cpl.thalesgroup.com #2020DataThreat

THALES

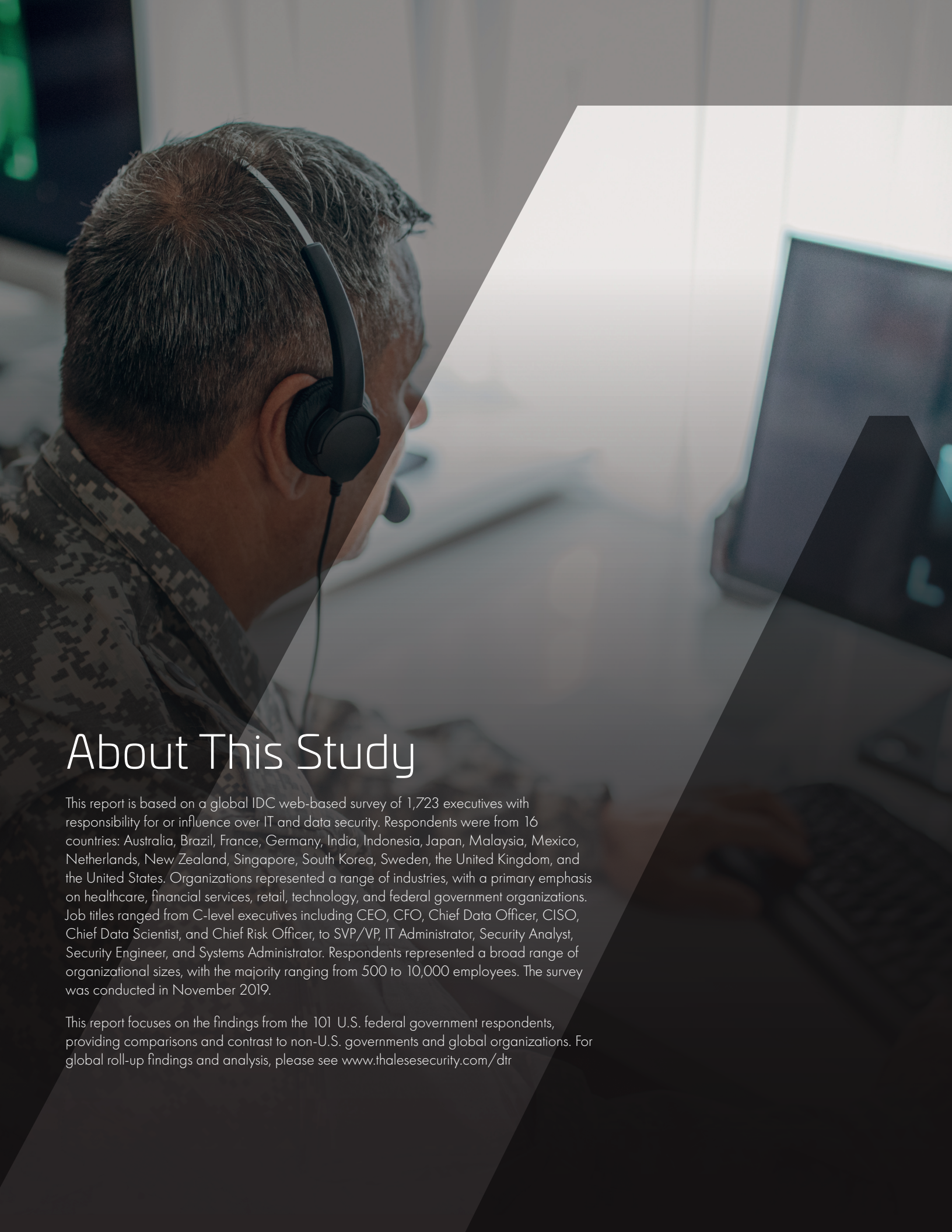
# Federal Government Looks to Zero Trust Approach to Data Security

# 2020 Thales Data Threat Report

## Federal 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 organizations. 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.

This report focuses on the findings from the 101 U.S. federal government respondents, providing comparisons and contrast to non-U.S. governments and global organizations. For global roll-up findings and analysis, please see www.thalesesecurity.com/dtr

# Contents



## Our sponsors are:

carahsoft. SENETAS KEYFACTOR OASIS Open standards. Open source. CSA cloud security alliance® FIRST TECH Ti Safe PURESTORAGE®

# Executive Summary

Governments continue to expand use of a wide variety of technologies, including cloud, mobile, and the Internet of Things (IoT) to transform their operations and improve constituent services, while creating efficiencies that allow them to do more with fewer taxpayer funds. IDC research shows that this digital transformation (DX) is well underway, with 68% of U.S. federal government agencies in our study saying they are either aggressively disrupting the services they provide or embedding digital capabilities that enable greater organizational agility. The difference between U.S. federal government opinions and those of their international peers is striking. The U.S. federal government views itself as a DX leader relative to the rest of the world, with only 30% of non-U.S. government organizations surveyed identifying as either aggressively disrupting their markets or embedding digital capabilities; among the sample of global organizations surveyed the number is 43%.

While DX can provide tremendous value, it also makes data security more complex. In the past, the trend was for organizations to focus on the network perimeter first, with the idea that a strong perimeter protected the IT infrastructure behind it. But as we know, the perimeter is increasingly permeable, or even non-existent with the rapid adoption of cloud and increasing amounts of sensitive data stored in the edge. We are at an inflection point with the cloud as 54% of all U.S. federal government data is now stored in cloud environments, and 51% of that data is sensitive. Additionally, most government organizations rely on multicloud environments. All of this adds up to today's data environments becoming increasingly complex; this complexity and its impact on performance and processes are top barriers to data security.

Agency beliefs are incongruent with the reality painted by survey results. Of U.S. federal government respondents in the study, 71% believe they are very secure, but agencies are not sufficiently 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 government organizations incorrectly look to their cloud providers to implement data security measures for the portion of the shared responsibility model that is owned by the government organizations themselves.

**68%**

of U.S. federal government agencies in our study say they are either aggressively disrupting the services they provide or embedding digital capabilities that enable greater organizational agility.

When it comes to overall investments in security, data security still represents a small proportional share of overall security budget for U.S. federal government agencies, though the rate is higher than their global government peers. Fifty-six percent of U.S. federal government agencies plan to increase data security spending in the next 12 months, a similar amount as last year. But these organizations still focus a disproportion of their spend on network security, as 34% of respondents' focus is on data security, yet data security averages just over 17% of overall IT security budget.

Numbers aside, it's worth noting that not all security-related work falls under the heading of security spending. Activities such as configuration management, network monitoring and management, and even disk imaging for new PCs or servers all can have a security element to them as proper configuration addresses vulnerabilities.

As we assess looming threats, quantum computing is on the horizon and promises to further complicate data security. Cryptography requirements will fundamentally change when quantum computing comes online, and 78% of U.S. federal government respondents see quantum cryptography affecting their organization in the next five years. A larger looming issue is that the power of quantum computing could make it easier for malicious actors to neutralize the crypto ciphers related to public key infrastructure or blockchains. The National Institute of Standards (NIST) and the Department of Defense (DoD) have multiple initiatives and research projects underway to help address these challenges.

As government agencies face expanding and more complex data security challenges, they need to invest budget and resources to continue to elevate their data security posture and evolve security policies to accommodate for digital transformation, cloud, and other disruptive innovative technologies. Government IT security teams need to take a multilayered approach to data security, from embracing cloud shared security responsibilities and adopting a zero trust access and data protection approach to data security that authenticates and validates 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, yet data security averages just over 17% of overall IT security budget.

**78%**

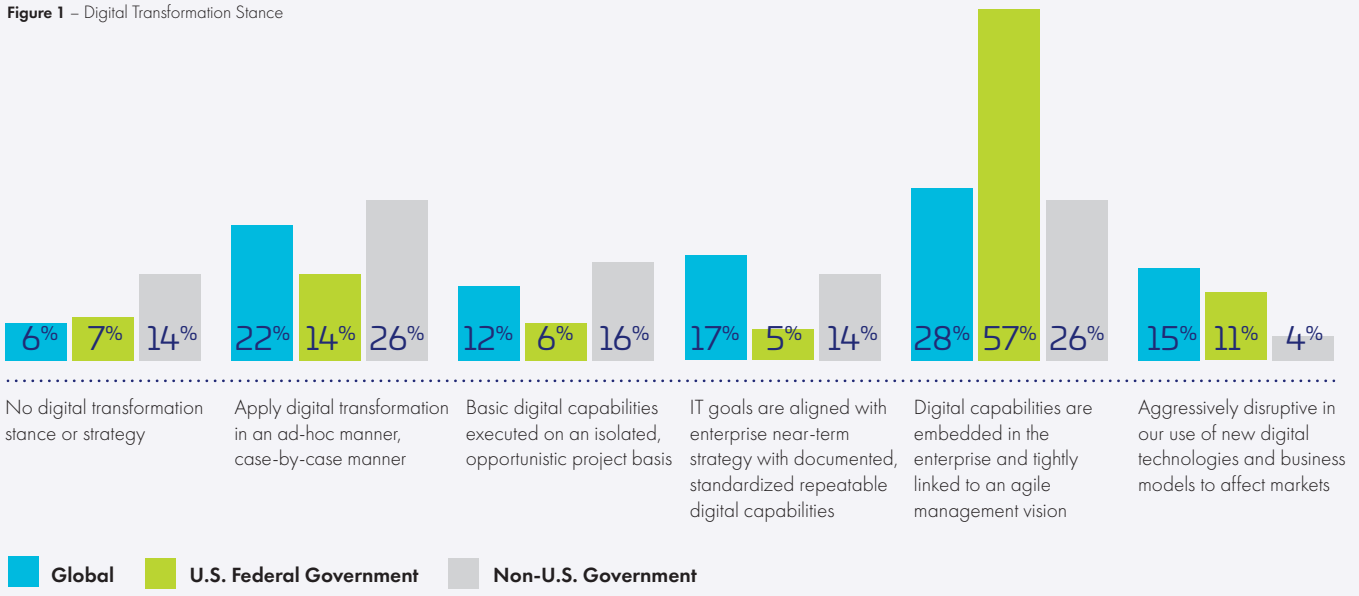
of U.S. federal government respondents see quantum cryptography affecting their organization in the next five years.

