Levels

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Likewise, many organizations are housing data in a similarly broad set of technologies. Seventy-eight percent store sensitive data in SaaS applications, 38% store data in IaaS environments, and 36% store data in PaaS environments. Ninety-eight percent of organizations store data in at least one of the technologies in our survey (see Figure 4).
U.S. data shows even higher rates of sensitive data stored in cloud environments, with 79% in SaaS applications, 48% in PaaS environments (compared to 36% globally), and 46% in IaaS environments (compared to 38% globally).



> "Securing the perimeter does little to protect off-premises data, which speaks to the need to take a zero trust access and data protection approach to security."

Figure 4 – Technology Environments Used to Store Sensitive/Regulated Data
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Note that there is a greater spread in the number of respondents who said they have adopted and store data in these environments than last year (in which 40%+ of respondents claimed to be using environments like big data and IoT to store sensitive data). IDC views this as a sign of maturity in the industry. We believe that respondents last year were reacting to technology buzzwords and reflexively taking credit for having adopted the relevant technologies. In contrast, respondents this year have a more realistic assessment of their organizations' use of these longer-tail technologies.

As companies expand their usage of 3rd Platform cloud, mobile, social, big data and IoT technologies, sensitive data potentially becomes increasingly vulnerable as a result. Thus, securing the perimeter does little to protect off-premises data, which speaks to the need to take a zero trust access and data protection approach to security. This zero trust approach eliminates the binary trust/don't trust approach of yesterday's on-premise, perimeter-centric reality and instead requires a least privileged, continuous validation and verification approach, providing both network and application centric access protections. Likewise, technologies like encryption and tokenization assure that if the data is hacked, leaked, or physical devices are stolen, data is also appropriately protected.

Clouds Now House the Majority of Data, Creating Significant Risk

Ninety-eight percent of organizations surveyed have some data in the cloud. Indeed, data stored in the cloud has reached an inflection point with our study indicating that an estimated 50% of data is in the cloud. More importantly, respondents say that an estimated 48% of that data in the cloud is sensitive. Organizations in the U.S. rely on the cloud to store data to a greater degree than global respondents. For U.S. respondents, an estimated 55% of data is stored in cloud environments and 54% of that cloud data is sensitive (see Figure 5).

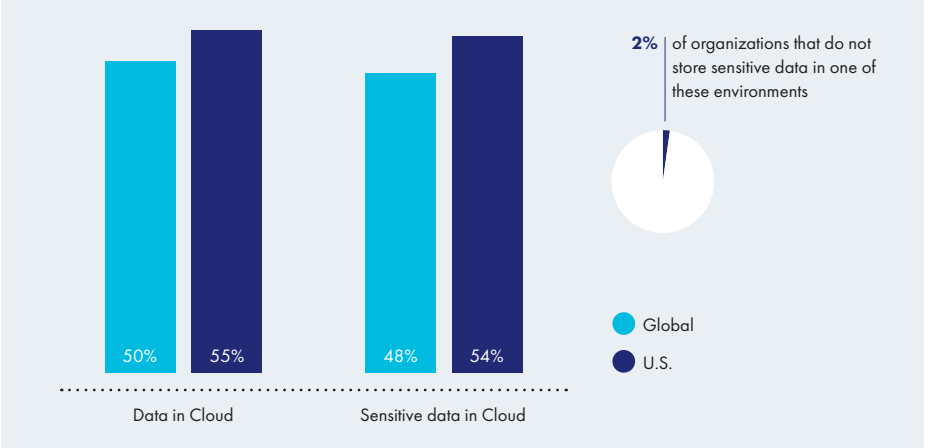


Figure 5 – Data Stored in Cloud Environments

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

As more sensitive data is stored in cloud environments, data security risks increase. Yet, despite this significant amount of sensitive data exposure, rates of data encryption and tokenization are low. In fact, 100% of respondents say at least some of their sensitive data in the cloud is not encrypted. Only 57% of sensitive data stored in cloud environments is protected by encryption and less than half – 48% – is protected by tokenization. The U.S. employs data encryption (63%) and tokenization (54%) to protect sensitive data in the cloud at higher rates than the global sample (see Figure 6).

> "100% of respondents say at least some of their sensitive data in the cloud is not encrypted."

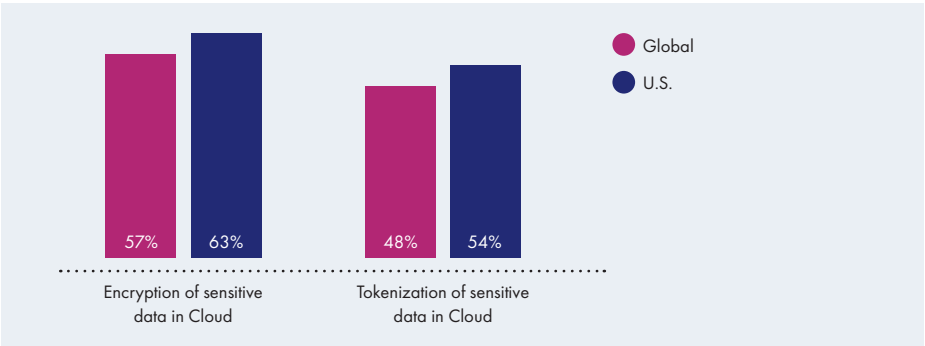


Figure 6 – Security of Sensitive Cloud Data

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Complexity is a Top Barrier to Data Security as Multicloud Becomes the Norm

As more data migrates to the cloud, security becomes more complex. But much of this complexity is self-inflicted, as multicloud environments have become increasingly common. Companies are using multiple IaaS and PaaS environments, as well as hundreds of SaaS applications. Eighty-one percent of global respondents are using more than one IaaS vendor (86% in the U.S.), 81% have more than one PaaS vendor (86% in the U.S.), and 11% have
more than 100 SaaS applications to manage (14% in the U.S.) (see Figure 7).

> "Respondents rate complexity as their top perceived barrier to implementing data security, followed closely by the pressure to avoid impact to business performance and process."

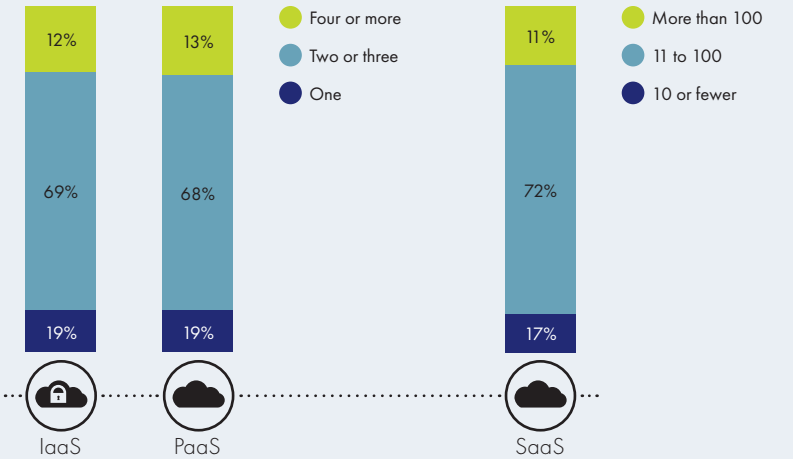


Figure 7 – Number of IaaS/PaaS/SaaS Vendors

Source: 2020 Thales Data Threat Report Survey, IDC , November 2019

The resulting complexity is making life more difficult for security professionals. Respondents rate complexity as their top perceived barrier to implementing data security, followed closely by the pressure to avoid impact to business performance and process (see Figure 8). The vast majority of organizations clearly recognize the importance of data security as a small minority find that "lack of perceived need" (26%) or "lack of organization buy-in" (25%) to be an issue.

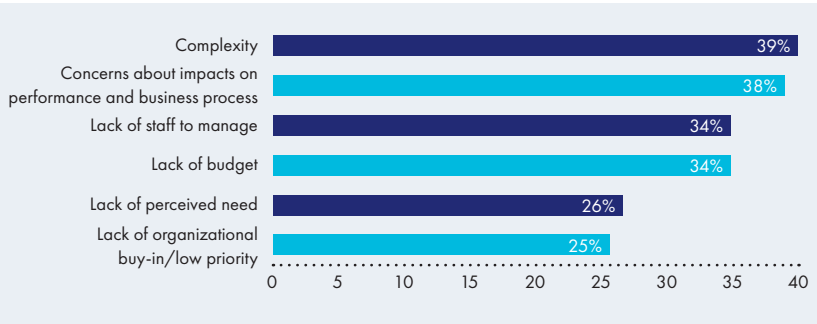


Figure 8 – Barriers to Implementing Data Security

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Quantum Computing Data Security Concerns are on the Horizon

Data security will only get harder with the advent of quantum computing. Cryptography requirements highlight a critical security issue brought on by the power of quantum computing. The impact of quantum computing is imminent as 72% of organizations see it affecting their cryptographic operations in the next five years (see Figure 9). Ninety-two percent of respondents are concerned quantum computing will create exposure for sensitive data, with 35% very/extremely concerned. U.S respondents perceive similar impacts, with 72% see it affecting cryptographic operations in the next five years, 91% concerned that quantum computing will compromise sensitive data, and 41% very/extremely concerned.

