harris poll

2015 VORMETRIC INSIDER THREAT REPORT

Trends and Future Directions in Data Security

Focus on U.S. Healthcare

Sponsoring Partners

Couchbase | FINANCIAL SERVICES Information Sharing and Analysis Center | CSA cloud security alliance | rackspace the #1 managed cloud company | fishnet SECURITY | OASIS | M.TECH Your Preferred I-Security Partner | ZM | PREVENTIA | fieldfisher | carahsoft | Raber+Märcker Prinzip Partnerschaft

2015 VORMETRIC
INSIDER THREAT REPORT – RETAIL AND FINANCIAL SERVICES FOCUS

Polling by Harris harris poll

818 IT DECISION MAKERS
US, UK, Germany, Japan, ASEAN

102 U.S. HEALTHCARE

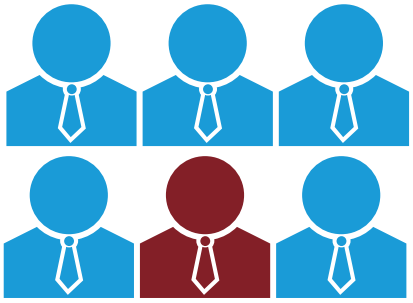
102 U.S. FINANCIAL SERVICES

102 U.S. RETAIL

100% Enterprises:
$200M + US
$100M + UK, Germany, Japan, ASEAN

Vormetric Data Security

WHERE DO
INSIDER THREATS COME FROM?