# 01
# Key Findings

# Digital Transformation Is Complicating Data Security

Digital transformation is enabling new and transformative ways for government organizations to provide constituent services, and to drive greater operational efficiencies so they can do more with fewer taxpayer dollars. U.S. federal government agencies are taking advantage of digital technologies like cloud, mobile, and IoT to digitally transform their operations. In particular, the DoD, the Department of Energy, the National Aeronautics and Space Administration (NASA), and the Justice Department have particularly sprawling IT architectures.

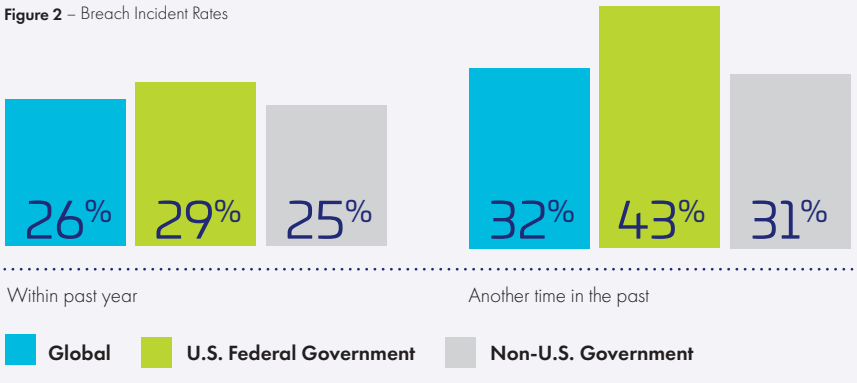
**Figure 1** – Digital Transformation Stance




Sixty-eight percent of U.S. federal government respondents 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). By comparison, the U.S. federal government views itself as a DX leader relative to the rest of the world, with only 30% of non-U.S. government organizations surveyed identifying as either aggressively disrupting their markets or embedding digital capabilities, while 43% of the global sample identifying as DX leaders.

But no organization is immune from data security threats, and despite its self-reported DX leadership, the U.S. federal government is no exception. In fact, U.S. federal agencies have been breached at higher rates than the global sample, with 29% of U.S. federal government agencies reporting that they have been breached in the past year (see Figure 2). Fifty-five percent have been breached at any point in the past, and 29% have failed a compliance audit in the past year.

**Figure 2** – Breach Incident Rates




**29%**

of U.S. federal government agencies report that they have been breached in the past year, a higher rate than the global sample and 29% have failed a compliance audit in the past year.

DX transformation positively correlates to data vulnerability: The more digitally transformed an organization, the more likely that it has experienced a data breach. Digitally Determined organizations (those organizations making the strategic, organizational, technological, and financial decisions that will set them up to digitally transform their organization 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 have been breached. Less sophisticated companies may have less exposure or may have been breached without knowing it.

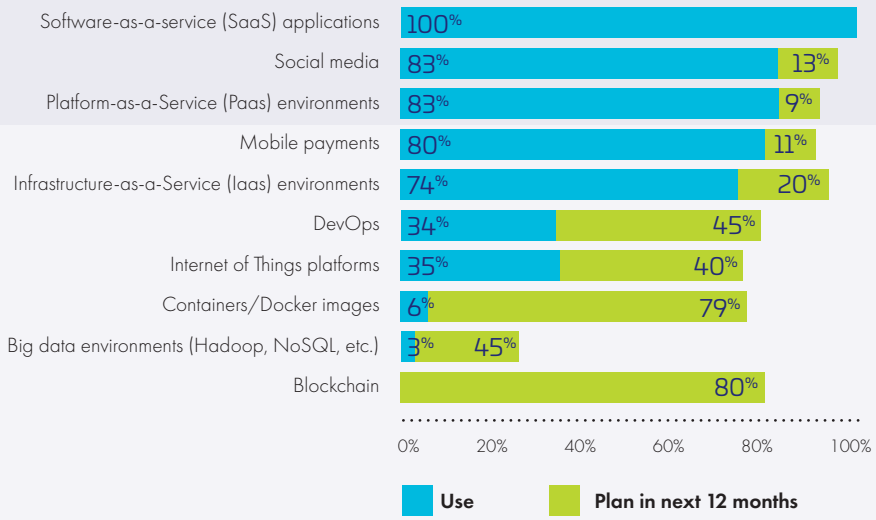
> "The more digitally transformed an organization, the more likely that it has experienced a data breach."

IDC has noticed that security spending has two faces in government agencies. The DoD, Homeland Security and the Department of Energy are usually sufficiently funded to address their cybersecurity priorities. Other agencies can find themselves challenged. Smaller agencies need assistance in strategically and creatively addressing new DX-related security challenges.

## Government Organizations Are Housing Sensitive Data Across a Broad Range of Technologies

U.S. federal government agencies are adopting a wide range of 3rd Platform technologies, which include cloud, mobile, social, big data, and Internet of Things. All U.S. federal government respondents in our survey have adopted SaaS applications, up from 78% in 2018 (see Figure 3). Social media, PaaS and IaaS cloud environments, and mobile payments also lead planned adoption. Note that many of these technologies, such as IoT and mobile, are edge technologies, which reinforces the message that data exposure is expanding well beyond the traditional network perimeter.

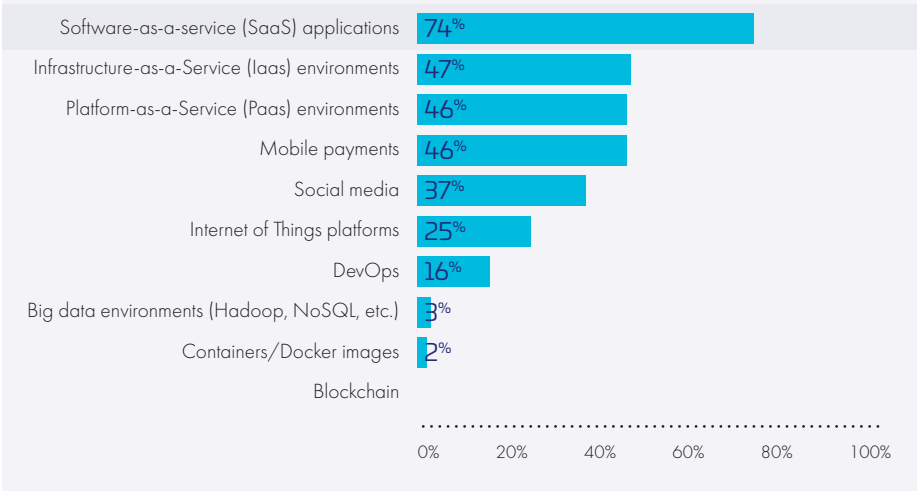
**Figure 3** – Technology Adoption Levels – U.S. Federal Government Agencies




Likewise, many government agencies are housing sensitive or regulated data in a similarly broad set of technologies. Seventy-four percent of U.S. federal government agencies store sensitive data in SaaS applications, 47% store data in IaaS, and 46% store data in PaaS environments. One hundred percent of U.S. federal government agencies say they are storing sensitive data in at least one of the technologies in our survey (see Figure 4).

> "Seventy-four percent of U.S. federal government agencies store sensitive data in SaaS applications, 47% store data in IaaS, and 46% store data in PaaS environments."

**Figure 4** – Technology Environments Used to Store Sensitive/Regulated Data – U.S. Federal Government Agencies



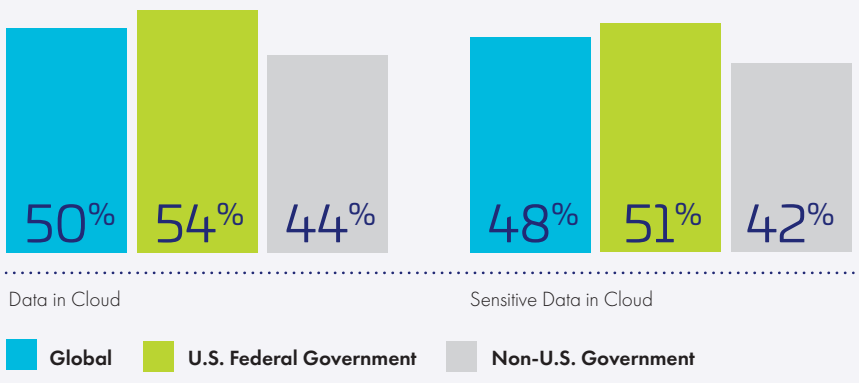

> "Today's strategy requires a least privileged, continuous validation and verification approach, reinforced with data security measures such as encryption or tokenization."