> "Ninety-two percent of respondents are concerned quantum computing will create exposure for sensitive data, with 35% very/extremely concerned."

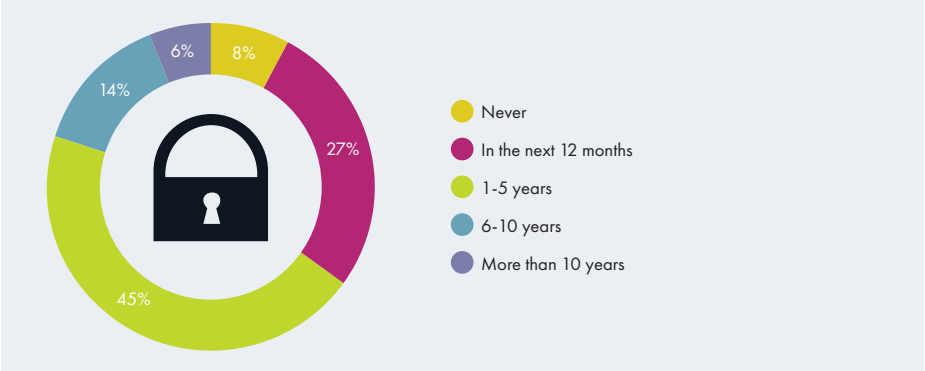


Figure 9 – Quantum Cryptography to Affect Organizations

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Top strategies to offset quantum computing threats are IT/security architecture changes (35%) and key management infrastructure deployment (34%). But many organizations are uncertain how to respond even though threats may surface within the next five years. Twenty-two percent of respondents plan to air gap critical systems, and 6% have no plans at all.

Organizations Sense of Data Security at Odds with Reality

Despite the pervasive and expanding threats to data security, enterprises feel less vulnerable in 2019 than they did in 2018. Sixty-seven percent of organizations felt vulnerable in 2019, down from 86% in 2018, even as security risks grow. Findings show every level of perceived vulnerability dropped year over year and 33% of respondents state they are "not at all vulnerable" compared to 14% in 2018 (see Figure 10). U.S. organizations hold a similar stance, with 69% feeling vulnerable and 31% not at all vulnerable.

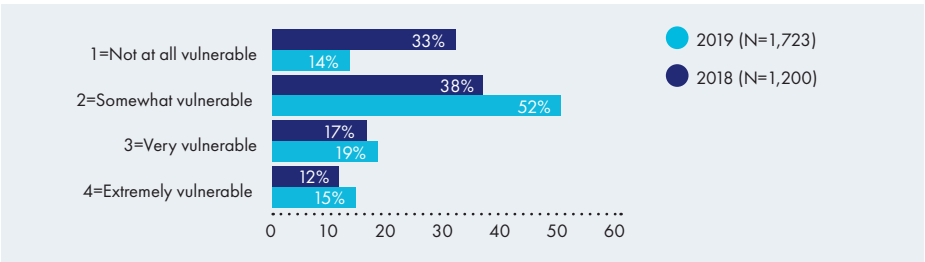


Figure 10 – Vulnerability to Data Security Threats, 2019 Compared to 2018

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

These low levels of perceived vulnerability point to a disconnect between perception and reality. The reported confidence respondents expressed is not supported by the appropriate reported data security practices or investments. Organizations haven't significantly changed their behaviors by using tools that would make them less vulnerable. As previously mentioned, encryption and tokenization rates of sensitive data in the cloud are low. Furthermore, only 61% of respondents implement file encryption, and 59% implement database encryption. Implementation of file and database encryption increased only slightly in 2019 from 2018 with implementation rates of 56% and 55%, respectively (see Figure 11). Note that U.S. findings show higher use of file encryption at 69% and database encryption at 65% than global respondents.

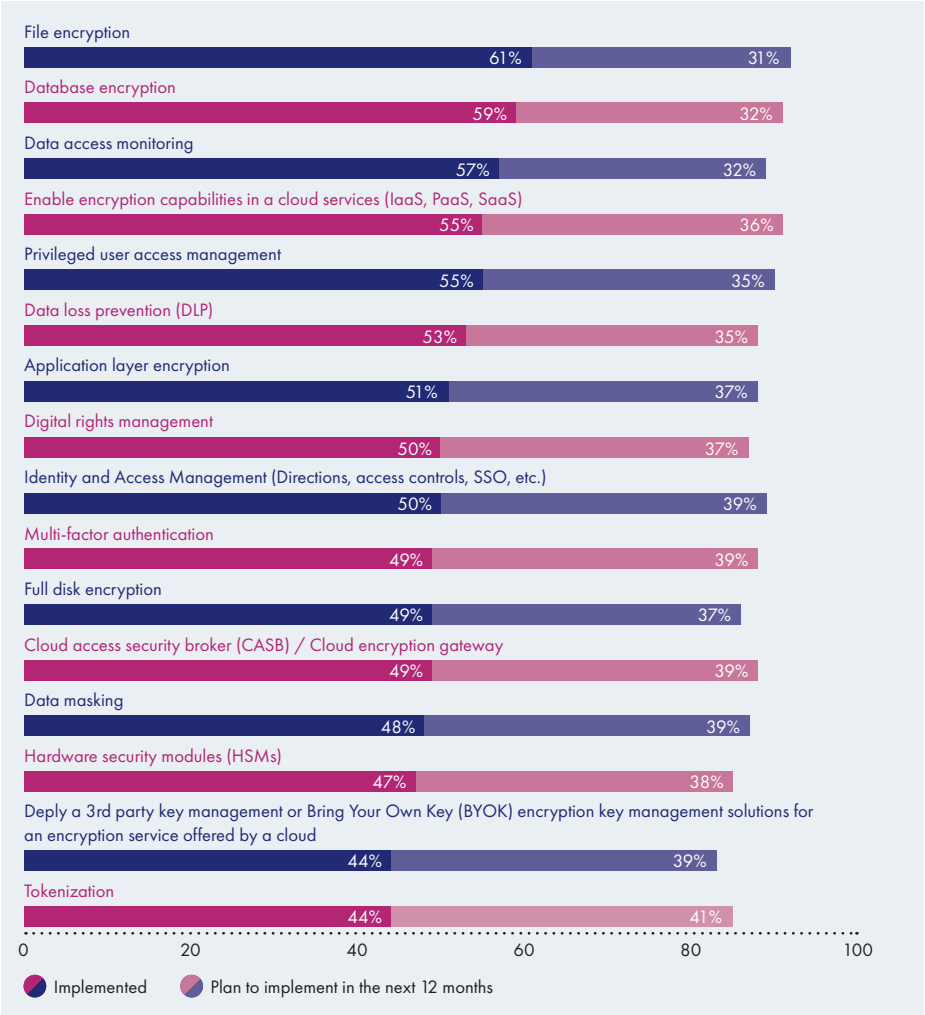


Figure 11 – Implementation of Encryption and Data Security Tools

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Higher Security Spend Doesn't Match Security Focus

Organizations plan to spend more money on data security in the upcoming year and do so at rates similar to last year. Forty-nine percent of respondents said they would be spending somewhat or much more on data security over the next 12 months. Yet data security budget growth is declining slightly, and nearly one in five organizations plan to decrease data security spending in 2020 (see Figure 12). U.S. companies see greater growth in data security budgets than global respondents, with 58% of U.S. companies increasing data security spending and only 13% decreasing data security spending.

58%

of U.S. companies increasing data security spending and only 13% decreasing data security spending.

