

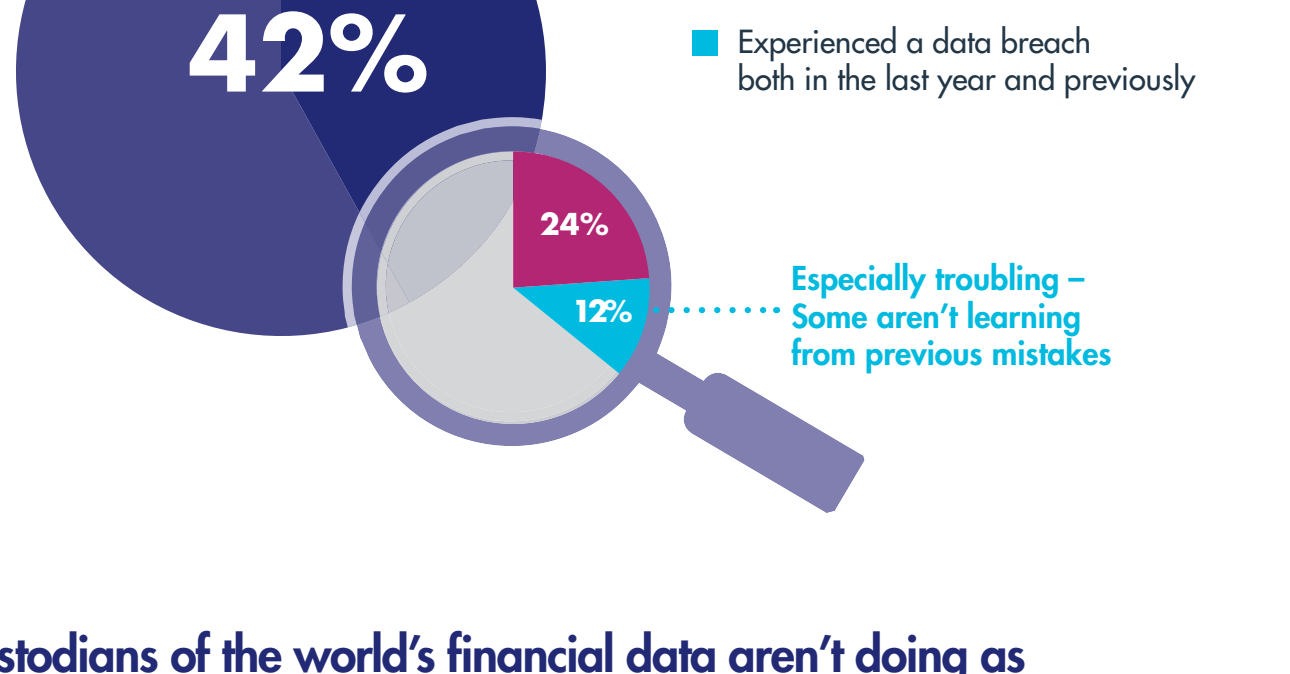
# FINANCIAL SERVICES

## THREATS TO FINANCIAL SERVICES DATA CONTINUE TO INCREASE

"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, 451 Research Principal Analyst, Information Security

