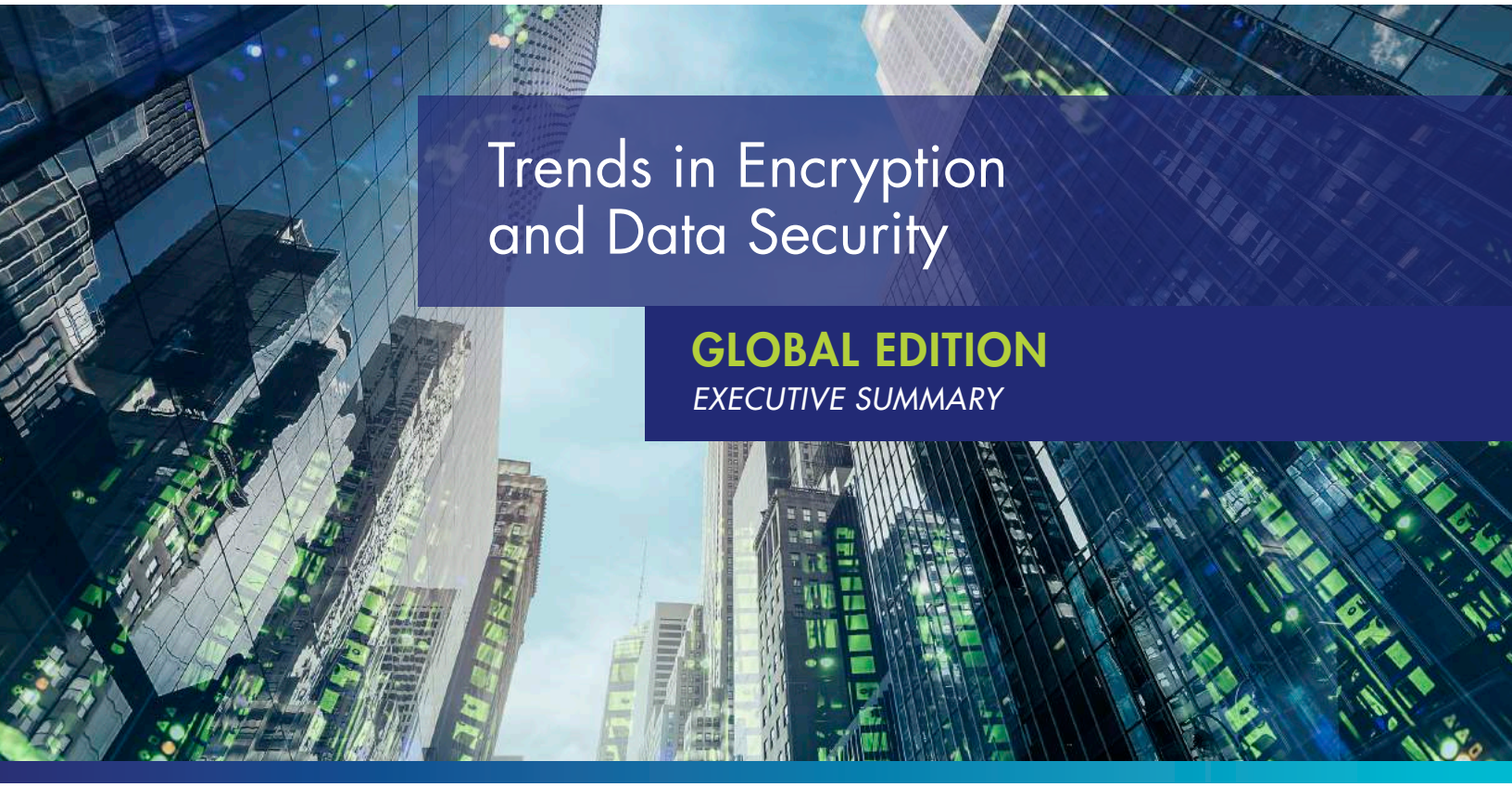
THALES

451 Research

2018 THALES DATA THREAT REPORT



Trends in Encryption and Data Security

GLOBAL EDITION

EXECUTIVE SUMMARY

#2018DataThreat

THE TOPLINE

Digital transformation is driving massive turmoil. Change how you protect your data – Or be breached. Again.

