2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

HEALTHCARE EDITION

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 | 100 U.S. HEALTHCARE | 89 GLOBAL HEALTHCARE

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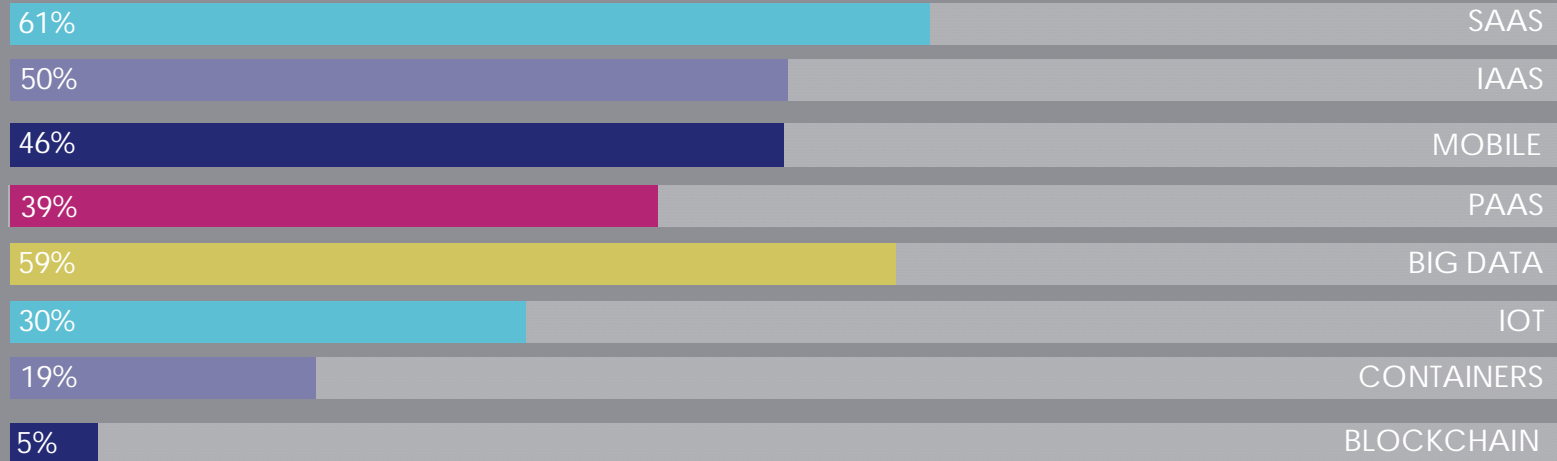
USING SENSITIVE DATA WITH ADVANCED TECHNOLOGIES
WITHOUT DATA SECURITY TO PROTECT INFORMATION

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

Technology	Percentage
SAAS	61%
IAAS	50%
MOBILE	46%
PAAS	39%
BIG DATA	59%
IOT	30%
CONTAINERS	19%
BLOCKCHAIN	5%

