

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

ADVANCED TECHNOLOGIES EDITION
CLOUD, BIG DATA, IOT, CONTAINERS

2017 THALES DATA THREAT REPORT

TRENDS IN ENCRYPTION AND DATA PROTECTION



Copyright 2017 Thales

1,100+ SENIOR IT SECURITY EXECUTIVES SURVEYED GLOBALLY | 500 U.S. | 100 EACH U.K., GERMANY, MEXICO, BRAZIL, JAPAN, AUSTRALIA



DEPLOYING SENSITIVE DATA – WITHOUT DATA SECURITY

“CLOUD, BIG DATA, THE INTERNET OF THINGS (IOT) AND INCREASINGLY CONTAINER TECHNOLOGY ARE ALL BEING ACTIVELY EMBRACED AND COLLECTIVELY PACK A POTENTIALLY DISRUPTIVE PUNCH TO THE BASIC GROUND RULES OF VENERABLE BUSINESSES.”

“NEARLY TWO-THIRDS (63%) OF RESPONDENTS ADMIT THAT THEIR ORGANIZATIONS DEPLOY THESE NEW INFORMATION TECHNOLOGIES PRIOR TO HAVING APPROPRIATE DATA SECURITY MEASURES IN PLACE.”

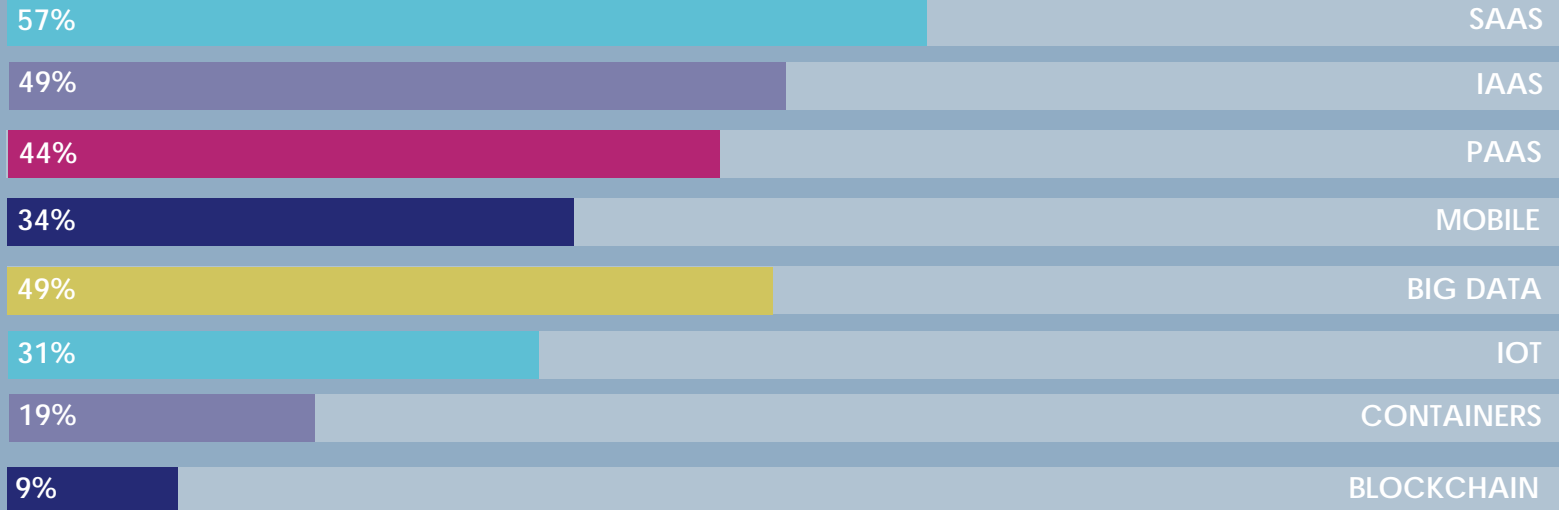
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES WITHOUT DATA SECURITY TO PROTECT INFORMATION

63%

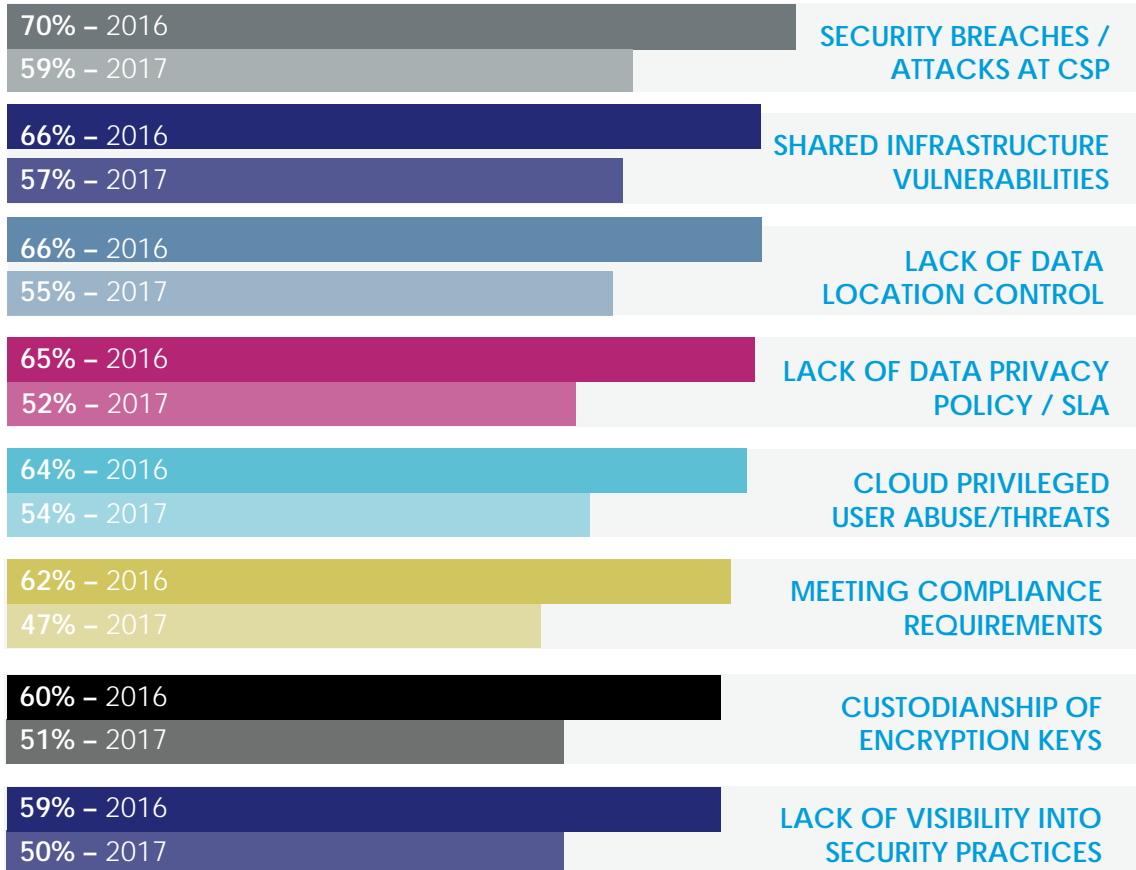
OF ORGANIZATIONS SURVEYED ARE
DEPLOYING NEW TECHNOLOGIES IN
ADVANCE OF HAVING APPROPRIATE LEVELS
OF DATA SECURITY IN PLACE

93%

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



CONCERNS ABOUT CLOUD SECURITY DECLINE IN SPITE OF HIGH USE OF SENSITIVE DATA



“Data breaches at cloud service providers to date have been rare, and generally not serious. Most major cloud providers have larger staffs of highly trained security professionals than any enterprise, and their scalability and redundancy can provide protection from the kinds of DDOS attacks that can plague on-premises workloads.”

“Perhaps as a result of the recognition of these public cloud security realities, security concerns overall for public cloud are waning.”