As government agencies expand their usage of 3rd Platform cloud, mobile, social, big data and IoT technologies and, thus, potentially make sensitive data increasingly vulnerable, securing the perimeter does little to protect off-premise data which speaks to the need to take a zero trust approach to data security. This zero trust approach eliminates the binary trust/don't trust approach of yesterday's on-premise, perimeter-centric reality. Today's strategy requires a least privileged, continuous validation and verification approach, reinforced with data security measures such as encryption or tokenization in the event that zero trust fails to prevent miscreants from accessing privileged data.

## Clouds Now House the Majority of Data, Creating Significant Risk

One hundred percent of U.S. federal government respondents surveyed have some sensitive data in the cloud. More importantly, data stored in the cloud has reached an inflection point with our study saying that globally an estimated 50% of data is in the cloud, with U.S. federal government organizations even further ahead at 54%. More importantly, U.S. federal government respondents say that an estimated 51% of that data in the cloud is sensitive. (see Figure 5).

**Figure 5** – Sensitive Data Stored in Cloud Environments

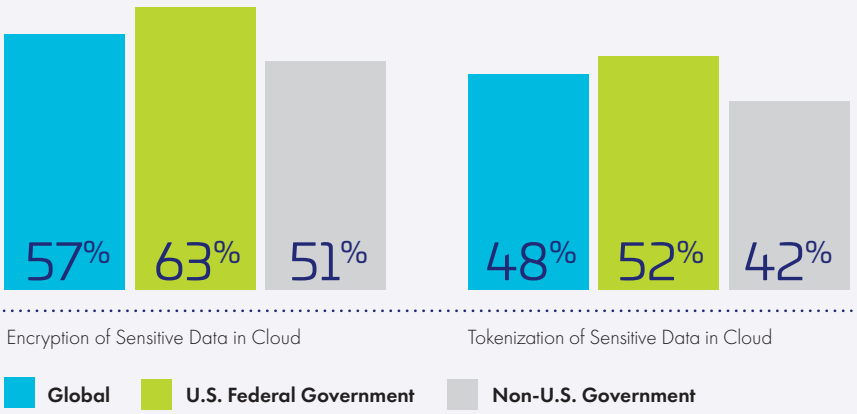


As more sensitive data is stored in cloud environments, data security risks increase. Yet, despite this significant amount of sensitive data exposure, rates of data encryption and tokenization are low. In fact, 99% of U.S. federal government respondents say at least some of their sensitive data in the cloud is not encrypted. We did find that in the U.S. federal government, encryption and tokenization are used to protect sensitive data in the cloud at higher rates than global respondents. Even so, only 63% of sensitive data stored in cloud environments is protected by encryption and slightly more than half – 52% – is protected by tokenization.

**99%**

of U.S. federal government respondents say at least some of their sensitive data in the cloud is not encrypted.

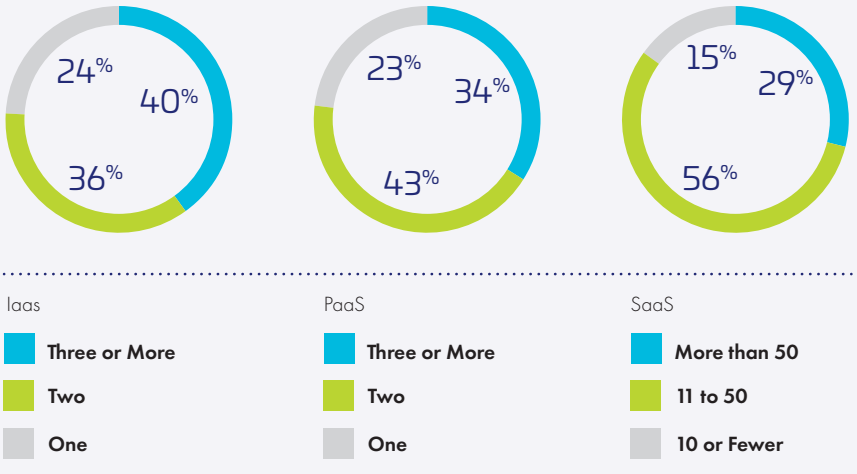
**Figure 6** – Security of Sensitive Cloud Data




## Complexity of Data Environments 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 has become increasingly common. Agencies are using multiple IaaS and PaaS environments, as well as hundreds of SaaS applications. Seventy-six percent of U.S. federal government agencies are using more than one IaaS vendor, 77% have more than one PaaS vendor, and 29% have more than 50 SaaS applications to manage (see Figure 7).

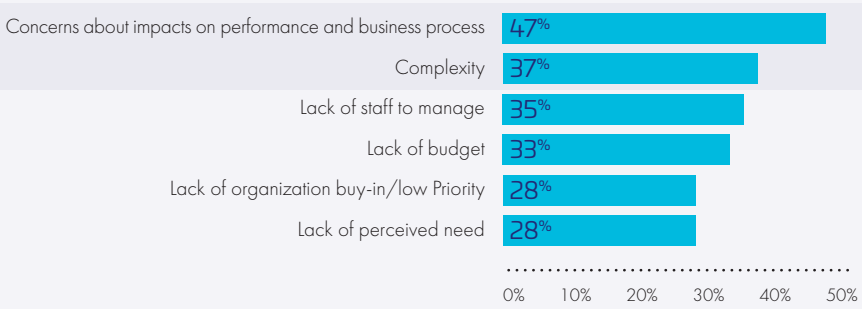
**Figure 7** – Number of Cloud Environments in U.S. Federal Government Agencies



The resulting complexity, including orchestrating independent key management solutions across a multicloud environment, is making life more difficult for security professionals and puts pressure on organizational processes and performance. Additionally, as cybersecurity threats have proliferated and computer technology has advanced, government data security compliance has become increasingly complex. The government mandates encryption, and major government security compliance regulations such as FISMA, NIST 800-53, FIPS (up to level 3), and Common Criteria need to be part of the any government data-security solution. And, as data moves to the cloud, government agencies need to comply with FedRAMP. Finally, depending on the government agency, HIPAA-HITECH and PCI DSS may also be important. It is no wonder that U.S. federal government respondents rate concerns about the impact data security has on performance and complexity as their top perceived barriers to implementing data security (see Figure 8).

> "U.S. federal government respondents rate concerns about the impact data security has on performance and complexity as their top perceived barriers to implementing data security."

**Figure 8** – Barriers to Implementing Data Security in U.S. Federal Government Agencies

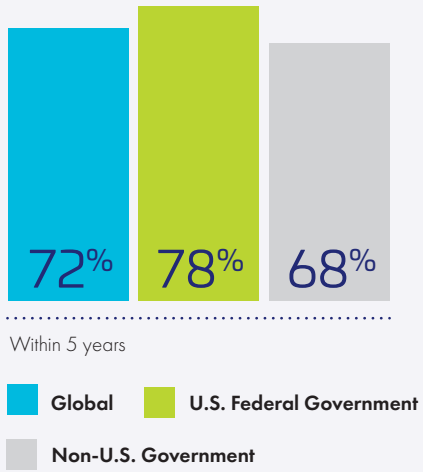



## Quantum Computing Data Security Concerns Are on the Horizon for Government Agencies

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 on the horizon as 78% of U.S. federal government agencies see it affecting their cryptographic operations in the next five years (see Figure 9). Ninety-four percent of these respondents are concerned quantum computing will create exposures for sensitive data, with 41% very/extremely concerned.

> "Ninety-four percent of these respondents are concerned quantum computing will create exposures for sensitive data, with 41% very/extremely concerned."

**Figure 9** – Quantum Cryptography to Affect Organizations

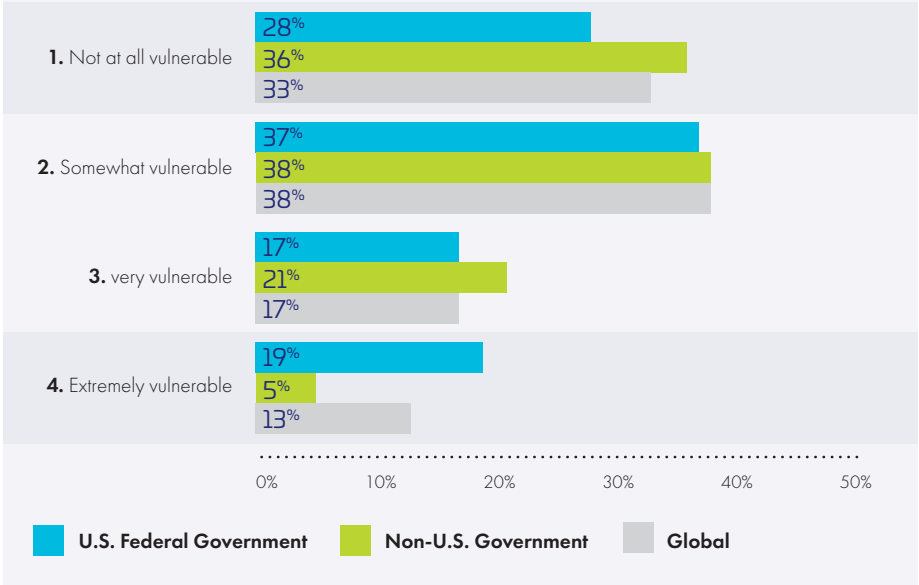


Top plans for U.S. federal government agencies to offset quantum computing threats are switching away from symmetric cryptography (42%), key management that supports quantum safe random number generators (37%), and the hybrid approach of a classic algorithm with a post-quantum one (36%). But many organizations are uncertain how to respond even though threats may surface within the next five years, represented by 13% of these respondents who plan to air gap critical systems and 6% who have no plans at all.

