Insider Threat Report

Sol Cates
CSO
scates@vormetric.com
@solcates @vormetric

Who is Sol

- **InfoSec for ~ 18 years**
- **Currently have 4 jobs**
  - Infrastructure
  - Product Strategy
  - Security Practitioner
  - Evangelist/Consultant/Shoulder

Vormetric Data Security

#DEFENDEROFDATA

- **Vision**
  - To Secure the World's Information
- **Purpose**
  - Protect business assets and brand
- **Customers**
  - 1500+ Customers Worldwide
  - 17 of Fortune 30
- **OEM Partners**
  - IBM – Guardium Data Encryption
  - Symantec – NetBackup MSEO
- **Global Presence**
  - Global Headquarters - San Jose, CA, USA
  - EMEA Headquarters - Reading, United Kingdom
  - APAC Headquarters -, Gangnam-gu, Seoul

BEST OF vmworld 2014 Gold Award Security/Compliance for Virtualized Environments

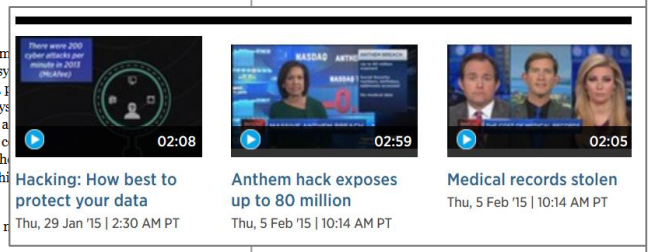
SC MAGAZINE AWARDS 2014 Europe WINNER

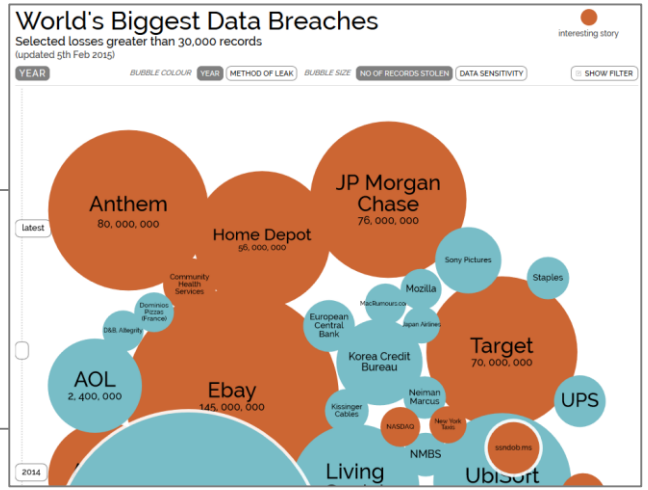
Deloitte. 2014 Technology Fast 500

A Shift in Business Reality

Global organizations being publicly exposed

- The perimeter has fallen and business is at risk
- Compliance is secondary to losing brand trust
- Growing legal exposure and class action lawsuits
- Protecting data: C-Suite and board level concern