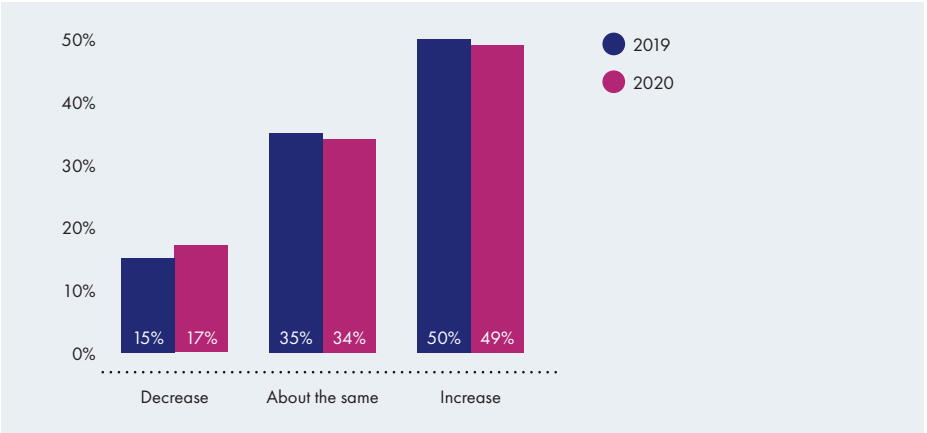


Figure 12 – Data Security Spend

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Enterprises have a roughly equal focus on network, data, and application security, with slightly more focus on network security than application or data security (see Figure 13). And while 34% of security focus is on data security, spending on data security lags considerably as only 15.5% of security budgets is spent on data security.

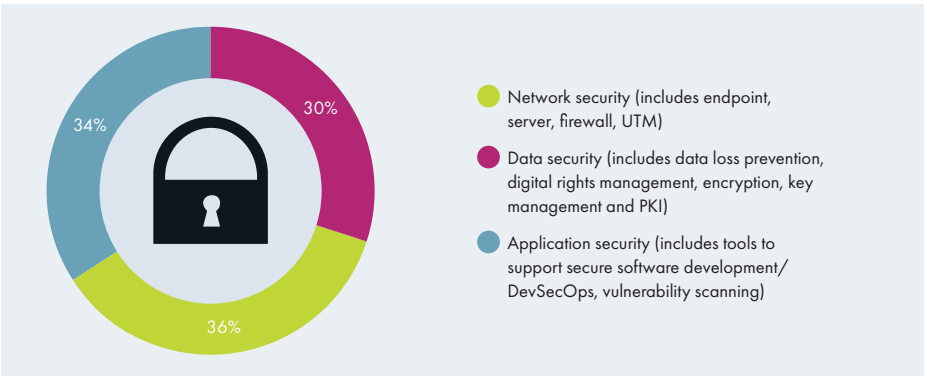


Figure 13 – Proportion of Security Focus

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Further demonstrating a disconnect between security budgets and the focus of security departments, respondents believe that malicious actors present the greatest risk to their data. Fifty-seven percent of companies are worried about cybercriminals who steal data for profit, and 52% are worried about cyberterrorists who damage companies by making them look bad publicly.

Interestingly, respondents are less concerned about day-to-day issues which may actually be a greater threat. These are issues involving entities and situations over which they have more control, such as partners with internal access, privileged user access, service provider accounts, and contractor accounts. Organizations must be careful of overprovisioning quantity and breadth of accounts, as the risk from contractors is often more about carelessness than malicious behavior (see Figures 14 and 15).

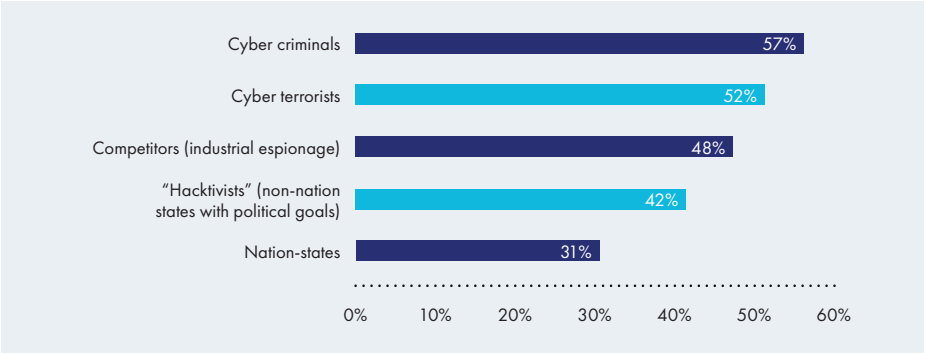


Figure 14 – Malicious Actor Data Threats

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

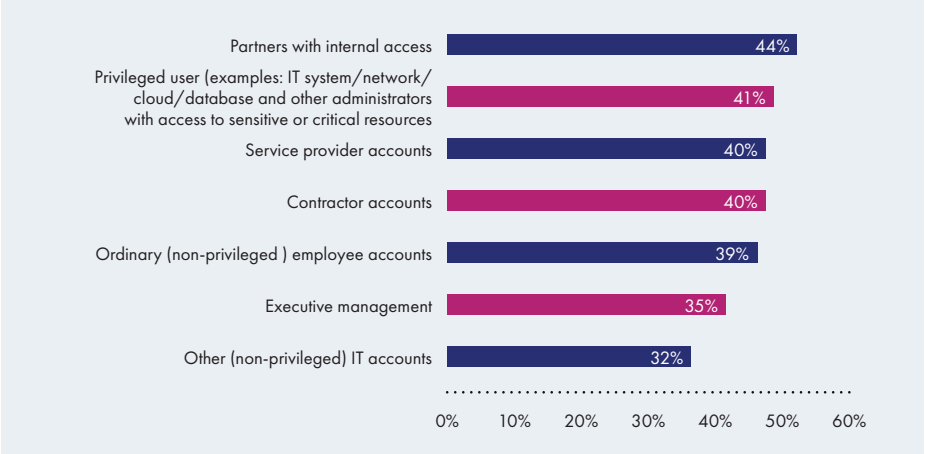


Figure 15 – Internal Data Threats

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

02

Cloud Data Security is at a Tipping Point

Each Cloud Environment Requires a Shift in Security Responsibility

More than half of data is now stored in the cloud, with a significant portion of that data being sensitive. As a result, IT security departments must now, more than ever, embrace and own their portion of the cloud shared responsibility model and implement data security best practices, as the cloud provider most often does not guarantee security at the data level.

Organizations are concerned about many data security issues regarding the cloud. Yet, organizations are seemingly most concerned about issues owned by their cloud providers, like security breaches at the provider and cases of security provider acquisition or failure (highlighted by the top red box in Figure 16). Although valid concerns, the real possibility of these issues happening are quite low. Organizations are seemingly less concerned about issues over which they have direct control, and which represent greater potential vulnerabilities, like encryption key management (highlighted by the second and third red boxes in Figure 16).

> "Organizations should shift their cloud security focus and concern to the portion of the shared responsibility model where the organization itself can influence the security of its own data."

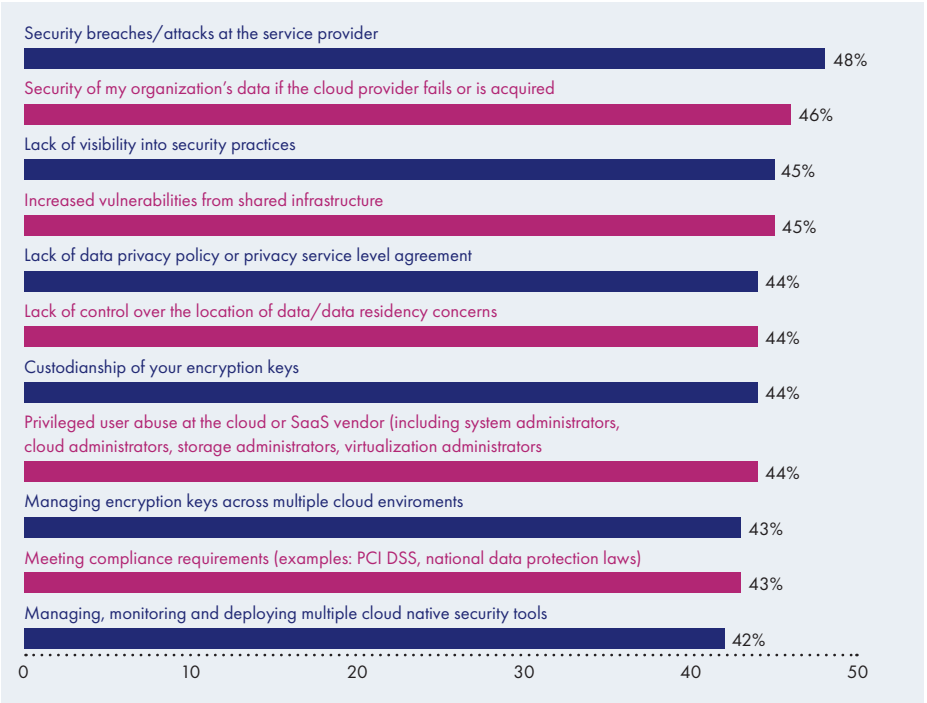


Figure 16 – Cloud Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

This mismatch between threats respondents perceive, and those threats that in reality pose the most risk, implies that respondents have not fully considered data security in a cloud-first world. Each type of cloud environment requires a shift in security responsibility for identities, data, applications, operating systems, server virtualization, network, infrastructure, and hardware. Organizations should shift their cloud security focus and concern to the portion of the shared responsibility model where the organization itself can influence the security of its own data (see Figure 17).