## Government Agencies Have a Greater Sense of Data Security Than Other Organizations

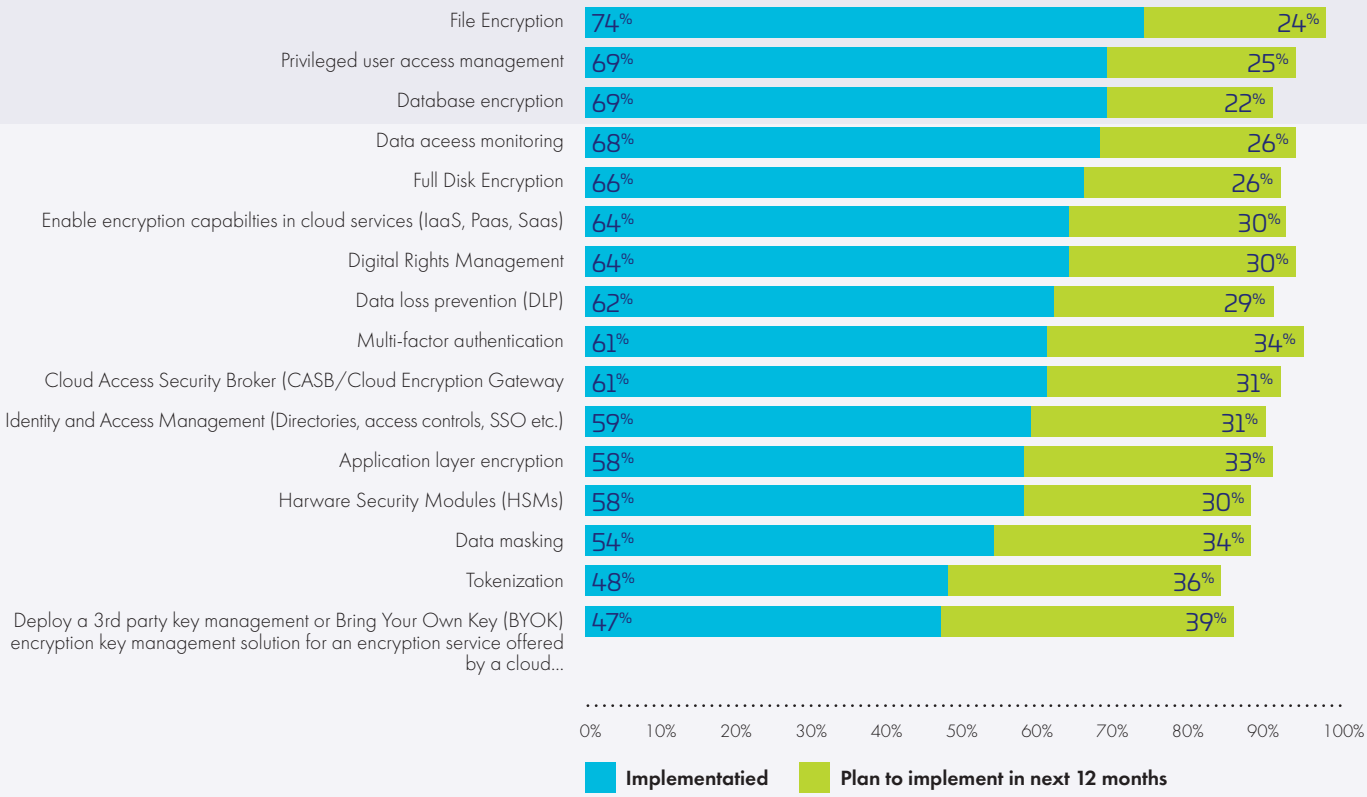
Despite the pervasive and expanding threats to data security, enterprises globally feel less vulnerable in 2019 (67%) than they did in 2018 (86%). U.S federal government respondents feel less vulnerable as well, though to a lesser extent. Seventy-two percent of U.S. federal government organizations feel vulnerable in 2019, down from 82% in 2018, even as security risks grow. Yet, findings show U.S. federal government agencies have a greater perception of vulnerabilities to data security threats than other organizations with 19% feeling "extremely vulnerable" compared to just 5% of non-U.S. governments and 13% of global respondents (see Figure 10).

**Figure 10** – Vulnerability to Data Security Threats




Yet the behaviors of U.S. federal government respondents belie their greater sense of vulnerability. Seventy-four percent of U.S. federal government respondents implement file encryption (higher than the global sample at 61%) and 69% implement database encryption (higher than the global sample at 59%) (see Figure 11).

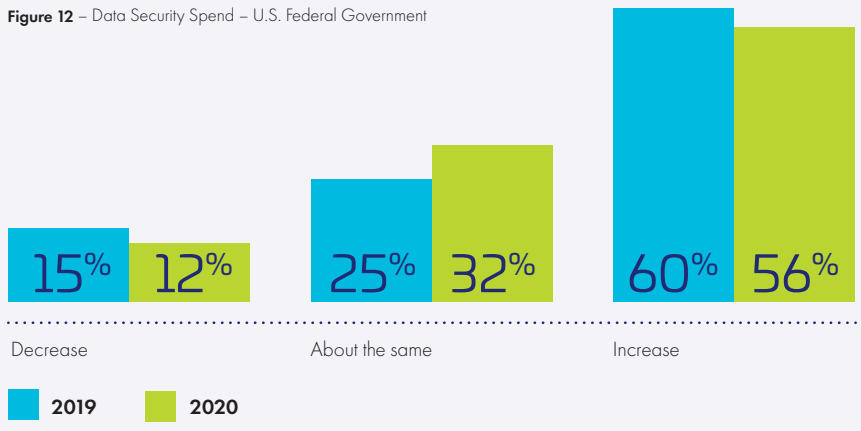
**Figure 11** – Implementation of Encryption and Data Security Tools – U.S Federal Government Agencies




## Security Spend of Federal Government Is Growing at Higher Rate Than the Global Total

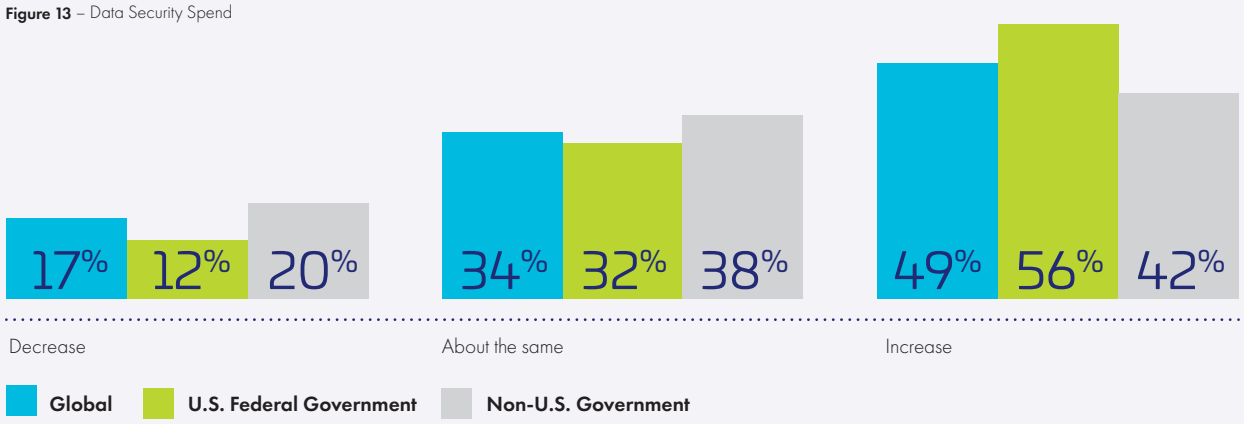
U.S federal government organizations plan to spend more money on data security in the upcoming year, at rates similar to last year. Fifty-six percent of respondents said they would be spending somewhat more or much more on data security in 12 months' time. But the number of U.S. federal government agencies whose data security budget is growing is down slightly, from 60% in the 2019 IDC survey (see Figure 12).

**Figure 12** – Data Security Spend – U.S. Federal Government



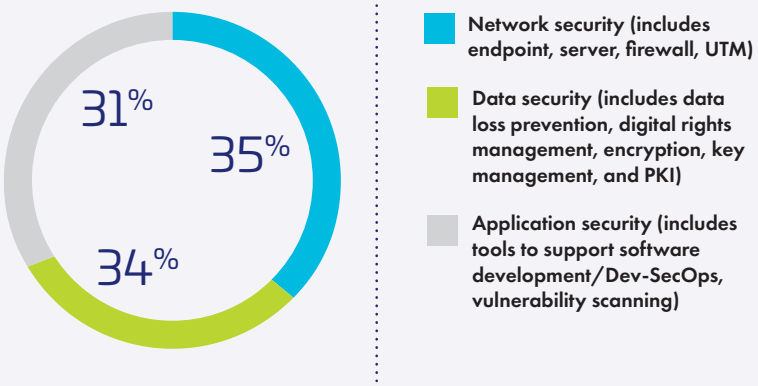
Additionally, U.S. federal government respondents see greater growth in 2020 data security budgets than non-U.S. governments (42%) and the global total (49%), with 56% increasing data security spending and only 12% decreasing data security spending (see Figure 13).

**Figure 13** – Data Security Spend




U.S. federal government agencies are still predominately focused on network security (35%), followed by data security (34%), and application security (31%) (see Figure 14). And while 34% of security focus is on data security, data security spending falls below that rate of attention as only 17.3% of U.S. federal government security budgets is spent on data security.

