Federal Edition

THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Navigating New Threats and Overcoming Old Challenges

#2024DataThreatReport
cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

United States Federal Government (USFED) agencies and those organizations directly funded by the U.S. government represent a major component of the U.S. economy, and by extension, the world economy. Federal agencies such as the National Institute of Standards and Technology, and organizations that contract with the US government, set security policies and best practices that are used worldwide. These agencies and organizations are highly attractive targets for criminals and nation-states, as successful attacks against these organizations represent significant risks to national and international security, economic prosperity, and public health and safety.

In this paper, we share key findings from the 2024 Thales Data Threat Report (DTR) focused on USFED agencies and organizations, examining the differences between USFED survey respondents and global responses across all industry verticals. Many of the USFED DTR survey results were similar to overall responses, but we do note some key differences.

S&P Global
Market Intelligence

Source: 2024 Data Threat Report custom survey from
S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

edvance
value added distributor

EXCLUSIVE NETWORKS

netpoleon
Network • Security

Key Findings

Data Breach Trends and Threats

About half (49%) of USFED agencies and organizations have been breached at some point, equal to the global survey figure. **The proportion of USFED organizations reporting a recent breach (in the last 12 months) dropped dramatically from 47% in 2021 to 13% in 2024** — a decrease of 34 percentage points, or 72% — likely a result of heavy security investments, executive orders (EO) and directives by the U.S. government, including White House EO 14028 on Improving the Nation's Cybersecurity, the National Cybersecurity Strategy, and National Security Memorandum 8: Improving Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.

49%

Ransomware attacks against USFED agencies and organizations continue to proliferate, with 40% reporting that they have experienced an attack — 12 percentage points higher than the global result (28%). Planning is still poor, with only one in five (20%) USFED respondents saying they would follow a formal plan in the event of an attack, similar to global respondents (21%).

40%

Among USFED agencies and organizations, human error and zero-day/novel/unknown vulnerabilities were tied as the leading causes of cloud-based data breaches at 27%, compared to human error as the leading cause in the global survey (31%). Failure to apply multifactor authentication (MFA) to privileged accounts was another major cause, at 20%, 3 percentage points higher than among global respondents. USFED agencies and organizations struggle with zero-day and MFA failures at rates higher than the global population.

27%

Identity Complexities and Compromise

On average, one-sixth (16%) of all external access to USFED IT systems and resources comes from "customers" (any source other than employees, contractors, vendors, and partners, such as constituents). This figure is identical for overall respondents.

16%

Among survey respondents who cited external identity as an emerging security concern, achieving security consistency across workforce and non-workforce identities is one of the top challenges, cited by 64% of the relevant subset of USFED respondents.

64%

Increasing DevOps Challenges

Among USFED respondents who cited cloud/DevSecOps security as an emerging security concern, the greatest proportion cited workforce identity and access management (IAM) issues such as privileged user management (68%) as the top DevOps challenge, trailed by secrets management (52%). Globally, the prioritization was reversed: 57% cited secrets management, while 50% identified privileged user management. **This significant difference may be attributable to a much higher proportion of privileged users in USFED agencies and organizations than in the global survey population.**

68%

Operational complexity remains a security concern. Two in five USFED respondents (41%) report that their organization uses five or more key management systems, which is down considerably from 2022 (58%), but still significant. The average number of SaaS apps reported in use by USFED agencies and organizations has risen from 20 in 2022 to 84 in 2024. **These results reflect a dramatic increase in cloud utilization by the U.S. government, likely driven by significant increases in the quantity of FedRAMP marketplace-certified vendors (337 classified as FedRAMP-authorized and 116 more in process at the time of this writing). This also illustrates encouraging trends in reducing hybrid cloud complexity.**

5+

Risks to Emerging Technologies

Regarding threats from quantum computing, future compromise of classical encryption techniques, enabling "harvest now, decrypt later" (HNDL) attacks, is leading interest in post-quantum cryptography (62% USFED, 68% Global). Among USFED respondents who identified PQC as an emerging security threat, 44% would likely create resilience contingency plans, and 50% would prototype or evaluate PQC algorithms in the next 18-24 months. **While USFED agencies and organizations are somewhat less concerned about HNDL attacks, they are deploying PQC at a similar rate globally. This is likely to increase due to significant focus on PQC driven by US law HR7535 (Quantum Computing Cybersecurity Preparedness Act, signed into law in late 2022), coupled with pressure on US government agencies to deploy PQC-ready encryption techniques.**

62%

The AI boom is underway: 31% of USFED respondent organizations plan to integrate AI into their core products and services in the next 12 months, 9 percentage points higher than global respondents. 27% of USFED organizations are experimenting with AI, compared to 33% of all respondents. **This suggests that USFED agencies and organizations are embracing innovations in AI through integration at a much higher rate than the general survey population.**

31%

Both groups indicated that managing fast-changing environmental risks associated with rapid ecosystem evolution and operational alterations is their greatest concern regarding the security of AI.

