

2017 THALES DATA THREAT REPORT

Trends in Encryption
and Data Security

FINANCIAL SERVICES EDITION

2017 THALES DATA THREAT REPORT

TRENDS IN ENCRYPTION AND DATA PROTECTION



Copyright 2017 Thales



U.S. FINANCIAL SERVICES – IT SECURITY SPEND INCREASES AND SO DO THE BREACHES

78% OF U.S. FINANCIAL SERVICES RESPONDENTS REPORTED THAT THEIR ORGANIZATIONS SPENDING ON IT SECURITY WILL BE INCREASED, BUT RATES OF BREACHES IN THE LAST YEAR INCREASED FROM 19% LAST YEAR TO 24% THIS YEAR

“ CLEARLY, THERE’S STILL A BIG DISCONNECT BETWEEN WHAT WE ARE SPENDING THE MOST OF OUR SECURITY BUDGET ON AND WHAT’S NEEDED TO ENSURE THAT OUR SENSITIVE DATA REMAINS SECURE.”

GARRET BEKKER – SENIOR ANALYST, INFORMATION SECURITY

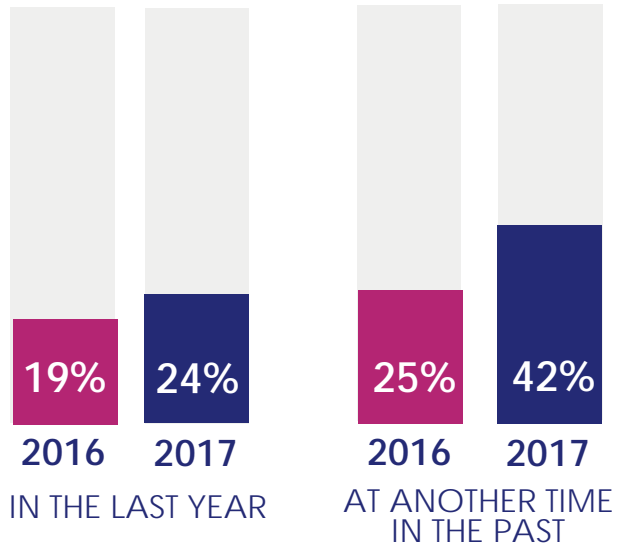
U.S. FINANCIAL SERVICES

INCREASINGLY A TARGET FOR DATA BREACHES

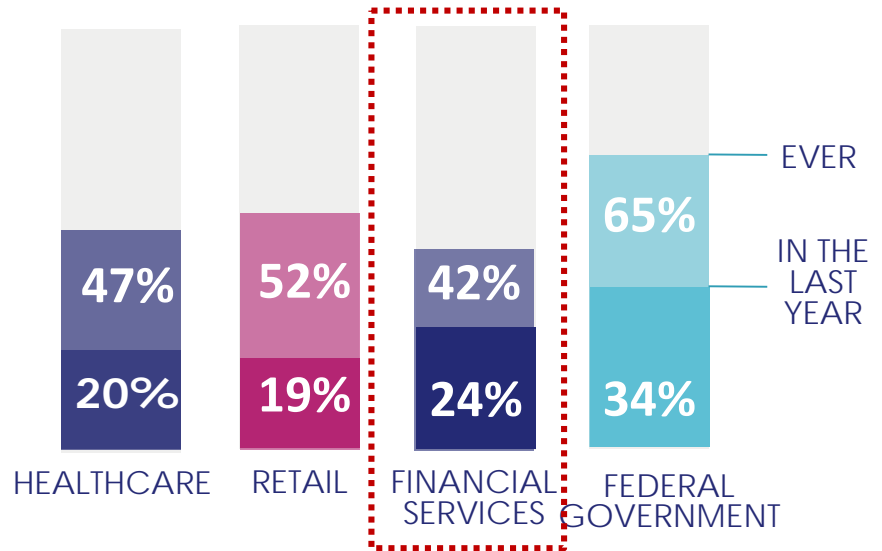
" 24% of U.S. financial firms reported a breach last year, slightly lower than the overall global average of 26%, but higher than most other U.S. verticals and also up markedly from 19% the previous year ... the implication is that U.S. financials are becoming more of a target.