ORDINARY EMPLOYEES

PRIVILEGED USERS

SERVICE PROVIDERS (INCLUDING CSPs) & CONTRACTORS

CRIMINAL HACKERS

NATION STATES

HACKERS TARGETING INSIDER ACCOUNTS

HEALTHCARE – FAILING

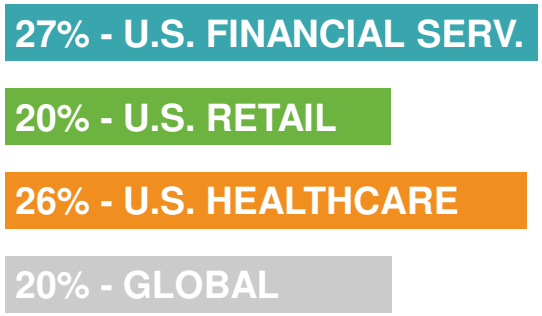
TO SECURE THEIR DATA

48%
ENCOUNTERED A DATA BREACH OR FAILED A COMPLIANCE AUDIT

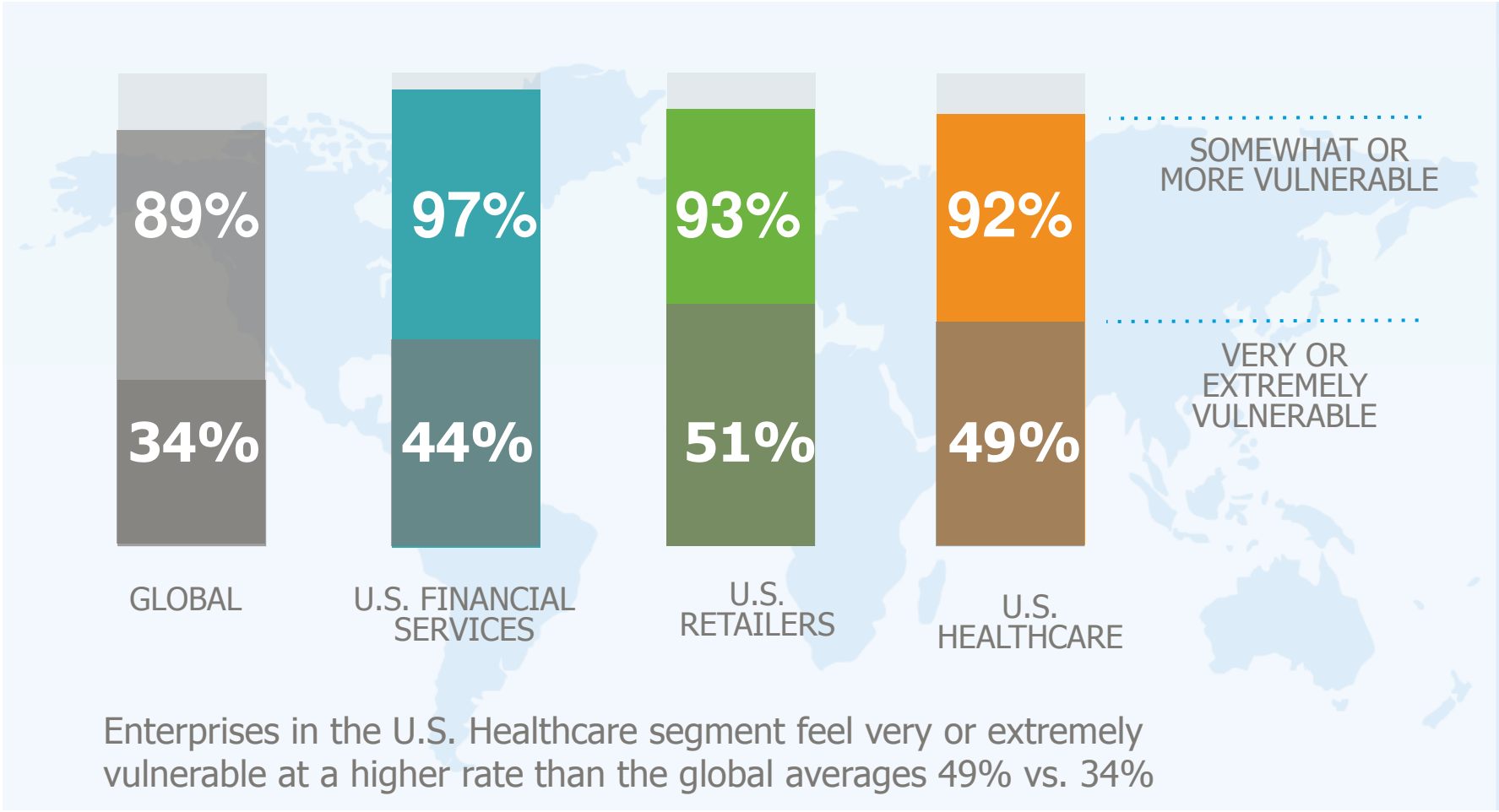
IN THE LAST 12 MONTHS

A PAST DATA BREACH

26% ARE PROTECTING DATA BECAUSE OF A PAST DATA BREACH

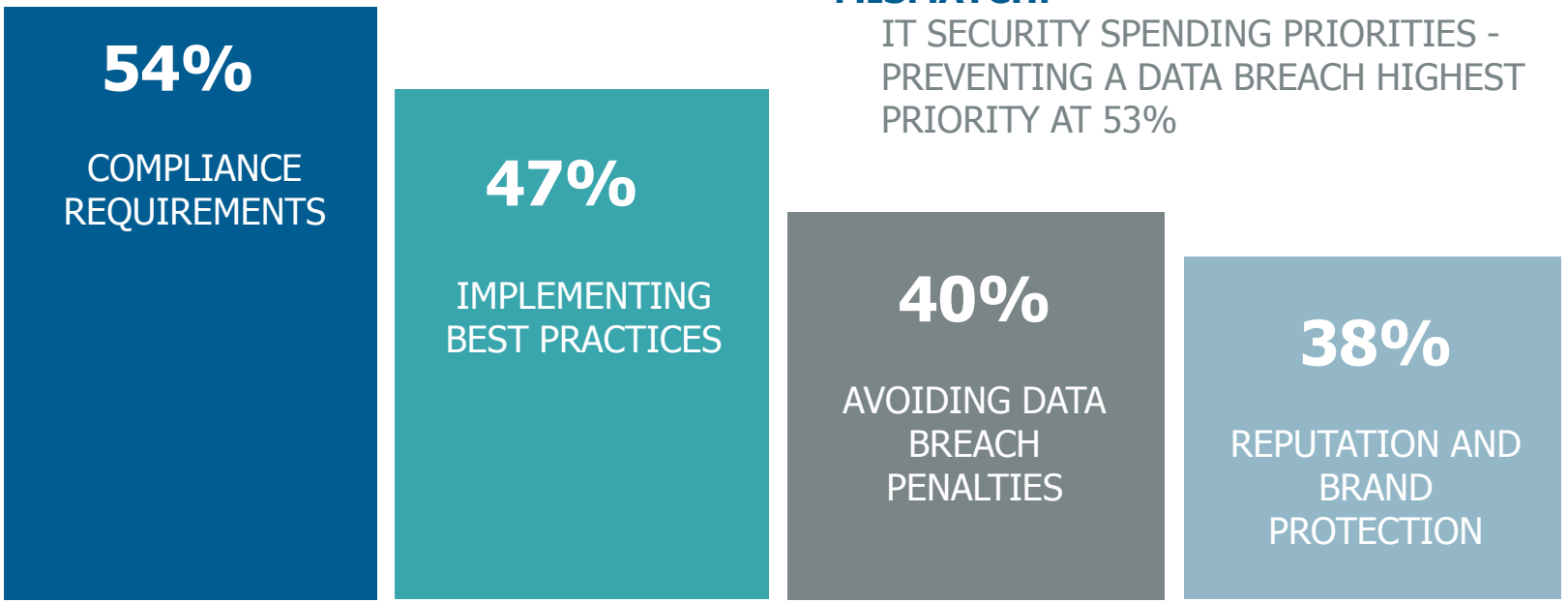


U.S. HEALTHCARE – HIGHLY VULNERABLE



Enterprises in the U.S. Healthcare segment feel very or extremely vulnerable at a higher rate than the global averages 49% vs. 34%

TOP REASONS FOR
SECURING SENSITIVE DATA



MISMATCH:
IT SECURITY SPENDING PRIORITIES - PREVENTING A DATA BREACH HIGHEST PRIORITY AT 53%

CONTRAST - TOP 3 GLOBALLY

51% REPUTATION AND BRAND PROTECTION
50% COMPLIANCE REQUIREMENTS
38% IMPLEMENTING BEST PRACTICES

THE MOST DANGEROUS INSIDERS
ADMINISTER & MANAGE INFRASTRUCTURE

Privileged Users

59% RETAIL
63% FINANCIAL SERVICES
62% HEALTHCARE

Privileged Users include System Administrators, Network Administrators, Linux/Unix Root Users, Domain Administrators and other IT roles.

Partners with Internal Access

51% RETAIL
43% FINANCIAL SERVICES
46% HEALTHCARE

Contractors/Service Provider Employees

(Snowden was a contractor)