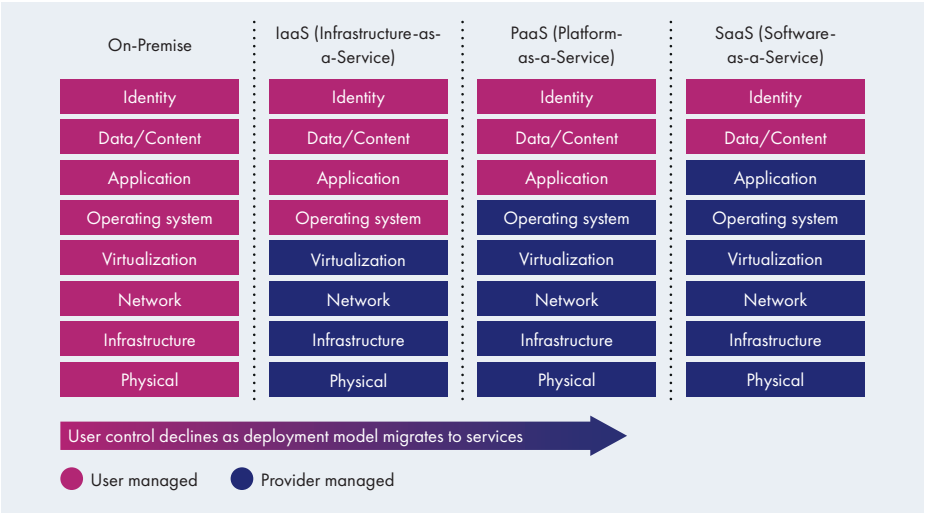


Figure 17 – IDC Shared Responsibility Model

Source:IDC, November 2019

Security concerns also shift as organizations deploy more data into SaaS applications, and IaaS and PaaS environments.

According to our study, 93% of respondents have at least some level of concern over data security of SaaS applications. SaaS security concerns span a broad range of risks, with encryption of data within the service provider's organization and ability to manage encryption with local encryption keys leading the list (see Figure 18).

> "SaaS security concerns span a broad range of risks, with encryption of data within the service provider's organization and ability to manage encryption with local encryption keys leading the list."

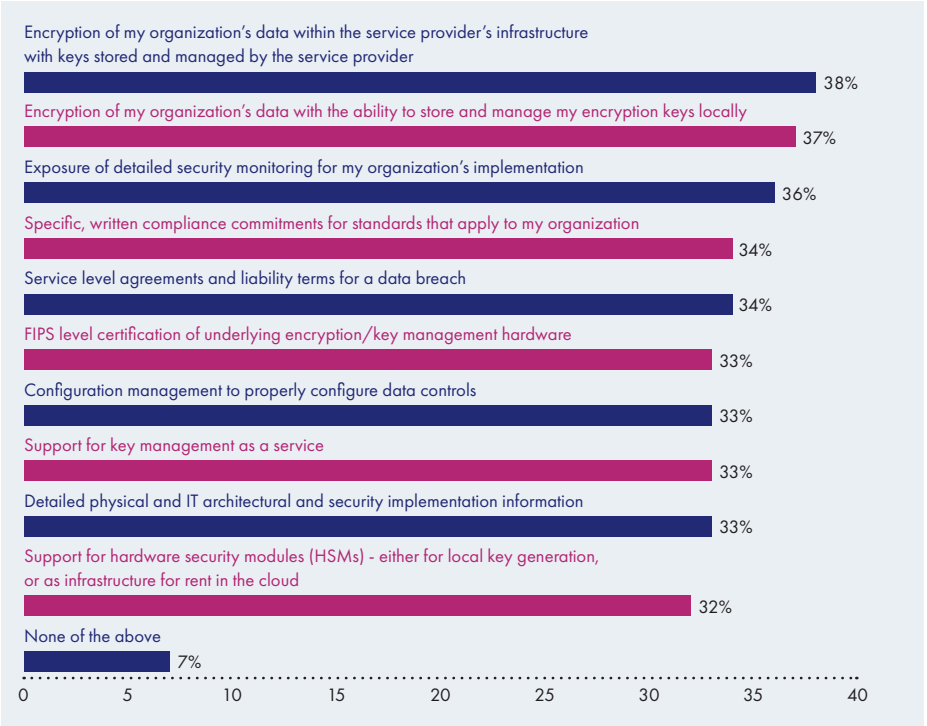
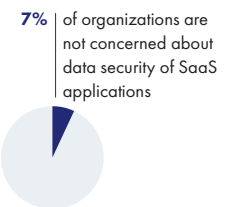


Figure 18 – SaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019



Ninety-one percent of respondents have at least some concerns over data security of IaaS environments. IaaS security concerns also cover a broad range of issues with local key integration and physical layout information as top concerns (see Figure 19).

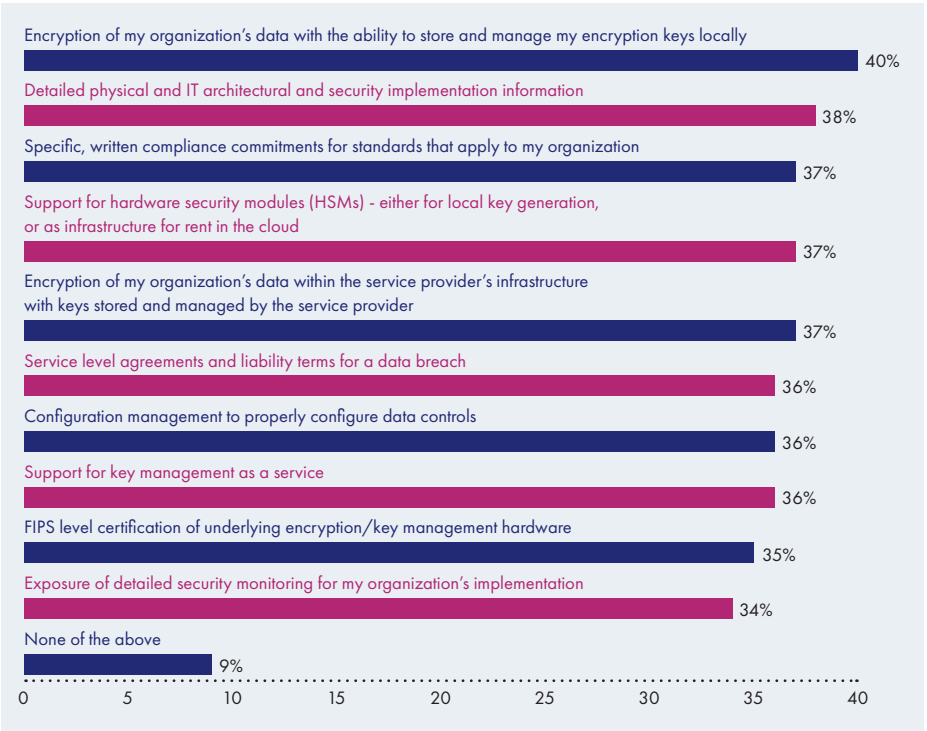
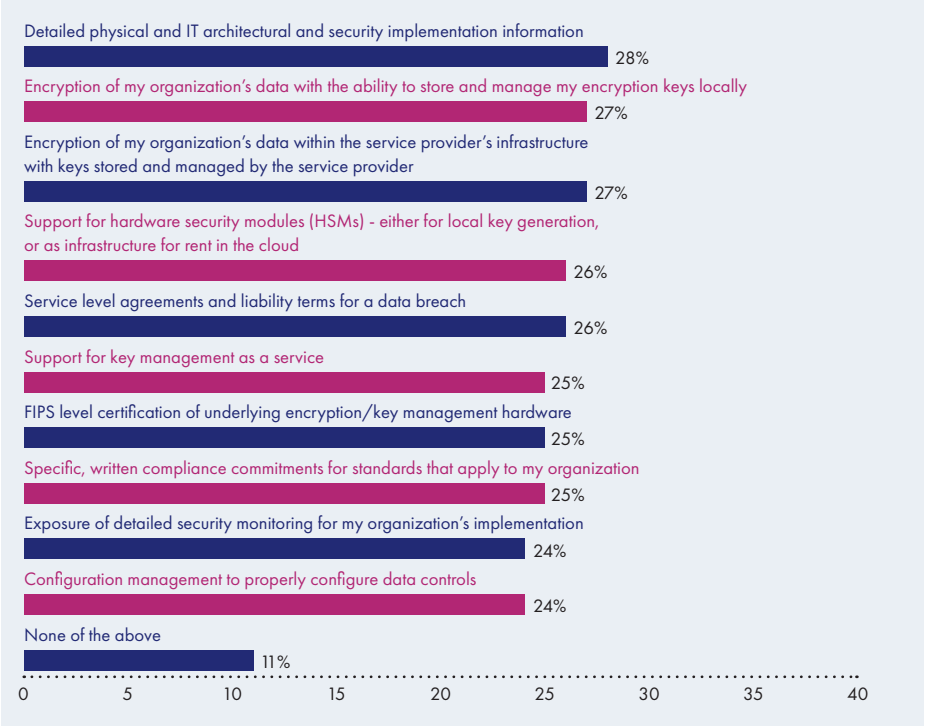