Garrett Bekker
Principal Analyst, Information Security, 451 Research

SAAS DATA SECURITY CONCERNS REMAIN HIGH WHILE SAAS USAGE FOR SENSITIVE DATA INCREASES

60% ONLINE STORAGE

56% ONLINE BACKUP

54% ONLINE ACCOUNTING

46% CRM / SOCIAL CRM

46% ERP

47% PROJECT / TASK MANAGEMENT

45% COLLABORATION TOOLS

44% ONLINE OFFICE SUITES

USING SENSITIVE DATA
IN SAAS
ENVIRONMENTS

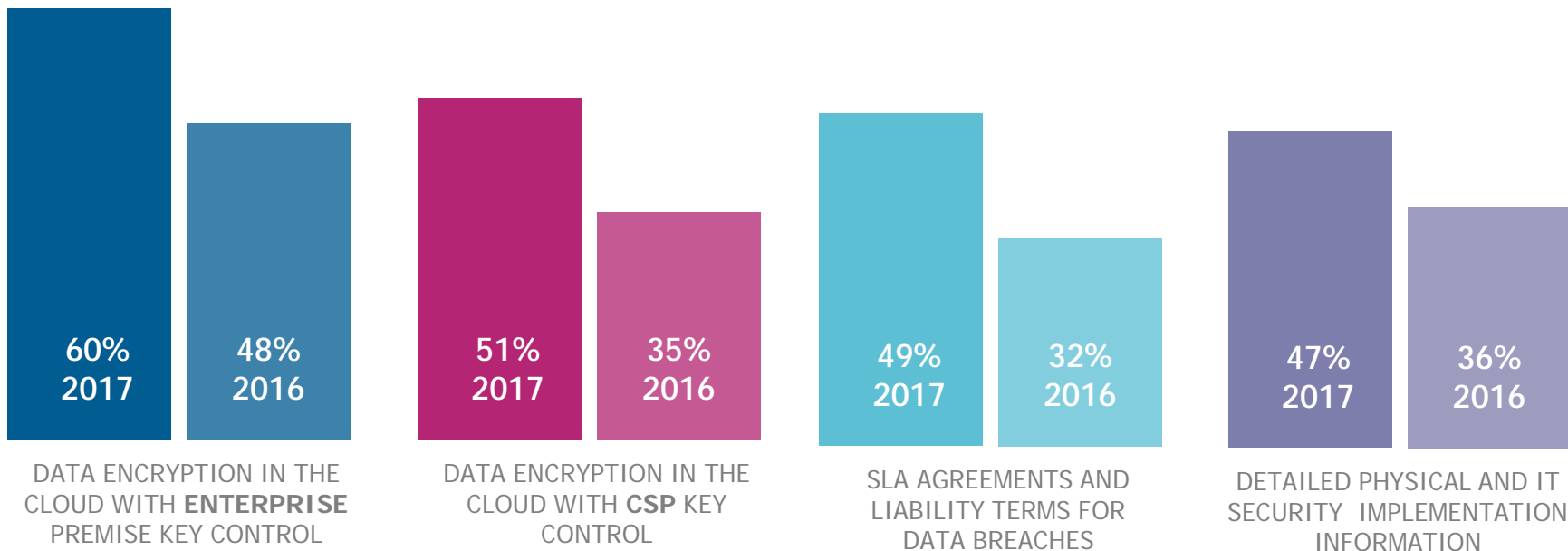
57%

2017

53%

2016

WHAT CAN CSPS AND SAAS PROVIDERS DO TO INCREASE ENTERPRISE CLOUD ADOPTION? – ENCRYPTION OFFERINGS

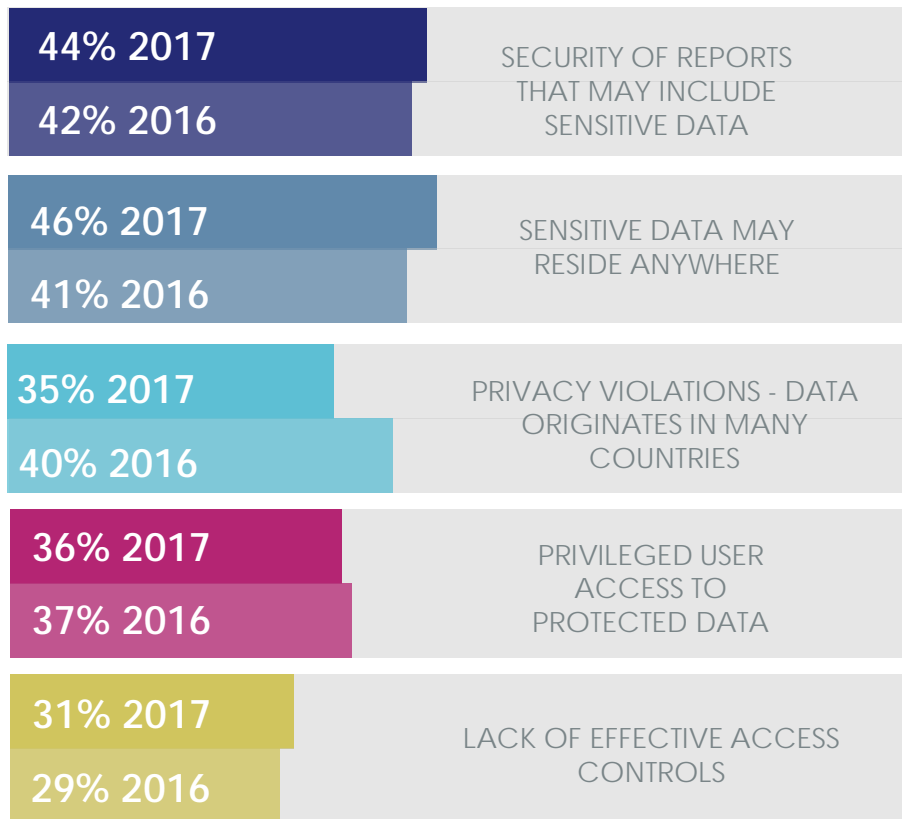


“Security remains a top barrier to further cloud adoption, and encryption with locally managed keys or BYOK (61%) is far and away seen as the technology that would most increase willingness to use public cloud globally, up sharply from 48% a year ago.”

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

BIG DATA – TOP DATA SECURITY CONCERNS AND STATS

TOP 5 CONCERNS



36%

USING ENCRYPTION
TO PROTECT DATA
IN BIG DATA
ENVIRONMENTS TODAY

47%

USING SENSITIVE
INFORMATION IN BIG
DATA ENVIRONMENTS

44%

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

IOT ADOPTION IS HIGH

USE OF SENSITIVE DATA A CONCERN

86%

ADOPTING IOT

31%

USING SENSITIVE
DATA IN IOT

32%

VERY CONCERNED ABOUT
SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

36% - PROTECTING SENSITIVE DATA
GENERATED BY IOT

30% - IDENTIFYING WHICH DATA
IS SENSITIVE

25% - PRIVACY VIOLATIONS

25% - PRIVILEGED USER ACCESS
TO DATA AND DEVICES

24% - IMPACT OF ATTACKS ON
IOT DEVICES

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

56% ENCRYPTION OF DATA

55% SECURE ID AND AUTHENTICATION

50% - ANTI-MALWARE
FOR DEVICES

43% - IOT NETWORK ISOLATION

41% - ANOMALY DETECTION/
BEHAVIORAL ANALYSIS

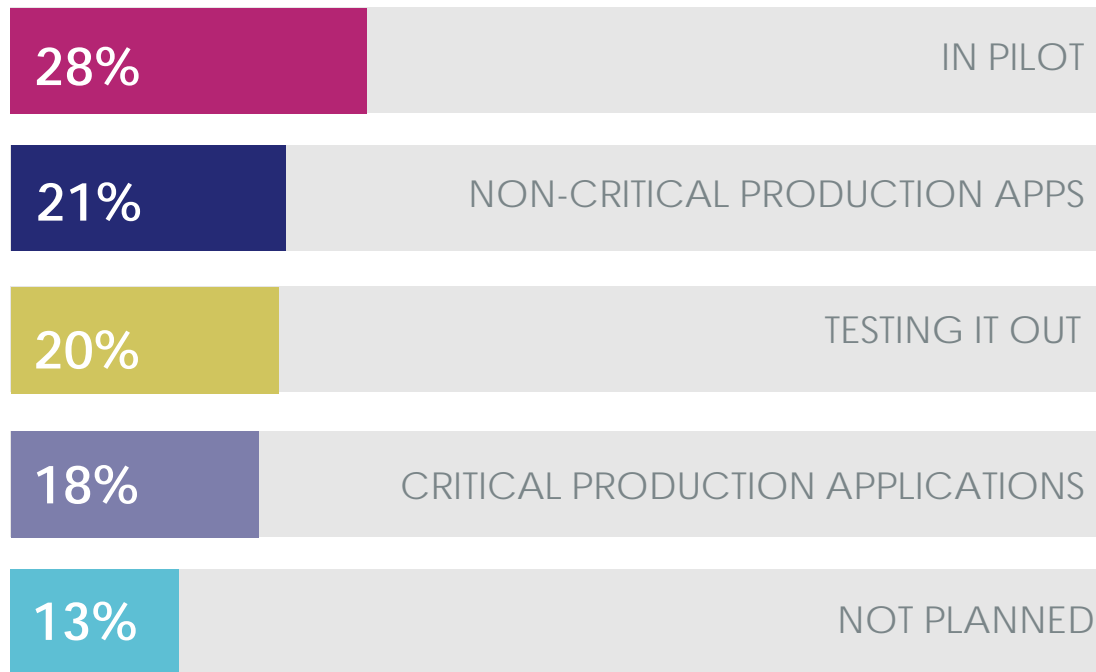
CONTAINERS SURPRISE

ONLY 4 YEARS AFTER TECHNOLOGY INTRODUCTION (DOCKER™)