MORE BAD NEWS
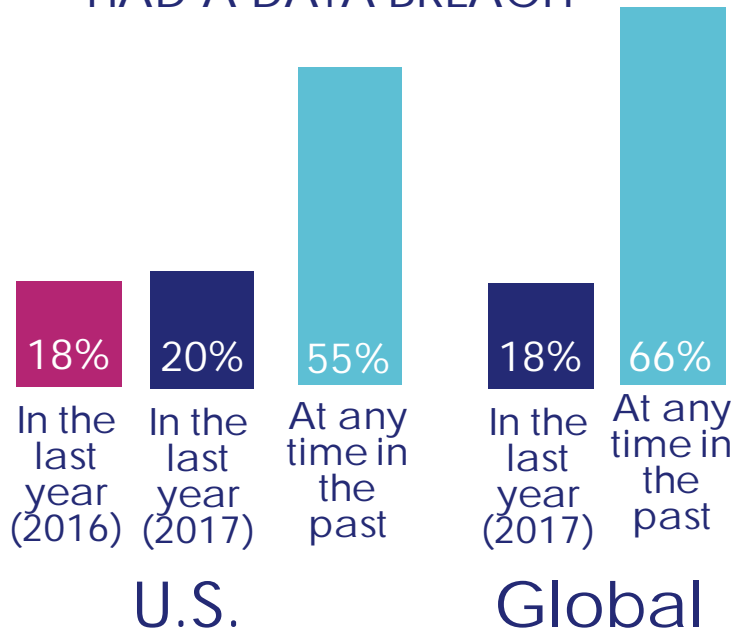## DATA BREACHES ARE UP IN SPITE OF INCREASE SPEND

"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

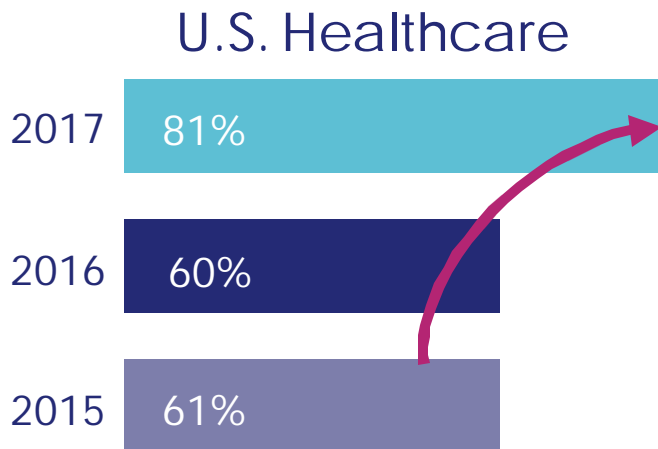| 18%	20%	55%	18%	66%
In the last year (2016)	In the last year (2017)	At any time in the past	In the last year (2017)	At any time in the past