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

U.S. FINANCIAL SERVICES DATA BREACHES



2017 DATA BREACH RESULTS BY U.S. VERTICAL



U.S. FINANCIAL SERVICES

42%

HAVE
EXPERIENCED A
DATA BREACH

- 24% IN THE LAST YEAR
(UP FROM 19% PREVIOUSLY)
- 12% MORE THAN ONCE



GLOBAL FINANCIAL SERVICES

49%

HAVE
EXPERIENCED A
DATA BREACH

- 28% IN THE LAST YEAR
- 21% MORE THAN ONCE

".. 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

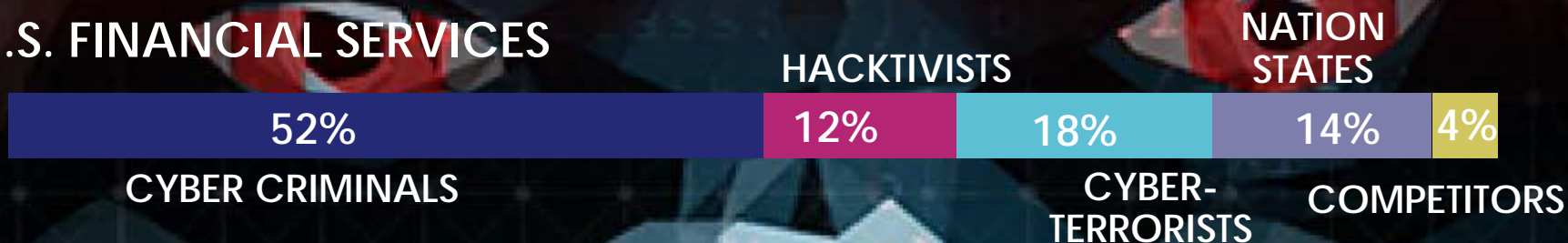
THE MOST DANGEROUS INSIDERS



“FINANCIAL FIRMS ARE A PRIME TARGET OF ATTACKERS, BECAUSE, IN THE INFAMOUS WORDS OF WILLIE SUTTON, ‘THAT’S WHERE THE MONEY IS.’”

TOP EXTERNAL THREAT ACTOR SELECTIONS

U.S. FINANCIAL SERVICES



GLOBAL FINANCIAL SERVICES



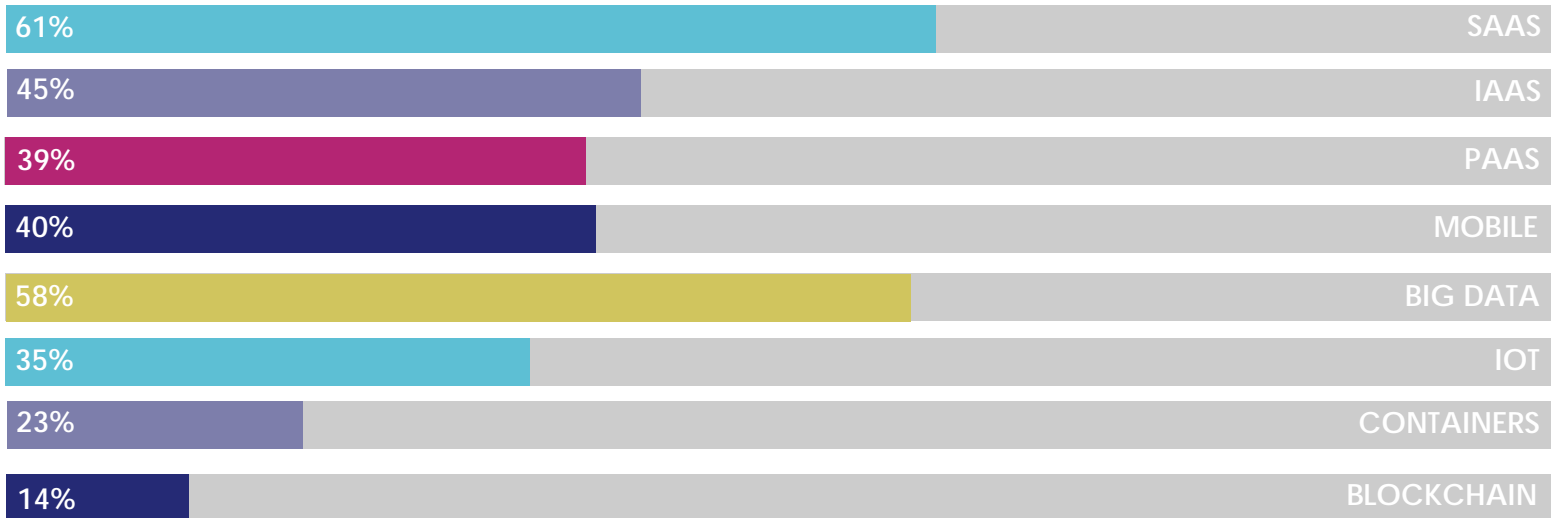
U.S. FINANCIAL SERVICES USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES WITHOUT DATA SECURITY

47%

OF U.S. FINANCIAL SERVICES RESPONDENTS
SURVEYED ARE DEPLOYING NEW TECHNOLOGIES
IN ADVANCE OF HAVING APPROPRIATE LEVELS
OF DATA SECURITY IN PLACE