"... **40%** of respondents are already using containers in production environments"

"... **87%** have plans for using containers this year"

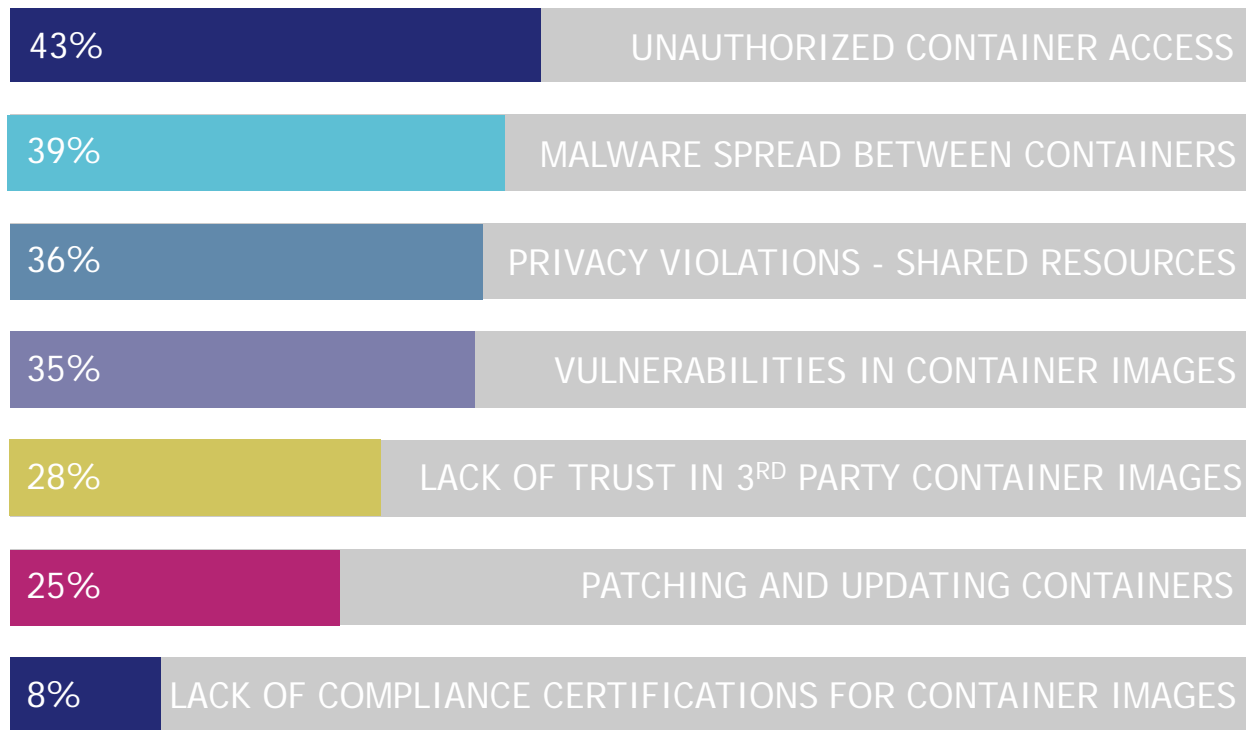
*Garrett Bekker
451 Research*



CONTAINER BASED APPLICATION DEPLOYMENTS

CONTAINER SECURITY CONCERNS ARE SLOWING ADOPTION

CONTAINER SECURITY CONCERNS



THE TOP BARRIER TO EXPANDED CONTAINER ADOPTION

47%
SECURITY

"Similar to the emerging IoT environment, there remains a lack of enterprise-grade security controls in most container environments today, owing largely to their relative immaturity."

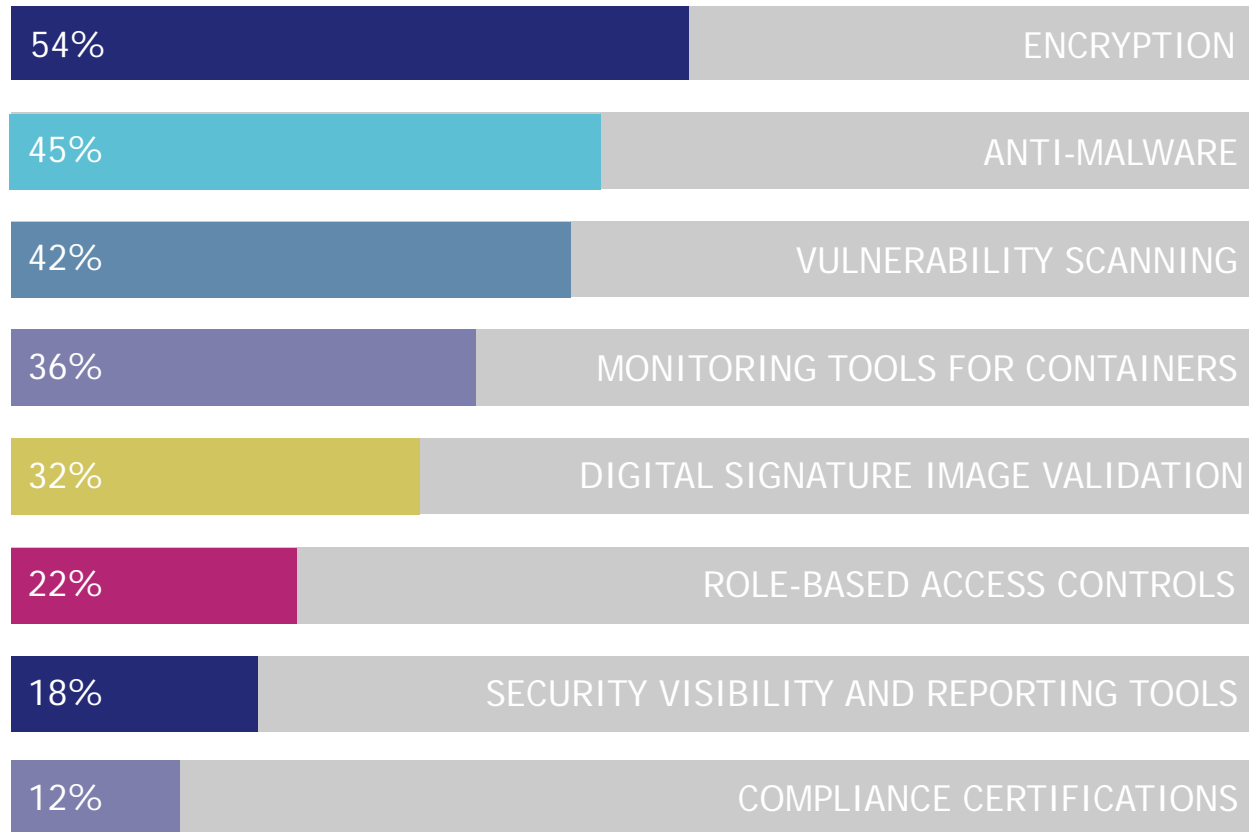
Garrett Bekker
451 Research

SECURITY CONTROLS TO INCREASE ENTERPRISE CONTAINER ADOPTION AND USE

SECURITY CONTROLS THAT WOULD INCREASE ENTERPRISE WILLINGNESS TO USE CONTAINERS

"As with all advanced technologies in our study, security is once again cited as the top barrier for container adoption (47%), followed closely by budget (44%) and staffing (33%). ."

