# 2018
THALES DATA THREAT REPORT

Trends in Encryption and Data Security

U.S. FINANCE EDITION

EXECUTIVE SUMMARY

#2018DataThreat

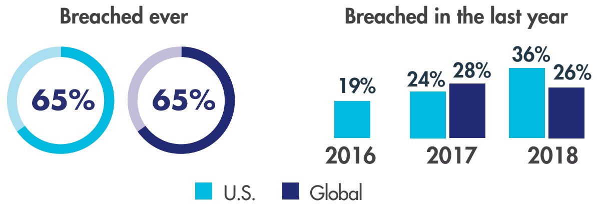
THE TOPLINE

Digital transformation, advanced attacks and strict new regulations all combine to leave financial services organizations at risk – from the life's blood of their operations, data.

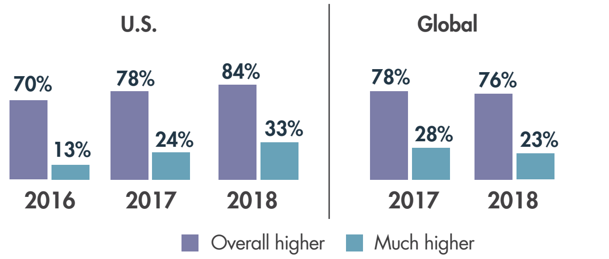
Any IT security pro from a financial services organization already knows, it's harder every year to protect their organization's and their data. Every piece of information used to run the business creates risk – financial data in accounts and investments, personal data on account holders, unique business methodologies, information stored or used in the cloud, blockchain implementations, mobile payments transactions, IoT deployments, big data lakes, and more.

INCREASES IN IT SECURITY SPENDING HAVEN'T STOPPED THE BREACHES

Rates of data breaches in financial services enterprises

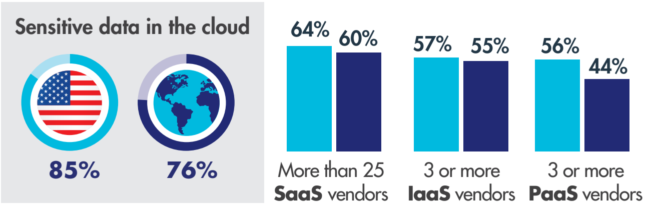


IT security spending increases for financial services enterprises

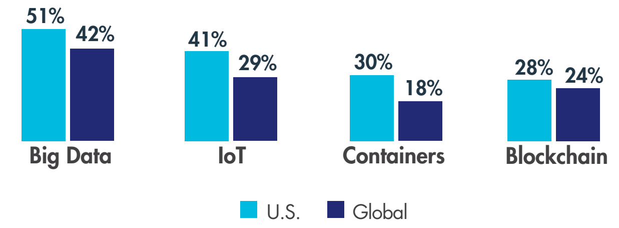


DIGITAL TRANSFORMATION EXPANDS DATA THREAT LANDSCAPES IN FINANCIAL SERVICES

With cloud adoption now universal, pervasive use of sensitive data across multi-cloud environments is a top problem

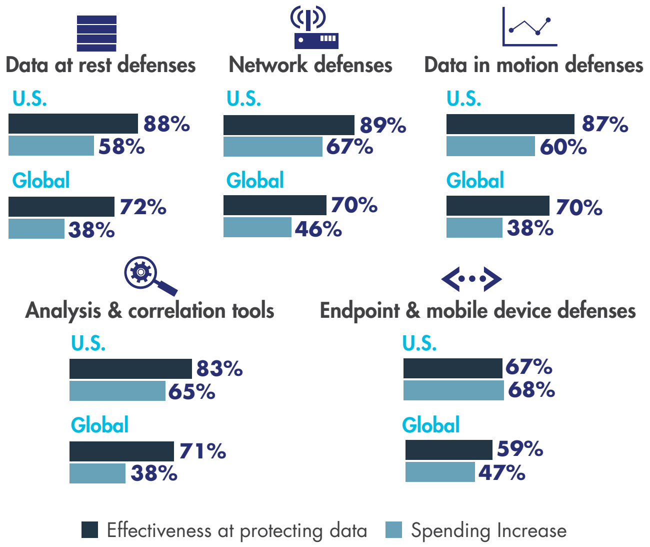


Rates of sensitive data use with other digital transformation environments



NOT PUTTING THEIR MONEY WHERE THEIR DATA IS

Respondents report their organizations increasing spending the least on the most effective tools for protecting data – data security