Now in its 6th year, the 2018 Thales Data Threat Report quantifies the extent of data breaches at medium and larger enterprises worldwide, pinpointing risks, detailing security spending plans and providing critical insights into how organizations can keep from becoming a data breach statistic.

This year, we found that organizations are dealing with massive change as a result of the latest round of digital transformation. As digital transformation inherently drives organizations into a data driven world, 94% of organizations are using sensitive data in cloud, big data, IoT, containers or mobile environments – this is creating new attack surfaces and new risks for data that need to be offset by data security controls.

DIGITAL TRANSFORMATION REQUIRES NEW DATA SECURITY APPROACHES

94% use digital transformation technologies with **sensitive data**

High levels of adoption compound the problem

100% Enterprise Cloud adoption is now universal

99% use Big Data

94% implement IoT

91% working on or using Mobile Payments

ORGANIZATIONS NEED TO CHANGE HOW THEY PROTECT THEIR DATA

Breached Ever

67% of enterprises have now been breached

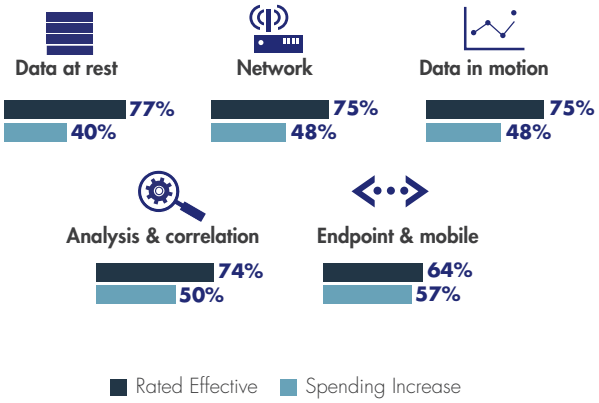
Breached in the last year

2018 **2017** **2016**

Every year, the rate of enterprises that are encountering data breaches grows

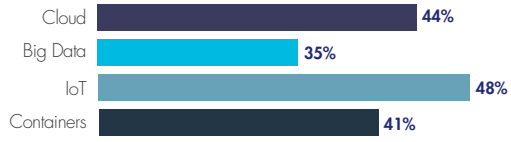
GROUNDHOG DAY: TIMES HAVE CHANGED, SECURITY STRATEGIES HAVE NOT

IT Security pros know what works to protect data – but aren't prioritizing increased spending on data at rest security



ENCRYPTION IS THE CRITICAL SOLUTION

Encryption needed to drive use of digitally transformative technologies:



Encryption tools top the plan for data security tools to be purchased in the next year:

44% Tokenization

43% Encryption with BYOK

41% Hardware Security Modules for secure

SENSITIVE DATA MORE AT RISK THAN EVER

Digital transformation is not only driving massive turmoil in IT, it also requires new approaches to data security.

Digital transformation drives efficiency and scale for existing products and services, while also making possible new business models that drive growth and profitability. Enterprises are embracing the opportunity by leveraging all digital technology offers, but can leave the security of their sensitive data at risk in the rush to deployment.

We found that the overall adoption of cloud, big data, IoT, containers, mobile payments and blockchain technologies by enterprises is at record levels to drive this transformation. With some technologies (like big data) reaching 99% adoption, and with 94% planning to use sensitive data within these environments. The scale of adoption makes this problem hyper-critical, as organizations are now using many vendors and environments.

High usage of digitally transformative technologies compounds the data security problem

94% of enterprises use **sensitive data** with tools for digital transformation.