*Garrett Bekker
451 Research*



THE RISE OF ENCRYPTION

ENCRYPTION A KEY TOOL ENABLING ADVANCED TECHNOLOGY ADOPTION

CLOUD

ENCRYPTION ENABLING FURTHER ADOPTION OF CLOUD BY ENTERPRISES

60%

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

51%

DATA ENCRYPTION IN THE CLOUD WITH **CSP** KEY CONTROL

BIG DATA

ENCRYPTION OFFSETS TOP SECURITY CONCERNS (encrypt and control access)

46%

SENSITIVE DATA EVERYWHERE

44%

SECURITY OF REPORTS

36%

PRIVILEGED USER ACCESS

IOT

ENCRYPTION TECHNOLOGIES TOP REQUIREMENTS FOR EXPANDED USE

56%

DATA ENCRYPTION

55%

SECURE IDENTITY (DIGITAL CERTIFICATES AND ENCRYPTION TECHNOLOGY)

CONTAINERS

ENCRYPTION THE TOP SECURITY CONTROL NEEDED TO INCREASE ADOPTION

54%

ENCRYPTION

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 firms 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

ADVANCED TECHNOLOGIES EDITION
CLOUD, BIG DATA, IOT, CONTAINERS

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

HEALTHCARE EDITION

MRN: 43215446121
DOB: 10/31/1980
(H) (408) 555-1212
(W) (408) 555-1212
Encounter Date: May 30 2015 4:35PM

Dear Mrs. Smith,
Your labs are normal.
Spence Smith, MD

Test Name
SODIUM
POTASSIUM
CHLORIDE
CO2
GLUCOSE
BLOOD UREA NITROGEN
CREATININE UNMA

30 May 2015 10:23AM

Reference

4.8 MMOLL
108 MMOLL
24 MMOLL
86 MG/DL
10 MG/DL
0.78 MG/DL
112 ML/MIN/1.73M2
130 ML/MIN/1.73M2

Danger!

2017 THALES DATA THREAT REPORT

TRENDS IN ENCRYPTION AND DATA PROTECTION



Copyright 2017 Thales



HEALTHCARE DIGITIZATION – A DOUBLE EDGED SWORD

“PUSHED BY INTENSE REGULATION AND COMPLIANCE REQUIREMENTS HEALTHCARE RECORDS ARE GOING DIGITAL. THE DOUBLE-EDGED SWORD OF DIGITIZATION IS THAT INDIVIDUAL HEALTHCARE DATA IS EXPOSED TO MORE PEOPLE, IN MORE PLACES AND ON MORE DEVICES.

“ELECTRONIC HEALTH RECORDS (EHR) CONTAIN A TROVE OF PERSONAL DATA, MAKING THEM AN IDEAL TARGET OF ONE-STOP HACKING FOR CYBER THIEVES”

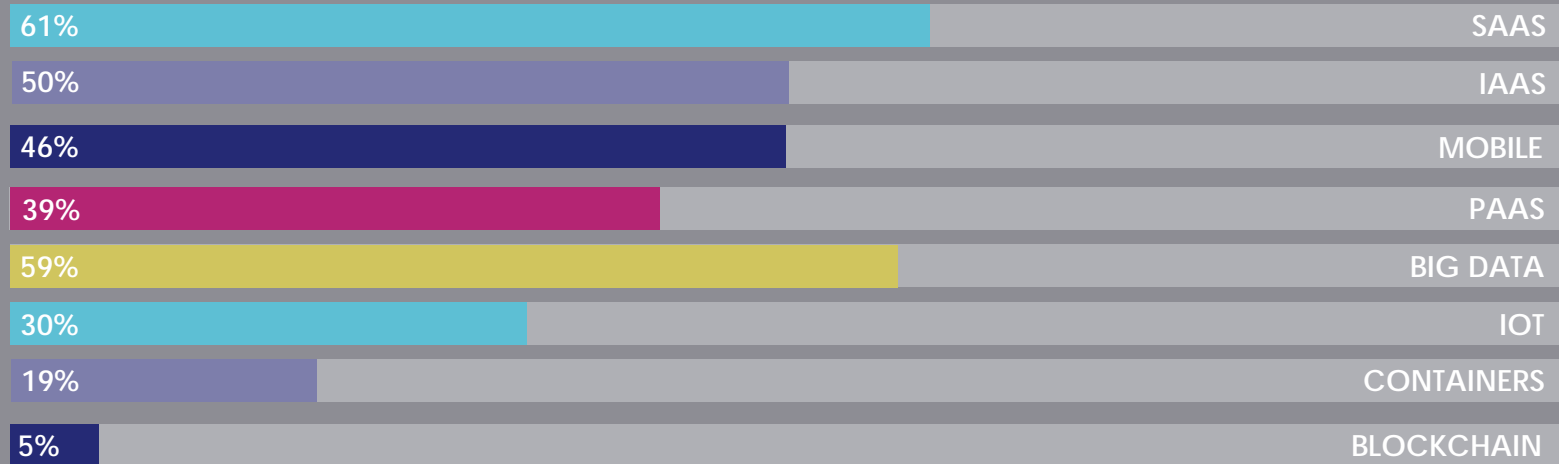
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES WITHOUT DATA SECURITY TO PROTECT INFORMATION

60%

"60% OF U.S. HEALTHCARE RESPONDENTS INDICATED THAT THEIR ORGANIZATIONS DEPLOY NEW TECHNOLOGIES IN ADVANCE OF HAVING APPROPRIATE LEVELS OF DATA SECURITY IN PLACE"

*Garrett Bekker,
451 Research*

94% of U.S. HEALTHCARE ENTERPRISES USE ADVANCED TECHNOLOGIES FOR SENSITIVE DATA



MORE BAD NEWS

DATA BREACHES ARE UP IN SPITE OF INCREASE SPEND

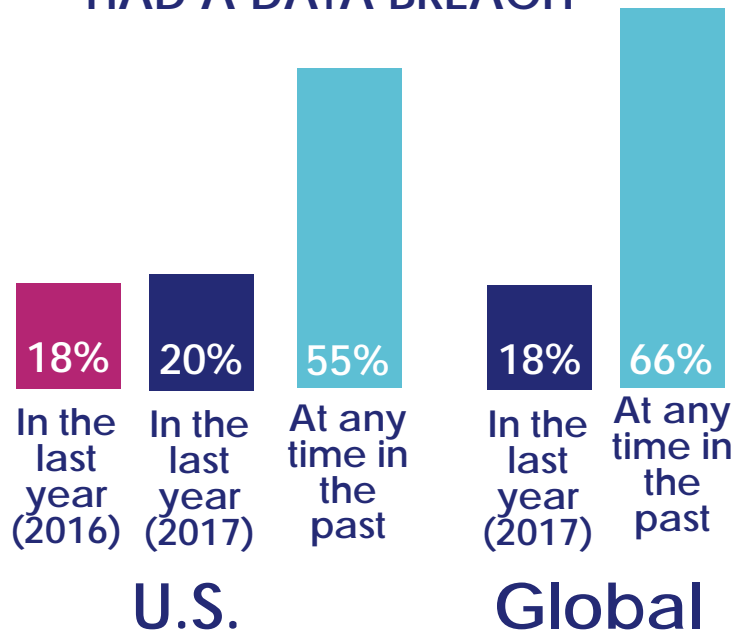
"90% of those in U.S. healthcare (and 88% in global healthcare) say their organizations are feeling some level of vulnerability to threats to sensitive data"