DIGITAL TRANSFORMATION – ENCRYPTION REQUIRED

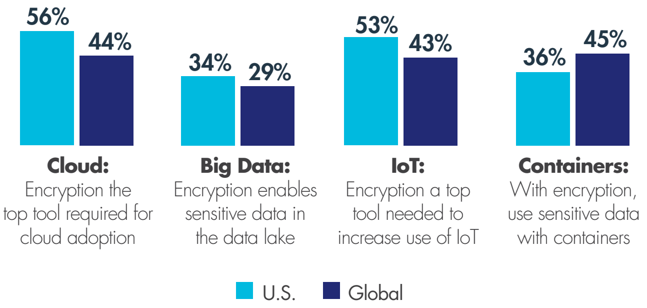
Encryption enables mobile payments and blockchain

Encryption establishes secure identity with digital birth certificates for mobile devices

Encryption protects data on devices

Encryption protects data-in-transit

Encryption and access controls help organizations meet compliance and privacy requirements



Financial services are also home to some of the strongest IT security controls, strictest regulations and highest rates of implementation for IT security best practices of any industry segment – but even this traditional emphasis hasn't stopped data breaches from causing fundamental damage. How bad is it? Our survey responses from IT security pros in financial services organizations in the U.S show a rate of data breaches over the previous 12 month period that is almost double that of two years ago – 36% were breached in this year's survey and 19% in our survey from two years ago. The overall rates of data breaches encountered in the past for US financial services organizations tracks this trend; 65% overall versus 42% overall last year. Elsewhere in the world, 65% of financial services organizations have now experienced a data breach versus just 49% last year.

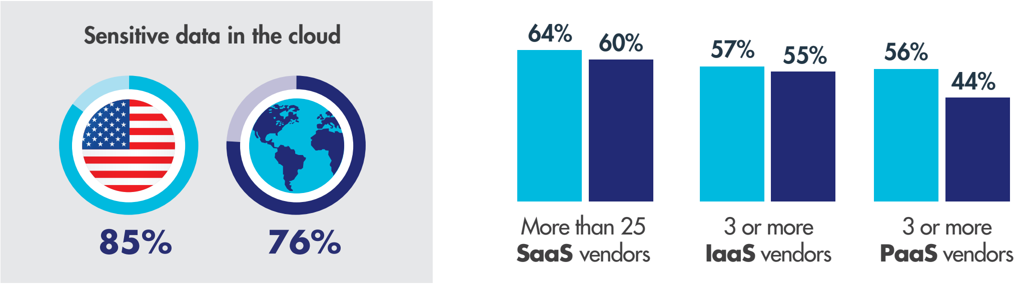
Moreover, this has been happening even in the face of ever increasing IT security spending. In the U.S., financial services respondents indicated that 70% were increasing spending two years ago, with 13% reporting much higher spending. This year 84% were increasing spending, with 33% reporting much higher spending. Looking at just that rate of "much higher" spending – the rate is up almost three times the earlier level. Results from outside the U.S. show similar results; 76% increasing spending this year, and 23% with much higher spending.