45% RETAIL
40% FINANCIAL SERVICES
45% HEALTHCARE

CLOUD AND DATABASES

ARE HIGH RISKS FOR DATA LOSS

HIGHEST VOLUMES OF DATA AT RISK


43% DATABASES


41% CLOUD


33% FILE SERVERS


49% DATABASES


39% FILE SERVERS


36% CLOUD

PERCEIVED GREATEST RISK TO DATA


40% CLOUD


39% DATABASES


31% MOBILE


40% CLOUD


39% MOBILE


38% DATABASES

U.S. HEALTHCARE

GLOBAL

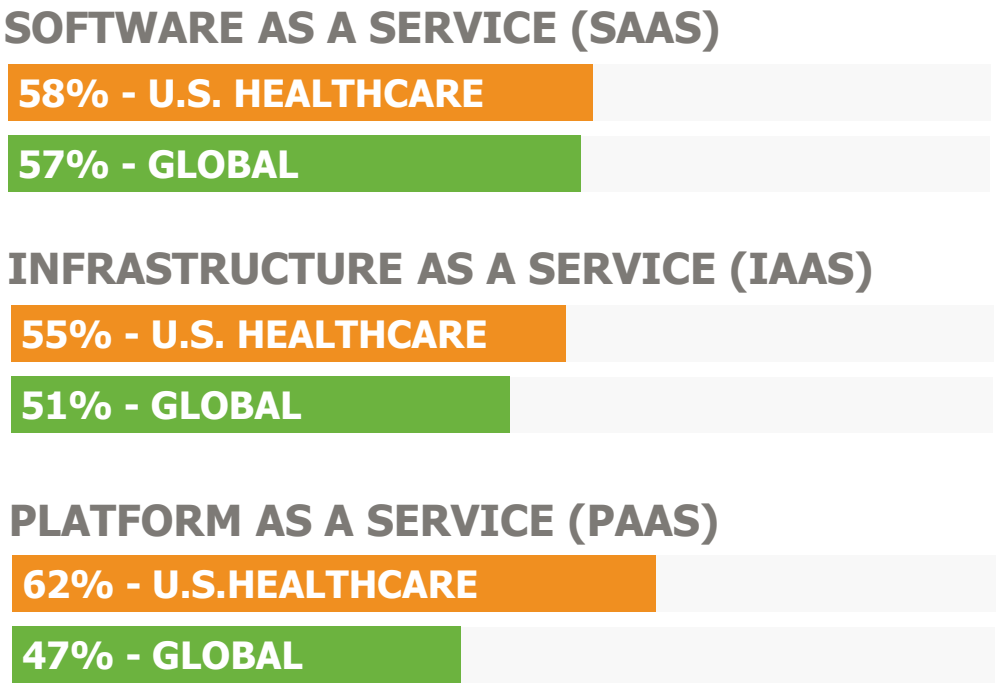
HIGH RATES OF SENSITIVE

DATA USE IN THE CLOUD

40%

CLOUD ENVIRONMENTS RATED THE **HIGHEST RISK** FOR LOSS OF SENSITIVE DATA BY HEALTHCARE RESPONDENTS

RATES OF SENSITIVE OR REGULATED DATA USE



BIG DATA – HEALTHCARE'S

SENSITIVE DATA USE IS GROWING

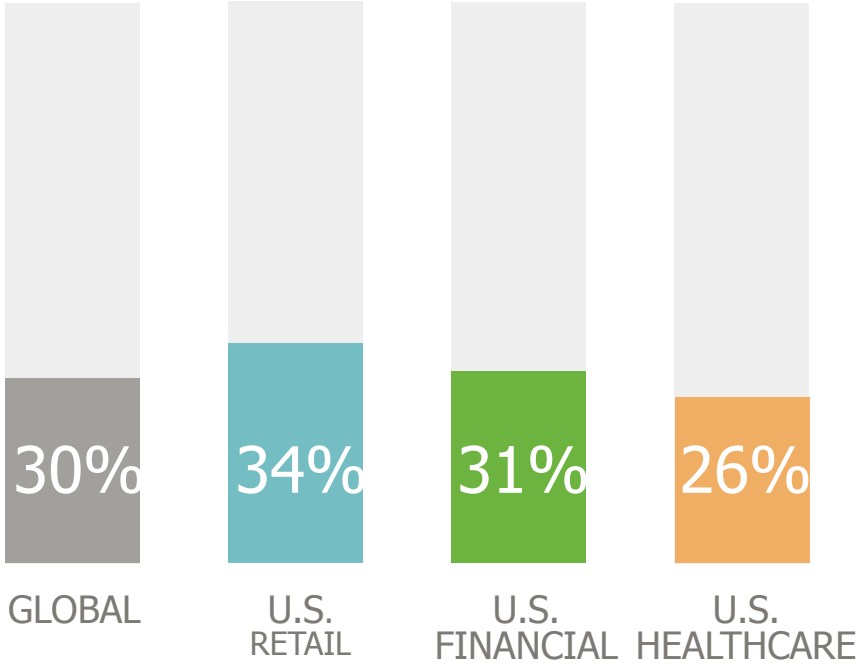
29%

CHOSE BIG DATA ENVIRONMENTS AS A TOP THREE RISK FOR LOSS SENSITIVE DATA

DOUBLE JEOPARDY

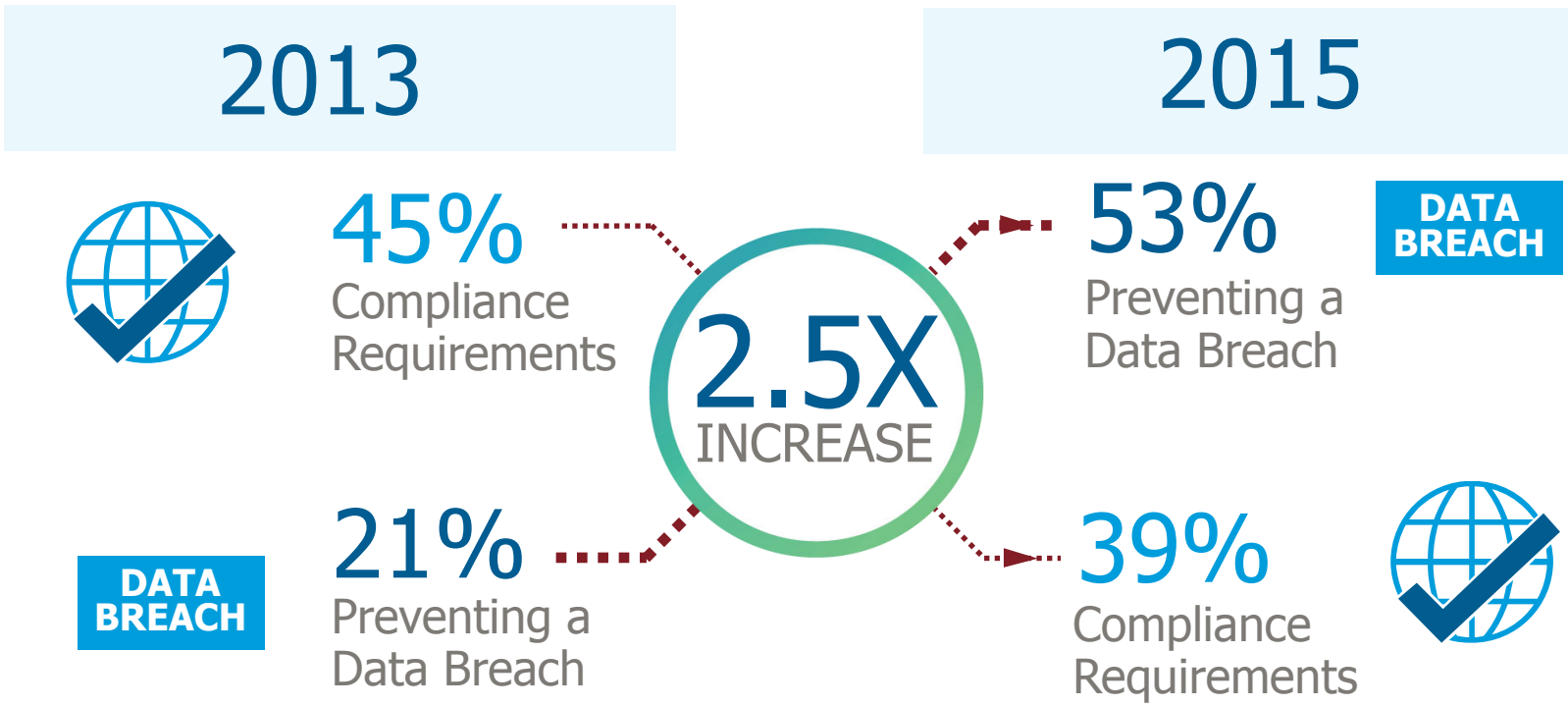
BIG DATA IS OFTEN IMPLEMENTED IN THE CLOUD