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

FEELING VULNERABLE TO DATA THREATS

90% U.S.
88% Global

HAD A DATA BREACH

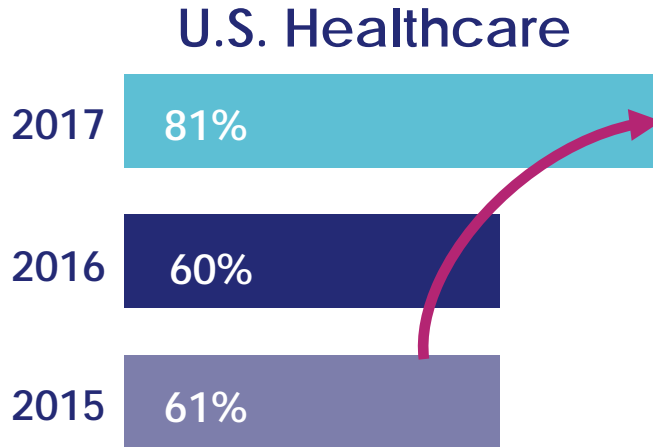


SAFE OPERATION

43% – U.S.
34% – GLOBAL*

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

INCREASING SPENDING TO PROTECT DATA



Global Healthcare

76%

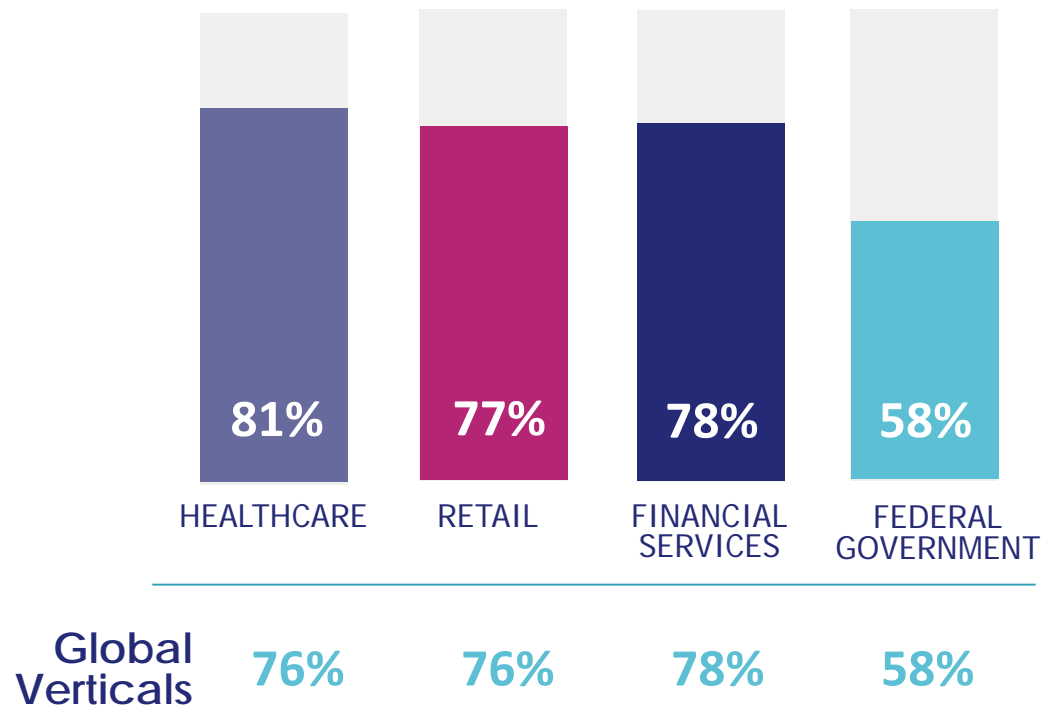
2017

* GLOBAL = OUTSIDE THE U.S. RESULTS

U.S. HEALTHCARE IS UPPING THEIR GAME

INCREASING SPEND MORE THAN OTHER VERTICALS

Increases in IT Security Spend by U.S. Vertical



“Spending increases by US Healthcare on cyber security will lead all other vertical markets surveyed in the Report, both within the U.S. and globally”

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

US RATES COMPLIANCE THE TOP DRIVER FOR IT SECURITY SPENDING BUT LESS REGULATED GLOBAL COUNTERPARTS DO NOT

“COMPLIANCE IS A MINIMUM TABLE STAKE FOR REGULATED ENTERPRISES ... BUT BEING COMPLIANT DOES NOT MEAN YOU WON'T BE BREACHED”

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

US HEALTHCARE IT SECURITY SPENDING PRIORITIES

57% COMPLIANCE

40% PREVENT DATA BREACHES

35% PROTECTING REP AND BRAND

34% BEST PRACTICES

27% INCREASED CLOUD USE

GLOBAL HEALTHCARE IT SECURITY SPENDING PRIORITIES

20% COMPLIANCE

39% PREVENT DATA BREACHES

39% PROTECTING REP AND BRAND

38% BEST PRACTICES

38% INCREASED CLOUD USE

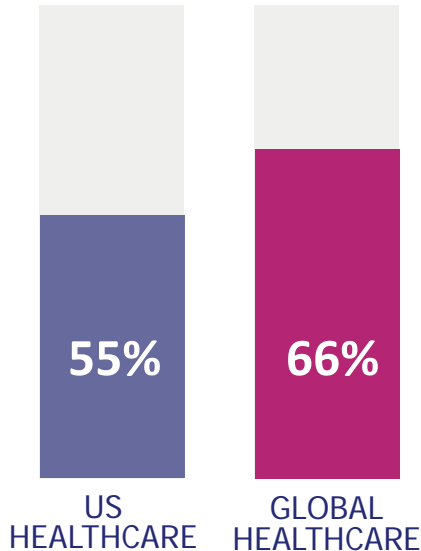
“Compliance ranked near the very bottom of spending drivers among global healthcare respondents, highlighting the differing effects of far more stringent regulatory and compliance requirements such as HIPAA/HiTech - in the US.”

COMPLIANCE SEEMS TO HELP U.S. HEALTHCARE COMPARED TO THEIR GLOBAL COUNTERPARTS

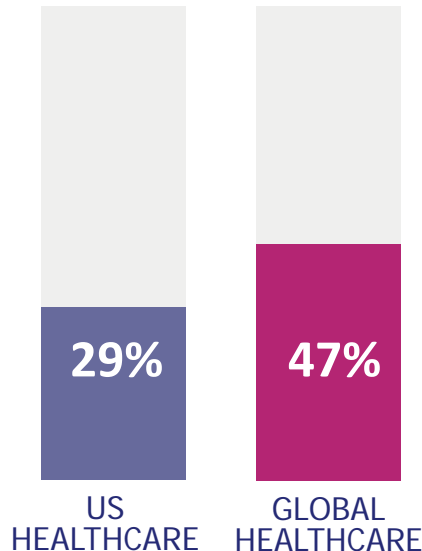
“Compliance is a minimum table stake for regulated enterprises ... But being compliant does not mean you won’t be breached”

*Garrett Bekker
Sr. Analyst Information
Security, 451 Research*

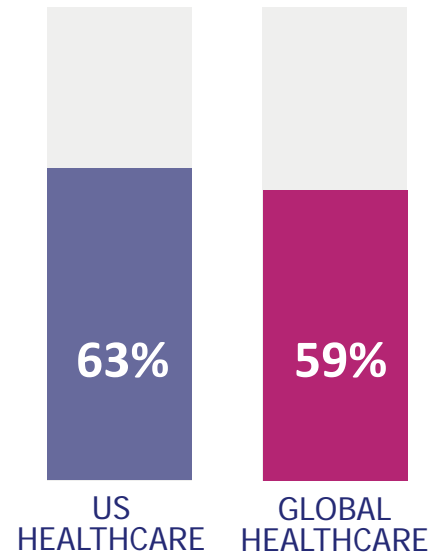
**COMPARATIVE DATA
BREACH RATES**
(SMALLER NUMBERS ARE BETTER)



**COMPARATIVE VERY OR
EXTREMELY VULNERABLE LEVELS**
(SMALLER NUMBERS ARE BETTER)



**RATES OF COMPLIANCE AS
“VERY” OR “EXTREMELY”
EFFECTIVE AT PREVENTING
DATA BREACHES**



U.S. HEALTHCARE INCREASING SPENDING THE MOST WHERE DEFENSES OFTEN FAIL TO PROTECT DATA

92%

+14% FROM 2016

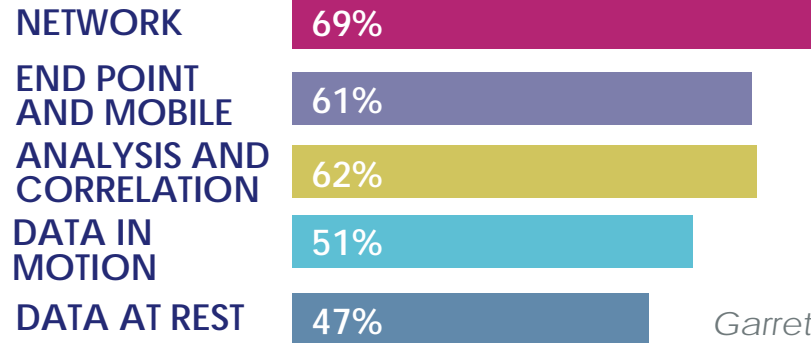
BELIEVE NETWORK
SECURITY VERY/
EXTREMELY EFFECTIVE
AT PROTECTING DATA

67%

+3% FROM 2016

BELIEVE ENDPOINT
PROTECTION
VERY/EXTREMELY
EFFECTIVE AT
PROTECTING DATA

IT SECURITY DEFENSE SPENDING INCREASES



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.”

“... 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”

* U.S. RESULTS

COMPLEXITY AND SKILL SHORTAGES

TOP BARRIERS TO DATA SECURITY DEPLOYMENT

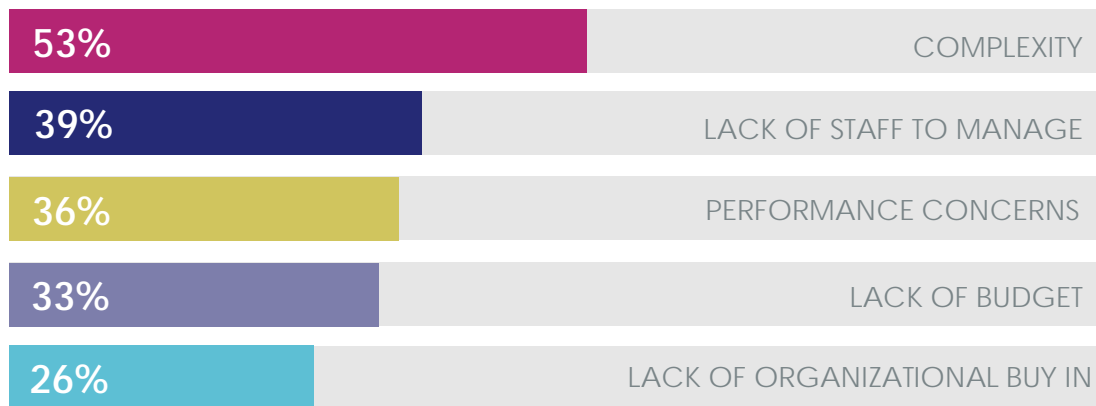
PERCEPTION OF
COMPLEXITY
UNIVERSALLY THE TOP
BARRIER

"...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

53%

PERCEIVE
COMPLEXITY AS THE
TOP BARRIER TO
ADOPTION DATA
SECURITY



PERCEIVED BARRIERS TO ADOPTING DATA SECURITY

* U.S. RESULTS

“.. 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
Sr. Analyst Information Security, 451 Research

THE MOST DANGEROUS INSIDERS

61%

PRIVILEGED USERS

46%

EXECUTIVE MANAGEMENT

33%

CONTRACTORS

26%

SERVICE PROVIDERS

* U.S. RESULTS

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. RESULTS

CLOUD DRIVING HEALTHCARE DATA SECURITY CONTROL PLANS

4 OF 5 PLANNED DATA SECURITY CONTROLS ARE DRIVEN BY CLOUD AND SAAS

NEXT 12 MONTHS: TOP 5 PLANNED DATA SECURITY TOOLS DEPLOYMENTS

45% - THIRD PARTY KEY OR BYOK

34% - CASB

35% - TOKENIZATION

36% - ENABLING CLOUD ENCRYPTION

38% - HARDWARE SECURITY MODULES



IN IMPLEMENTATION NOW: TOP 5 DATA SECURITY TOOLS

78% - DATABASE OR FILE ENCRYPTION

77% - DATA ACTIVITY MONITORING

73% - MULTIFACTOR AUTHENTICATION

70% - IDENTITY AND ACCESS MANAGEMENT

67% - SIEM

* U.S. RESULTS

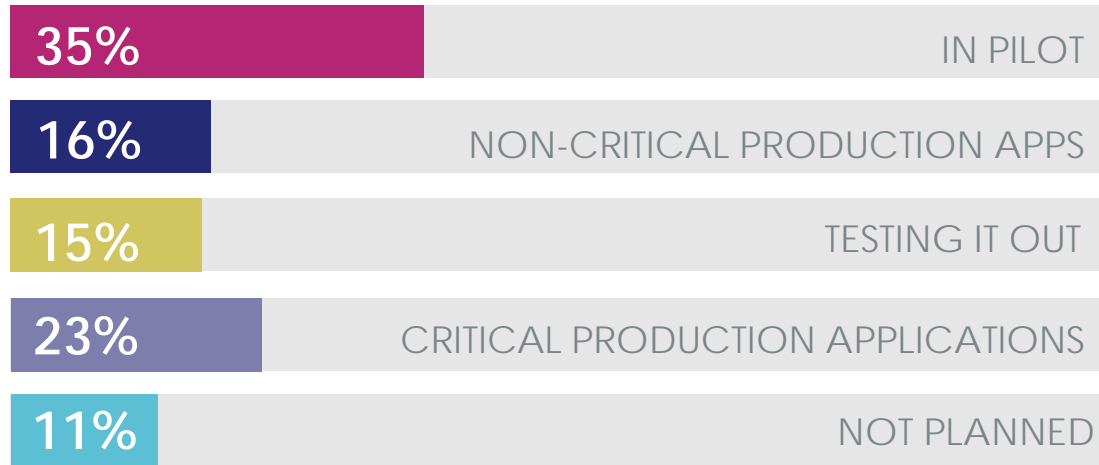
CONTAINERS SURPRISE

ONLY 3 YEARS AFTER TECHNOLOGY INTRODUCTION (DOCKER)

"... **39%** of respondents are already using containers in production environments

... **23%** in critical applications"

*Garrett Bekker
451 Research*



CONTAINER BASED APPLICATION DEPLOYMENTS

58% SELECTED ENCRYPTION

* U.S. RESULTS

AS THE #1 SECURITY CONTROL REQUIRED TO EXPAND CONTAINER USAGE

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 firms 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



Part of the **NUVIOS** group



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

HEALTHCARE EDITION

MRN: 43215446121
DOB: 10/31/1980
(H) (408) 555-1212
(W) (408) 555-1212
Encounter Date: May 30 2015 4:35PM

Dear Mrs. Smith,
Your labs are normal.
Spence Smith, MD

Test Name
SODIUM
POTASSIUM
CHLORIDE
CO2
GLUCOSE
BLOOD UREA NITROGEN
CREATININE UNMA

30 May 2015 10:23AM

Reference

4.8 MMOL/L
108 MMOL/L
24 MMOL/L

86 MG/DL
10 MG/DL
0.78 MG/DL

112 ML/MIN/1.73M2
130 ML/MIN/1.73M2

Danger!

