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

U.S.

U.K.

GERMANY

JAPAN

MEXICO

BRAZIL

AUSTRALIA

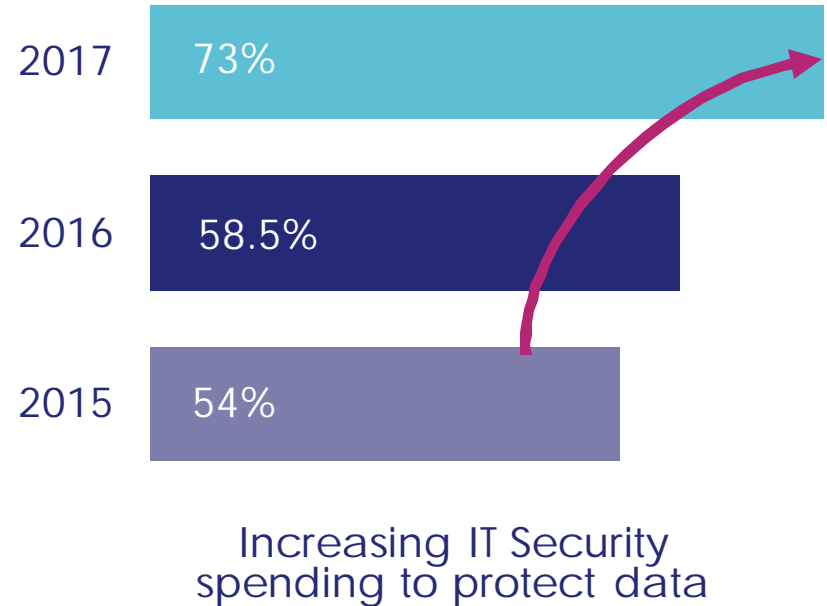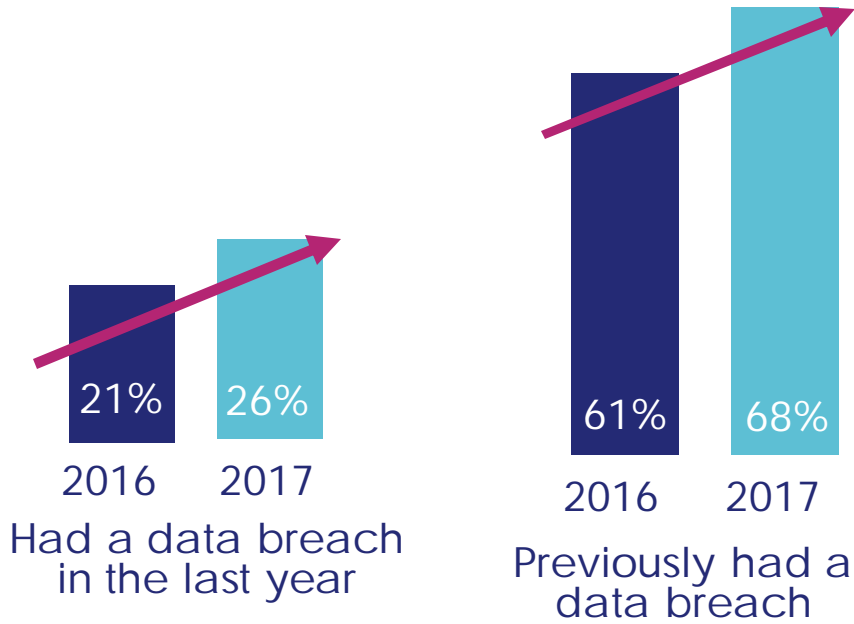1,100+ SENIOR IT SECURITY EXECUTIVES SURVEYED GLOBALLY | 500 U.S. TOTAL