DIGITAL TRANSFORMATION REQUIRES A NEW DATA SECURITY APPROACH

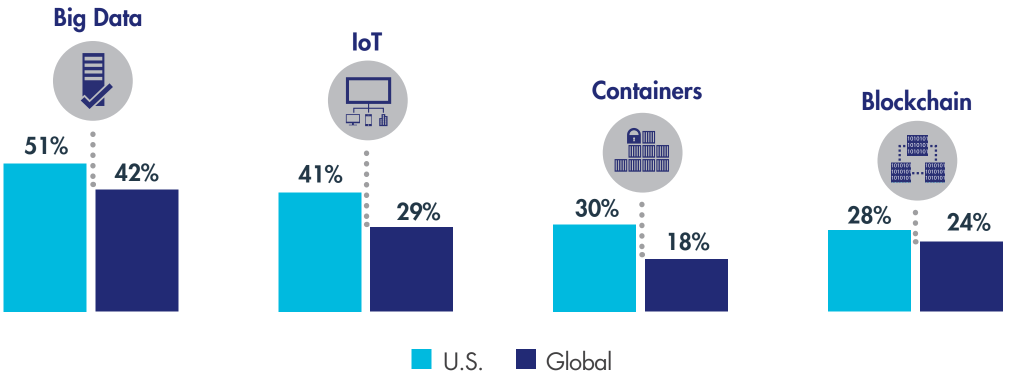
Digital transformation is driving essential innovation in financial services for both existing firms and newer financial technology (FinTech) companies. This drive for digital transformation in all the essentials of financial services businesses is creating an inflection point in the industry, where existing players adjust and innovate or be overtaken by newer more nimble competitors who leveraging technology changes to gain market share and profitability. For sensitive data, the risk is that the rush to deployment of digitally transformative technologies can leave sensitive data at risk. With these market forces in play, we found massive adoption of cloud, big data, IoT, mobile payments and blockchain technologies by financial services organizations. Cloud usage is now universal, with other new technology adoption rates all at the 90% plus level.

In each of these digital transformation environments, there are unique data security challenges that must be addressed for secure usage with sensitive data, but the cloud is the most problematic. Cloud usage with sensitive data is especially high at 85% for U.S. financial services organizations and 76% outside the U.S. With multiple cloud usage also at elevated levels, creating the new problem of how to secure sensitive data across multi-cloud deployments.

With cloud adoption now universal, pervasive use of sensitive data across multi-cloud environments is a top problem



Rates of sensitive data use with other digital transformation environments

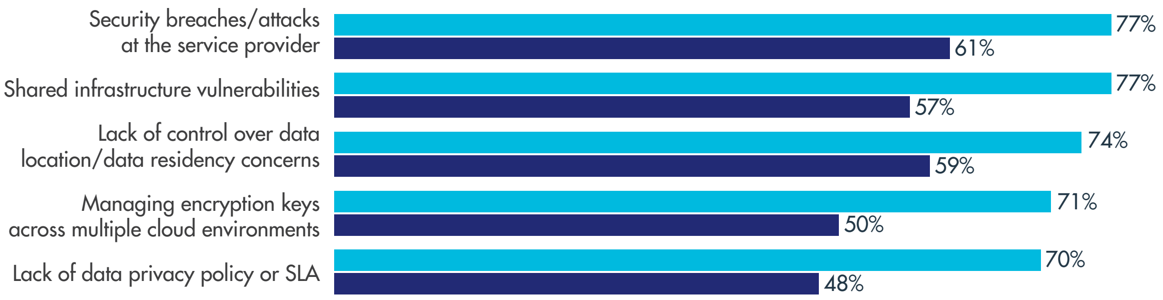


Multi-cloud operations creating big concerns for financial services

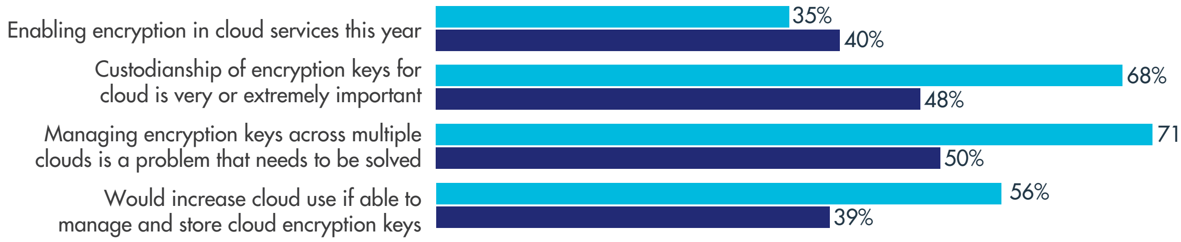
We found that 64% of U.S. respondents and 60% of respondents outside the U.S. identified that their enterprise uses more than twenty-five Software as a Service (SaaS) offerings, 57% in the U.S. were also using three or more Infrastructure as a Services (IaaS) offerings (55% outside the U.S.) and 56% in the U.S. three or more platform as a service (PaaS) offerings (44% outside the U.S.). This level of cloud service usage drives innovation and efficiency, but comes at a price for data security – and it can be measured by the unique requirements for protecting, and retaining control of, data within this range of environments.