2017 THALES DATA THREAT REPORT

Trends in Encryption
and Data Security

GLOBAL EDITION

451 Research™

THALES

2017 THALES DATA THREAT REPORT

TRENDS IN ENCRYPTION AND DATA PROTECTION



Copyright 2017 Thales

1,100+ SENIOR IT SECURITY EXECUTIVES SURVEYED GLOBALLY | 500 U.S. TOTAL



THE BIG DISCONNECT

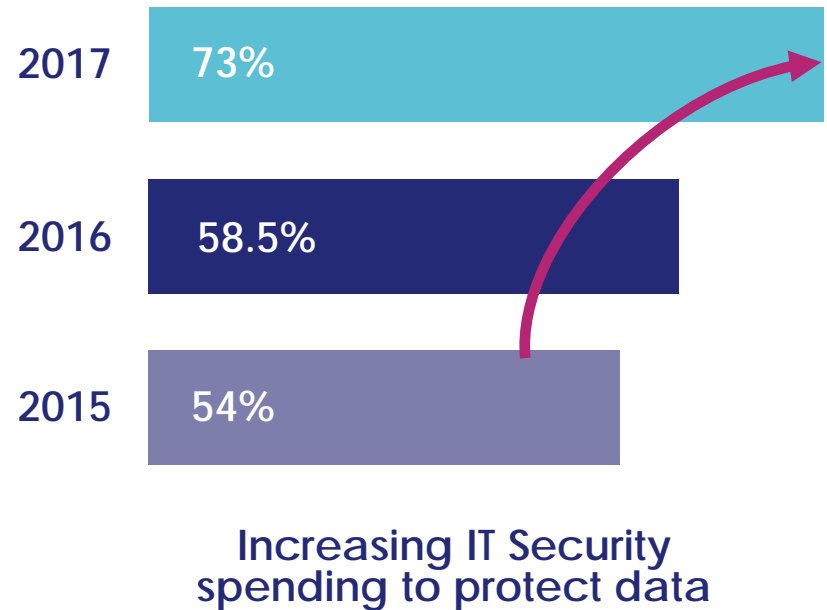
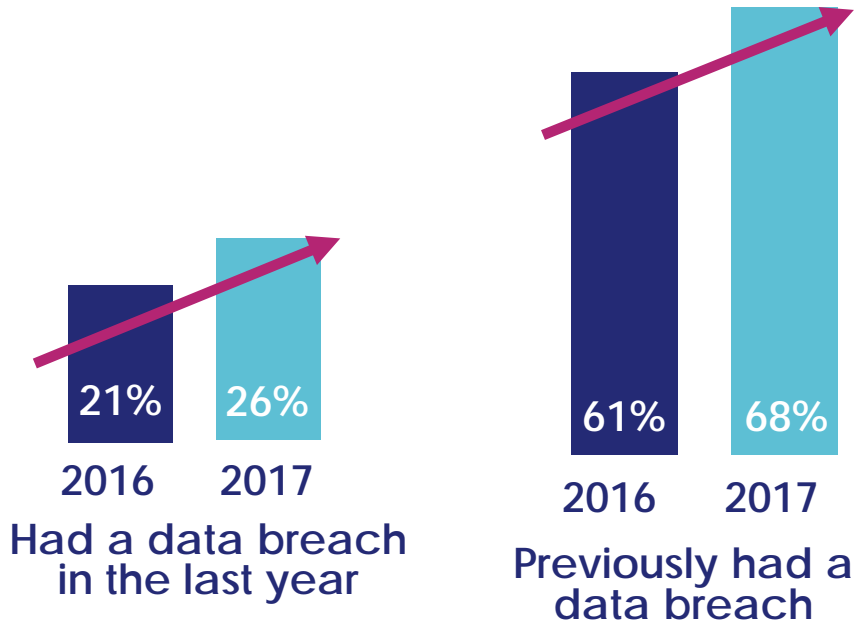
“OUR 2017 REPORT FINDS A GLOBAL SITUATION WHERE SPENDING ON SECURITY IS UP - SHARPLY IN SOME SECTORS – YET SUCCESSFUL DATA BREACHES ARE ALSO UP SIGNIFICANTLY.”

“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.”

BREACH RATES ARE ACCELERATING

DESPITE INCREASED IT SECURITY SPENDING TO PROTECT DATA

NO WONDER ENTERPRISES FEEL
VULNERABLE TO DATA THREATS

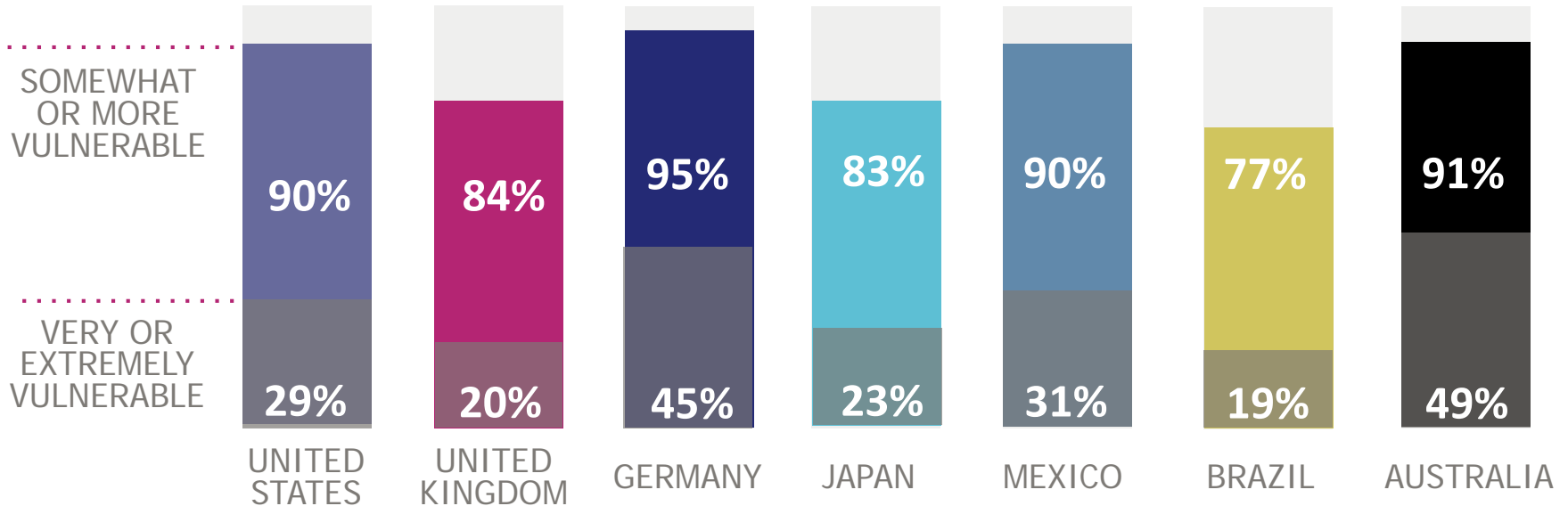


GLOBAL VULNERABILITY TO DATA THREATS

GLOBAL



REGIONAL



COMPLIANCE THE TOP DRIVER FOR IT SECURITY SPENDING AND RATED AS HIGHLY EFFECTIVE AT PROTECTING DATA

IN SPITE OF PRIORITIZING COMPLIANCE FIRST FOR THE LAST TWO YEARS, AND INVESTING TO MEET COMPLIANCE REQUIREMENTS, THE RATE OF BREACHES KEEPS RISING

59%

BELIEVE COMPLIANCE IS VERY OR EXTREMELY EFFECTIVE AT PREVENTING DATA BREACHES

IT SECURITY SPENDING PRIORITIES

44% COMPLIANCE

38% BEST PRACTICES

36% PROTECT REP & BRAND

35% PREVENT DATA BREACHES

35% INCREASED CLOUD USE

“Compliance is a minimum table stake for regulated enterprises ... But being compliant does not mean you won't be breached”

*Garrett Bekker
Sr. Analyst Information
Security, 451 Research*

INCREASING SPENDING THE MOST WHERE DEFENSES OFTEN FAIL TO PROTECT DATA

88%

+4.5% FROM 2016

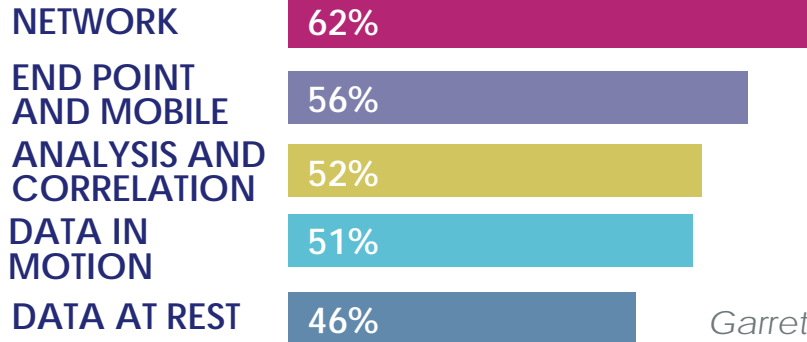
BELIEVE NETWORK
SECURITY VERY/
EXTREMELY EFFECTIVE
AT PROTECTING DATA

69%

+7% FROM 2016

BELIEVE ENDPOINT
PROTECTION
VERY/EXTREMELY
EFFECTIVE AT
PROTECTING DATA

IT SECURITY DEFENSE SPENDING INCREASES



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.”

“... 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”

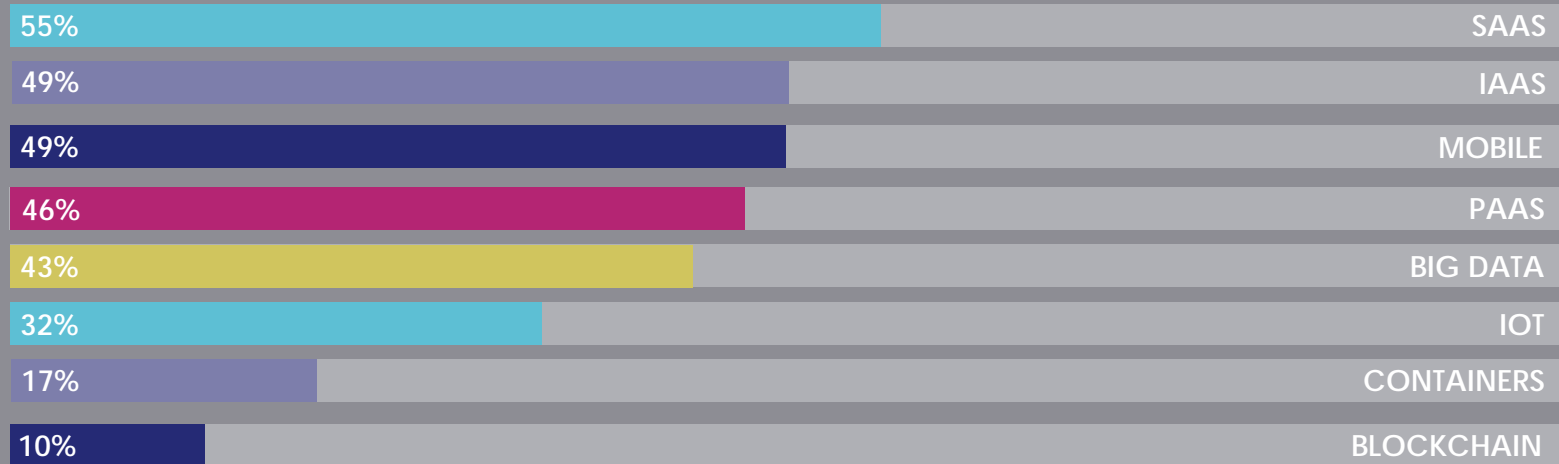
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES WITHOUT DATA SECURITY TO PROTECT INFORMATION

63%

"63% OF RESPONDENTS INDICATED THAT THEIR ORGANIZATIONS DEPLOY NEW TECHNOLOGIES IN ADVANCE OF HAVING APPROPRIATE LEVELS OF DATA SECURITY IN PLACE"

*Garrett Bekker,
451 Research*

ENTERPRISE USE OF ADVANCED TECHNOLOGIES FOR SENSITIVE DATA



COMPLEXITY AND SKILL SHORTAGES

TOP BARRIERS TO DATA SECURITY DEPLOYMENT

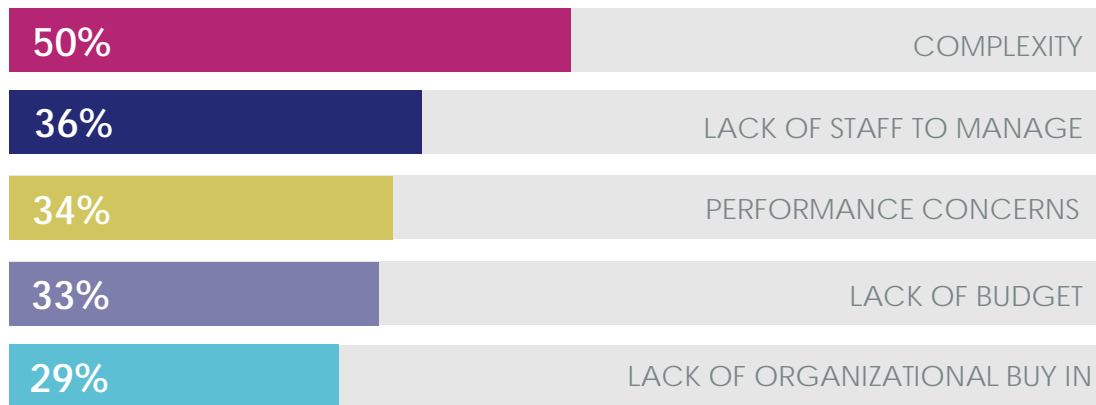
PERCEPTION OF
COMPLEXITY
UNIVERSALLY THE TOP
BARRIER

"...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

50%
-6% FROM 2016

PERCEIVE
COMPLEXITY AS THE
TOP BARRIER TO
ADOPTION DATA
SECURITY



PERCEIVED BARRIERS TO ADOPTING DATA SECURITY

“.. 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
Sr. Analyst Information Security, 451 Research

THE MOST DANGEROUS INSIDERS

58%

PRIVILEGED USERS

44%

EXECUTIVE MANAGEMENT

36%

ORDINARY EMPLOYEES

33%

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



CLOUD DRIVING DATA SECURITY CONTROL DEPLOYMENT

4 OF 5 PLANNED DATA SECURITY CONTROLS ARE DRIVEN BY CLOUD AND SAAS

2017

TOP 5 PLANNED DATA SECURITY TOOLS DEPLOYMENTS

39% - THIRD PARTY KEY OR BYOK

38% - CASB

37% - TOKENIZATION

36% - ENABLING CLOUD ENCRYPTION

34% - HARDWARE SECURITY MODULES



2016

TOP 5 PLANNED DATA SECURITY TOOLS DEPLOYMENTS

40% - APPLICATION ENCRYPTION

39% - MULTIFACTOR AUTHENTICATION

39% - TOKENIZATION

38% - CASB

38% - SIEM



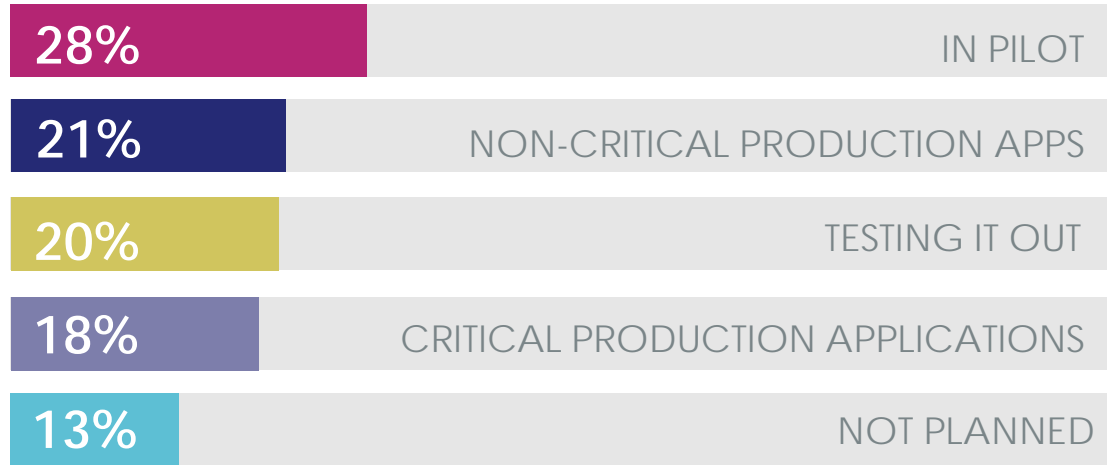
CONTAINERS SURPRISE

ONLY 3 YEARS AFTER TECHNOLOGY INTRODUCTION (DOCKER)

"... **40%** of
respondents are already
using containers in
production environments

... only **13%**
have no plans for
containers this year"

*Garrett Bekker
451 Research*



CONTAINER BASED APPLICATION DEPLOYMENTS

54% SELECTED
ENCRYPTION

AS THE #1 SECURITY
CONTROL REQUIRED TO
EXPAND CONTAINER USAGE

NEW REGULATIONS ARE DRIVING ENTERPRISE BEHAVIOR

DATA PRIVACY AND SOVEREIGNTY IMPACTING ENTERPRISES WORLDWIDE



72%

Globally are
Impacted by
Data Privacy
and
Data Sovereignty

ADDRESSING REQUIREMENTS BY:

64%

ENCRYPTING DATA

40%

TOKENIZING DATA

36%

MIGRATING CUSTOMER DATA

26%

WILL USE LOCAL HOSTING AND CLOUD

VARIATIONS IN IMPACT OF DATA PRIVACY/SOVEREIGNTY



U.S

75%

IMPACTED



GERMANY

81%

HIGHEST RATE



JAPAN

56%

LOWEST RATE

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 firms 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

The background of the slide is a blue-tinted cityscape at night. In the foreground on the right, there is a prominent clock tower with a yellow clock face and a statue on top. The rest of the image shows various skyscrapers and buildings with some lights visible, creating a dense urban environment.

Trends in Encryption and Data Security

GLOBAL EDITION