96%

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



* U.S. RESULTS

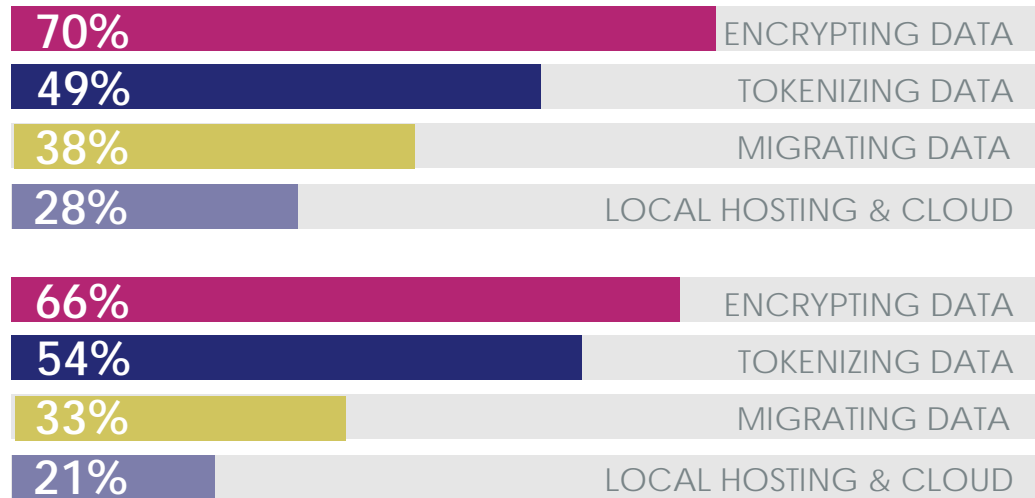
WITH NATIONAL REGULATIONS LIKE GDPR COMING WORLDWIDE DATA PRIVACY AND SOVEREIGNTY ARE MAKING WAVES EVERYWHERE



75% - U.S.
72% - GLOBAL

Impacted by Data Privacy and
Data Sovereignty

ADDRESSING REQUIREMENTS BY: **U.S. Fin Serv.**



GLOBAL FINANCIAL SERVICES

**100+ NATIONAL DATA
PRIVACY/SOVEREIGNTY
REGULATIONS WORLDWIDE**



EUROPE

**GDPR GOES
LIVE MAY 2018**



JAPAN

**AIPP DATA
PROTECTION AND
PRIVACY RULES LIVE
MAY 2017**



MEXICO

**LFPDPPP PRIVACY
LAW WITH FINES UP
TO £ 1.5M**



AUSTRALIA

**NEW DATA BREACH
DISCLOSURE
REQUIREMENT
ENFORCEMENT
BEGINS
FEBRUARY 2018**

86%

OF U.S. FINANCIAL SERVICES
RESPONDENTS FELT THEIR ORGANIZATIONS
WERE VULNERABLE TO DATA THREATS

27%

WERE VERY OR EXTREMELY VULNERABLE

"Today's unbroken string of high profile data breaches serves as stark proof that data on any system can be attacked and compromised."

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

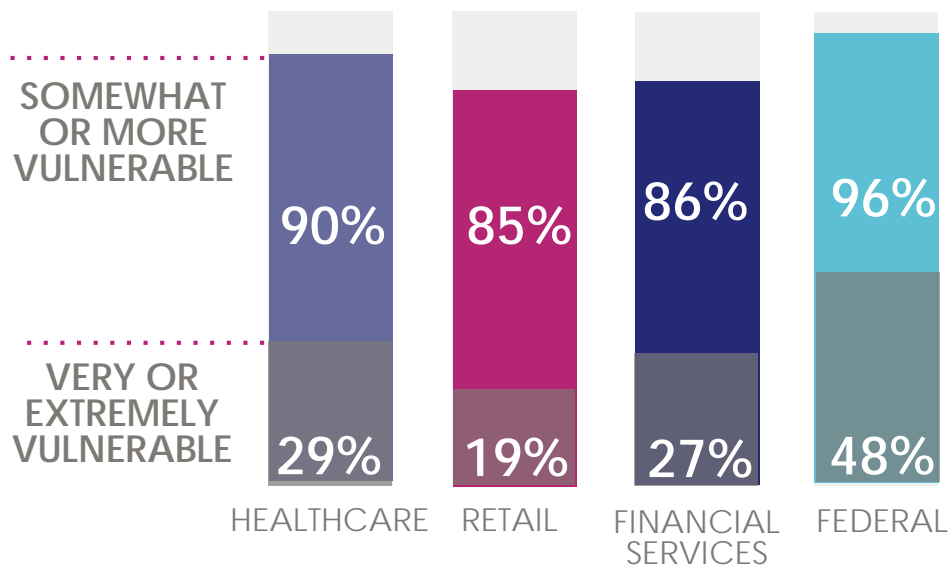
FINANCIAL SERVICES ORGANIZATIONS

FEELING VULNERABLE

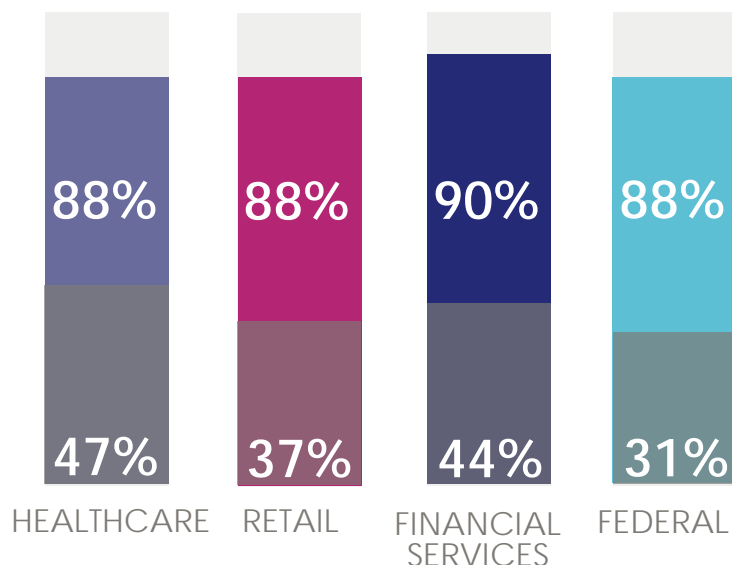
"Just 27% of U.S. respondents said they feel 'very' or 'extremely' vulnerable to data threats, slightly below the global average of 30%. Global financial respondents, however, show a much greater degree of concern, with a full 43% indicating 'very' or 'extremely' vulnerable."