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

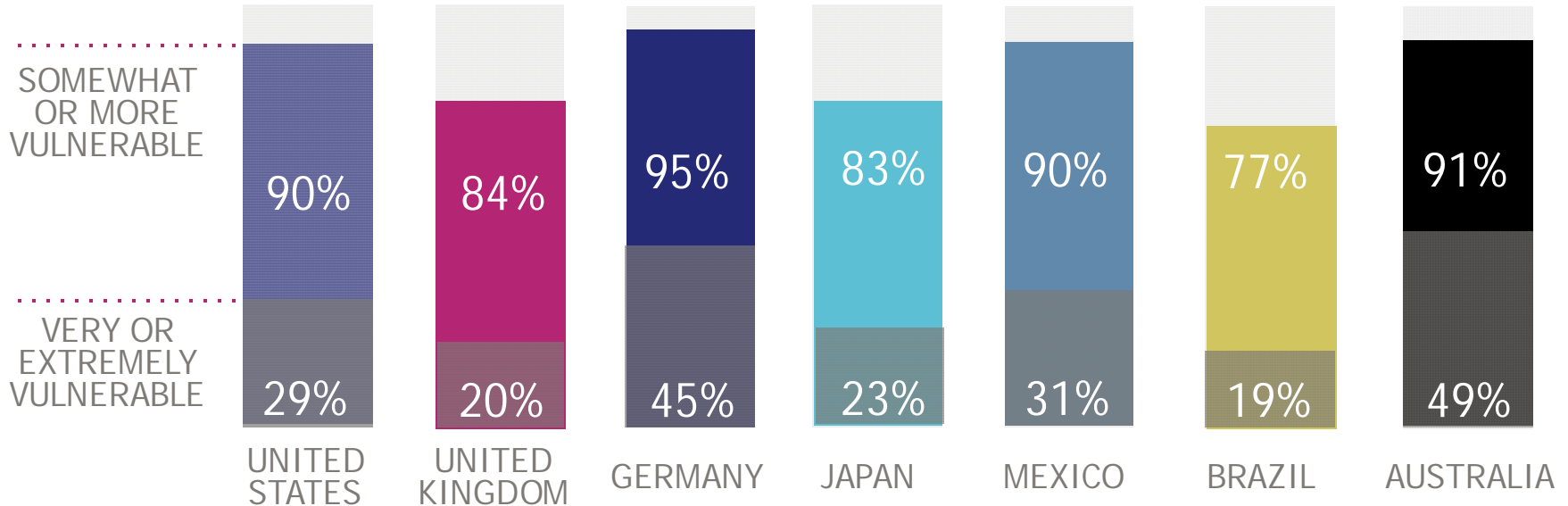NO WONDER ENTERPRISES FEEL VULNERABLE TO DATA THREATS

21% 2016
26% 2017

Had a data breach in the last year

61% 2016
68% 2017

Previously had a data breach

2017 73%
2016 58.5%
2015 54%

Increasing IT Security spending to protect data

GLOBAL VULNERABILITY
TO DATA THREATS

GLOBAL

88%
VULNERABLE

30%
VERY/EXTREMELY VULNERABLE

REGIONAL

SOMEWHAT
OR MORE
VULNERABLE

VERY OR
EXTREMELY
VULNERABLE

UNITED STATES	UNITED KINGDOM	GERMANY	JAPAN	MEXICO	BRAZIL	AUSTRALIA
90%	84%	95%	83%	90%	77%	91%
29%	20%	45%	23%	31%	19%	49%

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
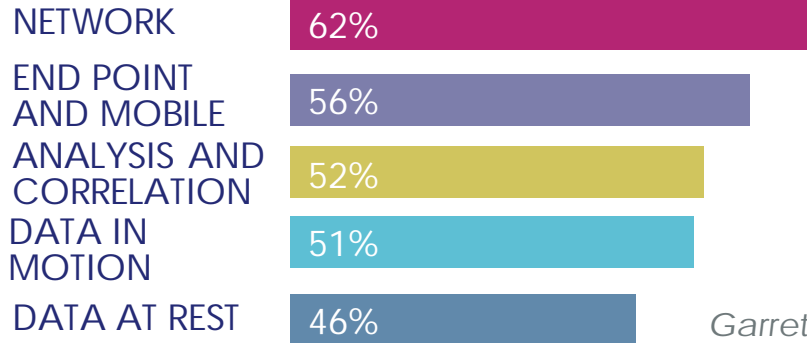## WHERE DEFENSES OFTEN FAIL TO PROTECT DATA

