THALES

451 Research®

2018 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

U.S. FEDERAL EDITION

EXECUTIVE SUMMARY

#2018DataThreat

THE TOPLINE

Federal agency data is under siege. Over half of all agency IT security pros surveyed report a breach in the past year

The U.S. federal government continues to struggle with the same cybersecurity challenges that most organizations are wrestling with, but against a different set of obstacles than typical commercial enterprises. Just as elsewhere, breach counts are continuing to mount even as record increases in IT security spending continue. Federal agencies, however, seem to be experiencing a "Perfect Storm" around data that is putting agency secrets, and the private data of over 330 million citizens, at risk by:

- Mounting cyber threats and attacks from cyber thieves and nation state hackers
- Requirements to make government more accessible and transparent via digital transformation
- The necessity of supporting and maintaining some of the oldest systems and software found anywhere

DATA BREACHES ARE THE NEW REALITY

Breached ever

71% of U.S. federal agencies have now been breached

Breached in the last year

Rates of breaches in the last year are up **3x** from 2016 in this year's results

CLOUD DRIVES EFFICIENCY, CREATES NEW EXPOSURES

Levels of concern are high

72% Fear increased vulnerabilities

68% Worry about breaches at the cloud provider

67% Think cloud privileged users are a threat

67% Are apprehensive about meeting their compliance requirements

Massive adoption compounds the problem

45% or more using **5 or more** IaaS or PaaS providers

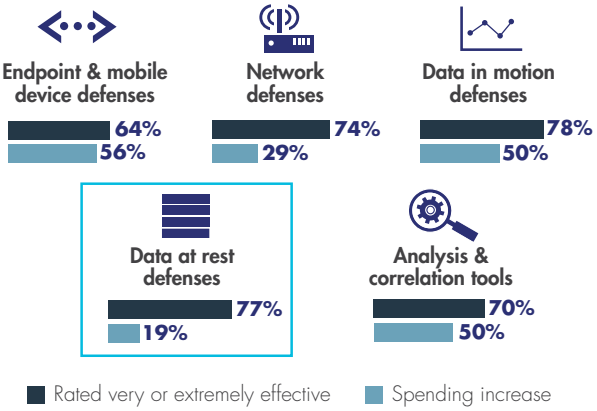
20% for commercial enterprises

48% Using more than **100 SaaS applications** – Where data is inherently harder to control

U.S. FEDERAL RESPONDENTS ARE STILL NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

"THE LARGEST AMOUNT OF RESPONDENTS PLAN TO INCREASE SPENDING ON ENDPOINT AND MOBILE DEVICES, DESPITE RANKING ENDPOINT AND MOBILE DEVICES AS LEAST EFFECTIVE AT PROTECTING SENSITIVE FEDERAL DATA – A MAJOR DISCONNECT."

—Garrett Bekker, 451 Research Principal Analyst, Information Security



ENCRYPTION IS THE CRITICAL SOLUTION

Encryption needed to drive use of digitally transformative technologies:

Good news – Agencies are implementing, or planning to implement, encryption technologies this year:

89% Data masking

88% Database and file encryption

84% Encryption in the cloud

77% Application layer encryption

FEDERAL AGENCY DATA IS UNDER SIEGE

Over half of all agency IT security pros surveyed report a breach in the past year

More than any industry we measured this year, federal agencies are experiencing higher rates of data breaches. Rates of data breaches in the last year reported by our federal respondents are 57% (versus 36% in our total sample), more than three times higher than the federal rate of 18% measured only two years ago. Federal agencies experience a very challenging threat environment in which they must protect sensitive data. They are targeted by criminals seeking citizen's private data, nation state hackers with their own agendas as well as suffering from perennial problems with funding, staffing and antiquated systems long since discarded by commercial enterprises. But these factors don't completely explain the steep rise in breach rates federal agencies are encountering.

Breached ever

71%

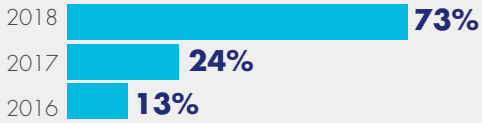
of U.S. federal agencies have now been breached

Breached in the last year

3x Rates of breaches in the last year are up **3x** from 2016 in this year's results

In spite of the challenges, agency IT security pros are reporting that positive developments are happening. Spending is sharply increasing this year. 93% in total reported that their agencies will increase IT security spending and 73% report that their IT security spending will be much higher. This change comes after several years where federal agencies rates of IT security spending increases were well below those of commercial enterprises. They also report implementing, or planning to implement, the encryption technologies that protect data best at rates of 77% or higher.