U.S.   Global

SAFE OPERATION

43% – U.S.
34% – GLOBAL*

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

INCREASING SPENDING TO PROTECT DATA

U.S. Healthcare

2017 — 81%
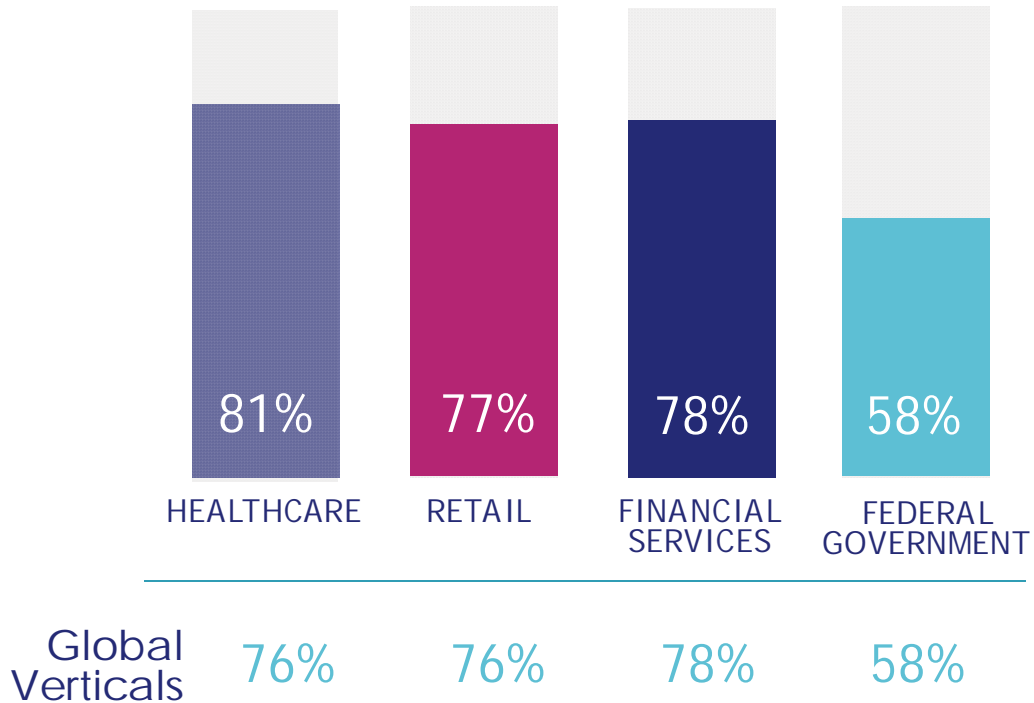2016 — 60%
2015 — 61%

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

81%	**77%**	**78%**	**58%**
HEALTHCARE	RETAIL	FINANCIAL SERVICES	FEDERAL GOVERNMENT

Global Verticals

76%	76%	78%	58%

"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
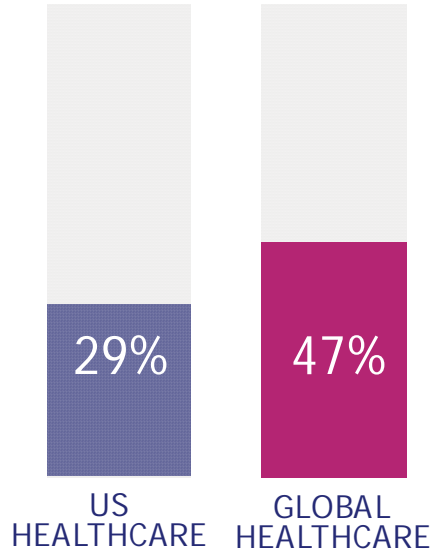## COMPARED TO THEIR GLOBAL COUNTERPARTS

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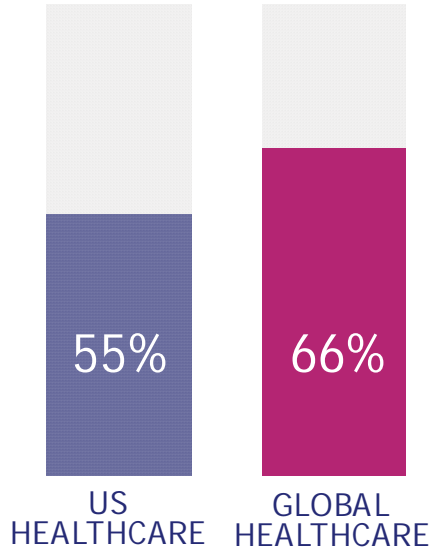
COMPARATIVE VERY OR
EXTREMELY VULNERABLE LEVELS
(SMALLER NUMBERS ARE BETTER)

RATES OF COMPLIANCE AS
"VERY" OR "EXTREMELY"
EFFECTIVE AT PREVENTING
DATA BREACHES

US HEALTHCARE	GLOBAL HEALTHCARE	US HEALTHCARE	GLOBAL HEALTHCARE	US HEALTHCARE	GLOBAL HEALTHCARE
55%	66%	29%	47%	63%	59%
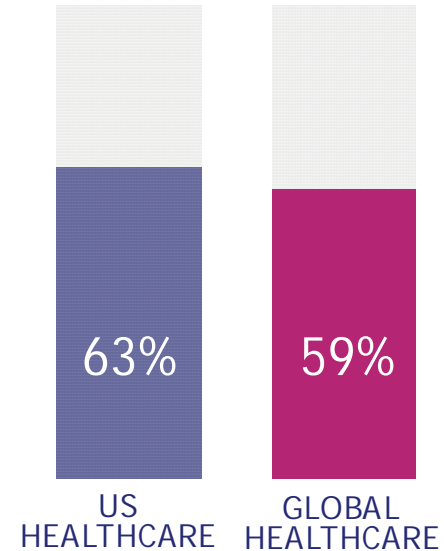
U.S. HEALTHCARE INCREASING SPENDING THE MOST
WHERE DEFENSES OFTEN FAIL TO PROTECT DATA
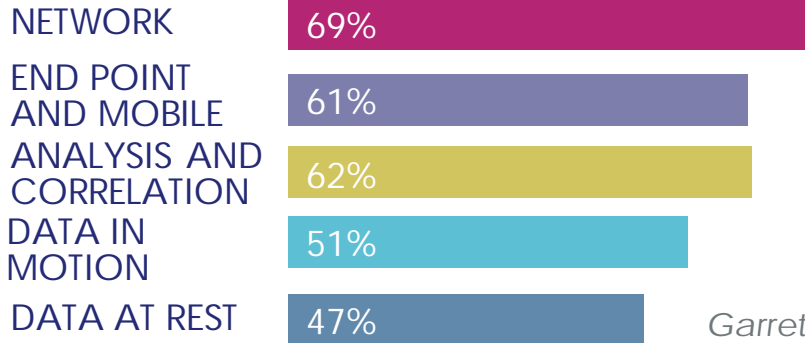
92%
+14% FROM 2016