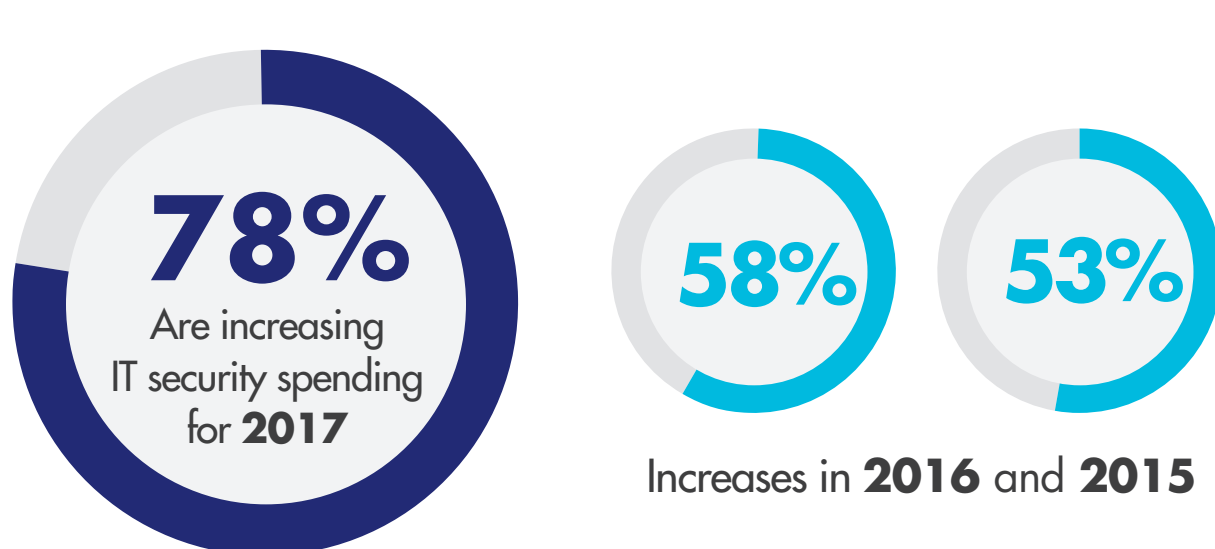
### INCREASING DATA BREACHES, EVEN WHILE IT SECURITY SPENDING CONTINUES TO RATCHET UP



Custodians of the world's financial data aren't doing as well as retailers or healthcare providers in the last year:



Even while data security spending at U.S. Financial Services firms increases for the third year in a row:

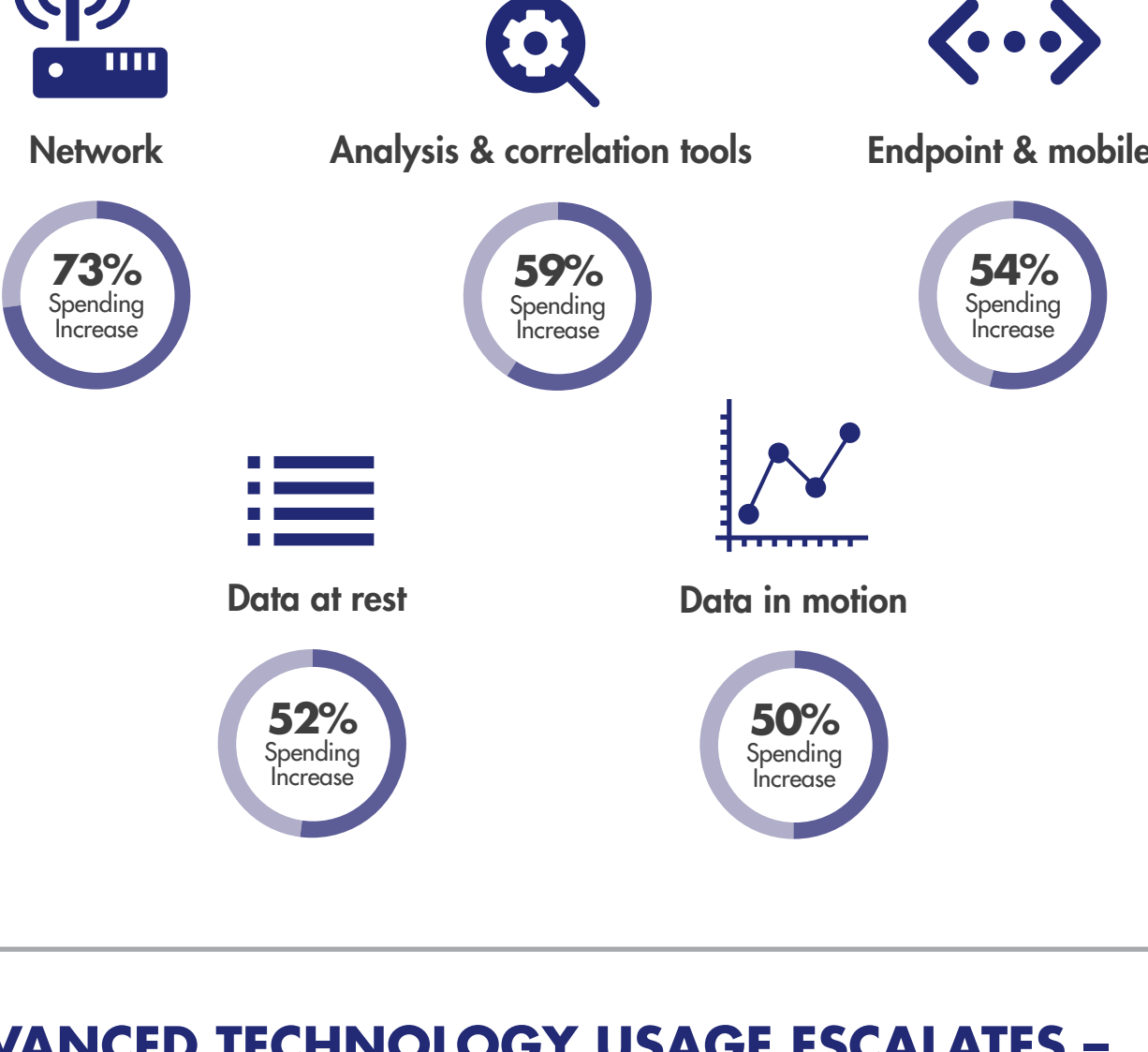


### DATA AT REST PROTECTION NEEDS TO BE A HIGHER PRIORITY

"What is perhaps more disturbing is that in both the U.S. and global financial services sectors, data security ranks at the bottom in terms of spending plans. For example, in U.S. financial services, data-at-rest security was selected by 52%, and data-in-motion defenses by 50%, dead last among all choices."

—Garrett Bekker, 451 Research Principal Analyst, Information Security

#### 2017 IT Security spending increases in U.S. Financial Services



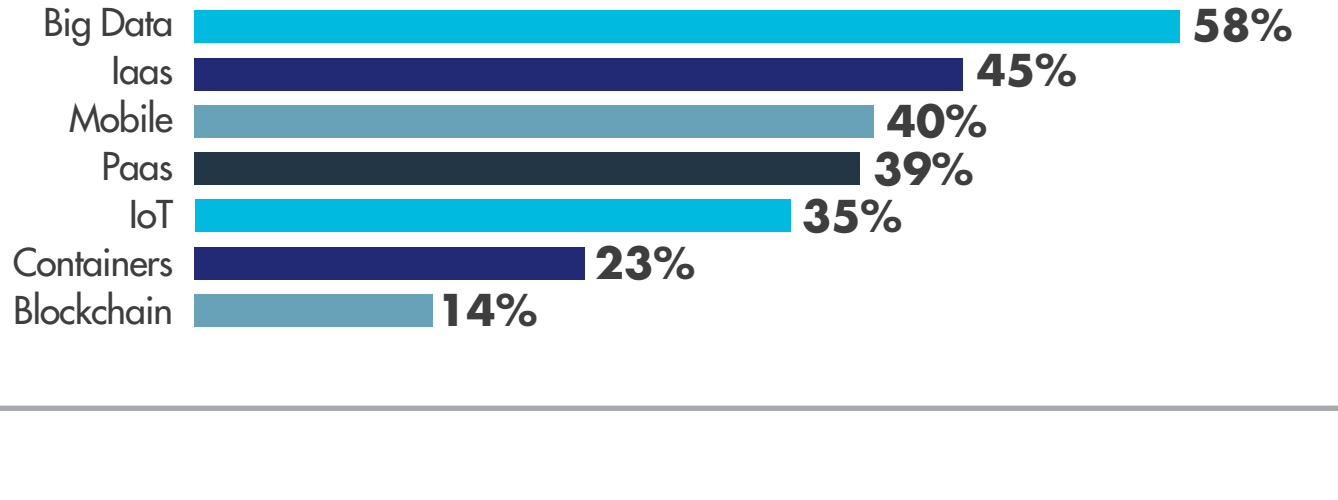
### ADVANCED TECHNOLOGY USAGE ESCALATES - COMPOUNDING THE PROBLEM

"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."

