

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

FEDERAL EDITION

2017 THALES DATA THREAT REPORT

TRENDS IN ENCRYPTION AND DATA PROTECTION



Copyright 2017 Thales

THE GOOD NEWS ABOUT FEDERAL DATA SECURITY

SAFE OPERATION

25% – U.S. FEDERAL
41% – GLOBAL FEDERAL*

NEVER HAD A DATA BREACH OR COMPLIANCE
FAILURE FOR DATA SECURITY VIOLATIONS

IT SECURITY SPEND UP YEAR OVER YEAR (U.S. FEDERAL)

61% – 2017
58% – 2016

“The U.S. Federal Government is racing to boost data security against odds not faced in the private sector the U.S. government spent \$14 billion last fiscal year on information and cyber security, and a Federal Cybersecurity Workforce Strategy published last year called for hiring of an additional 3500 ‘critical cyber security’ positions in 2017”

Garrett Bekker, 451 Research

* Global = Outside the U.S. results



STAFFING AND BUDGETS TOP BARRIERS TO DATA SECURITY

“U.S. FEDERAL ALSO HOLDS THE DUBIOUS TITLE OF LEADING OTHER VERTICAL AREAS AND COUNTRIES IN TERMS OF EXPERIENCING A SUCCESSFUL DATA BREACH IN THE PAST YEAR AT 34%”

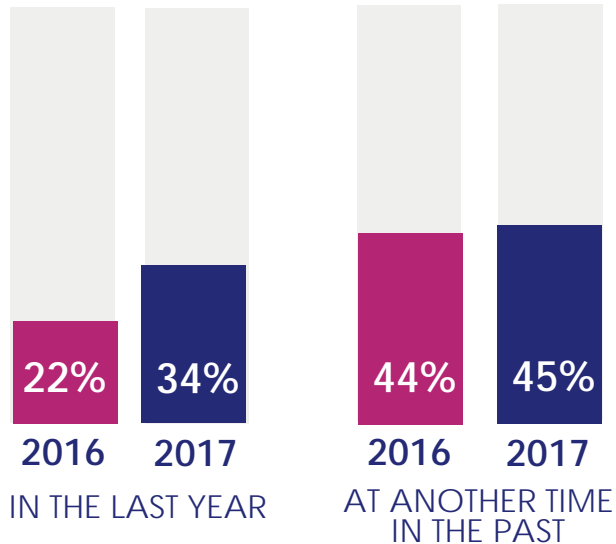
“BUDGET CONSTRAINTS AND STAFFING SHORTAGES ARE BOTH CITED BY 53% OF U.S. FEDERAL RESPONDENTS AS THE CHIEF BARRIERS TO SECURITY INITIATIVES”

U.S. FEDERAL AGENCIES MOST LIKELY TO BE BREACHED

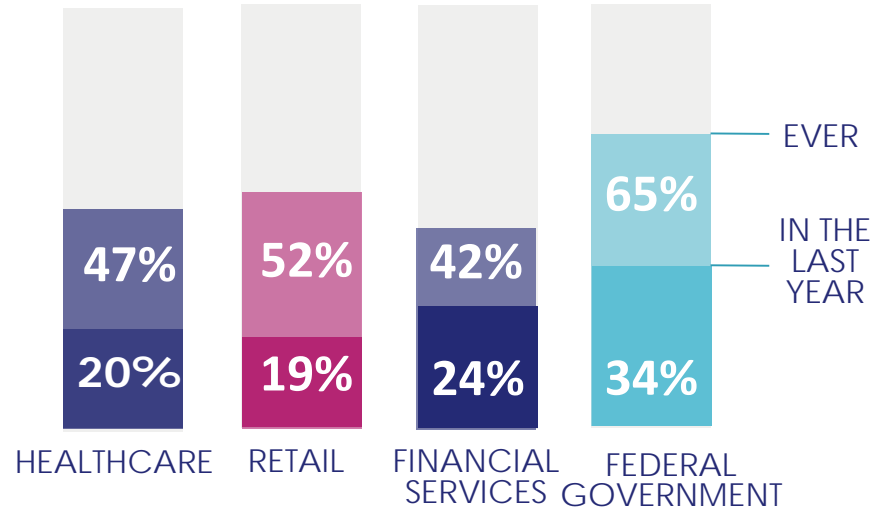
"U.S. federal also holds the dubious title of leading other vertical areas and countries in terms of experiencing a successful data breach in the past year at 34%, well above the global average of 26% and the average of all U.S. verticals of 24%."