2015 VORMETRIC
INSIDER THREAT REPORT

818 IT DECISION MAKERS

US, UK, Germany, Japan, ASEAN

100%

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

Retail | Healthcare | Financial Services | Other Enterprise

Polling by Harris

Analysis and Reporting by Ovum

Sensitive Data at Risk

Organizations feel more vulnerable than ever

93%

Organizations feel vulnerable to insiders

55%

Privileged users most dangerous insider

54%

Plan to increase spending next year

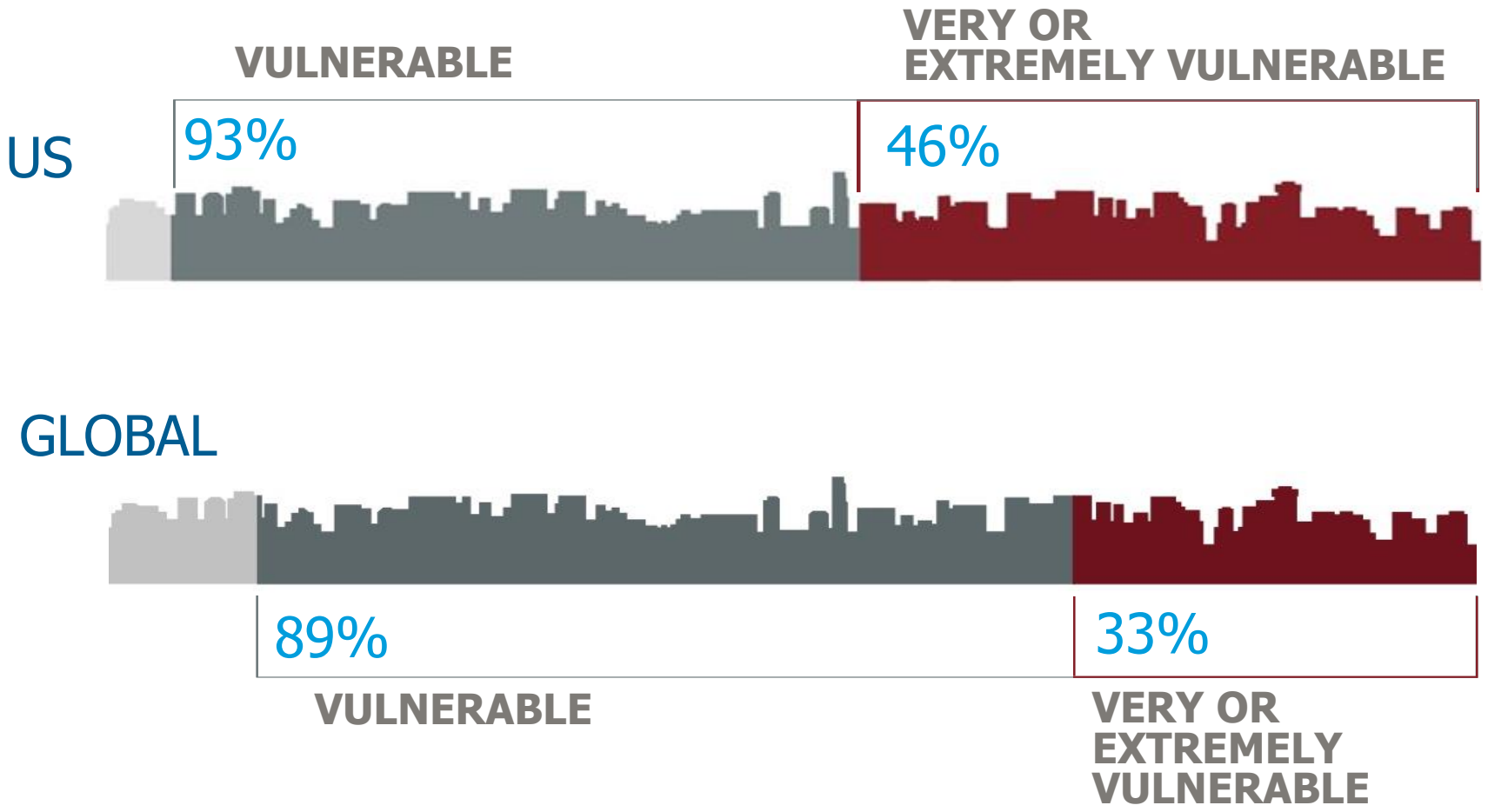
50%

Preventing Breach Top Business Priority

harris poll OVUM **2015 Vormetric Insider Threat Report – Global Edition**

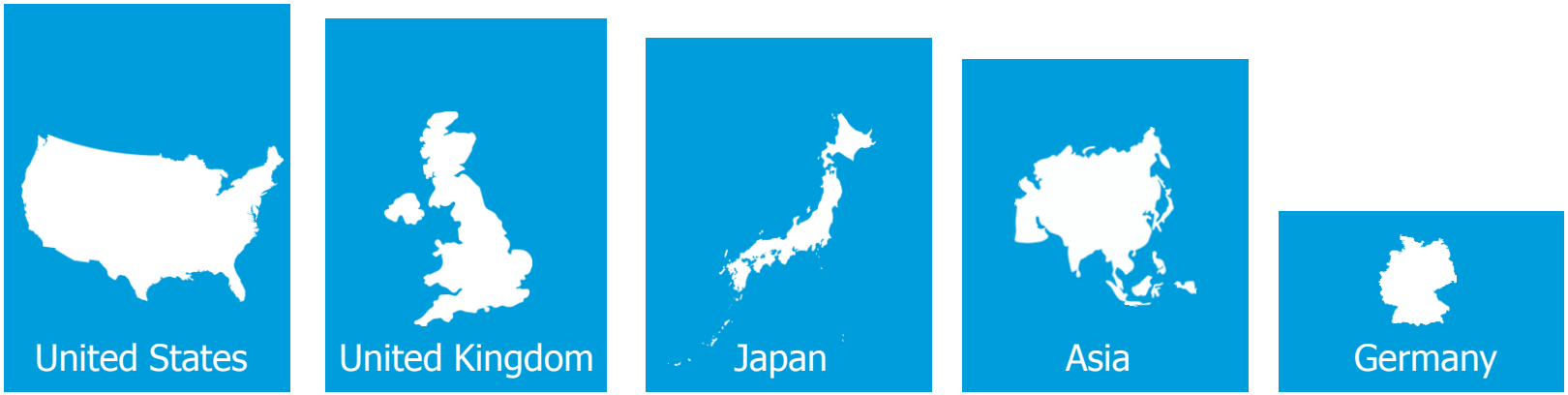
HIGHLY VULNERABLE

AT RISK TO INSIDER THREATS



THE US FEELS MOST VULNERABLE
TO INSIDER THREATS

THE US FEELS 2X MORE VULNERABLE THAN GERMANY



93% 91% 87% 84% 41%

GLOBAL ENTERPRISE VULNERABILITY TO INSIDER THREATS FROM MALICIOUS INSIDERS AND COMPROMISES OF INSIDER ACCOUNTS