**Figure 14** – Proportion of Security Focus – U.S Federal Government Agencies




Further demonstrating a disconnect between security budgets and the focus of security departments, U.S. federal government respondents believe that malicious actors (cybercriminals and terrorists) that create data risk with intentional threat to do harm represent the greatest data security threats. Sixty percent are worried about cyberterrorists damaging or making the government look bad publicly, followed by industrial espionage (54%), hacktivists (51%), and cybercriminals (50%).

Interestingly, respondents are less concerned about day-to-day issues which may actually be a greater threat as seen by news coverage of attacks often perpetrated by insiders, infamously including Edward Snowden. These internal data threats are issues agencies have more control over, including privileged user access, integrator partners with internal access, and service provider accounts. Agencies 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 15 and 16).

"Agencies must be careful of overprovisioning quantity and breadth of accounts as the risk from contractors is often more about carelessness than malicious behavior."

**Figure 15** – Technology Environments Used to Store Sensitive/Regulated Data – U.S. Federal Government Agencies

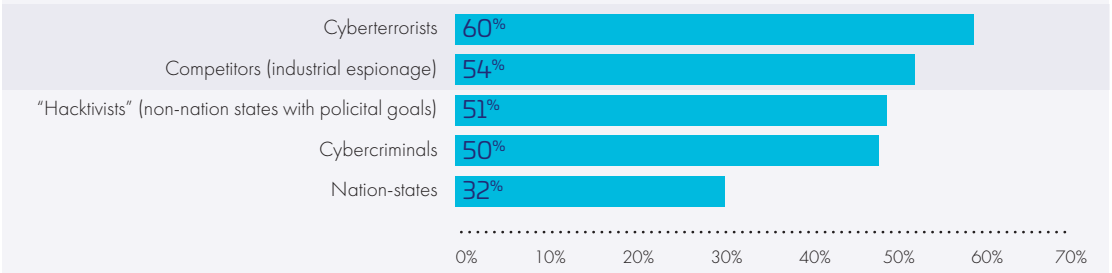
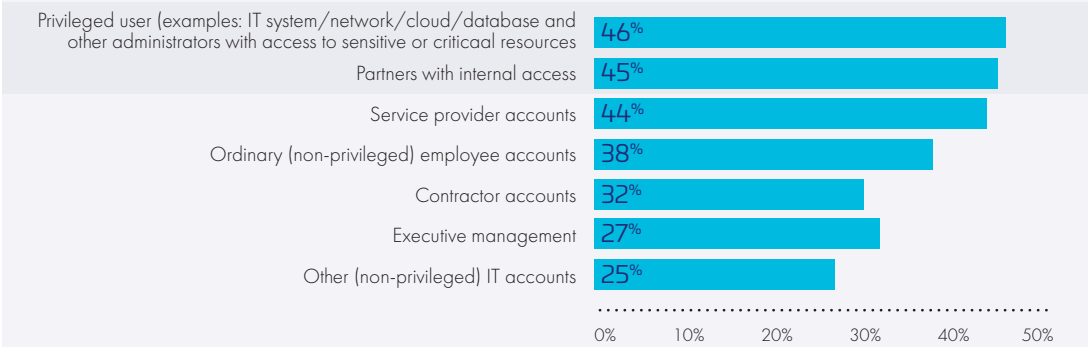



**Figure 16** – Internal Data Vectors of Vulnerability – U.S. Federal Government Agencies



# 02 Cloud Data Security Is at a Tipping Point

More than half of U.S federal government 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.

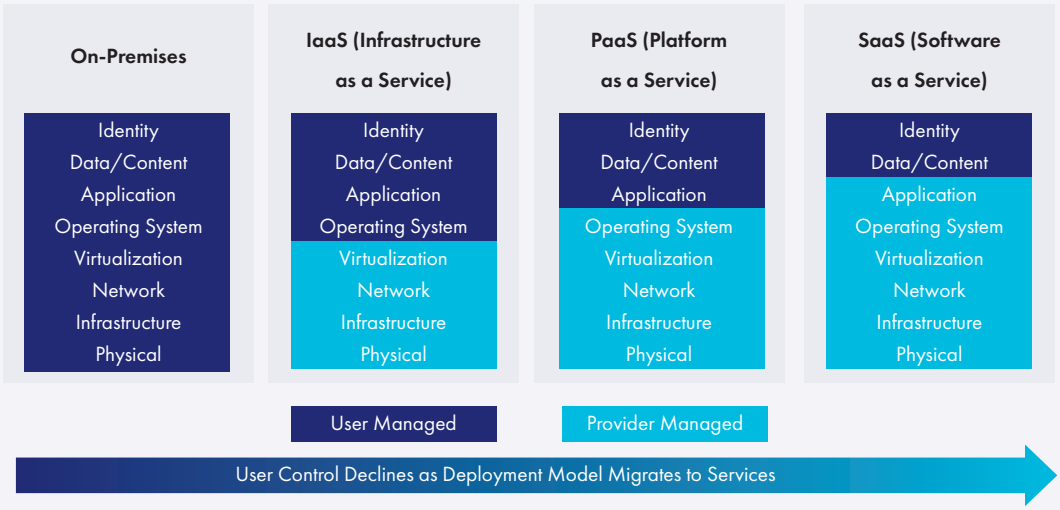
Government agencies are concerned about many data security issues regarding the cloud. Yet, U.S. federal government agencies are seemingly most concerned about issues owned by their cloud providers, like security breaches at the provider and privacy service level agreements (see Figure 17). Although valid, the real possibility of these issues happening are quite low. U.S. federal government respondents are seemingly less worried about issues over which they have direct control, and which represent greater potential vulnerabilities, like encryption key management.

> "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."

**Figure 17** – Cloud Security Concerns

This mismatch between threats respondents perceive and where they should actually focus their concern 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 can influence the security of its data (see Figure 18).

**Figure 18** – Shared Responsibility Model

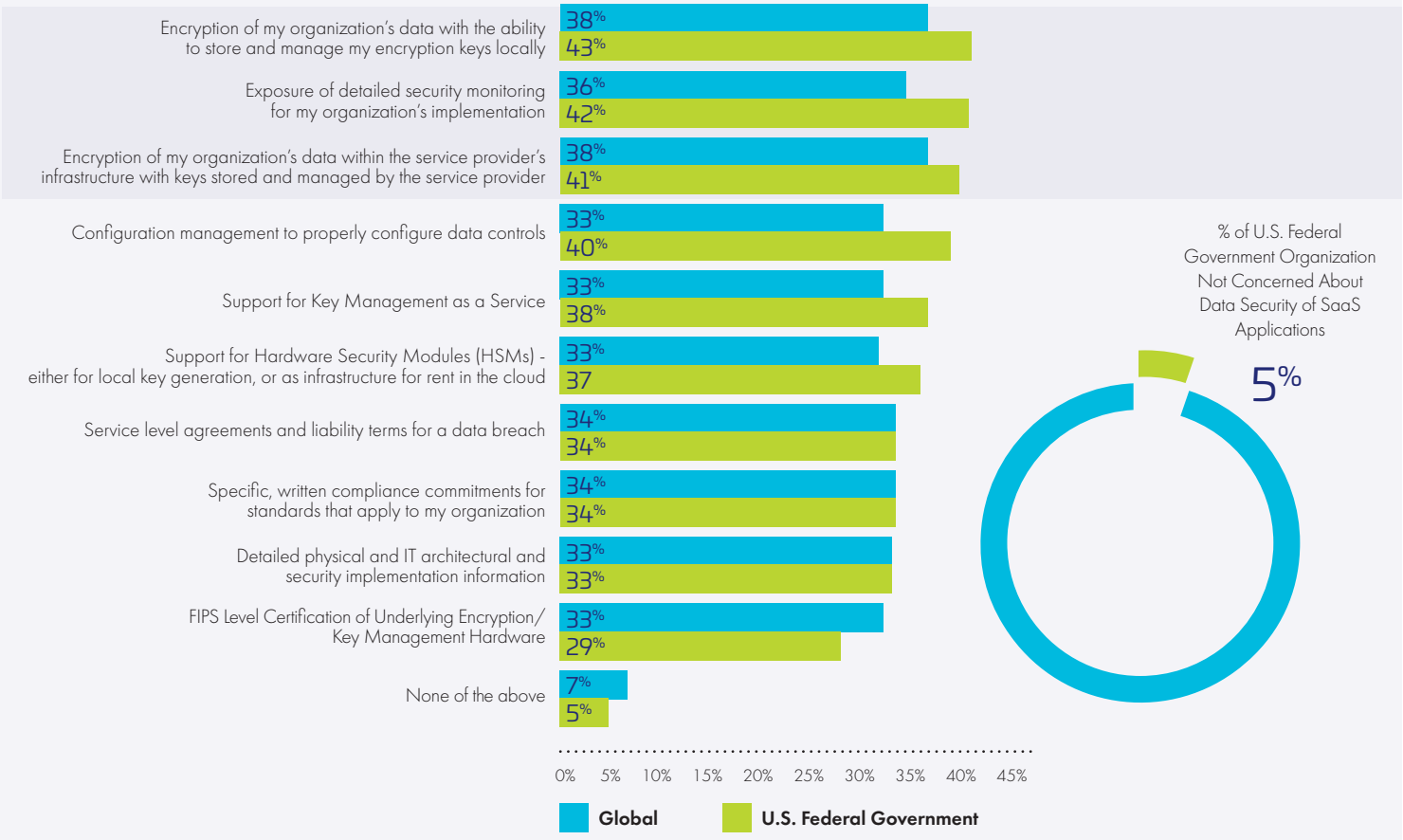


# Security Concerns Also Shift as Organizations Deploy More Data into SaaS, IaaS, and PaaS Environments

According to our study, 95% 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 the ability to manage encryption keys locally, security monitoring, and encryption of data within the service provider's organization leading the list (see Figure 19).