*Garrett Bekker
Principal Analyst, Information
Security, 451 Research*

U.S. FEDERAL DATA BREACHES



DATA BREACHES BY U.S. VERTICAL

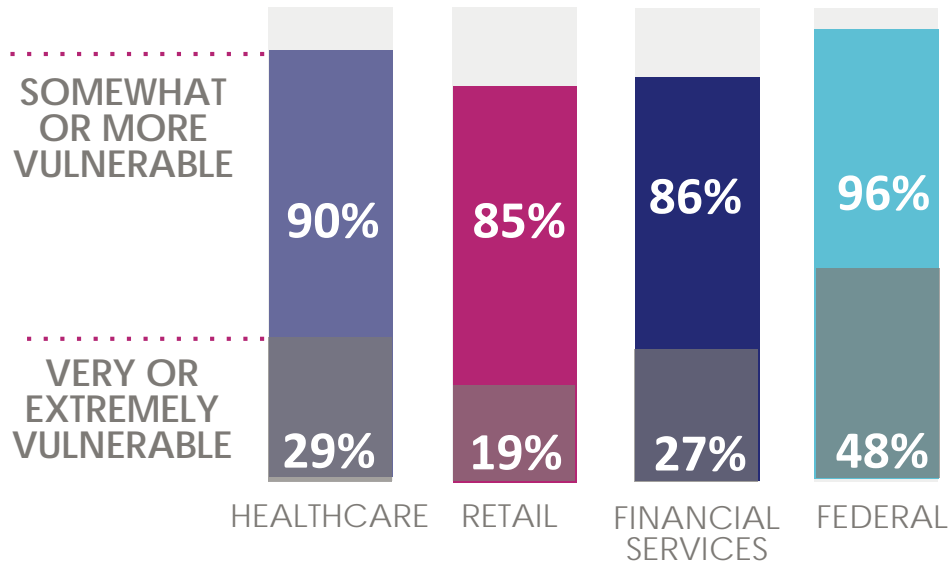


U.S. FEDERAL AGENCIES FEEL MOST VULNERABLE

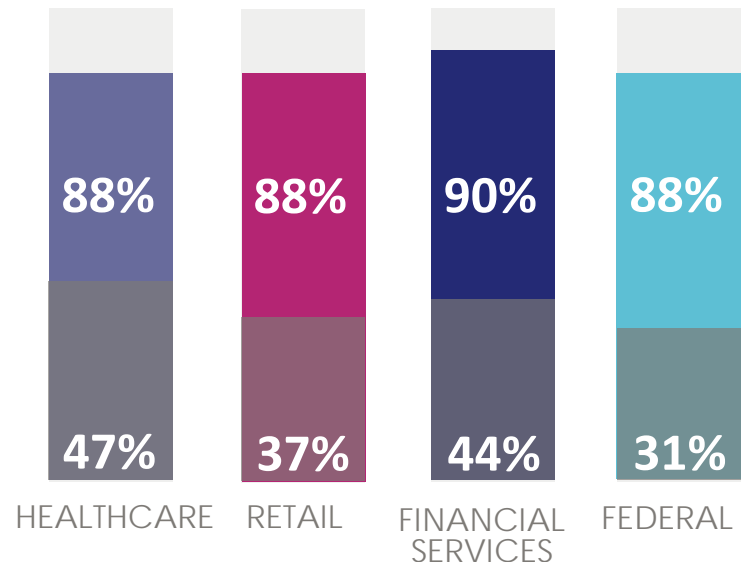
"96% of U.S. federal respondents report feeling vulnerable to threats to sensitive data, the highest of any other region or vertical surveyed."

Garrett Bekker
Principal Analyst, Information
Security, 451 Research

U.S. Verticals



Global Verticals



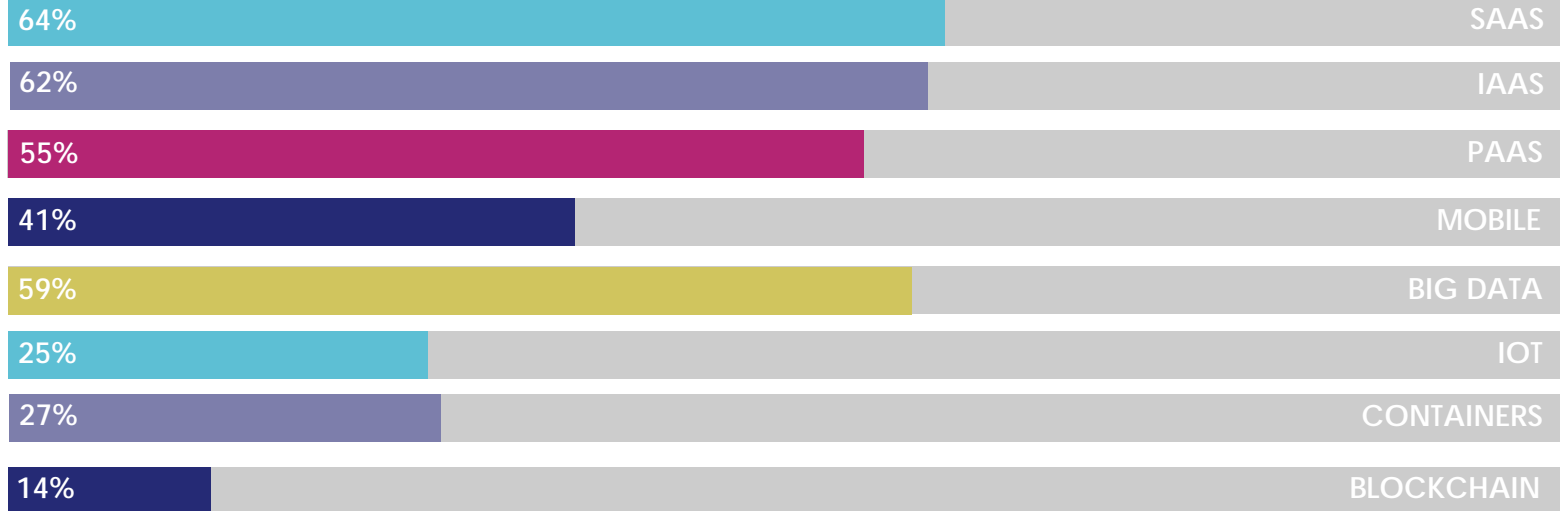
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES WITHOUT DATA SECURITY TO PROTECT INFORMATION