In a traditional data center, not only is data physically secured within the four walls of the enterprise, but all of the infrastructure underlying implementation tools and networks are also under the direct control of the organization. Now, for IaaS, a specific data security plan must be created for each deployment and environment, then enforced by policy, operational methods and tools. For SaaS and PaaS environments, the case is more complex. In many of these environments, organizations retain 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 or Salesforce implementations) managing encryption keys, and access controls become a new task, requiring new expertise and tools. Third party offerings that reduce this complexity with integrated management of encryption technologies for multiple environments are starting to become available, but are not yet widely recognized. Organizations are going to need them – a basic security maxim is that whoever controls the keys, controls the data. Encryption – with encryption key control either local or remote from the cloud environment managed – is required.

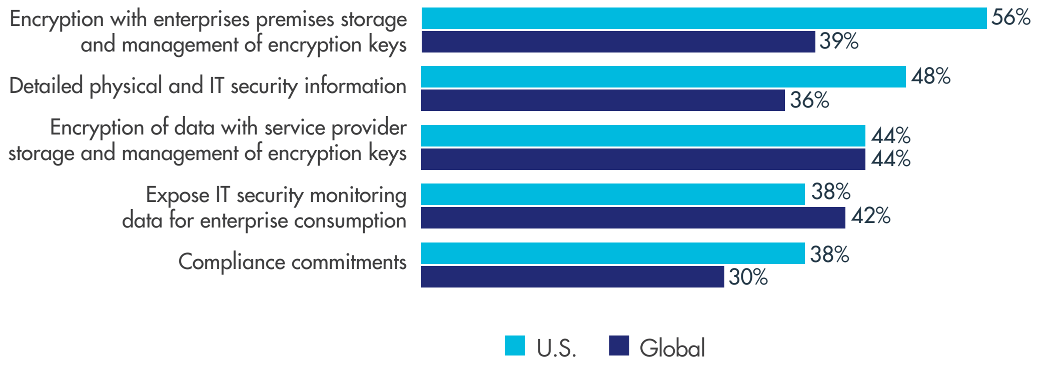
Top concerns with cloud computing



Recognition of the problem



Top it security tools need to expand cloud computing use



> “As organizations increasingly engage with multiple cloud providers, who maintains control over encryption keys has become a huge potential issue, particularly for those who take advantage of native encryption services.”

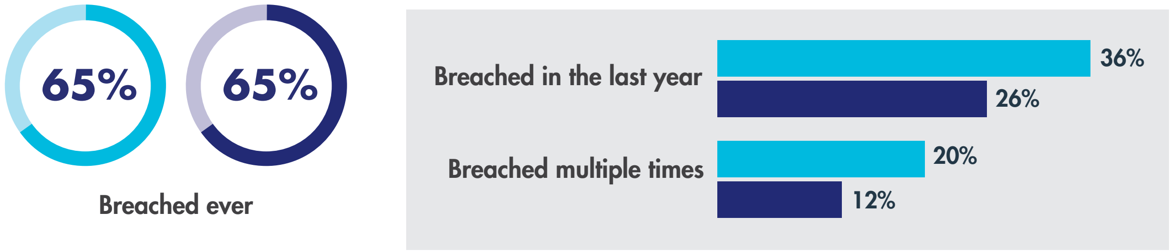
—Garrett Bekker, 451 Research Principal Analyst, Information Security
Author of the 2018 Thales Data Threat Report