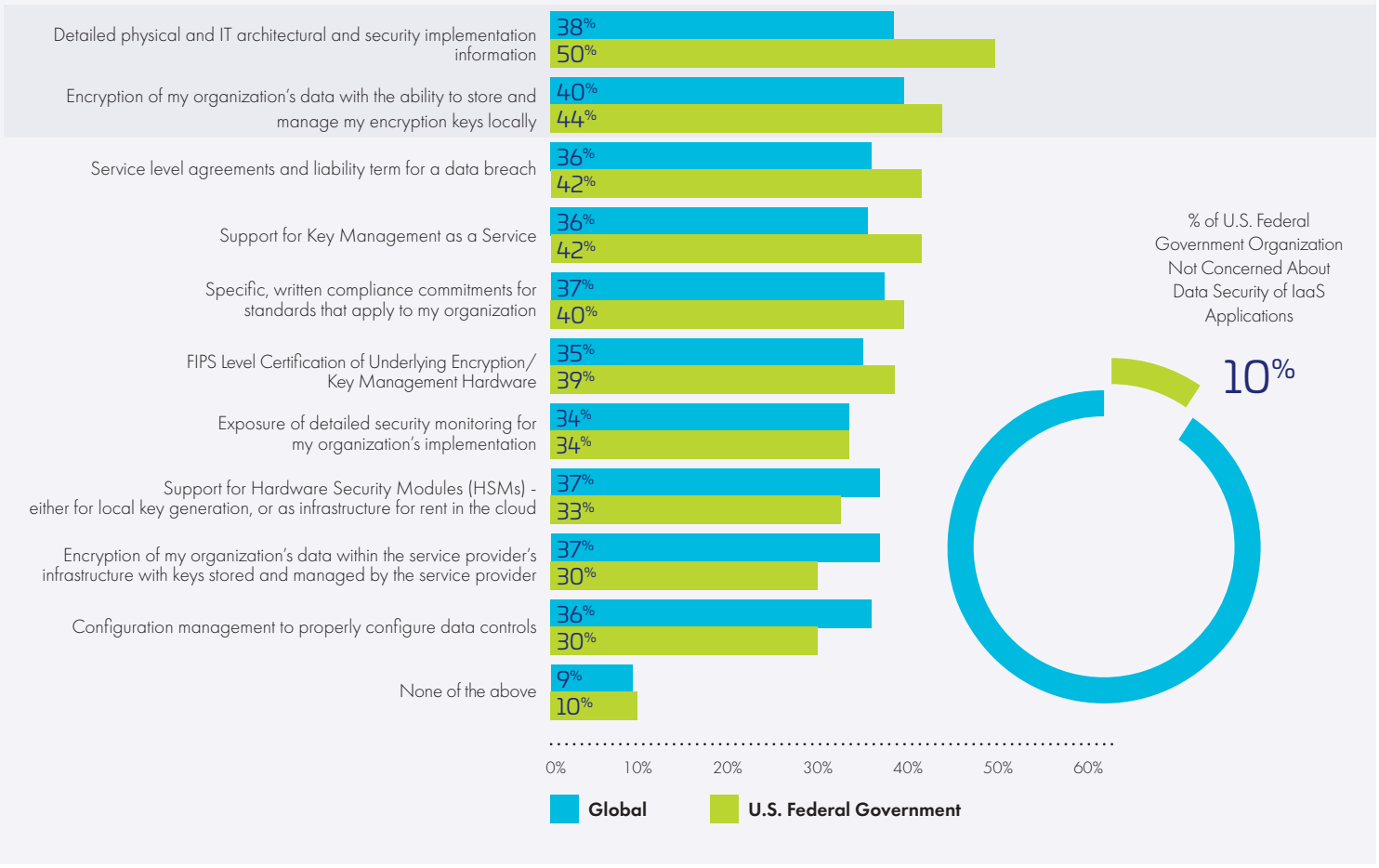
> "SaaS security concerns span a broad range of risks, with the ability to manage encryption keys locally, security monitoring, and encryption of data within the service provider's organization leading the list."

**Figure 19** – SaaS Security Concerns



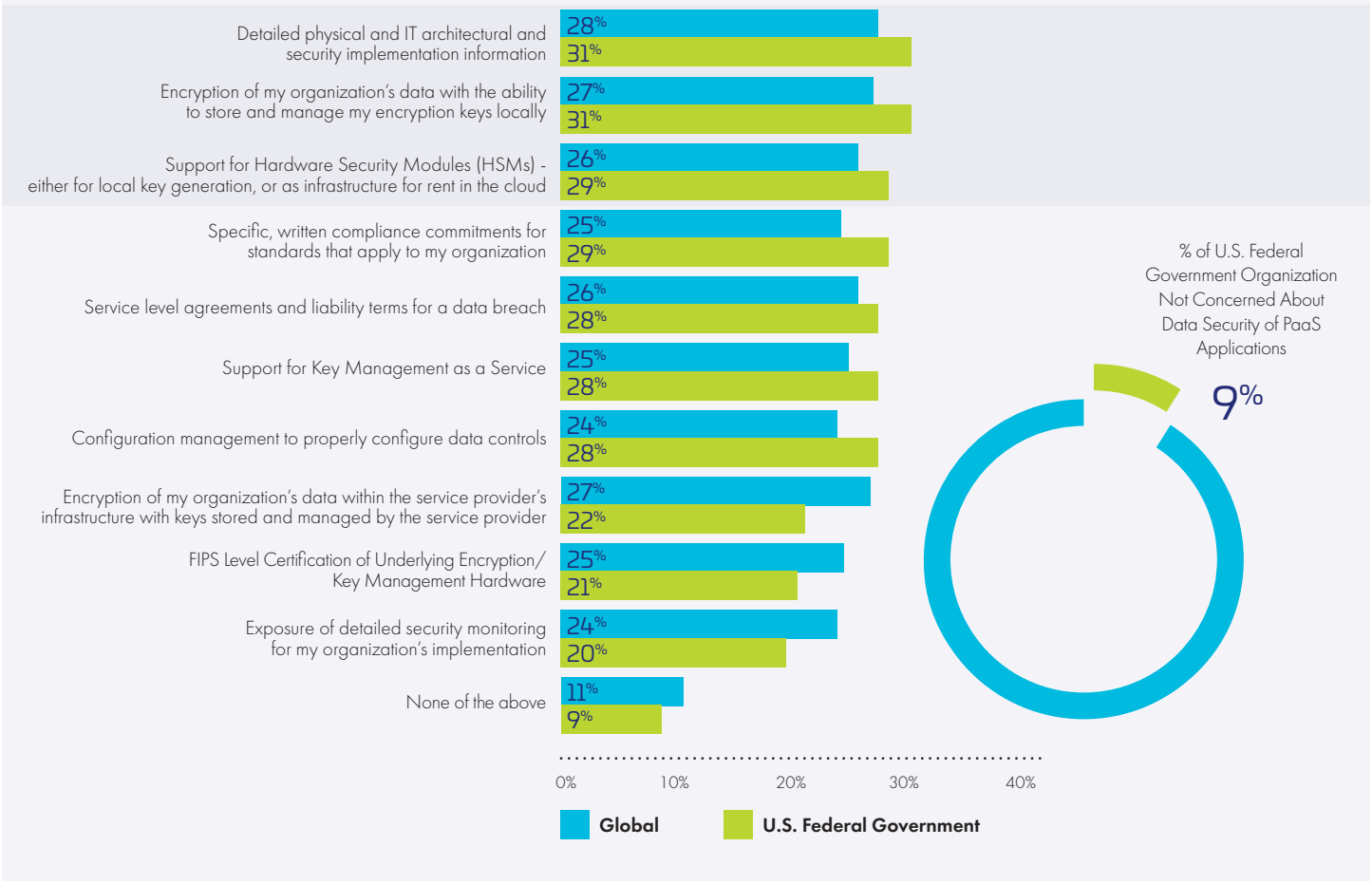
Ninety percent of U.S. federal government respondents have at least some concerns over data security of IaaS environments. IaaS security concerns also cover a broad range of issues with physical layout information and local key integration as top concerns (see Figure 20).

**Figure 20** – IaaS Security Concerns



Ninety-one percent of U.S. federal government respondents have at least some concern over data security of PaaS environments with physical layout information, data encryption, and hardware security modules (HSMs) leading the way (see Figure 21).

**Figure 21** – PaaS Security Concerns




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 organization's data with the ability to store and manage my encryption keys locally." The exact same concern was expressed in the global sample as well. Local storage of keys is important.

However, U.S. federal government respondents diverged from our global sample as it related to storage of keys by service providers. For the global sample, "Encryption of my organization's data within the service provider's infrastructure with keys stored and managed by the service provider" was a consistent concern across IaaS, PaaS and SaaS and increased in rank as the level of control in the infrastructure declines (as defined in Figure 18). Although still concerning for government respondents, it ranked slightly lower, which may simply indicate that government organizations may be less likely to have their keys managed by a service provider due to policy.

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

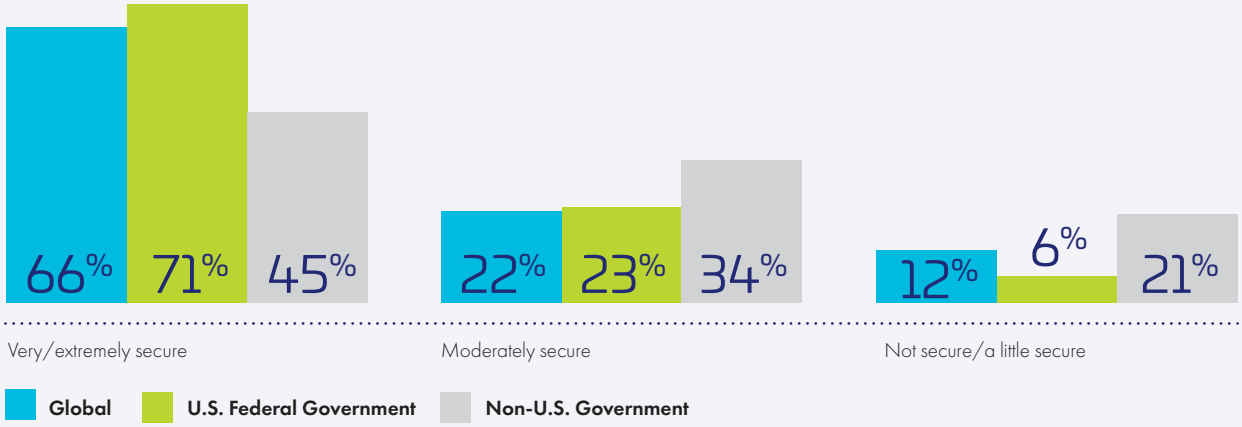
# 03

# Security Concerns and Methods of Alleviation by Data Environment

Just as digital transformation creates opportunities for new technologies, it also introduces new security concerns. Transformational technologies like IoT and DevOps allow government agencies to provide capabilities for better troubleshooting, repairing, expanding mission-critical optics, gathering more data, and streamlining more costly manual workflows. But these technologies introduce new complexities as federal agencies push an increasing amount of data and compute power to the edge. Almost by definition, data at the edge is no longer protected by perimeter-based defenses. An uptick in edge technologies demands that security spend shifts away from traditional enterprise security and even away from cloud. Thus, data defenses must be appropriately constructed for the environment in which the data "lives." For example, discovery of sensitive data and key management take on an even more critical role in data security. Yet data discovery and key management are not perceived as top concerns, creating potential gaps in data security practices.

U.S. federal government agencies in this study feel more secure as they push more data to new technology deployments, despite the additional data security complexity new technologies create. They feel more secure than the global sample, with 71% feeling very or extremely secure, higher than 66% of the global sample and 45% of non-U.S. governments that feel very or extremely secure (see Figure 22).

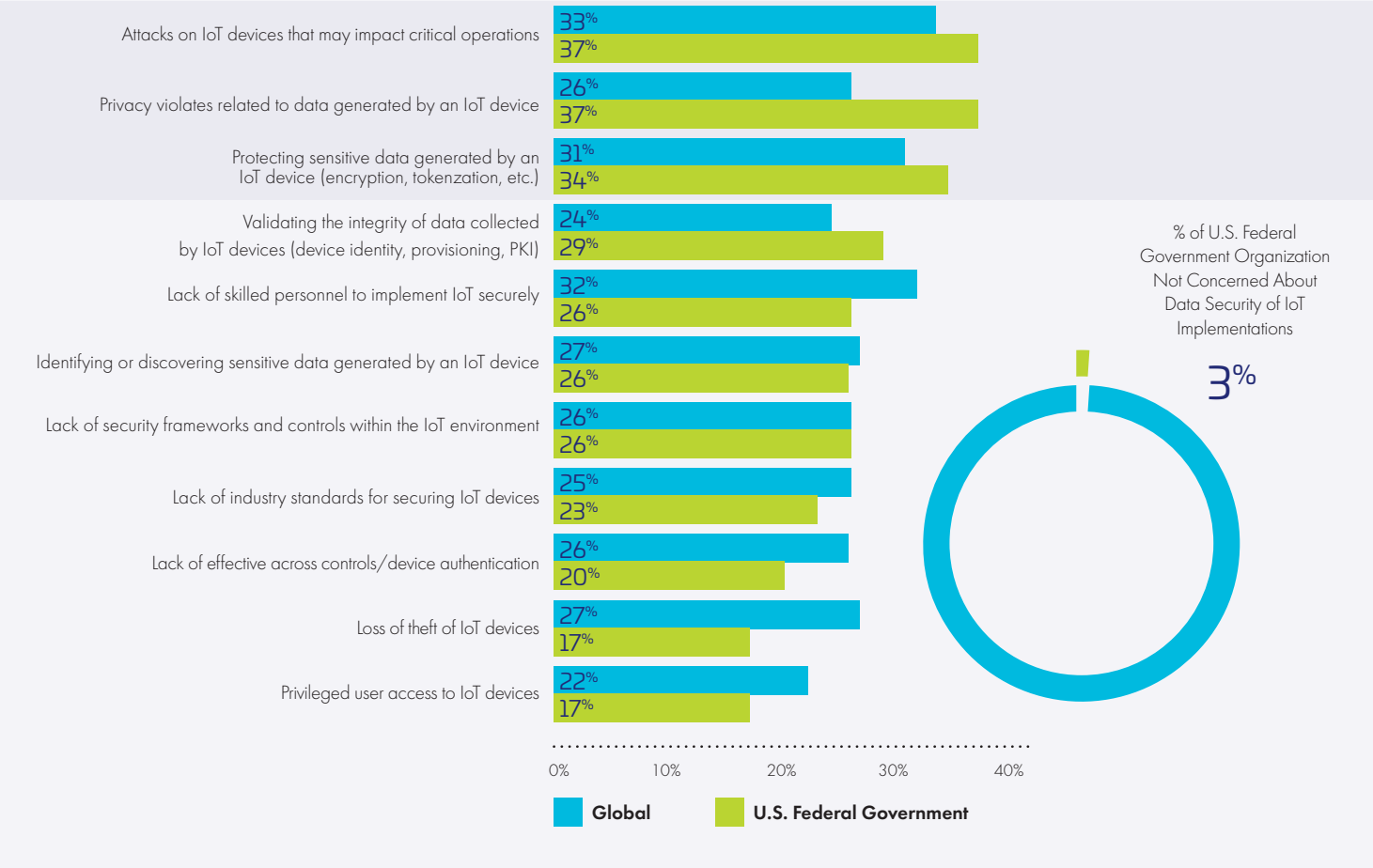
**Figure 22** – Security Level of New Technology Deployments



# Internet of Things Security Concerns

Ninety-seven percent of U.S. federal government agencies are concerned about data security in IoT environments. Top IoT security concerns include device attacks, privacy violations, and protecting sensitive data generated by IoT devices. Also of critical concern: identifying and discovering sensitive data generated by an IoT device was mentioned by 26% of U.S. federal government respondents (see Figure 23).

**Figure 23** – Internet of Things Security Concerns




Digital identity authentication and perimeter/gateway protection are the top responses to address the top IoT security concerns, which make sense given the "zero trust" buzz of the day. However, the zero trust access focus emphasizes securing the devices, not protecting the data the devices generate. As more IoT devices are deployed, key management is increasingly important to effectively implement identity security and data encryption on IoT devices.

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

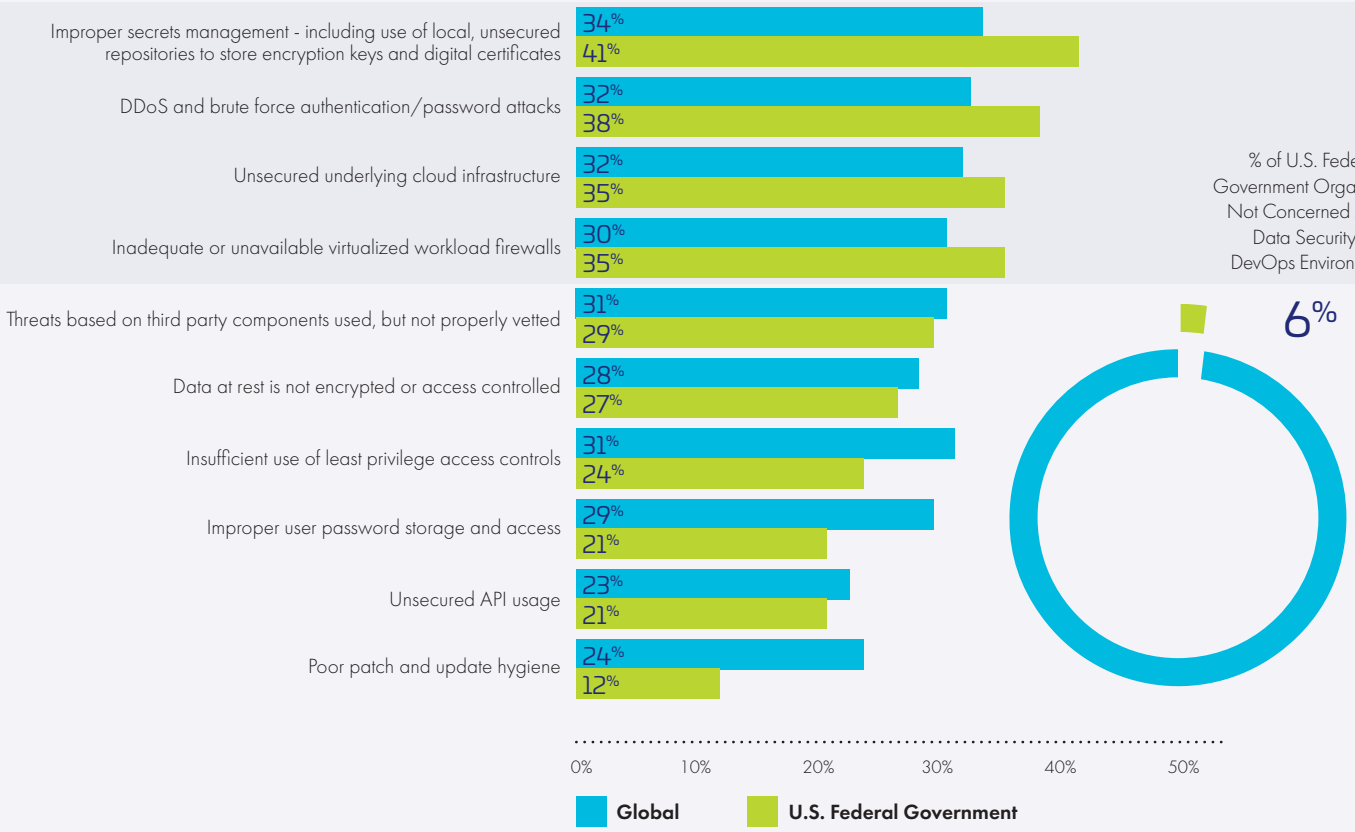
# DevOps Security Concerns

When it comes to DevOps, 94% of respondents are concerned about data security of their DevOps environment. Organizations are most concerned about improper secret management, including use of local unsecured repositories to store encryption keys and digital certificates, DDoS and brute force authentication password attacks and unsecured underlying cloud infrastructure (see Figure 24). Many different approaches are being considered to alleviate DevOps security concerns, led by continuous production environment security procedures and encryption.

**94%**

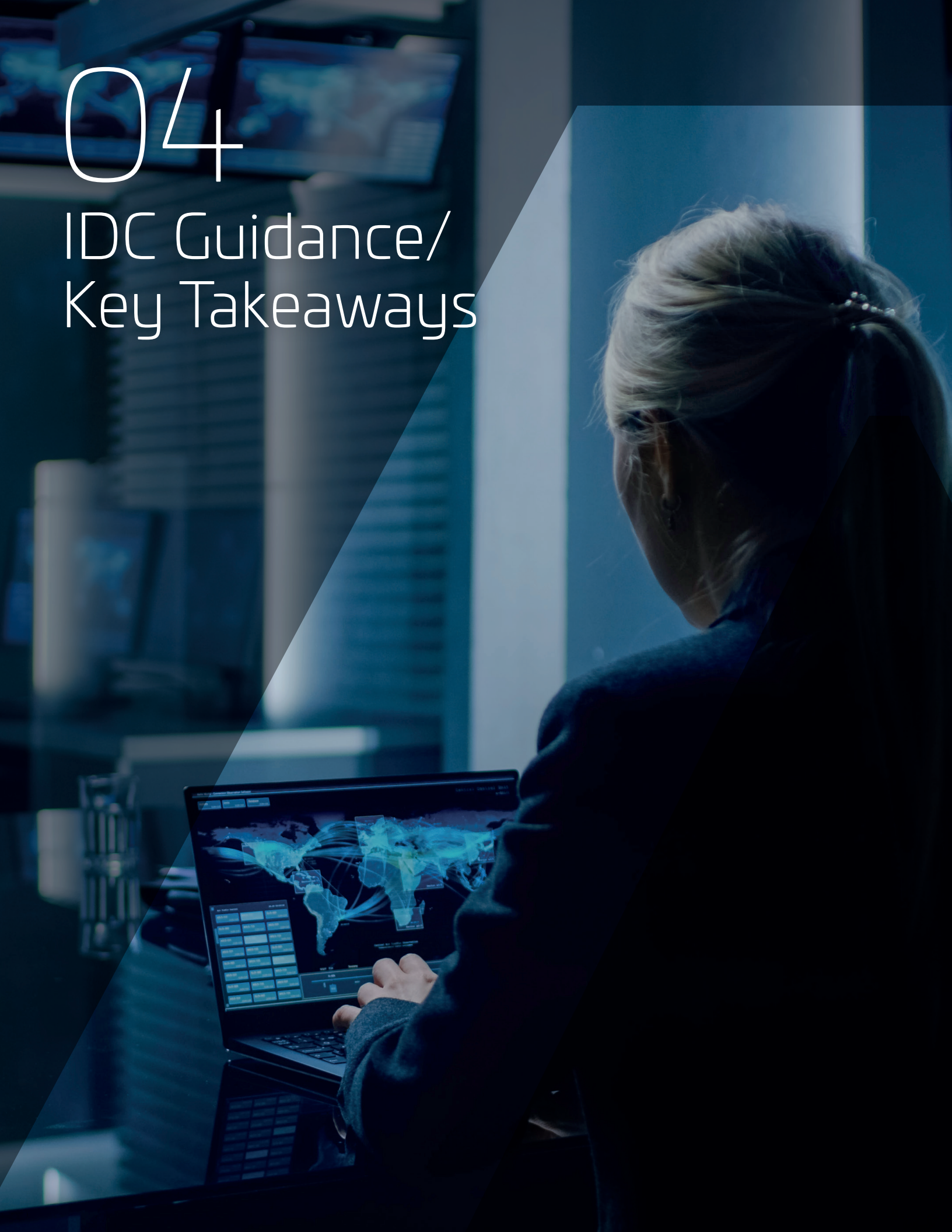
of respondents are concerned about data security of their DevOps environment.

**Figure 24** – DevOps Security Concerns



# 04

# IDC Guidance/ Key Takeaways



Government agencies face expanding and more complex data security challenges. The following are IDC's guidance and key takeaways to help government agencies elevate their data security posture and evolve their security policies:

- **Agency CISOs may need to serve as project champions. Most federal agencies are required to have a chief information security officer.** Agencies often have a patchwork of security solutions in place. As DX becomes increasingly prevalent in federal government agencies, the CISO must serve as the "security champion" to ensure employees and systems work in concert to make enterprise-wide security — throughout the DX transition and beyond — a reality.

- **Foreign threats are an ongoing concern.** The probing of federal networks by nation states is increasingly aggressive; the threat presented each day is worse than the previous day. Agencies must proactively monitor network, system and application probing, share best practice mitigation techniques with other agencies, and be aware of (and quickly react to) government-wide notifications. The DoD is planning to migrate to the new cybersecurity maturity model certification (CMMC) framework in order to assess and enhance the cybersecurity posture of the defense industrial base (DIB) by verifying that appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the department's industry partners' networks.

- **Invest in modern, hybrid and multicloud-based data security tools that make the shared responsibility model work.** Sensitive data is stored in the cloud at an increasing rate. Government agencies should focus on solutions that can simplify the data security landscape and reduce complexity across multiple clouds and legacy environments, as well as modern, cloud-based digital transformation technologies. Agencies should consider data security solutions that enable protection of data moving between clouds and out of the cloud to on-premise environments and should leverage centralized security solutions that orchestrate data security across multiple cloud platforms vendors. In a shared responsibility model, organizations cannot rely on service providers for data security measures as data security remains the responsibility of the organization. Organizations must additionally consider all the security elements which directly or indirectly impact the security of their data such as identity management, encryption and tokenization. The NIST Special Publication 800-57, which highlights key management guidelines for agencies, is a great starting point. Associated documents also cover how to handle periods when it's necessary to transition agency cryptographic algorithms and key lengths.

- **Adopt a zero trust model. Government agencies must still focus on network security and application security as they aim to control access to data.** Zero trust should go beyond that traditional edge, whether it's in the cloud, virtual environments, datacenters, or other DX technologies. Zero trust is a powerful approach to support data security. Zero trust provides network and application access protections to data, but it does not protect the data itself. Challenging data environments require a more persistent data security approach grounded in cryptography should zero trust access protections fail. Think defense in depth.

- **Increase focus on data discovery solutions and centralization of key management to strengthen data security.** Data security should evolve as the edge expands with greater adoption of the cloud, 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 an organization's data security stance by knowing where sensitive data is and how to access it. Additionally, as organizations increase their use of encryption to protect sensitive data, they should centralize key management to help simplify key management operations in otherwise complex environments. For high sensitivity, plans may need to be in place for rapid data removal or destruction, especially for defense or intelligence operations.

- **Prepare for quantum computing's impact on cryptography.** Data security doesn't get any easier as the power of quantum computing may expose 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.

- **Focus on the right threat vectors.** Yes, malicious actors are evolving their tactics, techniques, and procedures (TTP) daily. Security policies need to continually evolve to match. But focus on the threat vectors within your direct control, while still being aware of broader government-wide security alerts and requirements. Be careful of overprovisioning quantity and breadth of accounts both internally and externally with service providers and contractors. Also make sure, via routine checks, that your systems continue to meet appropriate federal information processing standards (FIPS) and Federal Information Security Management Act (FISMA) standards. These rules have specific agency-wide requirements.

- **Data security solutions, especially encryption, are critical to remain vigilant against today's data risk reality.** 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. You need new data security methods to protect today's IT landscape as data migrates away from the enterprise premises and to the cloud. This starts with encryption, including smart encryption with built-in access controls. Some agencies may require the encryption to be end-to-end across government systems.

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 <**


cpl.thalesgroup.com/Fed-DTR/

#2020DataThreat