Spending increases: Federal agency rates of increasing IT security spending at a 'Much Higher' rate by year



88% of federal agency IT security pros report their organizations are implementing, or plan to implement **database and file encryption this year.**

Implementing now, or planning to implement, these top tools for protecting sensitive data.

89% Data masking

88% Database and file encryption

84% Encryption in the cloud

77% Application layer encryption

DIGITAL TRANSFORMATION IS ENABLING GOVERNMENT EFFICIENCY, AND CREATING NEW RISKS FOR DATA

New environments require new approaches to protecting citizen data, government secrets and other sensitive information

As in the private sector, digital transformation has evolved as a significant driver for data threats at federal agencies. The overall adoption of Cloud and SaaS applications, Big Data implementations, IoT, containers, mobile payments and blockchain technologies also raise security risks owing to their relative newness, the unique approaches required to protect data within each environment and the sheer scale of deployments. What's more, sensitive data will be used within these environments – as reported by 81% of respondents.

Adoption of the technologies for digital transformation in federal agencies is high

81% Using sensitive data within these environments

Adoption levels for digital transformation technologies by U.S. federal agencies

Nowhere is the risk to federal agency data clearer than in cloud environments. Due to the requirements of digital government initiatives, agency IT security pros report much higher adoption of cloud environments than their commercial counterparts. 45% are using 5 or more IaaS or PaaS environments (versus only 20% for commercial enterprises) and 48% are using more than 100 SaaS applications (versus 22% of all surveyed globally).

Massive adoption compounds the problem

45% or more using **5 or more** IaaS or PaaS providers

Versus

20% for commercial enterprises

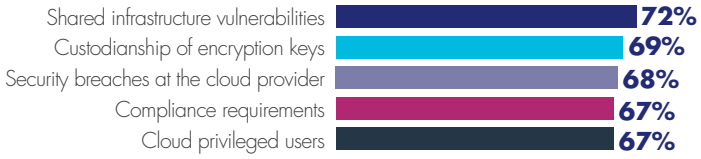
48% Using more than **100 SaaS applications** – Where data is inherently harder to control

For IaaS and PaaS, a specific data security plan must be created for each deployment and environment, then enforced by policy, operational methods and tools. For SaaS environments the case is more complex. In many environments agencies and enterprises are given little control over how their data is stored or protected, and in some cases where data security controls are available (such as AWS S3 storage buckets), we've often seen agencies fail to take control of their data with tools such as encryption that are readily available. Complicating the picture, agencies also seem to prefer that the cloud provider control their encryption keys rather than own and manage the keys themselves (34% to 32%), yet were also concerned about the custodianship of encryption keys in the cloud (69%). A basic security maxim is that whoever owns the keys, controls the data. Effectively, this leaves control of agency data security in the hands of the cloud provider. It's also a potential violation of NIST 800-53, FedRAMP and the federal risk management framework that requires agencies to maintain control of access to their data.

23% of federal agencies are using encryption to protect cloud data today

81% of federal agency IT security pros we surveyed report using sensitive data with tools for digital transformation – cloud, big data, IoT, containers, mobile payments and blockchain