Figure 19 – IaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Eighty-nine percent of respondents have at least some concern over data security of PaaS environments with physical layout information and data encryption leading the way (see Figure 20).

"Respondents expressed concern over 'Encryption of my organization's data with the ability to store and manage my encryption keys locally."



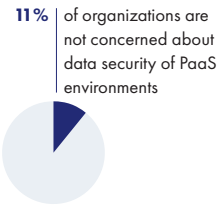


Figure 20 – PaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Certainly, each of the different cloud environments has its own unique concerns; however, survey respondents expressed some common themes across IaaS, SaaS and PaaS (Figures 18 through 20). In each of the highlighted red boxes in the preceding graphics that indicate the most concerning issues, respondents expressed concern over "Encryption of my organizations' data with the ability to store and manage my encryption keys locally."

Similarly, "Encryption of my organization's data within the service provider's infrastructure with keys stored and managed by the service provider." is a consistent concern and increases in rank as the level of control in the infrastructure declines (as defined in Figure 17). Unease about the control and management of encryptions keys is expressed by our respondents.

03

Security Concerns and Methods of Alleviation by Data Environment

Digital Transformation Introduces New Security Concerns

Just as digital transformation creates opportunities for new technologies, it also introduces new security concerns. Transformational edge technologies like IoT and mobile payments allow organizations to engage customers where they are but at the same time expand security concerns away from on-premise to cloud environments. Big data, containers, and DevOps technologies support the cloud and edge computing. With the cloud expanding adoption of these technologies, discovery of sensitive data and key management take on even more critical roles in data security. Yet data discovery and key management are not perceived as top concerns, creating potential gaps in data security practices.

Ninety-nine percent of companies in this study feel some level of security as they push more data to these new technology deployments, with 66% feeling very or extremely secure. U.S. respondents felt even more secure than their global counterparts, with 78% feeling very or extremely secure (see Figure 21).

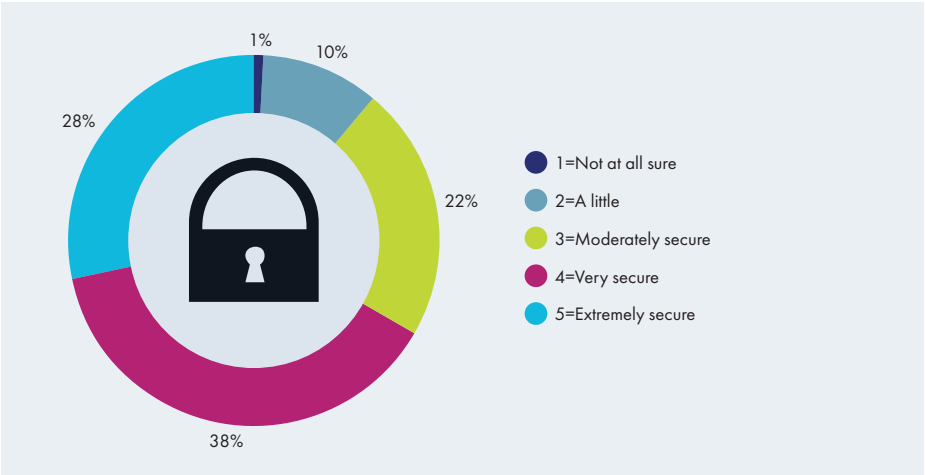
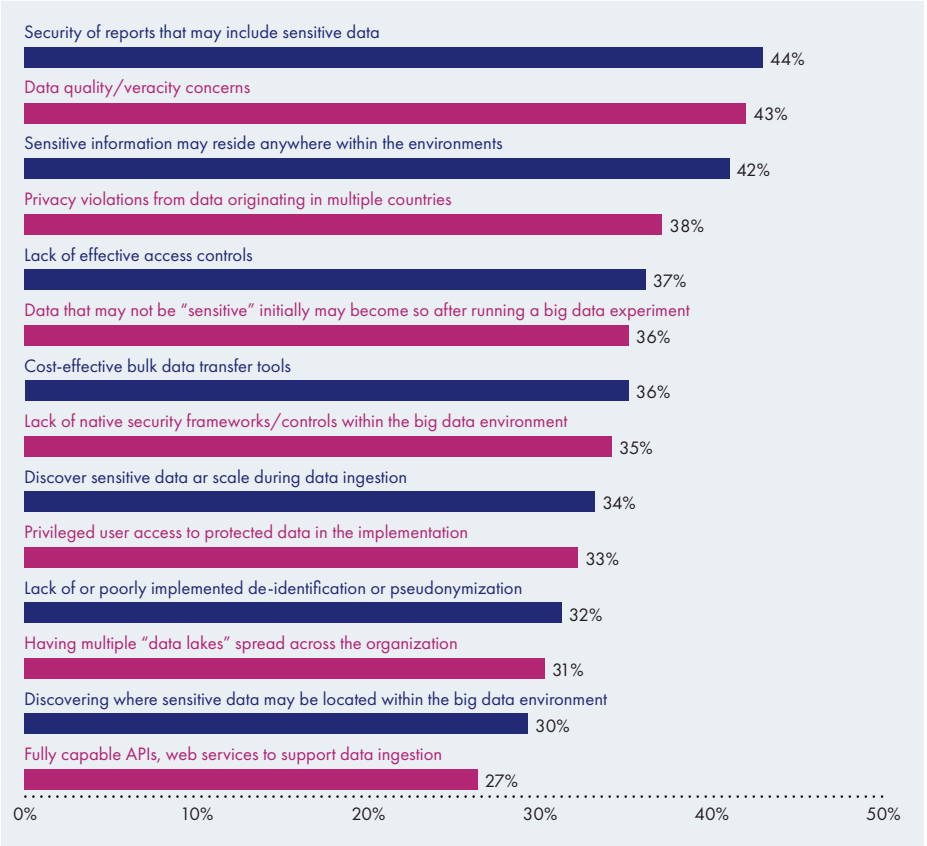


Figure 21 – Security Level of New Technology Deployments
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

"Just as digital transformation creates opportunities for new technologies, it also introduces new security concerns."

Big Data Security Concerns

One hundred percent of respondents are concerned about data security in their big data environments. The leading big data security concerns involve issues around report security, data quality, and ubiquity of sensitive data. Data discovery concerns are not perceived as top concerns. Discovering sensitive data at scale during data ingestion came in at 34% and discovering where sensitive data may be located in a big data environment came in at just 30% (see Figure 22).