FINANCIAL SERVICES IT SECURITY SPENDING IS UP – AND SO ARE DATA BREACHES

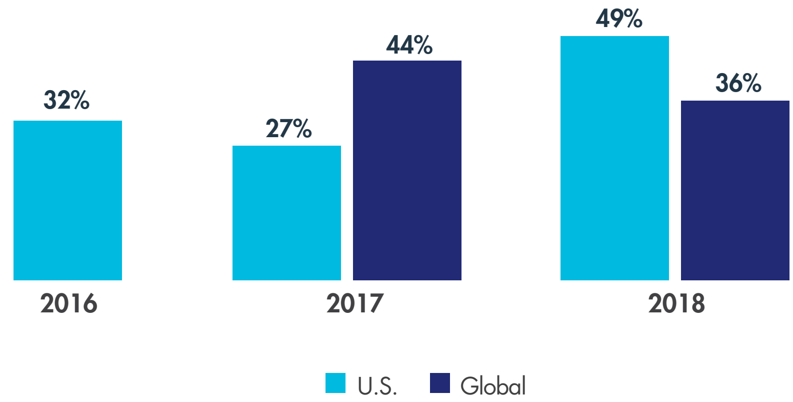
Of particular concern for financial services organizations are not only the elevated rates of breaches being encountered (65% in total for both the U.S. and Global respondents), but also the rates of being breached in the last year, being breached multiple times and for the U.S. the rate of increase in data breaches occuring each year. Breach rates occuring each year in the U.S. have increased from 19% just two years ago, to 36% in the current survey – Nearly doubling in that period. Outside the U.S., these rates have remained relatively high for both years that we've surveyed (this year and last) at 26% and 28% respectively – but these levels still reflect that one in four is being breached every year.

Last and most troublesome, are results for the U.S. showing that the rate of organizations in financial services that have had repeated breaches continues to grow; to 20% this year from 12% last year (data on this point was not collect for global financial services firms previously). This change indicates that 56% of U.S. financial services firms that were breached this year were also breached in the past – that they are not succeeding in putting in place the changes needed to reduce their risk and breach rate, or perhaps simply not making it a priority. There is some evidence that this may be the case for a minority of financial services organizations – 28% in the U.S. and 22% elsewhere selected "Lack of perceived need" as a barrier to deploying data security in their organizations.

Data breaches reported by financial services respondents



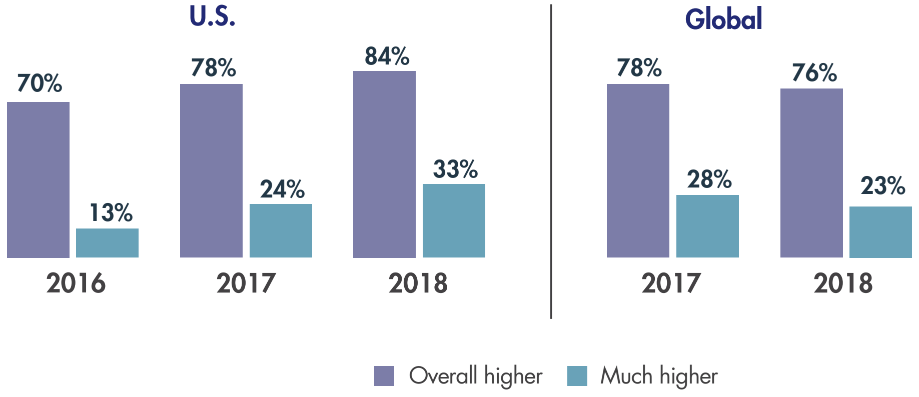
Feel that their organization is "very" or "extremely" vulnerable to data threats



Our results show good news as well. IT security budgets are starting to expand to counteract these threats. 84% in the U.S. and 76% globally of financial services firms are increasing their IT security spending, with 33% in the U.S. and 23% elsewhere reporting that IT security spending will be much higher this year. In the next section, well look at whether these deployments are being invested where they are most likely to succeed at protecting data.

> "Look for data security toolsets that offer services-based deployments, platforms, and automation that reduce usage and deployment complexity for an additional layer of protection for data."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

How will organizations mitigate these risks? – increasing spending



ORGANIZATIONS NEED TO CHANGE HOW THEY PROTECT THEIR DATA

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

We found that respondents clearly recognize the defenses designed specifically for protecting data are the most effective tools for doing so. Data-at-rest and data-in-motion defenses were rated as two of the top three tools for protecting data. In the U.S. with 88% and 87% responded that they were either 'very' or 'extremely' effective, and 72% and 70% elsewhere around the globe.