SELECTION AS A TOP 3 LOCATION FOR HOUSING VOLUMES OF SENSITIVE DATA

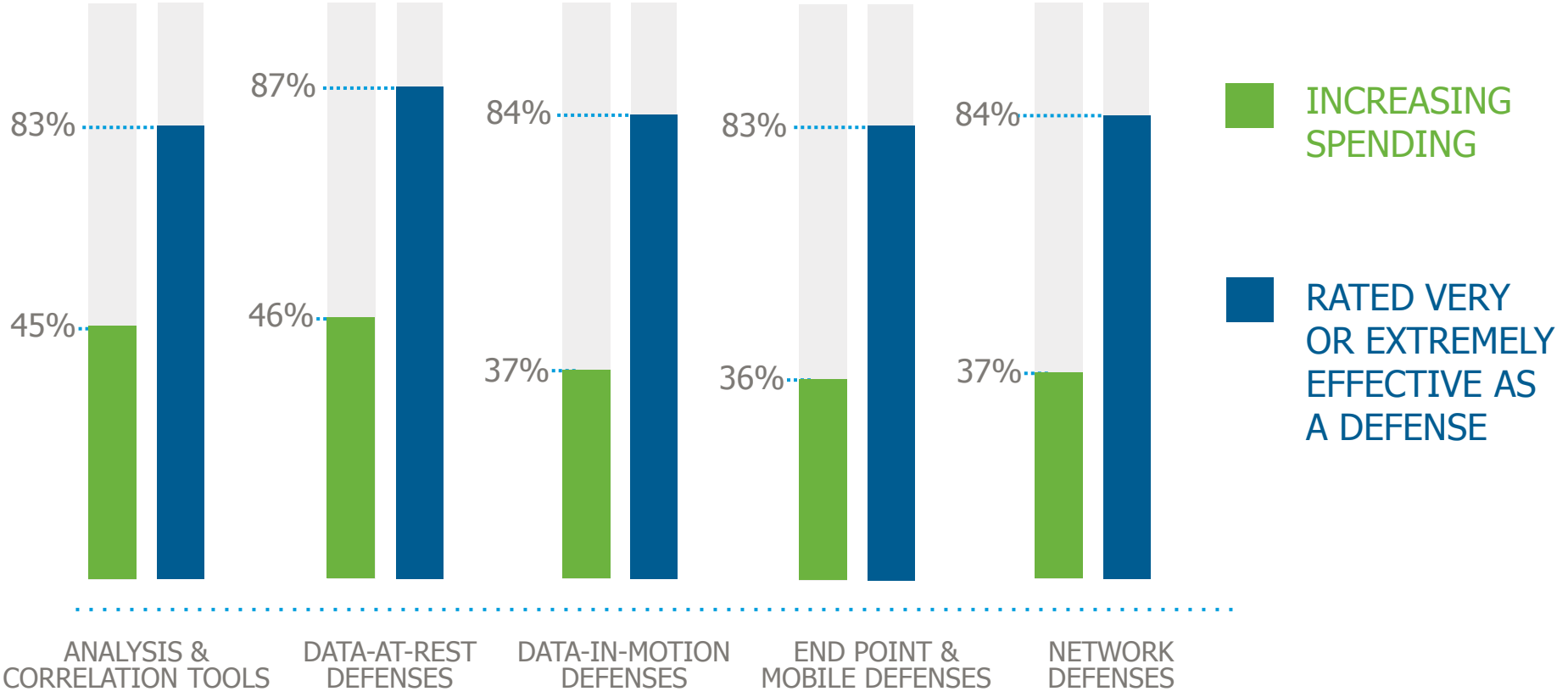


DRAMATIC CHANGES IN
IT SECURITY SPENDING PRIORITIES

63% OF HEALTHCARE RESPONDENTS ARE INCREASING SPENDING TO OFFSET THREATS TO DATA – AND WITH NEW PRIORITIES



U.S. HEALTHCARE –
INVESTING TO SOLVE THE PROBLEM



Investing more in Data-at-rest and Analysis / Correlation tools that help solve the problem … but still investing heavily in defenses that have failed

DATA-AT-REST
PROTECTIONS TODAY

49%
Database/File Encryption

45%
Data Access Monitoring

46%
Application Layer encryption

35%
Data Masking

22%
Tokenization

INSIDER THREATS

HOW TO PROTECT YOUR DATA

CONCENTRATE ON PROTECTING DATA AT THE SOURCE

MAKE ENCRYPTION WITH ACCESS CONTROLS THE DEFAULT

MONITOR AND ANALYZE DATA ACCESS PATTERNS

REPLACE POINT SOLUTIONS WITH DATA SECURITY PLATFORMS

THE STAKES HAVE CHANGED
CONSEQUENCES REACH THE C-SUITE

ALAN KESSLER – CEO FOR VORMETRIC

"The need to protect data is now a C-suite and board level concern – not just something for IT to worry about. From now on, if and when organizations are breached CEOs will be on the 6 O'clock news answering the question 'Was your sensitive data encrypted?'. "

"What's more, industry best practice will increasingly be used to demonstrate fiduciary responsibility. CEOs need to be able to say that their data was encrypted, that they controlled access and actively used data access logging to detect threats. *Without these protections, organization risk not only traditional data breach costs, but growing legal exposure to shareholder and class action lawsuits due to management's failure to protect critical internal and customer data assets.*"

Questions?