Enterprise Observations

This year's DTR provides additional insights into enterprise security and IT organizations. The need for data security as a discipline remains diffused throughout USFED agencies and organizations. Functions such as compliance, supply chain and design all incorporate data security.

Security and compliance initiatives are converging on common inputs, processes and outcomes. New cyber-resilience regulations such as Executive Order 14028 and pending updates to existing standards including the Federal Information Security Modernization Act (FISMA) are specific about what controls organizations need to implement. Meeting these standards requires increasing alignment between security and compliance teams.

KEY STATISTIC

In 2024, among USFED respondent agencies and organizations that had failed a compliance audit in the last 12 months, 83% reported at least one breach in their history.

83%

KEY STATISTIC

In contrast, for those USFED agencies and organizations that had not failed a compliance audit, only 32% reported a breach history, and just 3% had a breach in the last 12 months.

32%

Through the years, DTR findings have shown a strong correlation between compliance achievement and reduced breaches. In the 2024 survey, among USFED respondent agencies and organizations that had failed a compliance audit in the last 12 months, 83% reported at least one breach in their history (similar to the general study). In contrast, for those USFED agencies and organizations that had not failed a compliance audit, only 32% reported a breach history, and just 3% had a breach in the last 12 months.

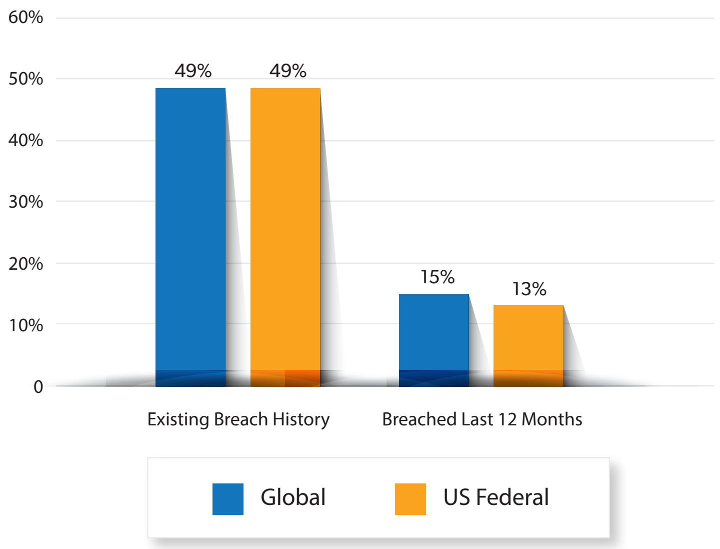
The Threat Landscape

In USFED agencies and organizations, as in the rest of the world, the attack landscape remains vast and growing. **Nine out of 10 USFED respondents (93%) said they were experiencing an increase in attacks.** The top three fastest-growing types of threats reported by USFED organizations were malware, phishing and ransomware. In the 2022 USFED survey, the top three threats were the same, though their order was shuffled, with ransomware and phishing/whaling tied for first place and malware a close third.

The most common root causes of cloud-based data breaches for USFED agencies and organizations were human error (27%), exploitation of a known vulnerability (27%) and failure to use MFA for privileged user accounts (20%). When we examined the root cause of attacks by attacker type, misconfiguration (human error) was ranked as the top root cause for attacks perpetrated by external attackers with financial motivations and geopolitical goals, as well as by malicious insiders with non-financial motivations. For attacks carried out by external attackers with other ideological goals, malicious insiders with financial motivations, and those deemed accidental incidents, the root cause was most often zero-day/unknown/novel vulnerabilities. Human error can be mitigated in part through deployment of MFA and by maintaining audit logs in conjunction with an access management solution.

Just over two-thirds of USFED respondents (69%) said they are or will be using MFA to secure access to data in the cloud, 2 percentage points lower than the overall survey population. This is encouraging, but organizations must ensure they utilize strong MFA such as hardware tokens and phishing-resistant MFA (e.g., public key infrastructure [PKI] or Fast Identity Online [FIDO] passkeys) instead of SMS or email challenges.

Overall Breach History and Recent Breach History



Source: S&P Global Market Intelligence's 2024 Data Threat custom survey

Ransomware response remains a challenge. For the last three years, fewer than 50% of overall respondents across all verticals and company sizes reported having a formal ransomware plan in place — and only 20% of USFED respondents have one. Among USFED respondents who have resolved a past ransomware attack, none did so by paying a ransom, while 13% of USFED agencies and organizations said they would pay a ransom to resolve a future attack. Initial breach response is increasingly led by legal teams interfacing with regulators or law enforcement.