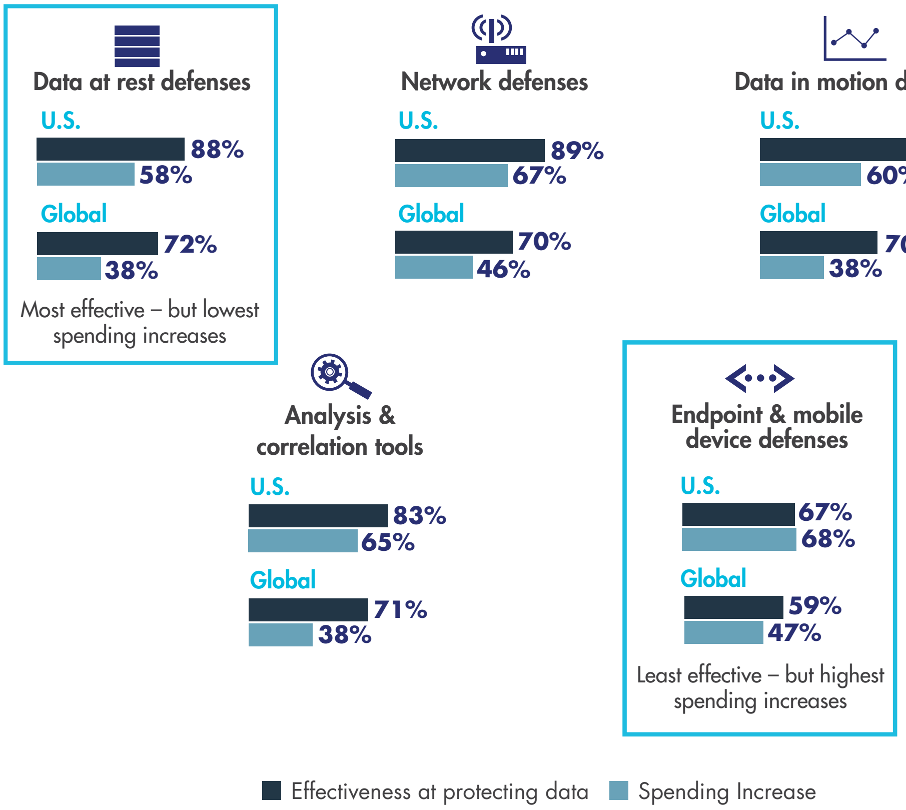
However, data-at-rest security tools, among the best methods for protecting data repositories, are not getting a high priority in spending increases. In fact, the data-at-rest defenses that are the most effective at protecting large data stores are the lowest priority for increases in IT security spending, with only 58% increasing spending in this area in the U.S. and 38% elsewhere – the lowest of all our categories measured.

At the same time, increases in IT security spending are greatest for end point and network defenses, even as these tools are no longer wholly effective against attacks designed to compromise data.

Not only does cloud computing also makes network security tools less relevant as new infrastructure is increasingly not implemented within the four walls of the enterprise, but modern attack methods make it almost impossible to keep intruders away from critical data stores solely with network and endpoint-based security controls. As respondents recognize, the most effective solutions are security controls that provide an additional layer of protection directly around data sets, and to help identify attacks underway against data based on analytics such as data access patterns. Data-at-rest and data-in-motion security tools can reduce attack surfaces and provide the information that analytics tools need to quickly find and stop attacks designed to mine critical data while in progress.

> "A common theme we have observed across virtually every vertical and geographic market in the *Thales 2018 global data threat report* also held true for U.S. Financial services: namely spending the most on defenses deemed least effective."
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

Respondents report their organizations increasing spending the least on the most effective tools for protecting data – data security