71%

OF U.S. FEDERAL REpondENTS SURVEYED ARE
DEPLOYING NEW TECHNOLOGIES IN
ADVANCE OF HAVING APPROPRIATE LEVELS
OF DATA SECURITY IN PLACE

92%

WILL USE SENSITIVE DATA IN AT
LEAST ONE OF THESE ADVANCED
TECHNOLOGY ENVIRONMENTS



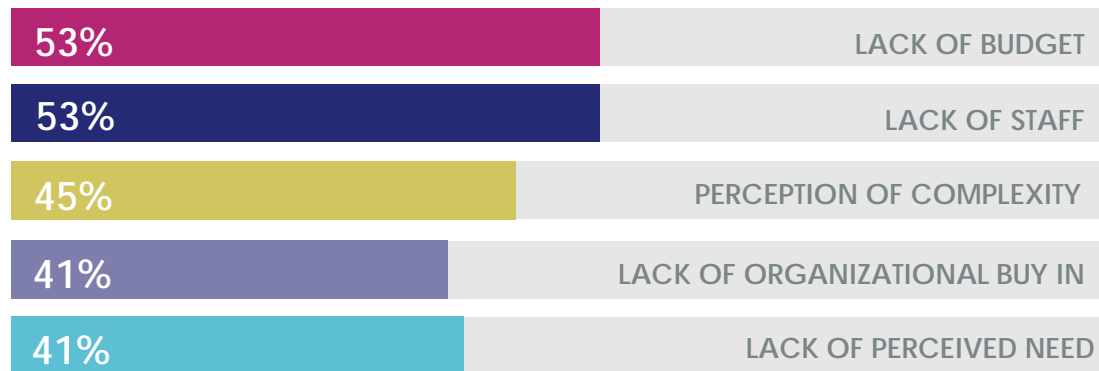
* U.S. RESULTS

LACK OF BUDGET AND STAFF IS PUTTING PUBLIC DATA AT RISK – ESPECIALLY IN THE U.S.

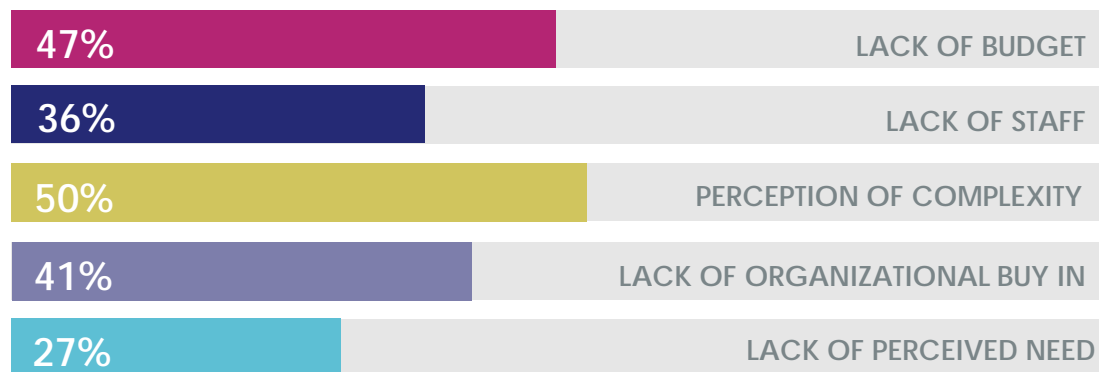
“While complexity is the main barrier to data security in most regions, for the U.S. Federal sector budget (53%, well ahead of global average of 33%), and lack of staff (also 53%) are the main challenges - though complexity remains the top barrier for Global Federal”