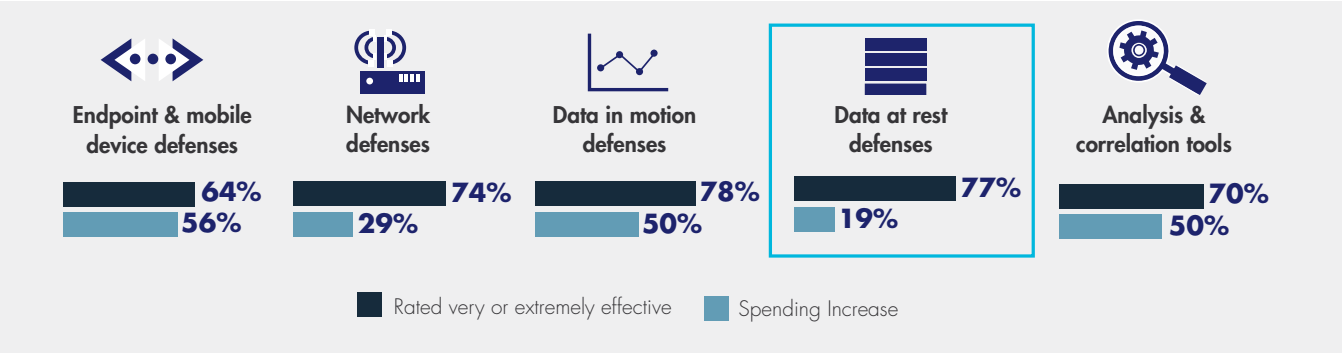
Top cloud security concerns



NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

Respondents report biggest spending increases in tools that no longer protect data effectively

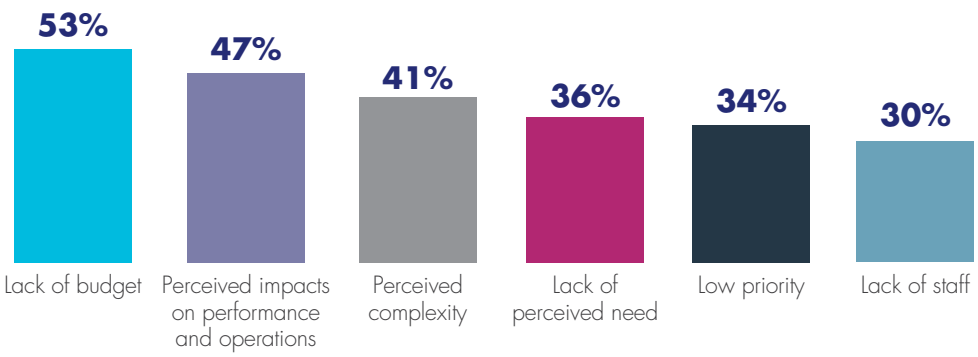
This year for the first time in our polling, we found that respondents clearly recognize that the defenses designed specifically for protecting data are the most effective tools for doing so. Data-in-motion and data-at-rest defenses were in a virtual tie at 78% and 77% respectively as the most effective tools for protecting data. But this isn't where increases in IT security spending are going. In fact, the data-at-rest defenses that are the most effective at protecting large data stores are getting the lowest increases in spending, at only 19%, while end point and mobile defenses garner the biggest increases (56%). In past years, there was often poor recognition of the most effective tools for data security, and so agencies could be at least partially forgiven for investing in the tools they "believed" were more effective. But not this year. It's clear respondents understood what's effective and working, but that's not where the money is going.



> "The largest amount of respondents plan to increase spending on endpoint and mobile devices, despite ranking endpoint and mobile devices as least effective at protecting sensitive federal data – a major disconnect."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

In part, the usual concerns about budget and priorities are cited as reasons for low data security adoption. But perhaps a larger part of the reason for the disconnect may be the perception that data security is hard, expensive and has a high impact on operations. Usually this perception is the result of having experience with older "legacy" data security tools. Modern tools have lower costs than in the past, extremely low performance overhead (as a result of using hardware encryption capabilities built into today's CPUS) as well as low impact on business processes and operations. In some cases, no changes are required to applications and operations on deployment of data security tools.