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

NETWORK	62%
END POINT AND MOBILE	56%
ANALYSIS AND CORRELATION	52%
DATA IN MOTION	51%
DATA AT REST	46%

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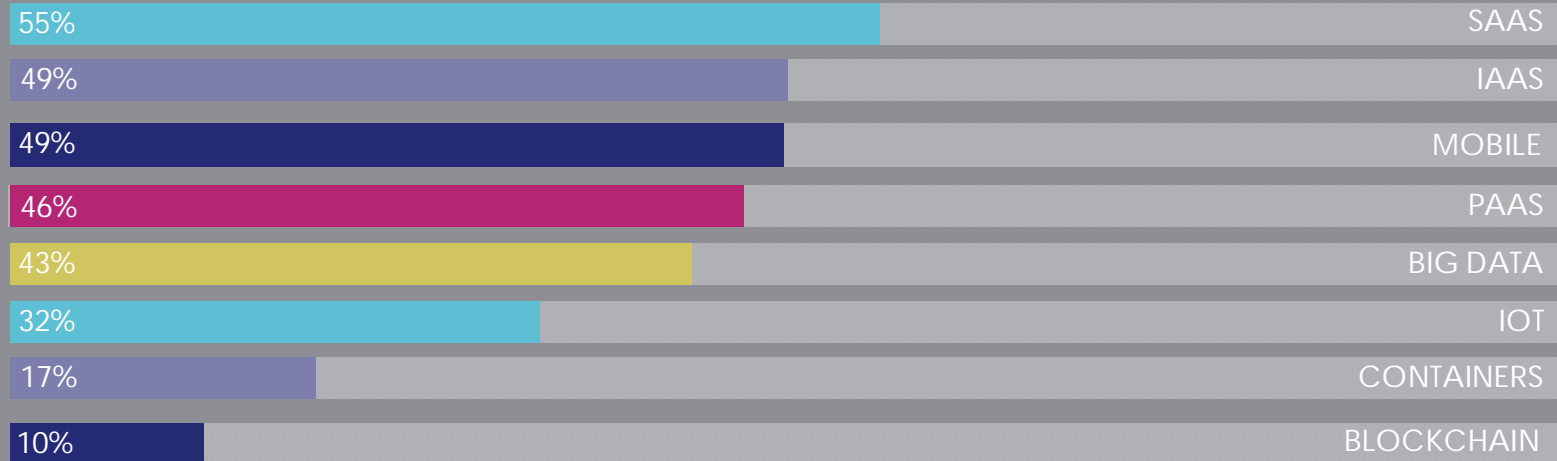
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES
WITHOUT DATA SECURITY TO PROTECT INFORMATION

63%

ENTERPRISE USE OF ADVANCED
TECHNOLOGIES FOR SENSITIVE DATA

"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

Technology	Percentage
SAAS	55%
IAAS	49%
MOBILE	49%
PAAS	46%
BIG DATA	43%
IOT	32%
CONTAINERS	17%
BLOCKCHAIN	10%