*Garrett Bekker
451 Research*

U.S. FEDERAL

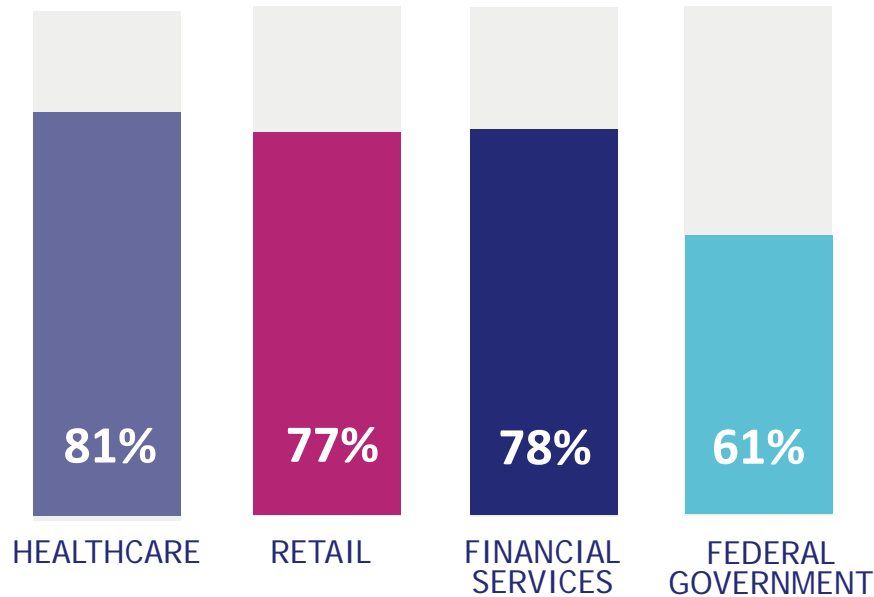


GLOBAL FEDERAL



U.S. FEDERAL INCREASING IT SECURITY SPENDING AND HIRING BUT NOT AS FAST AS OTHER VERTICALS

Increases in IT Security Spend
by U.S. Vertical



Global
Verticals

76%

76%

78%

58%

"... the U.S. government spent \$14 billion last fiscal year on information and cyber security"

"While most regions and verticals showed big year-over-year increases in spending plans, U.S. Federal showed a meager increase, to 61% from 58% in 2016. "

*Garrett Bekker
Principal Analyst, Information
Security, 451 Research*

OLD HABITS DIE HARD -

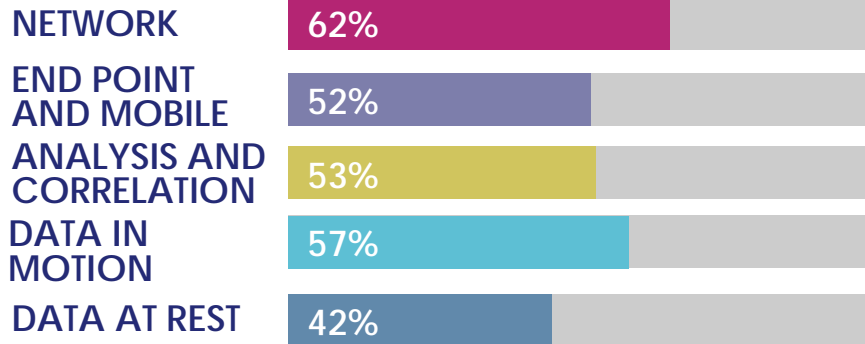
INVESTING LESS IN DATA AT REST SECURITY, THOUGH RATED HIGHLY EFFECTIVE

"...organizations keep spending on the same solutions that worked for them in the past but aren't necessarily the most effective at stopping modern breaches"

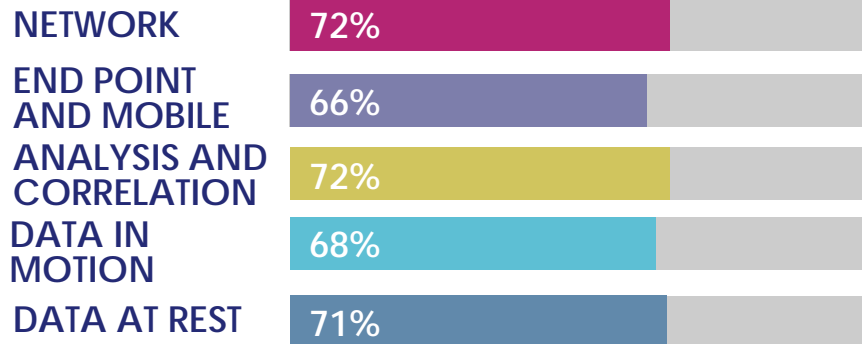
*Garrett Bekker,
451 Research*

"... spending on securing internal networks from external threats is less and less effective – and relevant – as both the data and the people accessing it are increasingly external."

IT SECURITY DEFENSE SPENDING INCREASES



RATES OF EFFECTIVENESS FOR PROTECTING DATA



* U.S. RESULTS

DATA PRIVACY AND SOVEREIGNTY

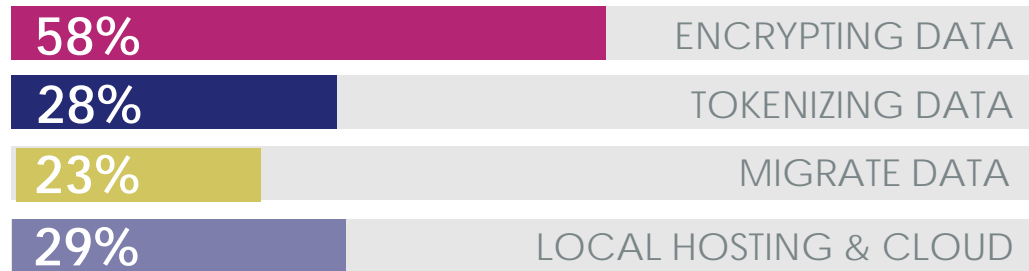
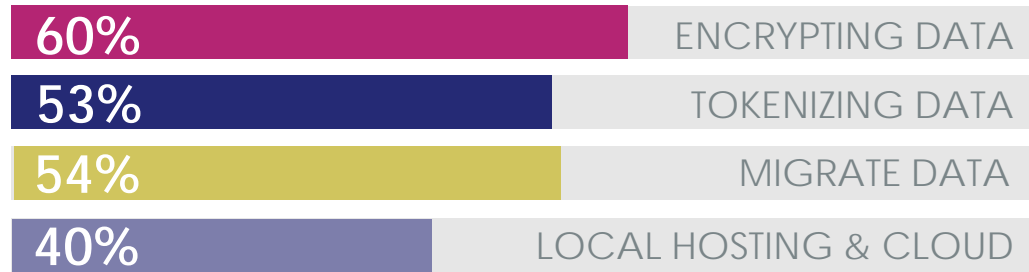
IMPACTING FEDERAL AGENCIES WORLDWIDE



73% - U.S. Federal
71% - Global Federal

Impacted by Data Privacy and
Data Sovereignty

ADDRESSING REQUIREMENTS BY:



“Data privacy has become a hot topic in light of concerns about government snooping, and not surprisingly a host of new privacy laws and regulations are in the process of being revised or enacted around the world, such as GDPR in Europe and the amended APPI in Japan.”

*Garrett Bekker
Principal Analyst
451 Research*

".. external attackers frequently masquerade as insiders by using stolen or compromised credentials to access all types of valuable data, including PII, PHI, financial data and intellectual property"

Garrett Bekker
Principal Analyst Information Security, 451 Research

THE MOST DANGEROUS INSIDERS

59% U.S. FEDERAL

62% GLOBAL FEDERAL

55% U.S. FEDERAL

38% GLOBAL FEDERAL

40% U.S. FEDERAL

50% GLOBAL FEDERAL

39% U.S. FEDERAL

34% GLOBAL FEDERAL

PRIVILEGED
USERS

EXECUTIVE
MANAGEMENT

ORDINARY
EMPLOYEES

CONTRACTORS

IN SPITE OF ALL THE FUROR AROUND NATION STATE HACKING,
CYBER CRIMINALS TOP THE LIST OF CONCERNS BY A WIDE MARGIN

TOP EXTERNAL THREAT ACTOR SELECTIONS

U.S. FEDERAL

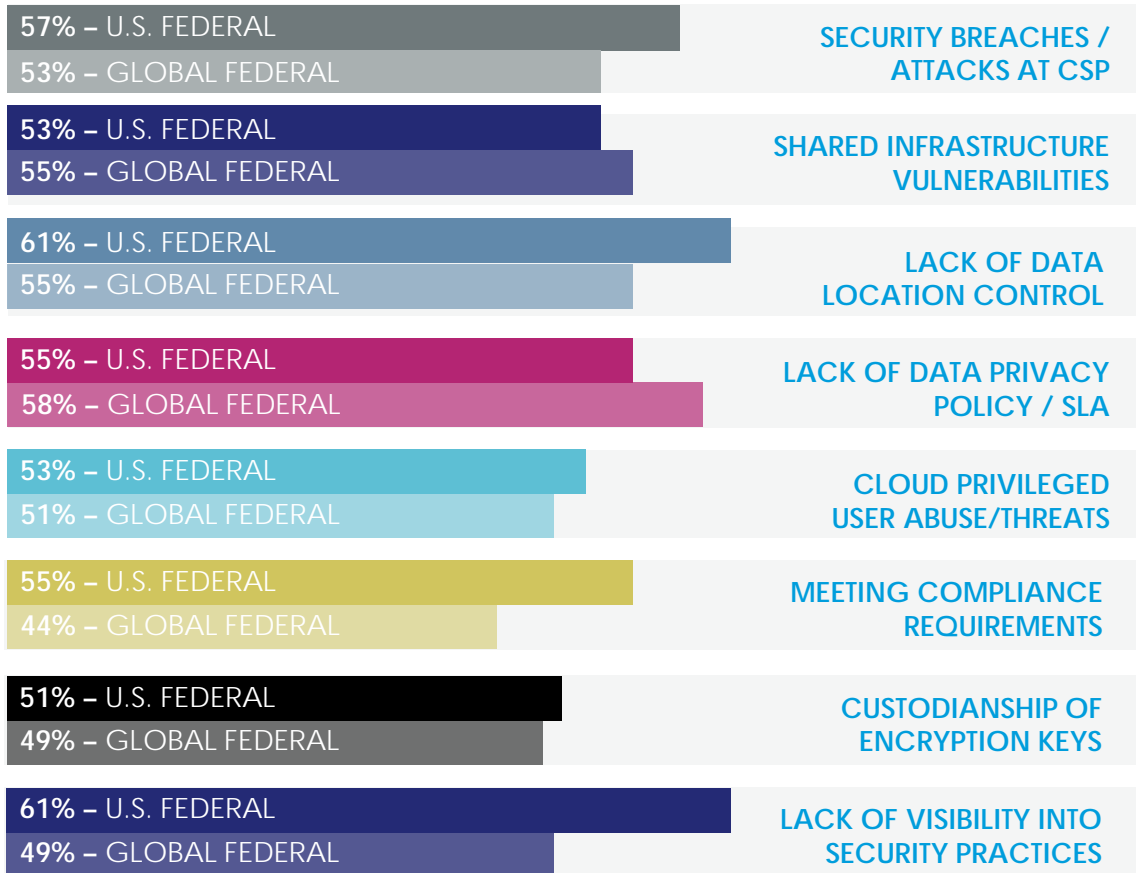


GLOBAL FEDERAL



TOP FEDERAL CONCERNS WITH CLOUD/SAAS ENVIRONMENTS

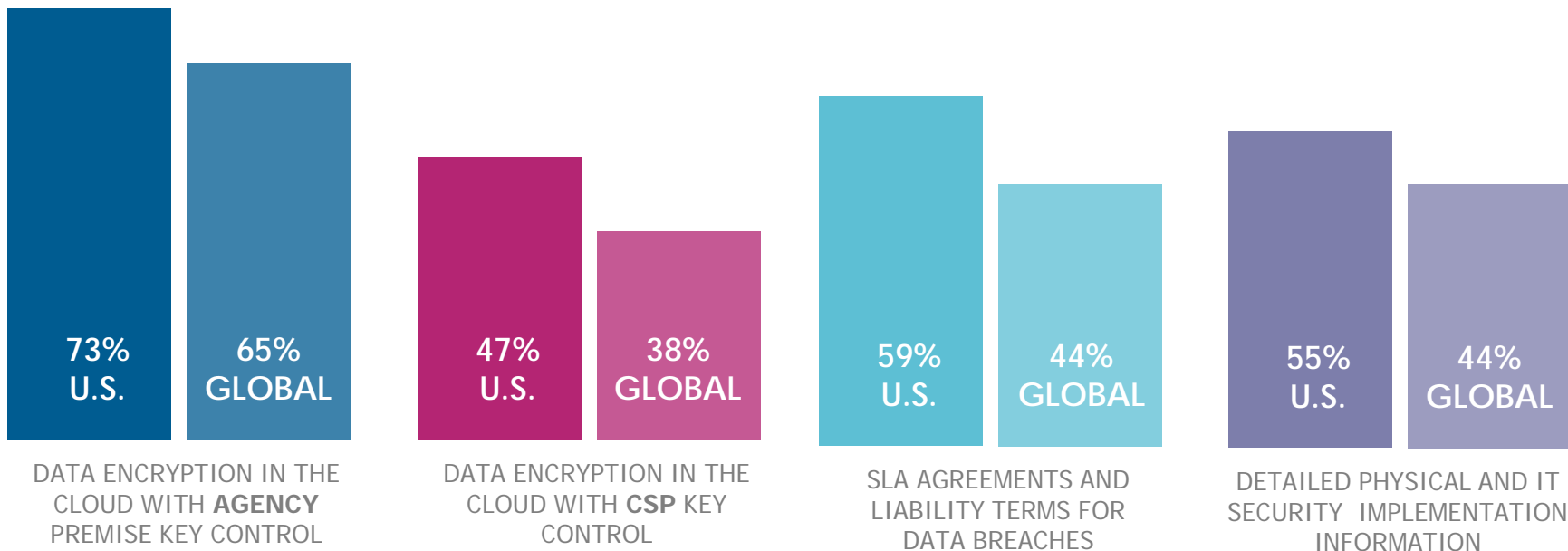
RATES OF VERY OR EXTREMELY CONCERNED



“While security breaches and attacks on public cloud providers was the top concern among the global average (58%), data residency and lack of visibility into the security practices of cloud service providers each elicited responses from 61% of U.S. federal respondents, putting them at the top of the list of public cloud concerns. For Global Federal, however, the top concern (58%) is the lack of a data privacy policy at public cloud providers”

*Garrett Bekker
Principal Analyst, Information Security, 451 Research*

WHAT CAN CSPS AND SAAS PROVIDERS DO TO INCREASE FEDERAL CLOUD ADOPTION?