Perceived barriers to data security

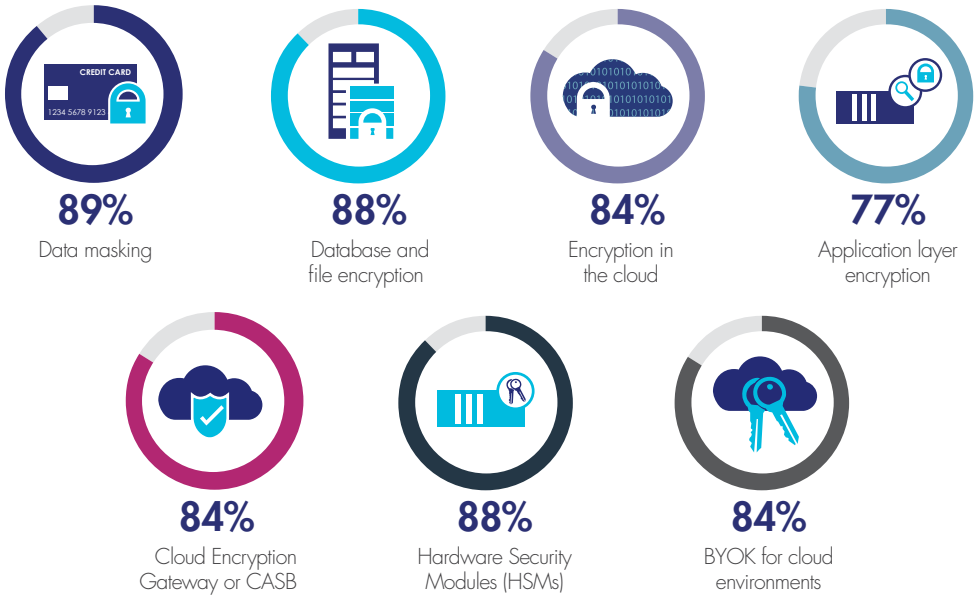


ENCRYPTION IS A CRITICAL TOOL NEEDED TO PROTECT SENSITIVE DATA

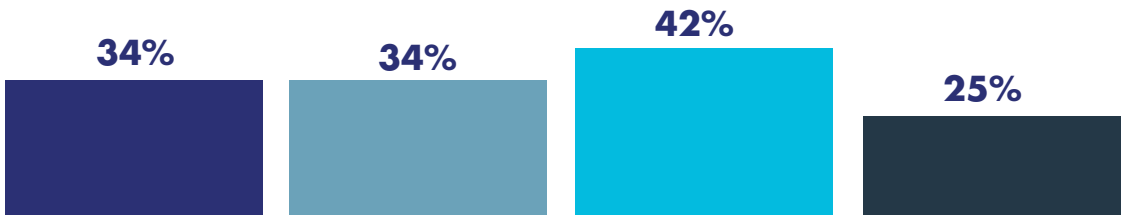
Protects data in traditional data centers, cloud, big data, and wherever sensitive information is used or stored

There's some good news to mix in with the other results this year. Not only did respondents identify that encryption technologies as the most effective way to protect data for the first time, but in spite of low spending levels, projects are underway to implement encryption for data protection at fairly high levels. Respondents identified that they are implementing now, or planning to implement encryption in the cloud, application layer encryption, database and file encryption and data masking at rates of 77% or higher in the next year. Considering that only 23% are using encryption in the cloud today, an 84% number for respondents implementing or planning to implement this year is an impressive turn around.

Good news – Agencies are implementing, or planning to implement, encryption technologies this year:



Encryption is also a clear leader among tools that agency professionals are looking for to increase usage of both cloud, big data, IoT and containers. Cloud encryption tools such as encryption gateways and third party encryption key managers for cloud environments are also showing strong plans for adoption as ways that respondents are looking at to bring cloud based data back under agency control.



Cloud: The top tool needed for more cloud use

Big Data: The capability to analyze encrypted/ tokenized data in big data environments the top tool needed for big data adoption

IoT: Secure authentication (an encryption technology) a top tool need for more IoT adoption

Containers: Encryption drives container usage

"The U.S. federal government continues to struggle with the same cybersecurity challenges that most verticals are wrestling with, but against a different set of obstacles that other markets don't usually face."

"Like most other sectors, data security spending plans in the U.S. federal sector are up compared to last year – WAY up. Perhaps more importantly, for the first time, U.S. federal ranks the highest of any U.S. vertical in terms of spending increase plans – more than 9 out of 10 (93%) plan to increase security spending in 2018."

"The bad news is that reports by U.S. federal respondents of successful breaches last year (57%) are far ahead of the global average (36%), and also the global federal sector (26%). Further, 70% of U.S. federal respondents say their agencies were breached at some point in the past."

—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

ENCRYPTION IS THE SOLUTION

Encryption technologies are critical to protecting data at rest, in motion and in use. Encryption secures data to meet compliance requirements, best practices and privacy regulations. It's the only tool set that ensures the safety and control of data not only in the traditional data center, but also with the technologies used to drive the digital transformation of the enterprise.

ABOUT THALES

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

CLICK HERE TO TO READ THE FULL REPORT

OUR SPONSORS

GuidePoint SECURITY

cloud security alliance℠

GEOBRIDGE

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com