High levels of adoption compound the problem

100% Enterprise Cloud adoption is now universal

99% use Big Data

94% implement IoT

91% working on or using Mobile Payments

Attacks are breaching enterprise defenses at record rates.

The extent and impact of increased threats is most clearly shown in levels of data breaches and vulnerability. Data breach rates are at an all time high – 67% of organizations now report that they have been breached globally (and 71% in the US). And data breach rates are highest in the last year – 36% of enterprises globally were breached in the last year alone (and almost half of all organizations – 46% – in the US). As a consequence, we found record levels of vulnerability in enterprises, with 44% Globally (and 53% in the US) feeling very or extremely vulnerable to data threats.

Breached Ever

67%

of enterprises have now been breached

Breached in the last year

2018 **2017** **2016**

Every year, the rate of enterprises that are encountering data breaches grows

DEPLOYING TO THE CLOUD – DATA SECURITY REQUIRED

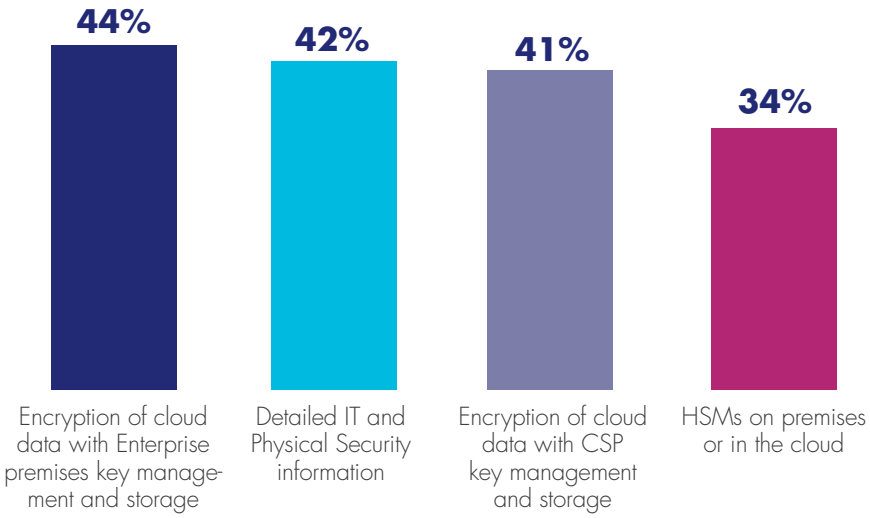
Securing data regardless of where it is deployed becomes a critical problem.

Cloud usage is nearly universal, and use cases are continuing to proliferate – causing enterprise adoption rates to skyrocket. Cloud computing (39%) is now tied with avoiding data breach penalties (39%) and closely followed by compliance (37%) as a top motivation for IT security spending.

Most firms are pursuing multi-cloud strategies, with SaaS usage especially high – 42% are using 50 or more SaaS applications, and the majority of companies are using 2 or more IaaS and PaaS vendors. The proliferation of cloud usage challenges the traditional concept of an enterprise "perimeter", as infrastructure and underlying software are no longer under enterprise control. The result is that data security becomes a front-line technology enabling usage with cloud encryption solutions the top security control needed (at 44%). The proliferation of vendors then creates another problem – managing, maintaining and storing encryption keys for all of these environments to retain control of data. Managing BYOK across multiple clouds, and against a growing set of compliance requirements, results in a need for solutions that enable enterprises to manage encryption keys and access data securely, and without unacceptable overhead.

Top Cloud Security Concerns
(rates of very/extremely concerned)

Encryption The top IT security control needed to expand cloud adoption



EVERYBODY IS USING BIG DATA – SENSITIVE DATA PROTECTION REQUIRED

Big Data is a global juggernaut. With 99% of enterprises now using big data (and 45% already using big data with sensitive information), these environments are increasingly at risk of for compliance, privacy regulation problems and data breaches. The complex, quickly changing nature of these environments results in the potential for sensitive data to be located anywhere within the environment, complicates the problem, and brings risks of inappropriate access as well. An added complexity, often big data is implemented in cloud environments – compounding enterprise perception of risk with infrastructure and the location of data no longer under enterprise control.