COMPLEXITY AND SKILL SHORTAGES
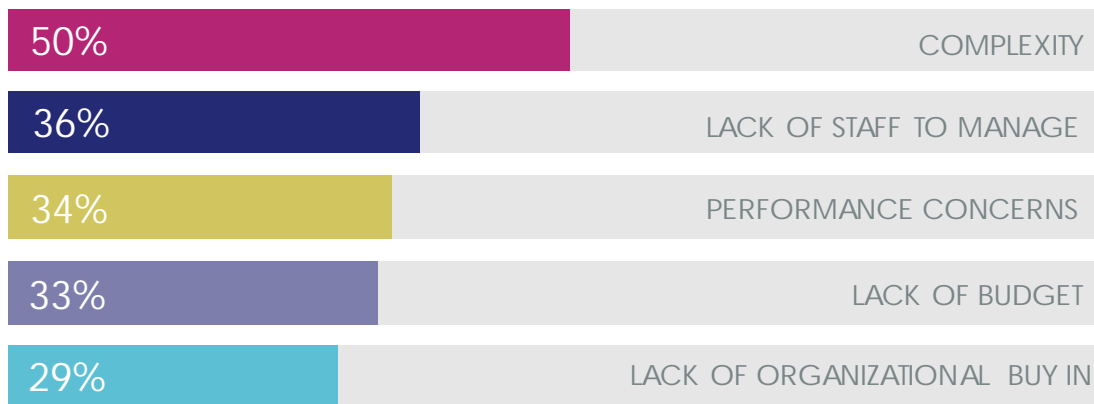## TOP BARRIERS TO DATA SECURITY DEPLOYMENT

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

50%	COMPLEXITY
36%	LACK OF STAFF TO MANAGE
34%	PERFORMANCE CONCERNS
33%	LACK OF BUDGET
29%	LACK OF ORGANIZATIONAL BUY IN

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

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
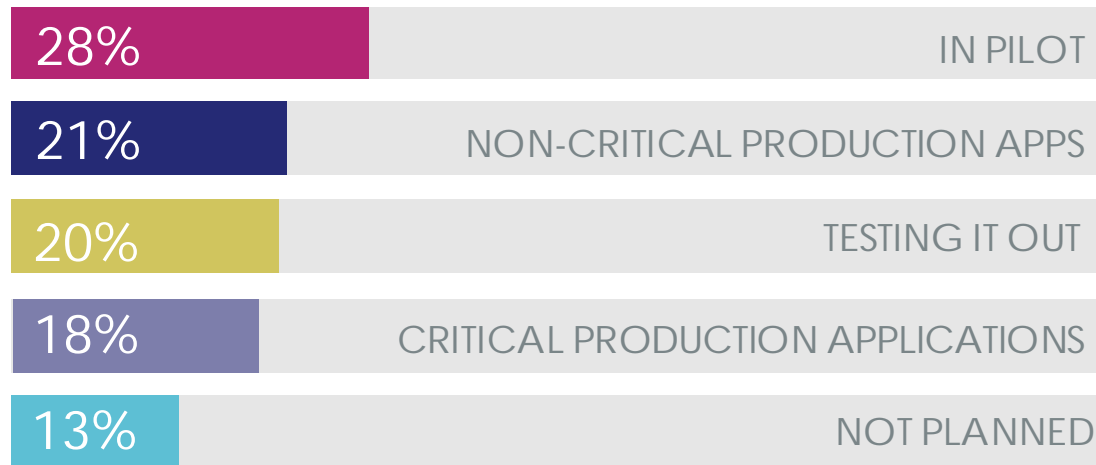- 39% - TOKENIZATION
- 38% - CASB
- 38% - SIEM

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

28%	IN PILOT
21%	NON-CRITICAL PRODUCTION APPS
20%	TESTING IT OUT
18%	CRITICAL PRODUCTION APPLICATIONS
13%	NOT PLANNED

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.

THALES   451 Research

2017
**THALES
DATA THREAT
REPORT**

Trends in Encryption
and Data Security

GLOBAL EDITION

#2017DataThreat

Our solutions protect data while eliminating complexity, inefficiency and cost

DB/ File Encryption	Application Encryption	Big Data	Code Signing	Tokenization Data Masking	Transaction Security	Public Key Infra (PKI)	Cloud Security
Customer Records	PII	Secure Analytics	Script Development	PCI, PHI	Payment related apps	Internet of Things	Cloud Migration

Use Cases

DATA PROTECTION
HARDWARE

DATA PROTECTION
SOFTWARE

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security