—Garrett Bekker, 451 Research Principal Analyst, Information Security



U.S. Financial Services rates of sensitive data use by advanced technology environment:



### GOOD NEWS - RECOGNITION THAT ENCRYPTION ENABLES DIGITAL TRANSFORMATION WITH ADVANCED TECHNOLOGIES



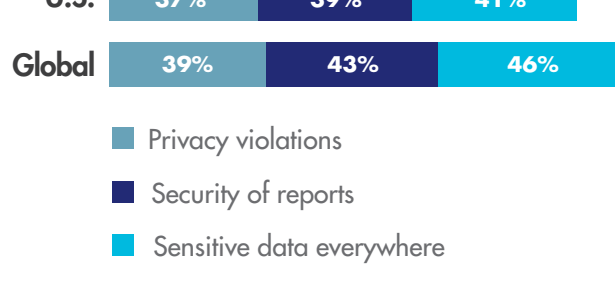
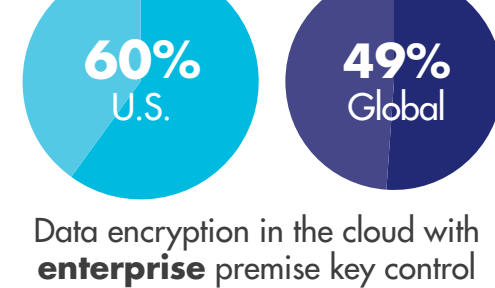
#### Cloud

Encryption enables further adoption of cloud



#### Big Data

Encryption offsets top security concerns



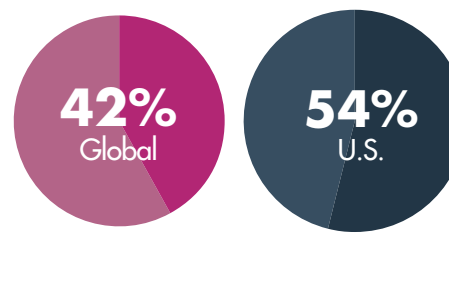
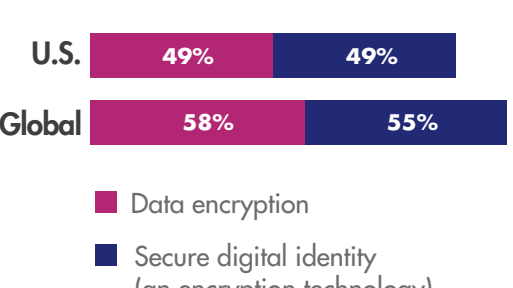
#### IoT

The top technologies needed to expand usage



#### Containers

Encryption the top control needed to enable greater adoption



# WHAT TO DO ABOUT IT

- ### 1 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
- ### 2 DISCOVER AND CLASSIFY

Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT
- ### 3 DON'T JUST CHECK OFF THE COMPLIANCE BOX

Move beyond compliance to greater use of encryption and BYOK, especially for cloud and other advanced technology environments
- ### 4 ENCRYPTION AND ACCESS CONTROL

Encryption needs to move beyond laptops and desktops

  - Data center:** File and application level encryption and access controls
  - Containers:** Encrypt and control access to data - within containers and underlying storage
  - Cloud:** Encrypt and manage keys locally, BYOK enables safe SaaS, PaaS and IaaS
  - 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
  - Big Data:** Encryption and access control within the environment

[CLICK TO DOWNLOAD REPORT](#)

FOLLOW US ON:

