harris poll

2015 VORMETRIC INSIDER THREAT REPORT

Trends and Future Directions in Data Security

Focus on U.S. RETAIL and FINANCIAL SERVICES

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

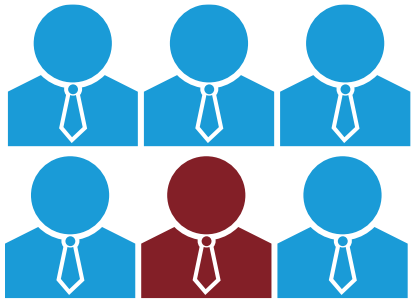
102 U.S. FINANCIAL SERVICES

102 U.S. RETAIL

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

Retail | Healthcare | Financial Services | Other Enterprise

WHERE DO
INSIDER THREATS COME FROM?



ORDINARY EMPLOYEES

PRIVILEGED USERS

SERVICE PROVIDERS & CONTRACTORS

CRIMINAL HACKERS

NATION STATES

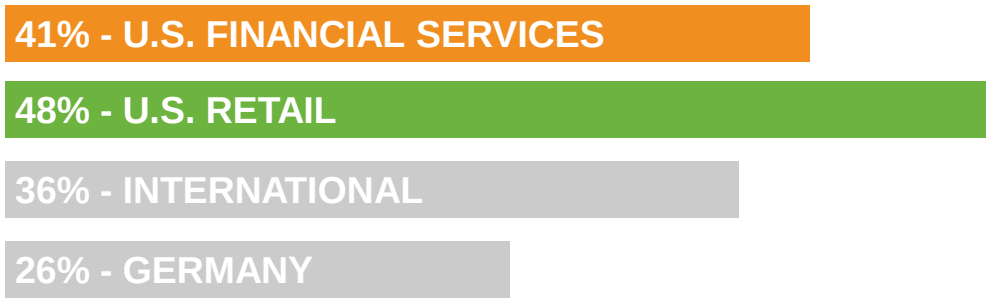
HACKERS TARGETING INSIDER ACCOUNTS

FAILING TO SECURE

THEIR DATA

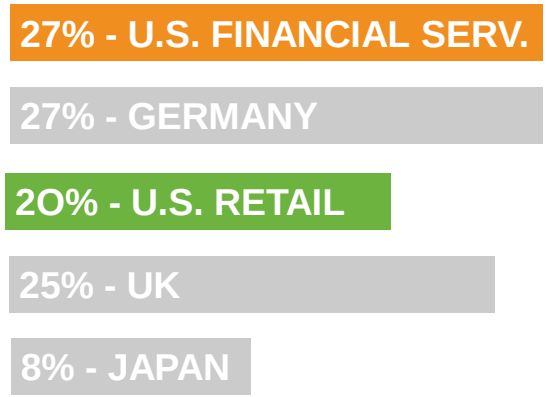
ENCOUNTERED A DATA BREACH OR FAILED A COMPLIANCE AUDIT

IN THE LAST 12 MONTHS

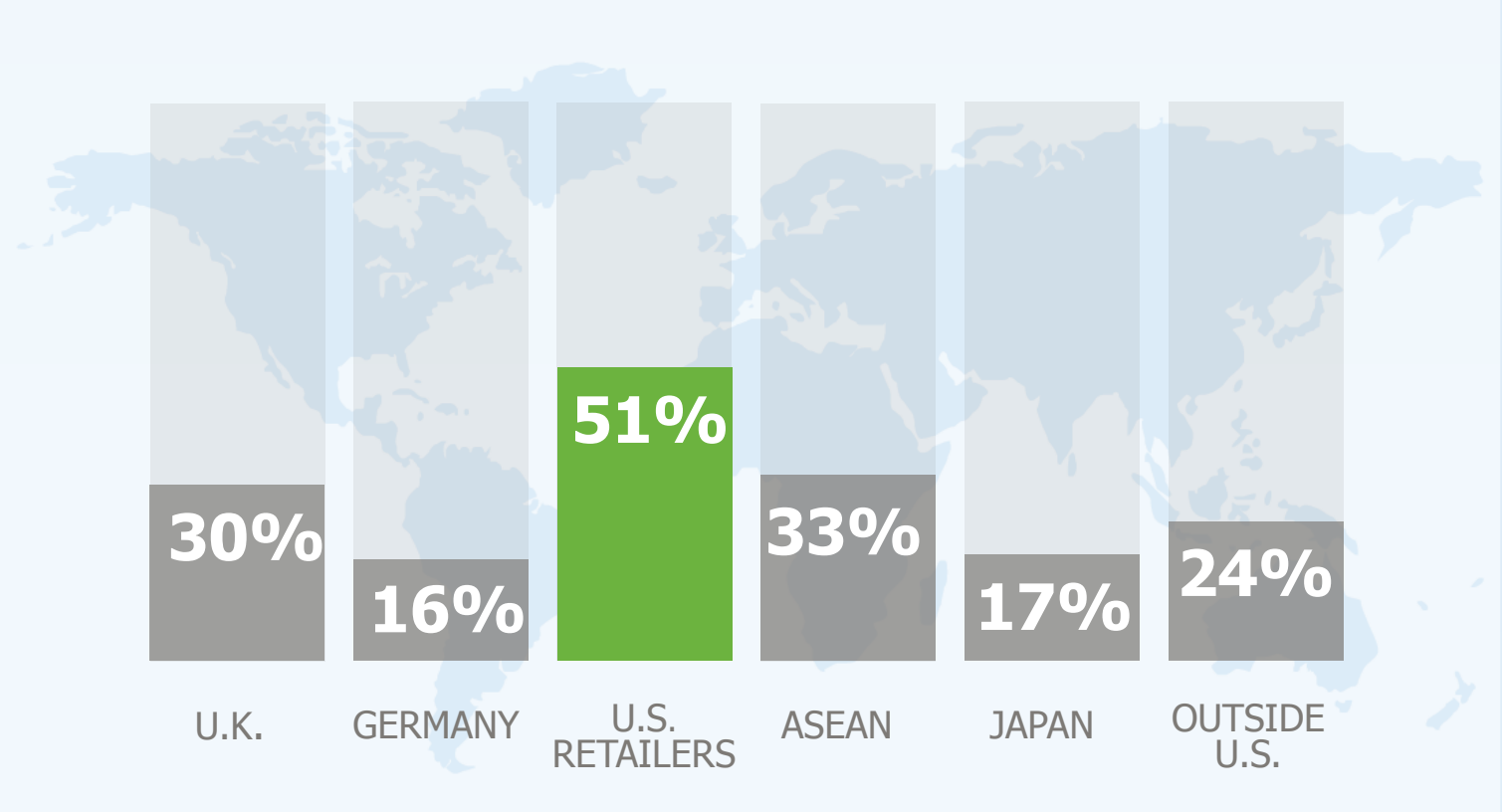


A PAST DATA BREACH

ARE PROTECTING DATA BECAUSE OF A PAST DATA BREACH



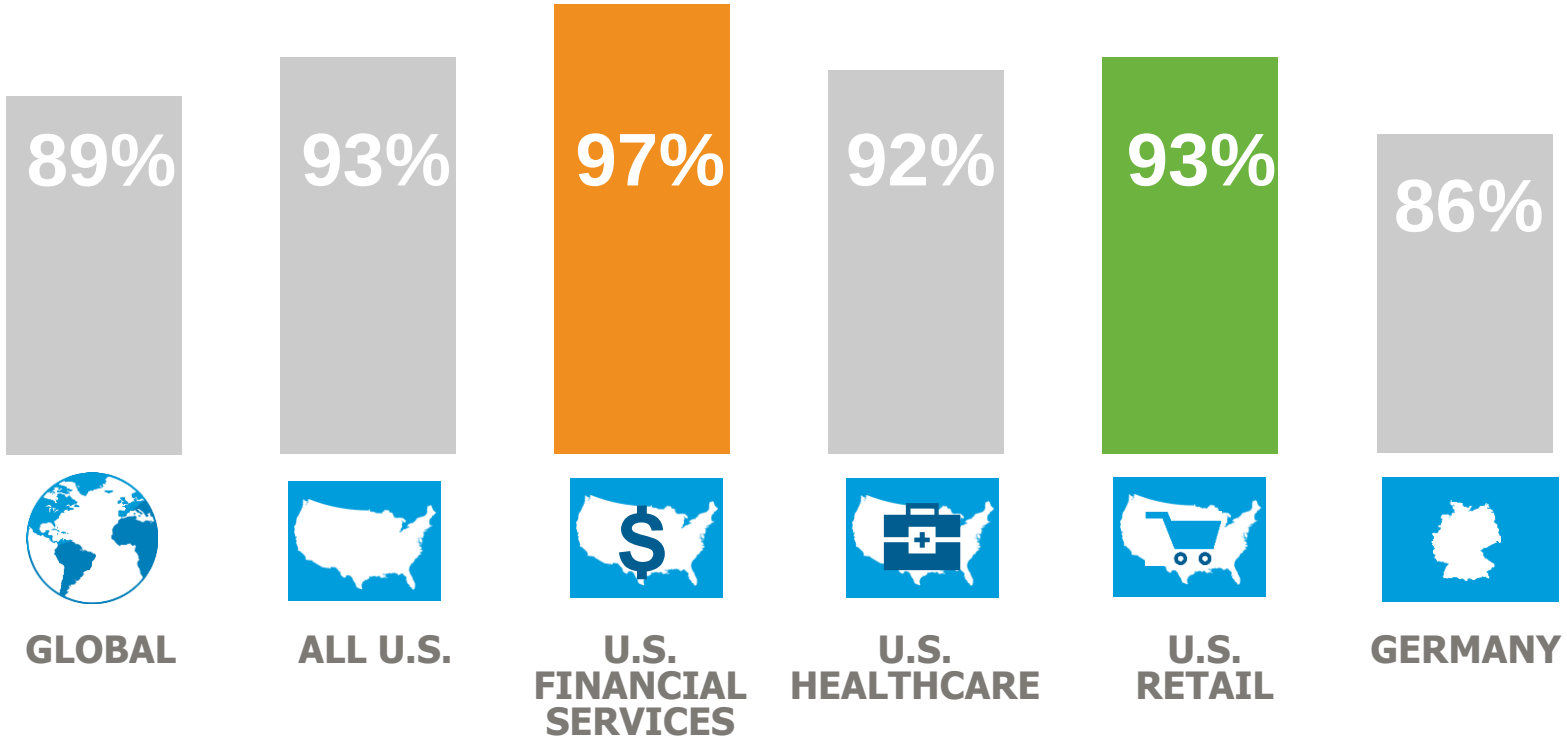
U.S. RETAILERS – HIGHEST RATES
OF VERY OR EXTREMELY VULNERABLE



2X U.S. Retail Enterprises feel very or extremely vulnerable at 2X the rate of non-U.S. enterprises polled

U.S. FINANCIAL SERVICES

HIGHEST OVERALL VULNERABLE RATE



CLOUD, BIG DATA AND DATABASES

ARE HIGH RISKS FOR DATA LOSS

HIGHEST VOLUMES OF SENSITIVE DATA


48% DATABASES


41% FILE SERVERS


36% CLOUD


49% CLOUD


42% DATABASES


34% BIG DATA

MOST WORRIED ABOUT DATA ON


47% MOBILE


45% DATABASES


42% CLOUD


51% CLOUD


37% BIG DATA


37% DATABASES

U.S. FINANCIAL SERVICES

U.S. RETAIL

THE MOST DANGEROUS INSIDERS
ADMINISTER & MANAGE INFRASTRUCTURE

Privileged Users

59% RETAIL

63% FINANCIAL SERVICES

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

Contractors/Service Provider Employees

(Snowden was a contractor)