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

U.S. Verticals



Global Verticals



\$ €

£

78%

EXPECT THEIR
SPENDING ON
IT SECURITY TO
INCREASE

2017

78%

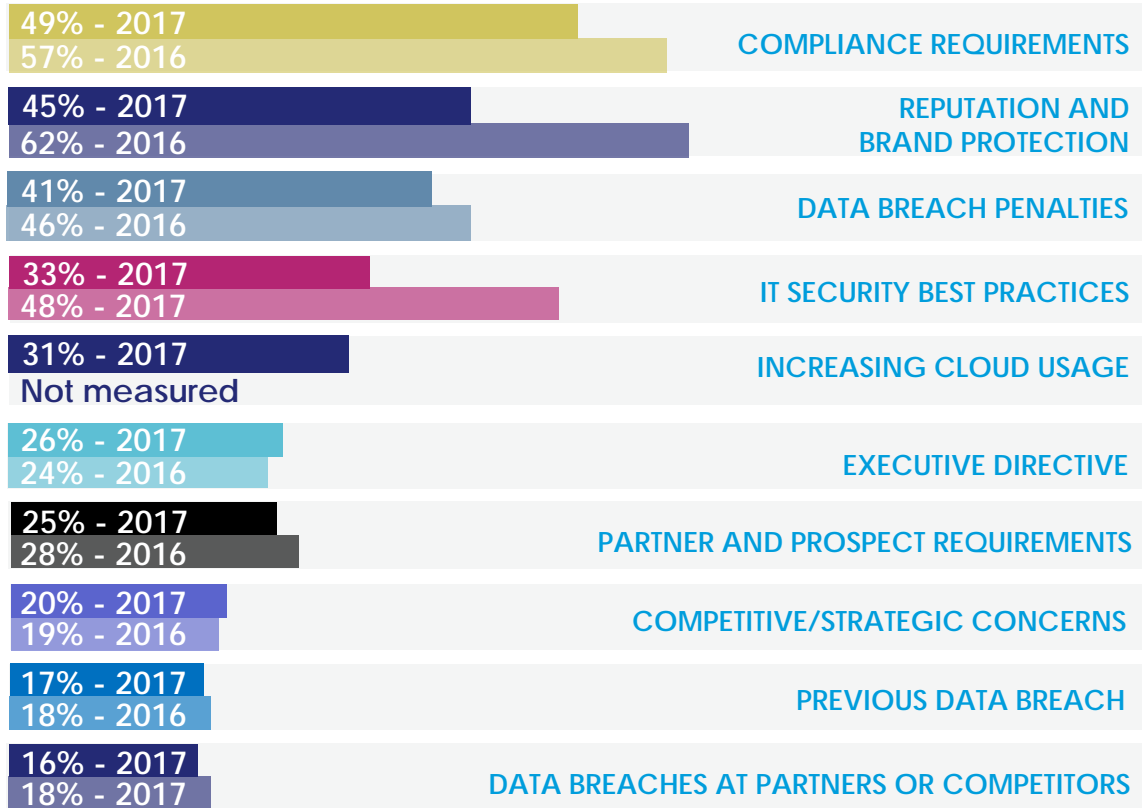
2016

70%

- UP FROM 70% IN 2016
- GLOBAL AVERAGE 73%

COMPLIANCE THE TOP PRIORITY FOR U.S. FINANCIAL SERVICES IT SECURITY SPENDING

IT SECURITY SPENDING PRIORITIES (RATES OF TOP 3 SELECTION)



“ONCE AGAIN OWING TO HEAVY REGULATIONS, COMPLIANCE REQUIREMENTS ARE THE TOP REASON FOR SECURITY SPENDING AT 49% FOR U.S. FINANCIAL RESPONDENTS, WITH REPUTATION AND BRAND SECOND AT 45%, FOLLOWED BY PENALTY AVOIDANCE – WHICH IS CLEARLY RELATED TO COMPLIANCE – AT 41%.