0% of organizations not concerned about data security of big data environments

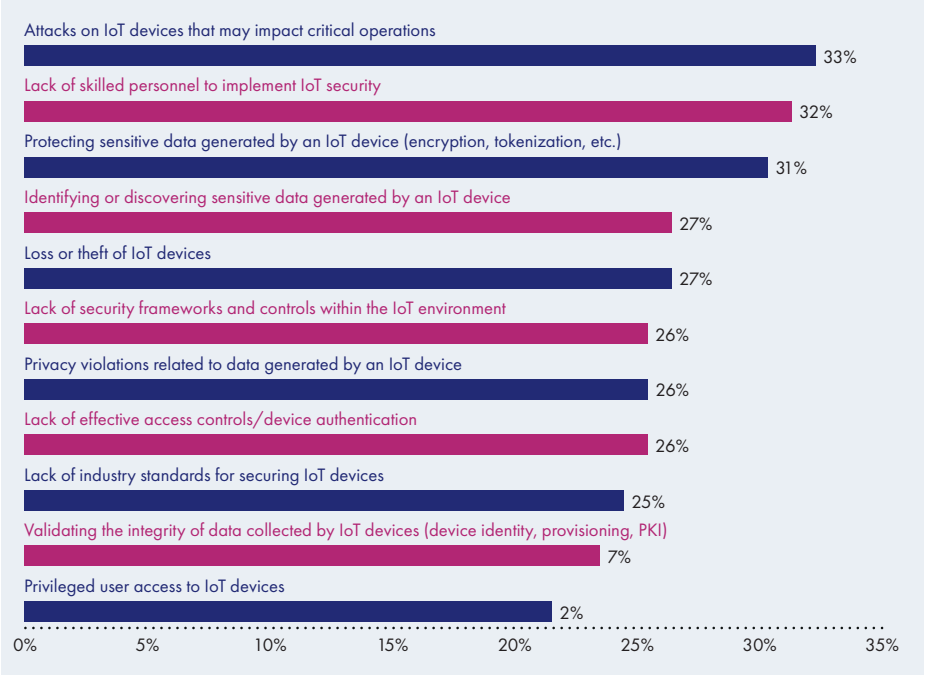
Figure 22 – Big Data Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Leading methods to alleviate big data security concerns include stronger authentication and data encryption or tokenization. Though stronger authentication and encryption are important to improve big data security generally, these measures do not directly alleviate the aforementioned report security and data quality concerns. Additionally, discovery and classification of sensitive data ranked low as a big data security solution.

Internet of Things Security Concerns

Top IoT security concerns from the 99% percent of respondents who have an IoT data security concern include device attacks, lack of skilled personnel, and encryption/tokenization. In addition, identifying and discovering sensitive data generated by an IoT device was fourth among critical concerns at 27% (see Figure 23). Digital identity authentication, data encryption, and anti-malware are appropriate responses to address the top IoT security concerns. As IoT devices are deployed, key management is increasingly important to effectively implement identity security and data encryption on IoT devices.



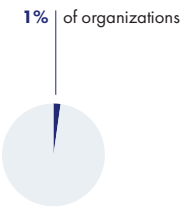


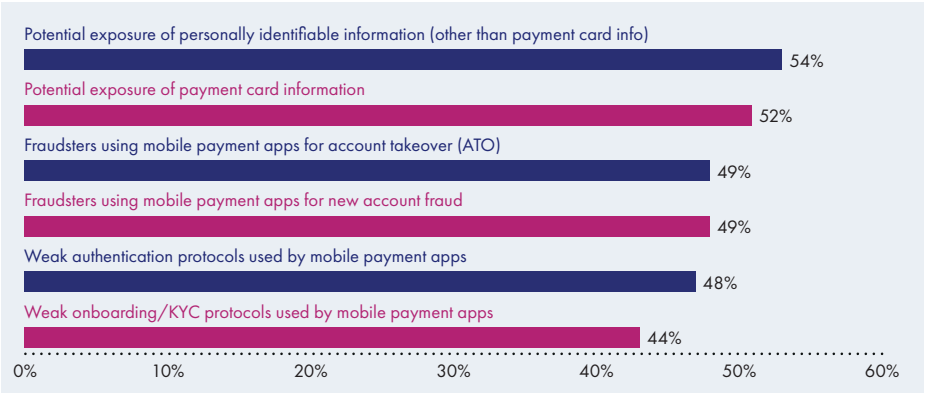
Figure 23 – Internet of Things Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

"As IoT devices are deployed, key management is increasingly important to effectively implement identity security and data encryption on IoT devices."

Mobile Payments Security Concerns

Ninety-nine percent of respondents have at least some data security concerns with mobile payments. Exposure of personally identifiable information (PII) and payment card exposure are top concerns (see Figure 24). Many wide-ranging solutions are considered to address mobile payment security. Chief among them are account data encryption, password controls, secure/encrypted wireless network protocols, and lock screens.



1% of organizations not concerned about data security of mobile payments applications

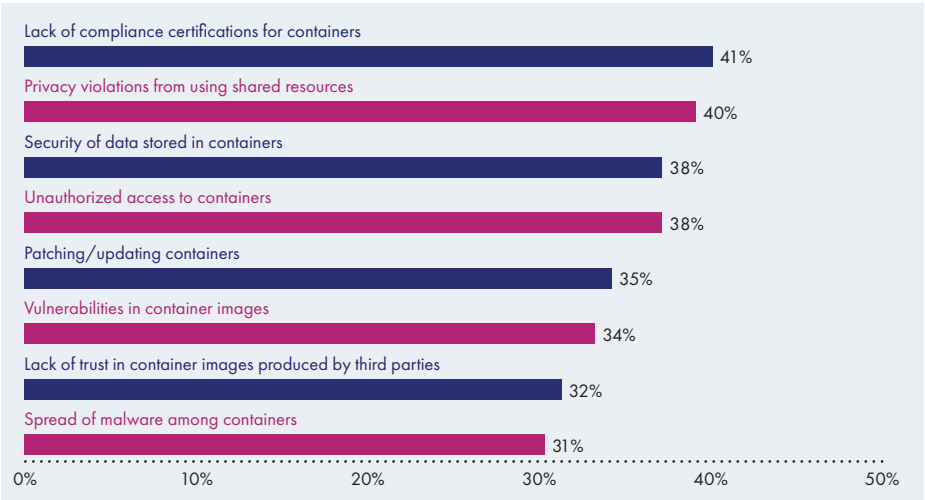
Figure 24 – Mobile Payments Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Container Security Concerns

Given the relative lack of maturity of container-related security technologies, organizations are concerned about many different issues as they continue to better understand containers and container security, though 96% express some data security concern with containers. Lack of compliance certifications and privacy violations lead the list, followed by security of data stored in containers, and unauthorized container access (see Figure 25). Encryption, anti-malware, and digital signatures are important solutions for organizations to employ as understanding of containers develops.

> "Encryption, anti-malware, and digital signatures are important solutions for organizations to employ as understanding of containers develops."



4% of organizations not concerned about data security of container environments

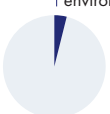
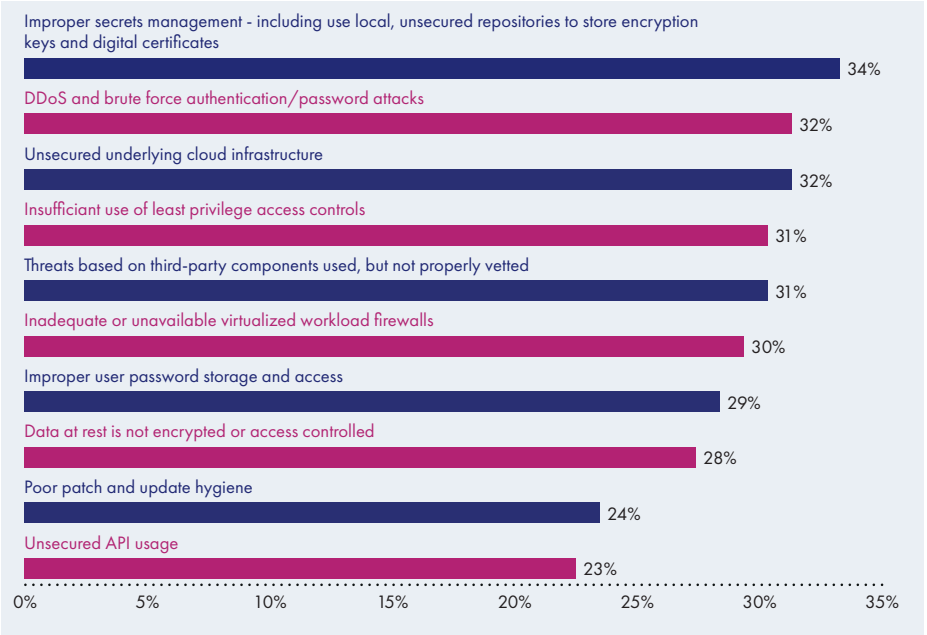


Figure 25 – Containers/Docker Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

DevOps Security Concerns

When it comes to DevOps, 98% of respondents are concerned about data security of their DevOps environment. Organizations are most concerned about improper key and certificate storage practices. This concern further speaks to the importance of key management and the use of hardware security modules. Other top DevOps security concerns are exposure to external DDoS threats and general cloud infrastructure security within the DevOps environments (see Figure 26). Poor patch and update hygiene and unsecure API usage ranked surprisingly low, possibly implying that responsibility for these issues falls on production and not dev. Many different approaches are being considered to alleviate DevOps security concerns, led by continuous production environment security procedures, encryption, tokenization, and ongoing education of DevOps teams.