45% RETAIL

40% FINANCIAL SERVICES

DRAMATIC CHANGES IN
IT SECURITY SPENDING PRIORITIES

2013
SPENDING PRIORITIES

45%
Compliance Requirements

DATA BREACH

21%
Preventing a Data Breach

3X
INCREASE RETAIL

2015
SPENDING PRIORITIES

63% RETAIL
57% FINANCIAL SERVICES

DATA BREACH

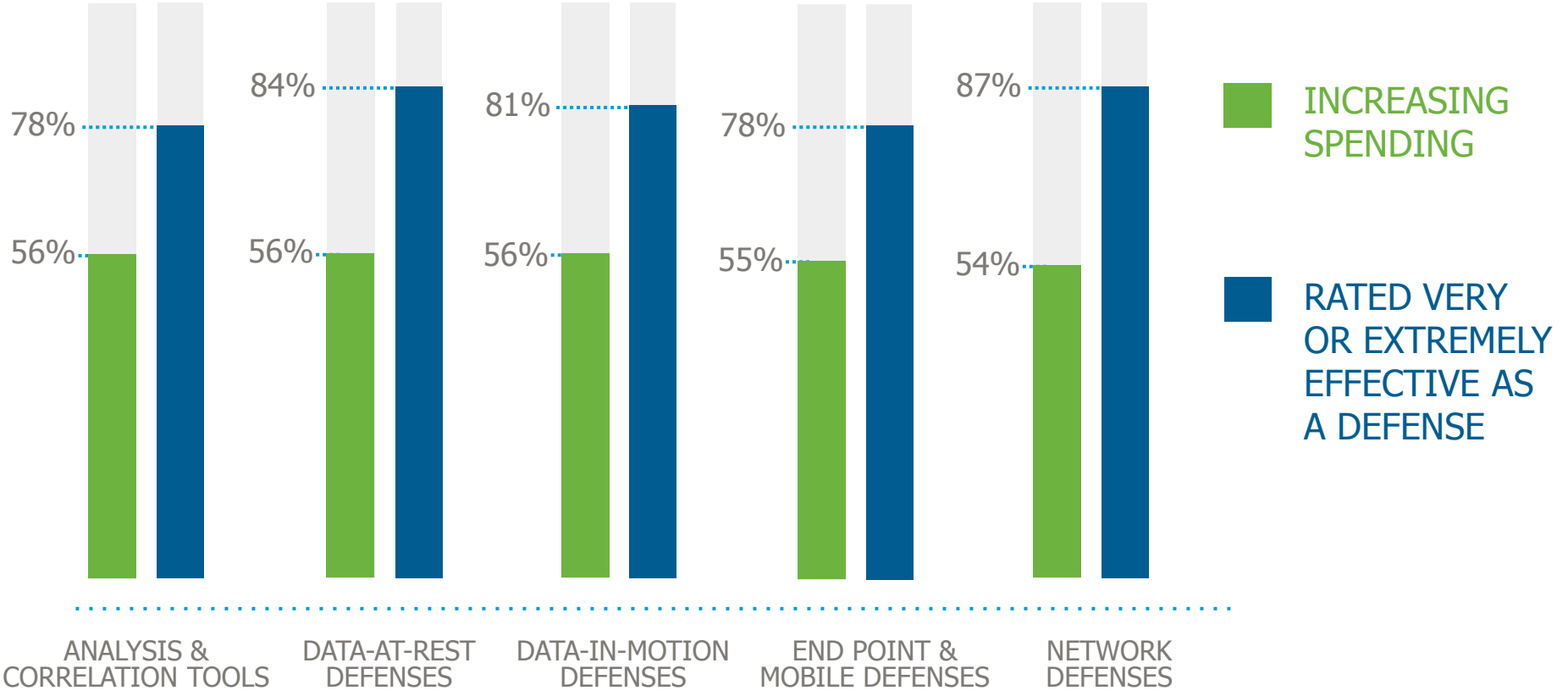
Preventing a Data Breach

27% RETAIL
39% FINANCIAL SERVICES

Compliance Requirements

U.S. RETAILERS ARE NOT SURE

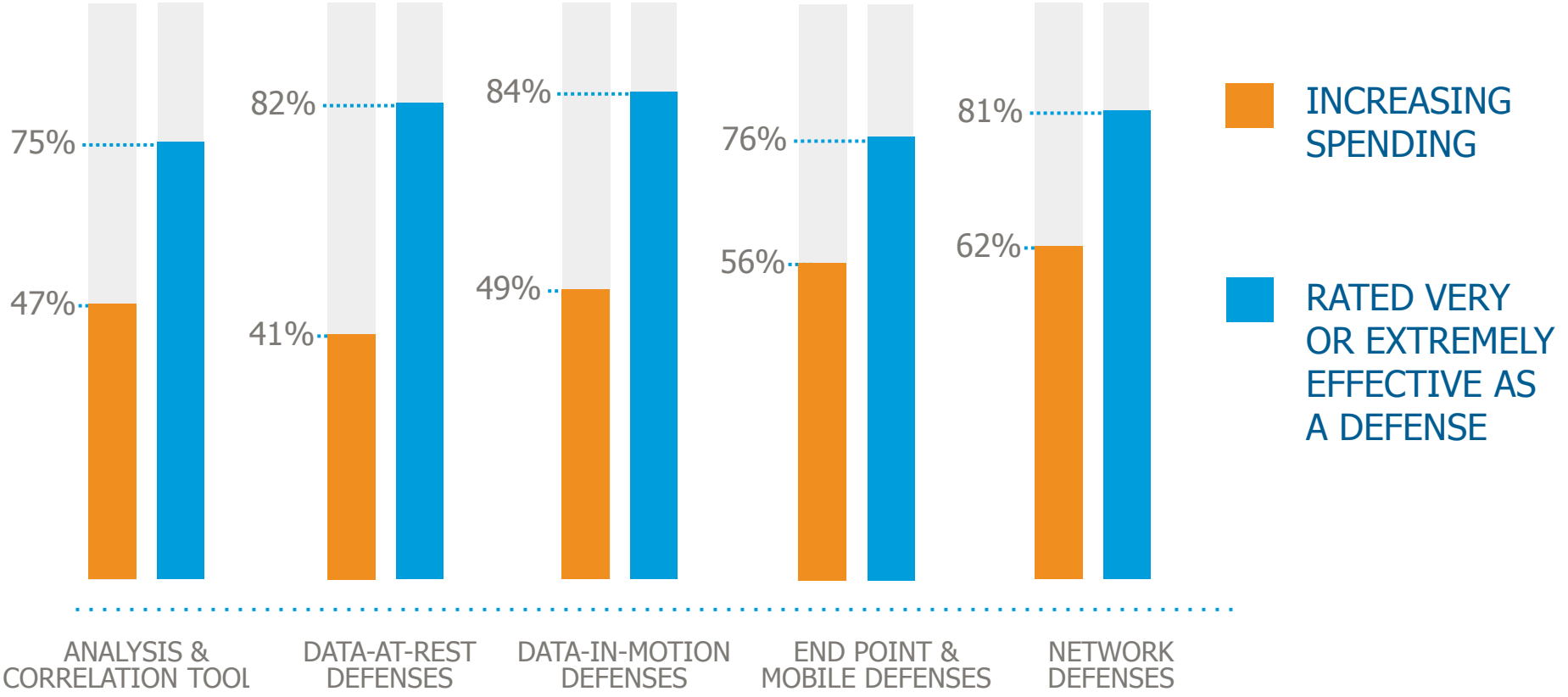
HOW TO SOLVE THE PROBLEM



Organizations both plan to invest in, and also rate as effective end point and network defenses that are consistently penetrated in insider attacks

U.S. FINANCIAL SERVICES

SIMILAR CONFUSIONS



EVEN LOWER INCREASES IN DATA AT REST SPENDING (56% RETAIL)

EVEN HIGHER INCREASES IN NETWORK DEFENSE SPENDING (54% RETAIL)

EXISTING PROTECTIONS
FOR DATA AT REST

58% RETAIL
54% FINANCIAL SERVICES

Database/File Encryption

48% RETAIL
51% FINANCIAL SERVICES

Data Access Monitoring

42% RETAIL
40% FINANCIAL SERVICES

Application Layer encryption

31% RETAIL
50% FINANCIAL SERVICES

Data Masking

28% RETAIL
26% FINANCIAL SERVICES

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?