Two-thirds (62%) of USFED respondents cited future encryption compromise as the top concern among security threats related to quantum computing, 6 points below the overall survey population. More than two in five USFED respondents (44%) said they will create resilience contingency plans to satisfy quantum computing security concerns in the next 18-24 months, similar to the survey-wide result.

The complexity of cloud resources among end users, operators and developers continues to grow. Curiously, the percentage of USFED agencies and organizations saying they have 50 or more SaaS apps in use dropped 7 percentage points to 32% in the 2024 survey, compared with 39% in 2022. However, based on a weighted calculation, USFED respondent agencies and organizations on average have approximately 84 SaaS apps in use, up from 20 in 2022. The percentage of USFED agencies and organizations that agree or strongly agree that managing security in the cloud is more complex than managing security on-premises increased 10 percentage points, from 39% in 2022 to 49% in 2024.

USFED respondents stated that, on average, 42% of their data stored in cloud is sensitive, compared with 41% in the 2022 survey, leading to the conclusion that while these organizations are moving critical workloads to the cloud, the amount of sensitive data stored there is not changing substantially. Meanwhile, 25% of USFED respondents depend on cloud providers to control the encryption keys for more than half of their applications, similar to the overall survey population (27%). For those keys specifically under their control, 20% of USFED respondents have chosen the bring your own key (BYOK) approach, a figure that has increased 6 percentage points since 2022 (14%).

This year's DTR survey asked respondents to select their top four areas of security concern among emerging technologies, including cloud and DevOps, AI, workforce IAM, external IAM, IoT/5G, PQC and digital sovereignty. USFED agencies and organizations are most concerned with digital sovereignty, external identity management and IoT/5G.

When asked what aspects of 5G security are the most concerning, 59% of USFED respondents cited protecting the identities of devices, people and things connected to 5G networks as their top worry. Meanwhile, 57% of USFED organizations identified IoT as one of their greatest emerging security concerns.

Access Control

There is a bit of a sea change underway in terms of how access control is managed — and by whom. Almost half (48%) of USFED respondents in the latest survey agree that agencies and organizations should maintain control over their access security, more than double the percentage in the 2022 survey (20%), indicating that USFED agencies and organizations are increasingly bringing (or maintaining) access security in-house. About two in five USFED respondents (38%) agree that access security solutions should be delivered by an agnostic security provider rather than a cloud service provider, 5 percentage points lower than in the 2022 survey (43%), while 29% agree that an agnostic access management solution can best protect multicloud environments.

Additionally, 41% of USFED respondents agree that access management and authentication plays a key role in achieving zero-trust security. Having more than 50 SaaS apps necessitates a deeper dive into authentication journeys. USFED agencies and organizations have a highly disparate user base, ranging from internal users to external contractors, as well as citizens accessing government services, and enabling zero-trust with the plethora of SaaS apps and broad array of users requires flexible access policies. Additionally, for air-gapped environments, an on-premises authentication solution is needed to protect resources.

KEY STATISTIC

Almost half (48%) of USFED respondents in the latest survey agree that agencies and organizations should maintain control over their access security.

48%

Next Steps

The importance of the U.S. Federal segment must not be understated. Its wide reach includes hundreds of federal agencies and an extensive range of government-funded organizations that impact every citizen and resident while also imparting major influence on the world economy. In response, the U.S. Federal Ggovernment needs to take proactive measures to protect its assets and people.

While technologies such as AI, quantum computing, cloud, edge computing and 5G are driving new efficiencies and advancements within the U.S. Federal segment, they also create new threat vectors. The U.S. Federal Government has issued numerous cybersecurity-related policies and strategies in the last few years to address its security vulnerabilities. These polices underscore the importance of protecting critical data.

Although policy compliance is well underway, USFED organizations must look beyond a "check the box" approach to security. Data protection best practices should be applied to drive agencies to a position of greater security and less susceptibility. Examples include deploying phishing-resistant MFA; encrypting data at rest, in transit and in memory; ensuring that cryptographic keys are secure, managed and controlled by the organization and stored separately from encryption software; and implementing quantum-safe cryptography.

About This Study

This research is based on a subset of the global DTR survey of 2,961 respondents that was fielded in November and December 2023 via a web interface and aimed at professionals in security and IT management. This subset data comprises targeted populations in the United States federal segment for a total of 106 respondents.

In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million. Most respondents (81%) were affiliated with organizations reporting annual revenue or budgets between US$100 million and US$999.9 million. This research was conducted as an observational study and makes no causal claims.

Revenue	Number of Respondents
$100m to $249.9m	0
$250m to $499.9m	25
$500m to $749.9m	29
$750m to $999.9m	732
$1 Bn to $1.49 Bn	10
$1.5 Bn to $1.99 Bn	9
$2 Bn or more	1

THALES

Building a future we can all trust

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/federal-data-threat-report