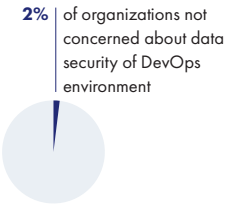


Figure 26 – DevOps Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

04 Data Security by Industry

The Approach to Data Security Depends on the Industry

The 2020 Thales Data Threat Report also explored how different industry verticals perceive and address data security. Government, financial services, healthcare, and retail sectors embrace digital transformation in varying degrees as well as the security challenges that come with it.

Organizations in each vertical reported somewhat different stances in their DX journey. Interestingly, federal government organizations viewed themselves as most advanced, with 49% of government respondents reporting that their organizations are either aggressively disrupting the markets they participate in or are embedding digital capabilities that enable greater enterprise agility. Healthcare followed closely at 47%, retail at 45%, and financial services at 30%.

Industries that are more Digitally Determined may have greater threat exposure. Fifty-four percent of financial services respondents experienced a data breach or failed compliance audit this year, followed by government at 52%, retail at 49%, and healthcare at just 37%. Industries that are more Digitally Determined often have increased regulatory compliance and data security requirements, which are also driving DX. In some cases, government agencies are driven to comply with certain goals or system upgrades that might be required via special bills or spending packages. While government is sometimes a laggard in DX spending, such laws can help accelerate transitions. For example, in the U.S., government agencies have been under great pressure to close older datacenters and move applications to the cloud and virtualized servers.

The challenge for organizations in different industries increases as they store more of their data in cloud environments. Ninety-nine percent of financial services organizations store data in the cloud. Ninety-eight percent of retail and healthcare, and 97% of government organizations, store data in the cloud respectively (see Figure 27).

98%

of respondents are concerned about data security of their DevOps environment.

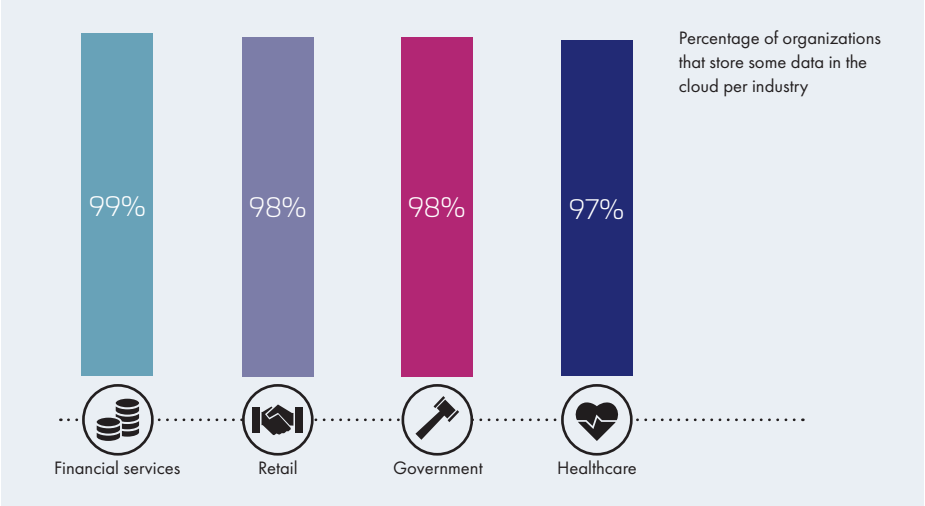


Figure 27 – Data in the Cloud by Industry

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

More importantly, much of that cloud data is sensitive. An estimated 51% of data in the cloud is sensitive for the financial services industry and 50% for the healthcare industry. Government and retail have slightly lower rates of sensitive data in the cloud with an estimated 47% and 44%, respectively (see Figure 28).

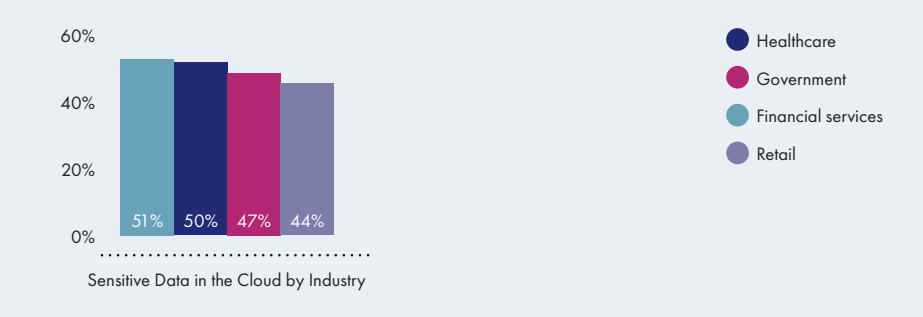


Figure 28 – Sensitive Data in the Cloud by Industry

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Organizations are spending more money on data security, with financial services increasing the most at 55%, followed by retail, government, and healthcare (see Figure 29). The average percentage of security budget assigned to data security differs by industry, led by financial services at 16.1%. Healthcare has the second highest data security percentage at 15.9%, followed by government at 15.2% and retail at 15.0%.

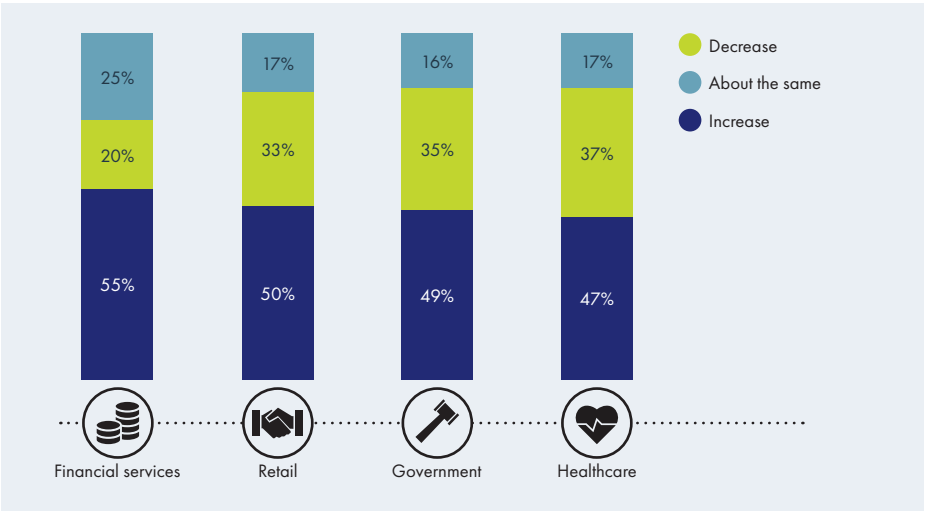


Figure 29 – Data Security Spend by Industry

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

55%

Organizations are spending more money on data security, with financial services increasing the most at 55%

The disconnect between perception of data security versus reality extends across industries.

For the public sector, keep in mind that some types of security are built into other solutions and thus may not be tracked as pure security spending. For example, network monitoring, configuration management, control of available server ports, and so forth are important to a robust agency security posture. But many agencies don't track these as part of their security budget. We also see investments targeted at improved security for government apps, software and connected services, followed by IoT management and mobile management.

Retail companies feel most secure with their new technology deployments, with 71% of that sector's respondents feeling very or extremely secure. Financial services firms are also feeling very or extremely secure at 70% (see Figure 30).

Figure 30 – Very/Extremely Secure New Deployments by Industry
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "The realities of data security and encryption don't get any easier. Industries must also prepare for the impact quantum computing may have on their data security on the near horizon."

As with the global sample, industry respondents are not concerned enough about the issues creating the most risk. Encryption and tokenization rates across all industries remain low.

While network security has long been a core focus for government agencies, now agencies are putting an equal amount of effort into data security and application security. Yet implementing multifaceted approaches to security isn't easy. Agencies require tools to help them manage greater amounts of complexity, including those capable of spanning legacy on-premise needs as well as modern, cloud-based, edge technology-oriented technologies with solutions like encryption and tokenization. As edge computing and edge-based AI grows, this complexity will only increase.

Retail companies have the lowest rate of encryption of sensitive data at 54%, meaning 46% of sensitive data is not protected by any encryption. Likewise, only 45% of retailers protect sensitive data with tokenization. Healthcare organizations use the highest level of encryption and tokenization of sensitive data (59% and 49% respectively), though these levels are also considered low (see Figure 31).