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

NETWORK	69%
END POINT AND MOBILE	61%
ANALYSIS AND CORRELATION	62%
DATA IN MOTION	51%
DATA AT REST	47%

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
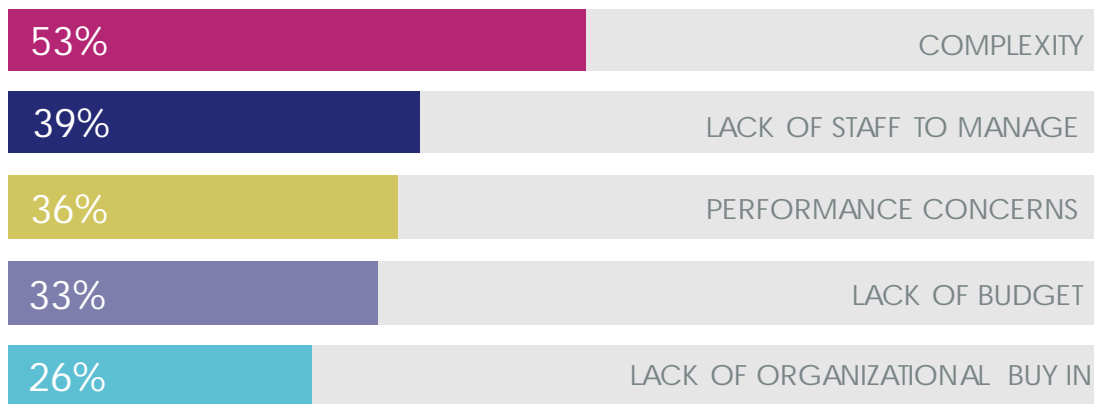## TOP BARRIERS TO DATA SECURITY DEPLOYMENT

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

53%	COMPLEXITY
39%	LACK OF STAFF TO MANAGE
36%	PERFORMANCE CONCERNS
33%	LACK OF BUDGET
26%	LACK OF ORGANIZATIONAL BUY IN

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

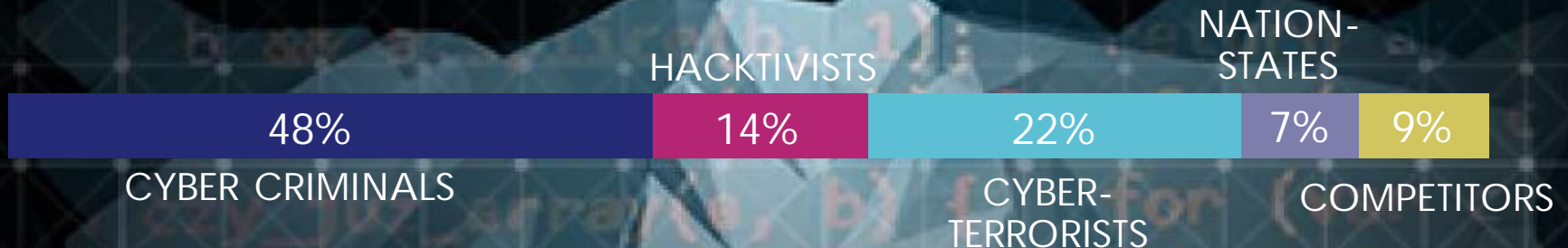|	
61%	PRIVILEGED USERS
46%	EXECUTIVE MANAGEMENT
33%	CONTRACTORS
26%	SERVICE PROVIDERS