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

OLD HABITS DIE HARD – INVESTING HEAVILY IN NETWORK/END POINT SECURITY AS THEY BECOME LESS EFFECTIVE AND LESS RELEVANT

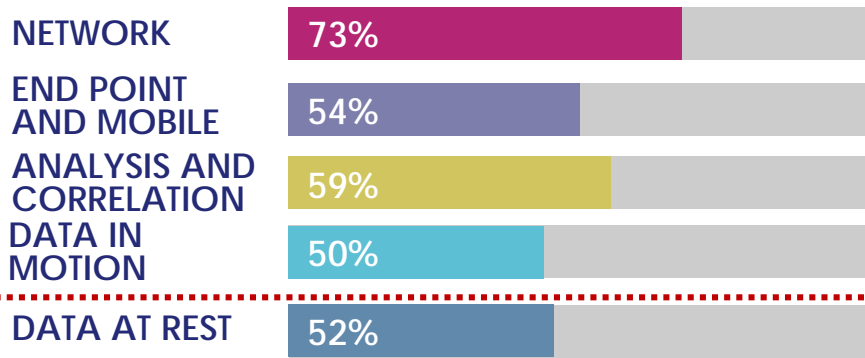
89%

+4% FROM 2016

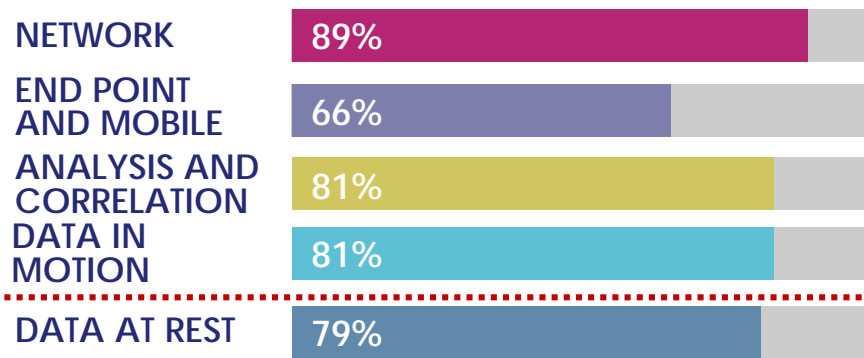
BELIEVE NETWORK SECURITY VERY/EXTREMELY EFFECTIVE AT PROTECTING DATA

“The sad truth is that as the data breaches continue to pile up, we continue to spend the bulk of our resources on the same old solutions, while approaches like data security that could arguably do a better job of protecting data, particularly among new technologies like cloud, Big Data and IoT, continue to lag.”

IT SECURITY DEFENSE SPENDING INCREASES



RATES OF EFFECTIVENESS FOR PROTECTING DATA



COMPLEXITY AND POTENTIAL PERFORMANCE IMPACTS

TOP BARRIERS TO DATA SECURITY DEPLOYMENT – U.S. FINANCIAL SERVICES

PERCEPTION OF
COMPLEXITY
UNIVERSALLY THE TOP
BARRIER

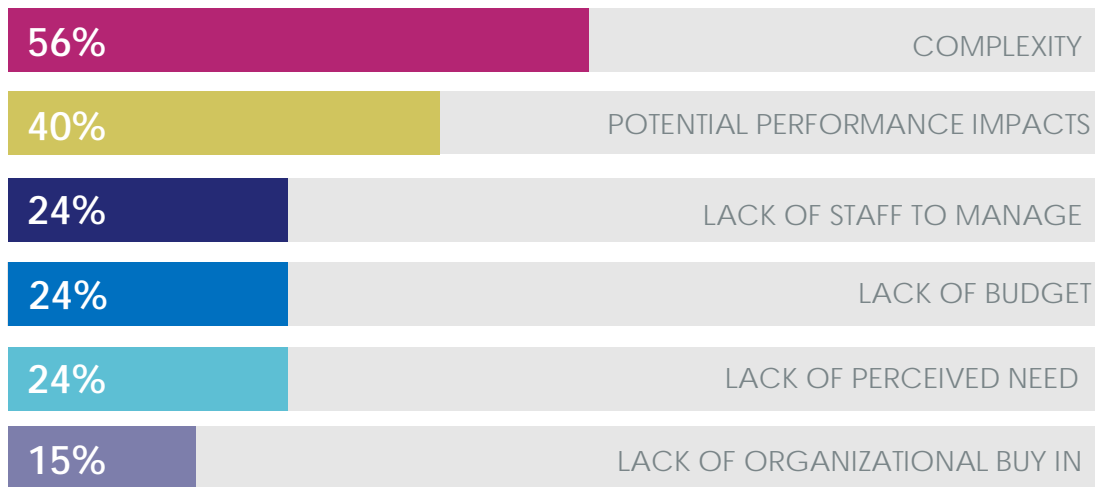
56%

GLOBAL – 50%

PERCEIVE
COMPLEXITY AS THE
TOP BARRIER TO
ADOPTION DATA
SECURITY

"...The lack of skilled security staff has been a consistent theme in 451's research efforts the past few years, and in conjunction with complexity, makes a strong case for data security functionality delivered as a service"