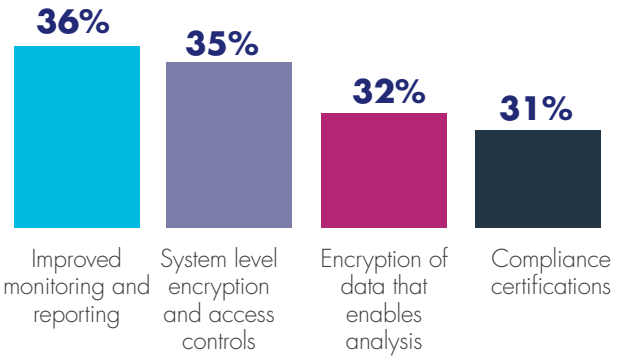
99% of enterprises now use big data

45% are using sensitive data within their big data environments

Top concerns for sensitive data within big data environments

What's needed to speed Big Data adoption?

38%
Stronger user authentication



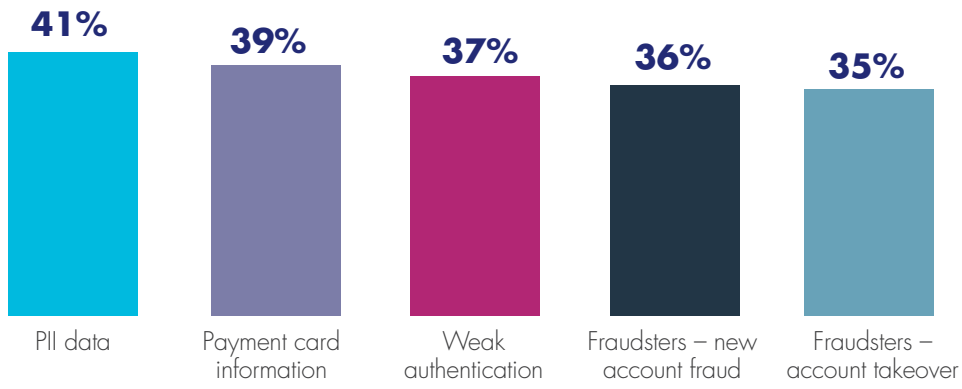
MOBILE PAYMENTS ON THE RISE – ENCRYPTION REQUIRED

Mobile payment applications are gaining wide adoption. 91% of enterprises we surveyed this year either have a mobile payment application in development or already deployed. But at the same time there are many concerns for vulnerabilities within the mobile payment ecosystem. Mobile payments inherently require data security at all phases of usage because of the potential loss of financial and personal information inherent in their use. Encryption thus becomes a key technology needed to secure the end-to-end mobile payment environment, as well as to meet quickly evolving regulations and industry standards.

91%
Using or planning to use mobile payments

37%
are using sensitive data with mobile applications today

Top concerns with mobile payments



Encryption a key tool enabling safe use of mobile payments

- Encryption establishes secure identity with digital birth certificates for devices
- Encryption protects data-in-transit
- Encryption protects data on devices
- Encryption and access controls help organizations meet compliance requirements for back end data stores

"Successful breaches have reached an all-time high for both mid-sized and enterprise class organizations, with more than two-thirds (67%) of global organizations and nearly three fourths (71%) in the U.S. having been breached at some point in the past. Further, nearly half (46%) of U.S. respondents reported a breach just in the previous 12 months, nearly double the 24% response from last year, while over one-third (36%) of global respondents suffered a similar fate."

"Clearly, doing what we have been doing for decades is no longer working. The more relevant question on the minds of IT and business leaders, then, is more direct: 'What will it take to stop the breaches?.'"

—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

GEOBRIDGE CRITICALSTART CSA cloud security alliance OASIS

THALES

www.thalesesecurity.com