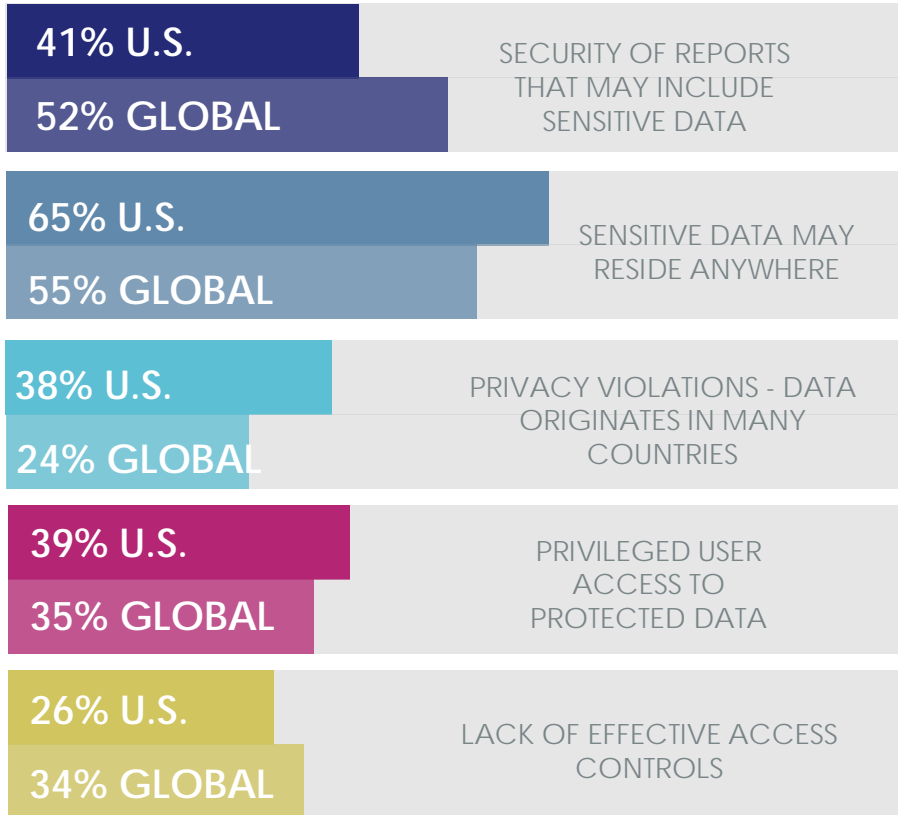


"To guard against threats to sensitive data stored and processed in the public cloud, both U.S. Federal (73%) and Global Federal (65%) put encryption with the option for local key control (BYOK) at the top of the list - in fact encryption with BYOK was the top choice across virtually all categories surveyed."