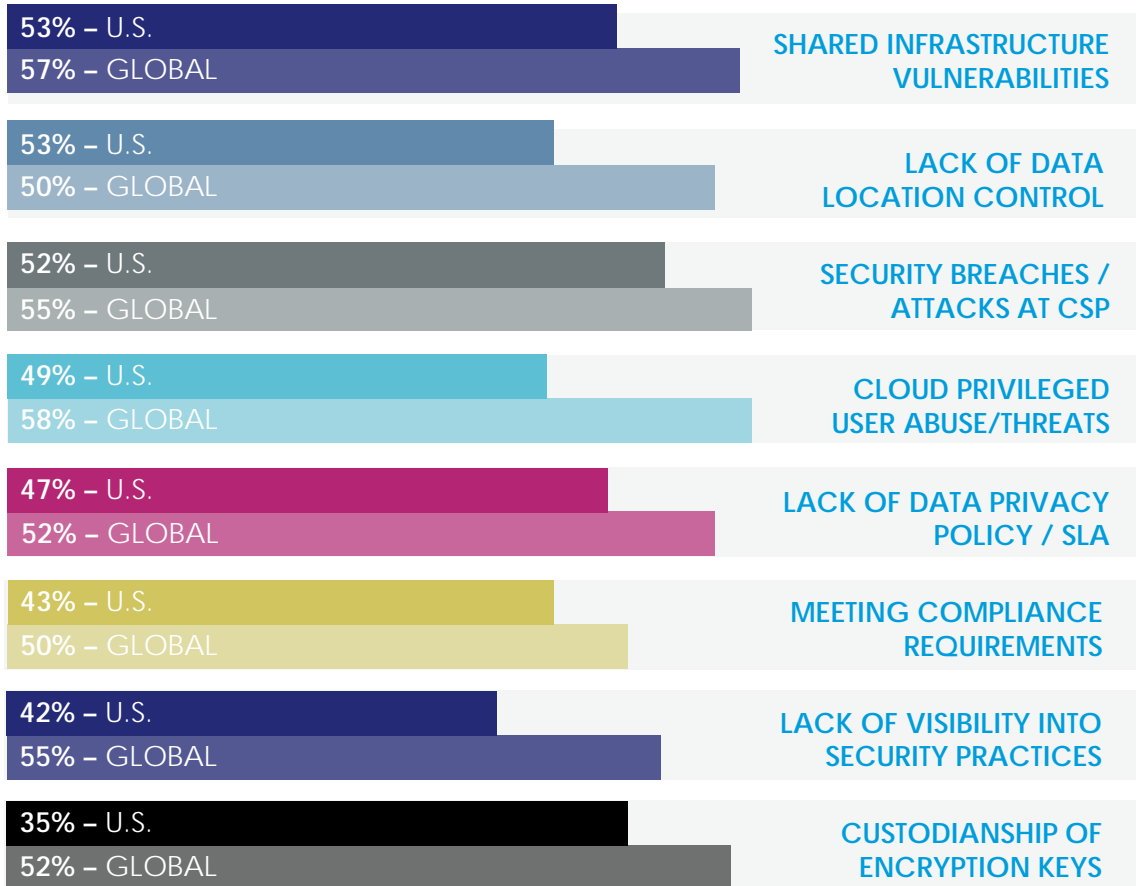
*Garrett Bekker
451 Research*



PERCEIVED BARRIERS TO ADOPTING DATA SECURITY

TOP CONCERNS WITH CLOUD/SAAS ENVIRONMENTS

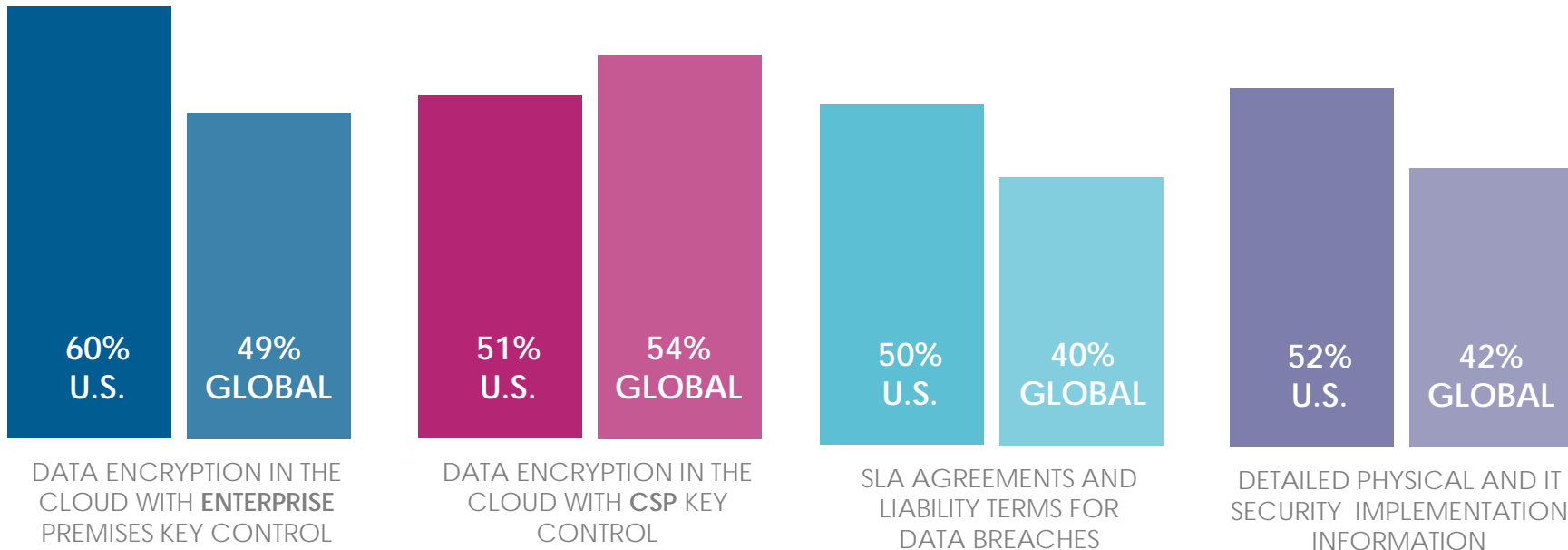
RATES OF VERY OR EXTREMELY CONCERNED – FINANCIAL SERVICES



“With tidal volumes of data and applications moving to the cloud, global respondents are most concerned about attacks on the cloud service provider (59%). However, for U.S. financial respondents, 53% are most concerned with security vulnerabilities from shared infrastructure, while slightly less (52%) are concerned with security breaches and attacks at the cloud service provider level.

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

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



“U.S. financial services organizations that would choose encryption of their data in public cloud services also have a preference towards the storage of encryption keys locally.”

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

BIG DATA – TOP FINANCIAL SERVICES DATA SECURITY STATS

TOP 5 CONCERNS

41% U.S.

46% GLOBAL

SENSITIVE DATA MAY
RESIDE ANYWHERE

39% U.S.

43% GLOBAL

SECURITY OF REPORTS
THAT MAY INCLUDE
SENSITIVE DATA

37% U.S.

39% GLOBAL

PRIVACY VIOLATIONS - DATA
ORIGINATES IN MANY
COUNTRIES

36% U.S.

30% GLOBAL

LACK OF EFFECTIVE ACCESS
CONTROLS

29% U.S.

38% GLOBAL

PRIVILEGED USER
ACCESS TO
PROTECTED DATA

42% U.S.

35% GLOBAL

USING ENCRYPTION
TO PROTECT DATA
IN BIG DATA
ENVIRONMENTS TODAY

58% U.S.

39% GLOBAL

USING SENSITIVE
INFORMATION IN BIG
DATA ENVIRONMENTS

53% U.S.

39% GLOBAL

VERY CONCERNED THAT
THEY ARE USING SENSITIVE
INFORMATION IN BIG
DATA WITHOUT DATA
SECURITY CONTROLS

IOT ADOPTION IS HIGH FOR U.S. FINANCIAL SERVICES

USE OF SENSITIVE DATA A CONCERN

84%

ADOPTING IOT

35%

ALREADY USING
SENSITIVE DATA IN IOT

32%

VERY CONCERNED ABOUT
SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

37% - IDENTIFYING WHICH
DATA IS SENSITIVE

35% - PROTECTING SENSITIVE DATA
GENERATED BY IOT

25% - PRIVACY VIOLATIONS
GENERATED BY IOT

25% - LOSS OR THEFT OF
IOT DEVICES

24% - PRIVILEGED USER ACCESS
TO DATA AND DEVICES

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

54% - ANTI-MALWARE
FOR DEVICES

49% ENCRYPTION OF DATA

49% SECURE ID & AUTH

33% - ANOMALY DETECT/
BEHAV ANALYSIS

33% - IOT NETWORK
ISOLATION

CONTAINERS: TOP SECURITY CONTROLS TO INCREASE

FINANCIAL SERVICES CONTAINER ADOPTION AND USE

84%

DEPLOYING
CONTAINERS
THIS YEAR.

SECURITY THE TOP BARRIER
TO DEPLOYMENT

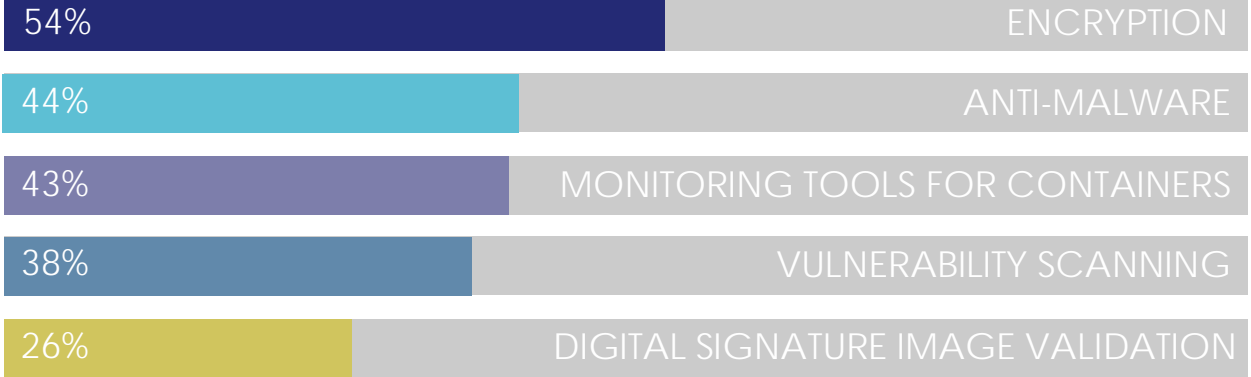
45%

U.S.