* 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

CYBER CRIMINALS	HACKTIVISTS	CYBER-TERRORISTS	NATION-STATES	COMPETITORS
48%	14%	22%	7%	9%

* 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
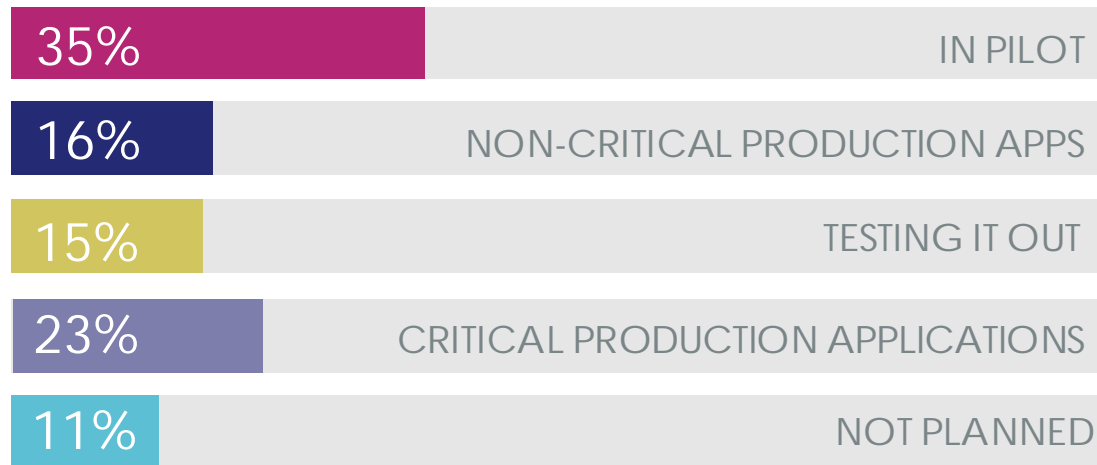
70% - IDENTITY AND ACCESS MANAGEMENT

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

35% — IN PILOT

16% — NON-CRITICAL PRODUCTION APPS

15% — TESTING IT OUT

23% — CRITICAL PRODUCTION APPLICATIONS

11% — NOT PLANNED

CONTAINER BASED APPLICATION DEPLOYMENTS

58% SELECTED ENCRYPTION AS THE #1 SECURITY CONTROL REQUIRED TO EXPAND CONTAINER USAGE

* U.S. RESULTS

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
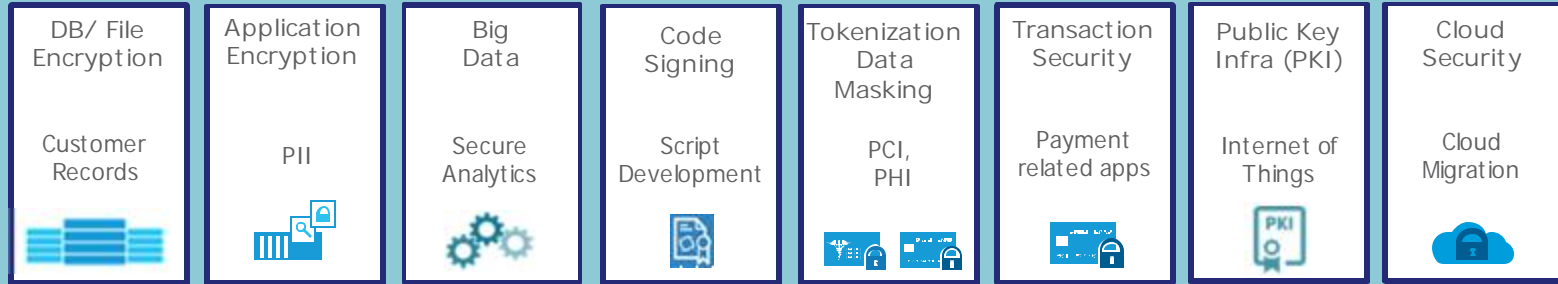
ABOUT THALES E-SECURITY

- **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

Use Cases

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

DATA PROTECTION HARDWARE

Transparent Encryption • Application Encryption • Tokenization • Encryption Gateway • Key Management • Security Intelligence

DATA PROTECTION SOFTWARE