*Garrett Bekker
Principal Analyst, Information
Security, 451 Research*

BIG DATA – TOP FEDERAL DATA SECURITY CONCERNS AND STATS

TOP 5 CONCERNS



IOT ADOPTION IS HIGH FOR U.S. FEDERAL USE OF SENSITIVE DATA A CONCERN

73%

ADOPTING IOT

25%

USING SENSITIVE
DATA IN IOT

34%

VERY CONCERNED ABOUT
SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

34% - PROTECTING SENSITIVE DATA
GENERATED BY IOT

33% - IDENTIFYING WHICH DATA
IS SENSITIVE

25% - LACK OF SECURITY
FRAMEWORKS & CONTROLS

23% - PRIVILEGED USER ACCESS
TO DATA AND DEVICES

21% - IMPACT OF ATTACKS ON
IOT DEVICES

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

65% SECURE ID AND AUTHENTICATION

63% ENCRYPTION OF DATA

42% - ANTI-MALWARE
FOR DEVICES

59% - IOT NETWORK ISOLATION

45% - ANOMALY DETECTION/
BEHAVIORAL ANALYSIS

TOP SECURITY CONTROLS TO INCREASE FEDERAL CONTAINER ADOPTION AND USE

TOP BARRIERS TO CONTAINER DEPLOYMENT

60%

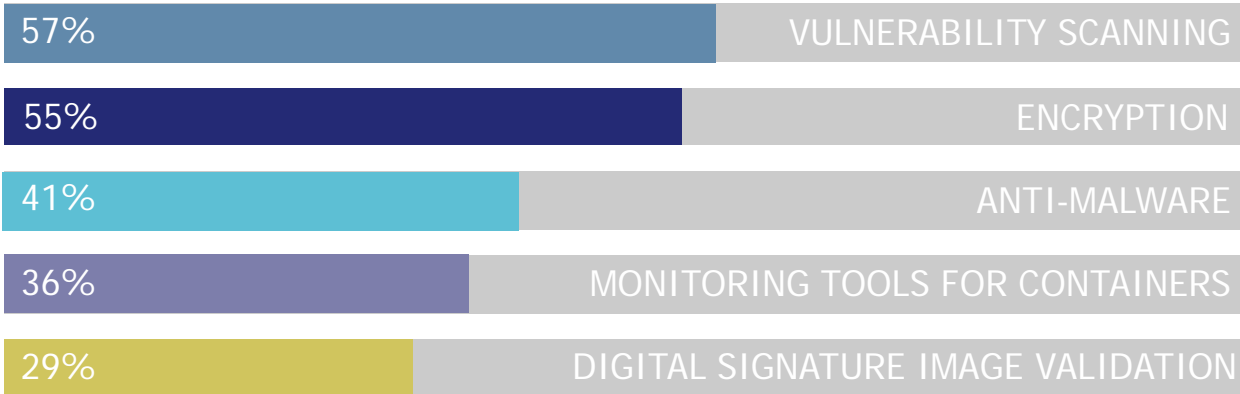
52%

U.S. DATA SECURITY
GLOBAL BUDGET

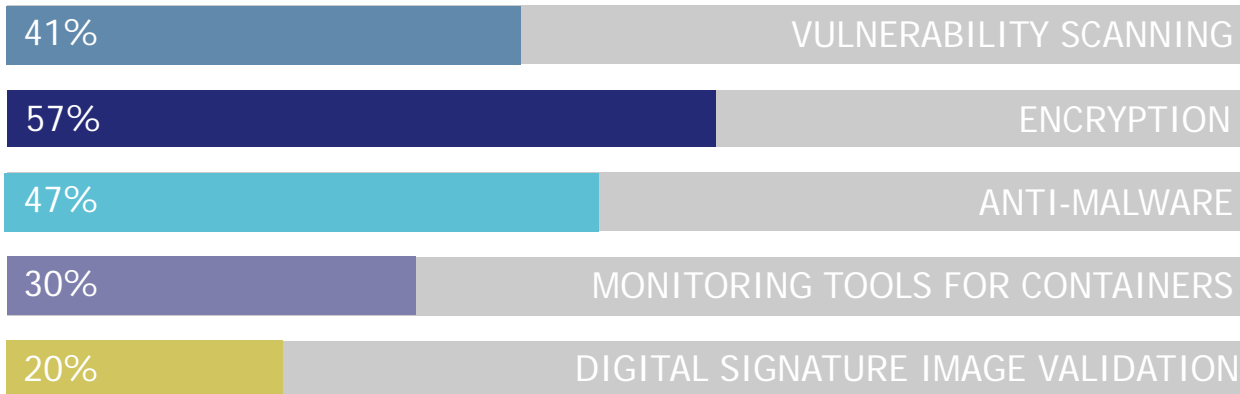
"As is typical with any fast-emerging technology, security concerns abound, and security (60%) not surprisingly emerged as the top adoption barrier for U.S. Federal container deployments, as was the case with most other regions.

Garrett Bekker
451 Research

U.S. FEDERAL



GLOBAL FEDERAL



ENCRYPTION ENABLES DIGITAL TRANSFORMATION

A KEY TOOL REQUIRED FOR ADVANCED TECHNOLOGY ADOPTION

CLOUD

ENCRYPTION ENABLING FURTHER ADOPTION OF CLOUD

73%

U.S.

DATA ENCRYPTION IN THE CLOUD WITH **AGENCY** PREMISE KEY CONTROL

GLOBAL

65%

BIG DATA

ENCRYPTION OFFSETS TOP SECURITY CONCERNS

U.S.

39%

41%

65%

PRIVILEGED USER ACCESS
SECURITY OF REPORTS
SENSITIVE DATA EVERYWHERE

35%

52%

55%

GLOBAL

IOT

THE TOP TECHNOLOGIES NEEDED TO EXPAND USAGE

U.S.

63%

65%

DATA ENCRYPTION
SECURE DIGITAL IDENTITY
(AN ENCRYPTION TECHNOLOGY)

51%

47%

GLOBAL

CONTAINERS

ENCRYPTION THE TOP CONTROL NEEDED TO ENABLE GREATER ADOPTION

57%

55%

GLOBAL FEDERAL

U.S. FEDERAL

BEST PRACTICE RECOMMENDATIONS

GARRETT BEKKER, 451 RESEARCH

Re-prioritize your IT security tool set

Cloud and SaaS break legacy IT Security models – Data security with encryption and access controls across environments is required. Service-based solutions and platforms that include automation are preferred for reduced costs and simplicity.

Discover and classify

Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT

Don't just check off the compliance box

Global and industry regulations can be demanding, but agencies should consider moving beyond compliance to greater use of encryption and BYOK, especially for cloud and other advanced technology environments.

Encryption and access control

Encryption needs to move beyond laptops and desktops.

Data center: File and application level encryption and access controls

Cloud: Encrypt and manage keys locally, BYOK enables safe SaaS, PaaS and IaaS

Big Data: Encryption and access control within the environment

Containers: Encrypt and control access to data both within containers and underlying data storage locations

IoT: Use secure device ID and authentication, as well as encryption of data at rest on devices, back end systems and in transit to limit data threats

OUR SPONSORS



ABOUT THALES E-SECURITY

■ Instilling trust across the data landscape

Our powerful technology platform provides advanced data security for more servers, applications, and environments than any other security alternative

■ What we do

Thales e-Security provides companies everything they need to protect and manage their data and scale easily to new environments and requirements—encryption, advanced key management, tokenization, authorization, privileged user control, and HSMs.

■ Our customers


Our customers include 19 of the world's 20 largest banks, four of the world's five largest oil companies, 27 NATO country members and 15 of the Fortune 25.



Our solutions protect data while eliminating complexity, inefficiency and cost

DB/ File Encryption

Customer Records



Application Encryption

PII




Big Data

Secure Analytics




Code Signing

Script Development




Tokenization Data Masking

PCI, PHI



Transaction Security

Payment related apps



Public Key Infra (PKI)

Internet of Things



Cloud Security


Cloud Migration



Use Cases



DATA PROTECTION HARDWARE



DATA PROTECTION SOFTWARE

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

FEDERAL EDITION