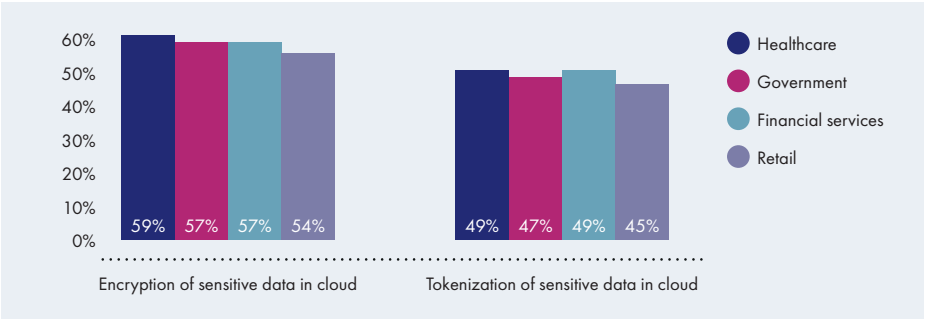
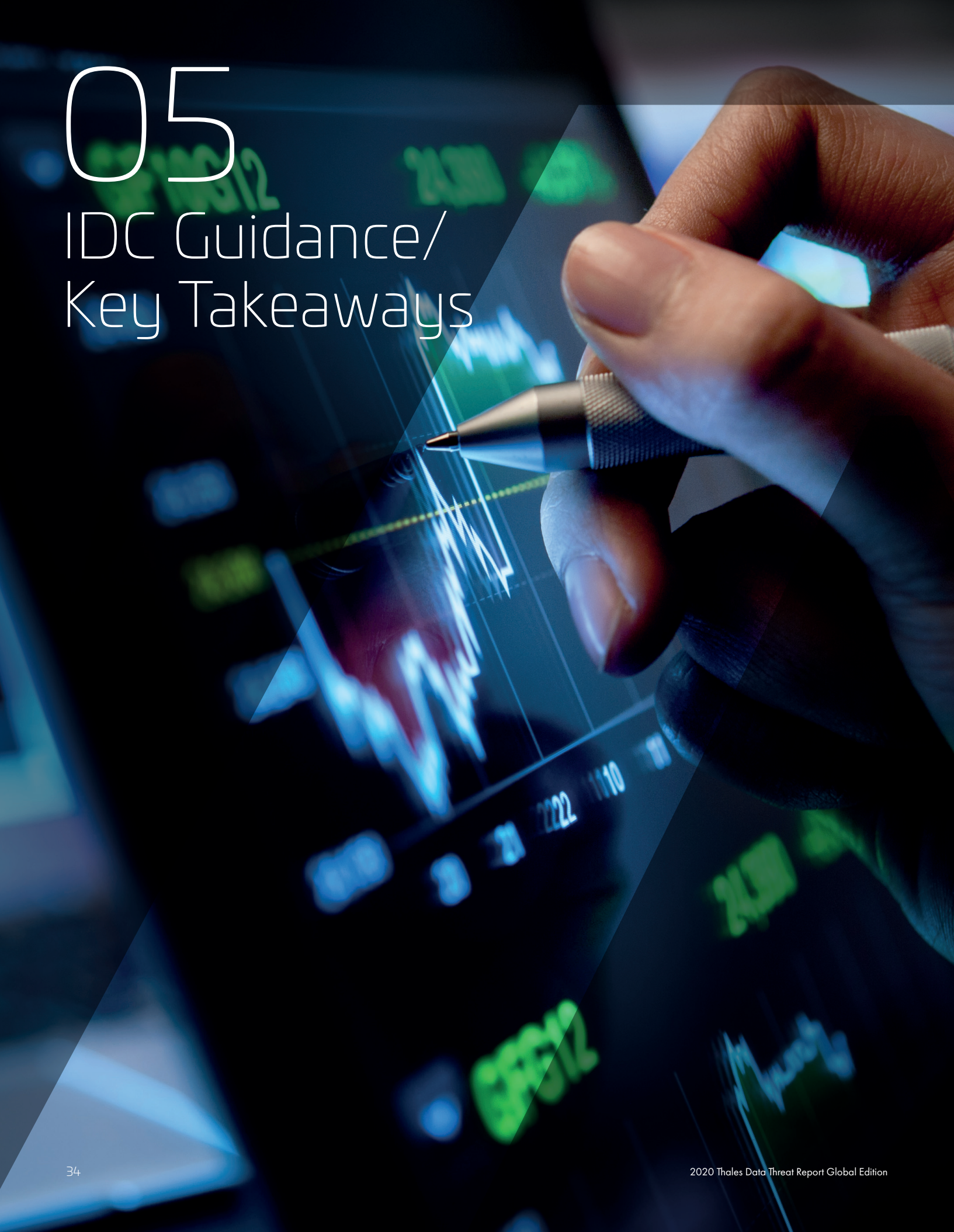


Figure 31 – Security of Sensitive Data in the Cloud by Industry
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

The realities of data security and encryption don't get any easier. Industries must also prepare for the impact quantum computing may have on their data security on the near horizon.

Within 1-5 years, 77% of financial services firms expect quantum cryptography to impact them, followed by retail at 75%, and healthcare and government at 73%. Industries are concerned quantum computing will create exposure for sensitive data. Financial services firms are most concerned, with 94% expressing concern about quantum computing's potential for creating data exposure, with 46% as very or extremely concerned. Ninety-two percent of government organizations are concerned, followed by retail at 90% and healthcare at 88%.

05 IDC Guidance/ Key Takeaways



Organizations Must Implement Smarter Approaches to Data Security

Invest in modern, hybrid and multicloud-based data security tools that make the shared responsibility model work. Sensitive data is being stored in the cloud. Organizations should focus on solutions that can simplify the data security landscape and reduce complexity across multiple clouds, legacy environments, and modern, digital transformation technologies. The shared responsibility model reminds organizations that they cannot rely on service providers for data security measures. Companies must in addition consider all the data security elements directly in their control, like identity, encryption (both at transit and at rest), key management, tokenization, and data loss prevention.

Consider a zero trust model to secure data. Organizations still focus on network security as they aim to control access. Data security goes beyond the traditional edge, whether it's in the cloud, virtual environments, datacenters, or other DX technologies. These data environments require a more persistent, zero trust model that does not abdicate data security as someone else's problem but forces organizations to implement least privileged access to data. By reducing the attack surface and hardening data access using approaches such as encryption of data at rest, sensitive data is protected from not only external actors but also from malicious insiders, drastically reducing the internal threat risk. Note, 82% of respondents felt vulnerable to external threats to their data; 67% respondents felt vulnerable to internal threats. Both threat vectors must be addressed.

Increase focus on data discovery solutions and centralization of key management to strengthen data security. Data security concerns evolve as the edge expands with greater adoption of big data environments, IoT devices, mobile payments, containers, and DevOps environments. Greater emphasis on sensitive data discovery in these environments, as well as for existing environments, strengthens the data security stance by identifying where sensitive data is and how to access it. Additionally, encrypting sensitive data is critical, and organizations must proactively manage key management to help simplify encryption in otherwise complex environments. For cloud environments where native encryption is enabled, bring your own key APIs should also be used to maintain responsibility and control of the data.

Quantum computing's impact on cryptography is on the horizon. Data security does not get any easier as the power of quantum computing exposes sensitive data sooner rather than later. Organizations must begin planning their infrastructure and key management adjustments to counter fundamental changes to cryptography brought on by quantum computing. When making new infrastructure investments,
be sure they offer crypto agility and will support the new NIST standards as they become available.

Focus on the right threat vectors. Yes, bad actors are evolving their methods daily. Security professionals must continually evolve in response. Be careful of overprovisioning quantity and breadth of accounts both internally and externally with service providers and contractors.

Data security solutions, especially encryption, are critical to remain vigilant against the reality of today's data risk. Even as CSOs and CISOs shift their focus and budgets from traditional network security to data, apps, and identity, they cannot become overconfident by assuming they are less vulnerable. Organizations must evolve data security measures to protect today's IT landscape as data migrates away from the enterprise premise to the cloud. This modern evolution is grounded in encryption.

Rapid cloud adoption has diminished the effectiveness of on-premises-centric content protection measures. Our data lives in the cloud; thus, the multicloud reality has stoked the growth of location agnostic, SaaS-based content security. For government agencies especially, on-premises-centric security solutions are no longer a viable option to protect cloud-based, modern enterprises and applications. The result is complexity. Although selecting solutions that are appropriate to each new cloud environment is a better approach, the complexity problem would be address with point product complexity. Creating a cohesive multiload, multi-environment data security approach that protects data regardless of where it lives or where it may go is clearly a best practice. As you implement such a platform, much like a parent asks about the there kids after dark, make sure you can "yes" to the question, "Do you know where your keys are?"

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <

thalesesecurity.com/DTR

#2020DataThreat