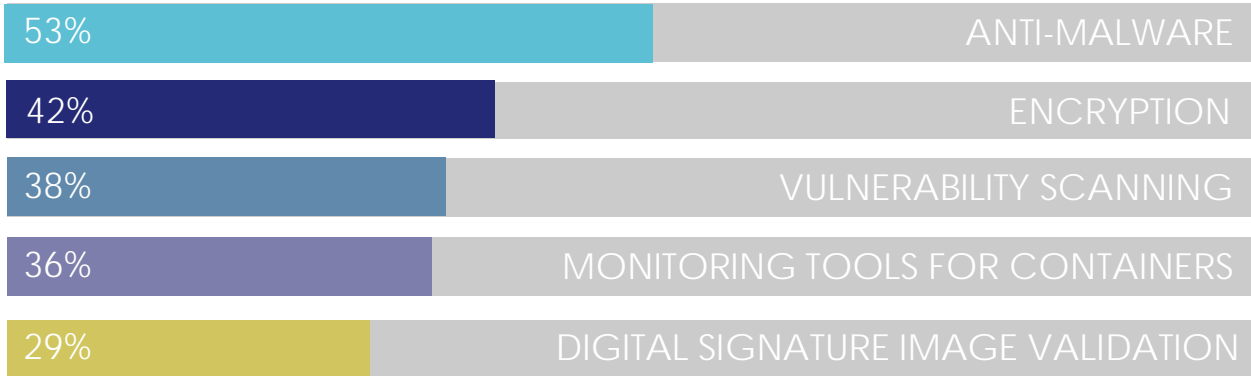
48%

GLOBAL

U.S.



GLOBAL



ENCRYPTION ENABLES DIGITAL TRANSFORMATION IN FINANCIAL SERV.

A KEY TOOL REQUIRED FOR ADVANCED TECHNOLOGY ADOPTION

CLOUD

ENCRYPTION ENABLING FURTHER ADOPTION OF CLOUD

60%

U.S.

DATA ENCRYPTION IN THE CLOUD WITH ENTERPRISE PREMISE KEY CONTROL

GLOBAL

49%

BIG DATA

ENCRYPTION OFFSETS TOP SECURITY CONCERNS

U.S.

37%

39%

41%

PRIVACY VIOLATIONS
SECURITY OF REPORTS
SENSITIVE DATA EVERYWHERE

39%

43%

46%

GLOBAL

IOT

THE TOP TECHNOLOGIES NEEDED TO EXPAND USAGE

U.S.

49%

49%

DATA ENCRYPTION
SECURE DIGITAL IDENTITY
(AN ENCRYPTION TECHNOLOGY)

58%

55%

GLOBAL

CONTAINERS

ENCRYPTION A TOP CONTROL NEEDED TO ENABLE GREATER ADOPTION

42%

54%

GLOBAL

U.S.

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

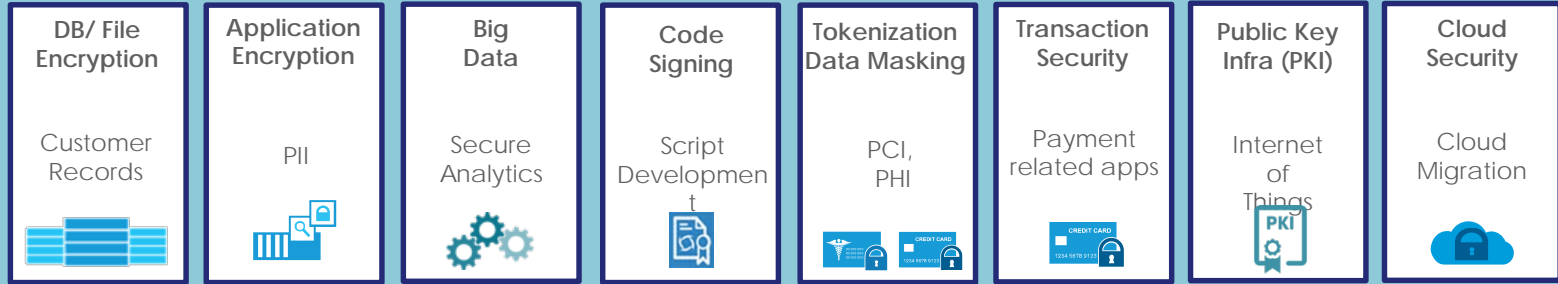
Thales e-Security provides companies everything they need to protect and manage their data and scale easily to new environments and requirements—encryption, advanced key management, tokenization, authorization, privileged user control, and HSMs.

■ Our customers

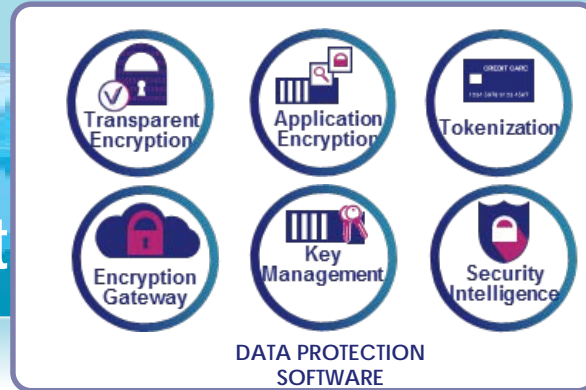
Our customers include 19 of the world's 20 largest banks, four of the world's five largest oil companies, 27 NATO country members and 15 of the Fortune 25.



Our solutions protect data while eliminating complexity, inefficiency and cost



Use Cases



2017 THALES DATA THREAT REPORT

Trends in Encryption
and Data Security

FINANCIAL SERVICES EDITION