ENCRYPTION IS A CRITICAL TOOL FOR PROTECTING SENSITIVE DATA – WHEREVER IT RESIDES

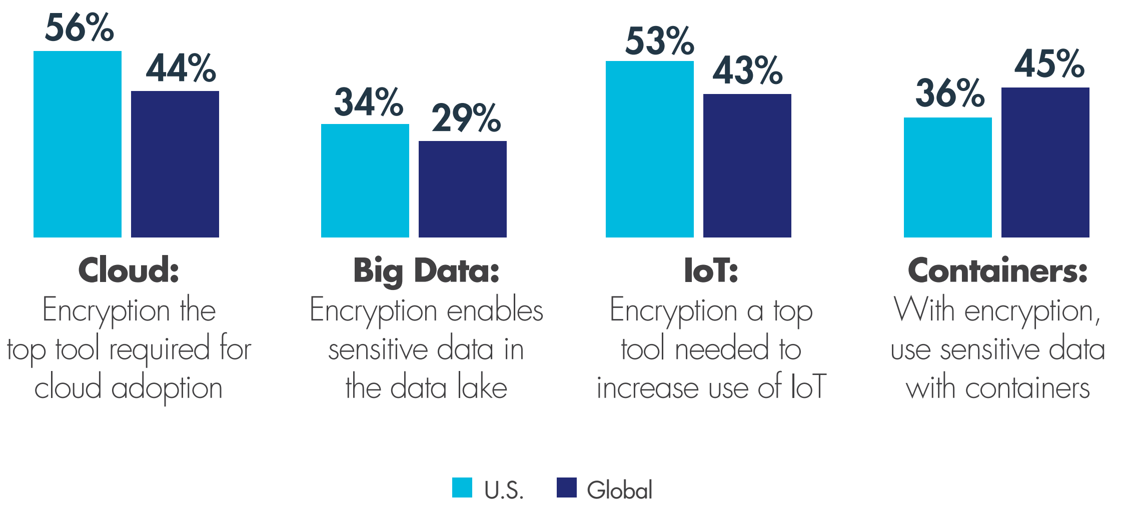
Protects data in traditional data centers, cloud, big data, and wherever sensitive information is used or stored

Good news. Not only did our respondents identify that encryption technologies as among the most effective way to protect data, but in spite of lower comparative spending levels for these data security controls, projects are underway to implement encryption for data protection. Data masking and database/file encryption were two of the top 3 data security tools planned to be implemented this year, and encryption was also recognized as the top tool needed to meet global data privacy requirements such as GDPR.

Top 5 data security tools that are being implemented this year in financial services

	U.S.	Global
Data access monitoring	72%	55%
Data masking	67%	61%
Database/ file encryption	64%	60%
Application layer encryption	58%	47%
Enable encryption in a cloud service (SaaS, PaaS, IaaS)	58%	42%

Digital Transformation – Encryption Required



Encryption establishes secure identity with digital birth certificates for mobile devices

Encryption protects data on devices

Encryption protects data-in-transit

Encryption and access controls help organizations meet compliance and privacy requirements

> “Firms should consider greater use of encryption and BYOK, especially for cloud and other advanced technology environments to both address growing compliance mandates and also to move closer to industry best practices.”
>
> *—Garrett Bekker, 451 Research Principal Analyst, Information Security*
> ***Author of the 2018 Thales Data Threat Report***

"Don't just check off the compliance box – More than three-fourths of U.S. Financial respondents still have considerable faith in compliance mandates. However, financial organizations should consider moving beyond compliance and adopting security tools such as encryption or tokenization that may be more appropriate as new technologies like cloud, IoT and mobile payments are increasingly adopted by financial firms looking for a competitive edge."

"Year-to-year increases in IT security spending across a broad range of vertical markets and geographies have done little to stem the tide of breaches … The obvious – or what should be obvious – question is whether the cyber defenses that are being deployed today need to be re-examined for overall effectiveness and recalibrated."

"Financial firms are putting most of its security spending in support of technologies and solutions it ironically deems least effective, while budgeting the least spending in areas it deems most effective at stopping breaches"

"In such a highly regulated industry as financial services and with GDPR in full bloom, data sovereignty looms large. Only 19% of U.S. Financial respondents and Global Financial respondents say they won't be impacted by GDPR (13% global average)."

"Two-thirds (67%) of U.S. Financial respondents and 68% of Global Financial respondents report that using machine language or AI helps increase data security by recognizing and alerting on attacks. On the flip side, 43% of U.S. Financial respondents and 46% of Global Financial say the use of AI/Machine Learning is resulting in increased breaches due to their ongoing use by sophisticated hackers."

—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 a 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

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

SAMSUNG

THALES

www.thalesesecurity.com