THE MOST DANGEROUS INSIDERS
ADMINISTER & MANAGE INFRASTRUCTURE

55%
Privileged Users

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

46%
Contractors/Service Provider Employees
(Snowden was a contractor)

43%
Partners with Internal Access

EXCEPTION
JAPAN

56%
ORDINARY EMPLOYEES

EVOLVING THREATS

INSIDER THREATS HAVE CHANGED

TRADITIONAL INSIDERS

IN THE PAST

COMPANY EMPLOYEES WITH KNOWLEDGE-REQUIRED ACCESS

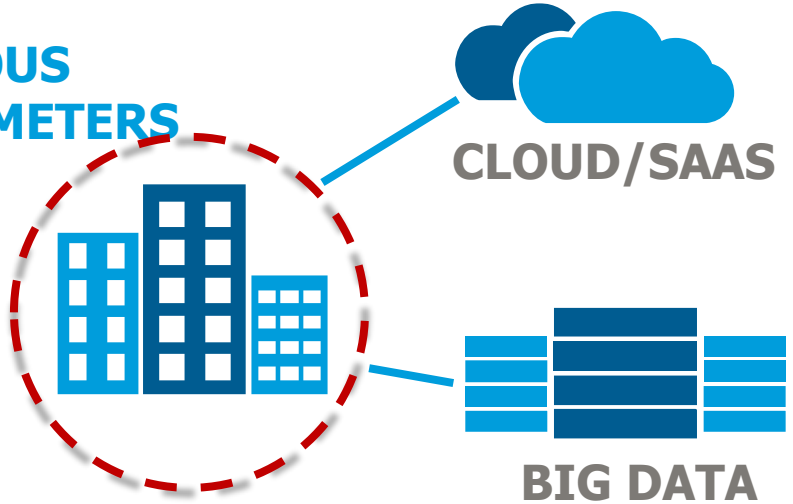
TODAY WE MUST ADD

IT PERSONNEL, CONTRACTORS SERVICE PROVIDER EMPLOYEES

COMPROMISE OF INSIDER ACCOUNTS

POROUS PERIMETERS

HACKERS ACTIVELY TARGET INSIDER ACCOUNTS WITH ACCESS TO DATA – REGARDLESS OF LOCATION



DATA CENTERS AND CLOUD

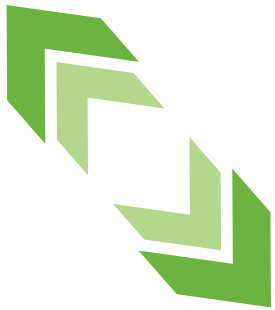
HOUSE THE LARGEST VOLUMES OF SENSITIVE DATA

49% **DATABASES**

39% **FILE SERVERS**

36% **CLOUD**

HIGHEST VOLUMES OF SENSITIVE DATA



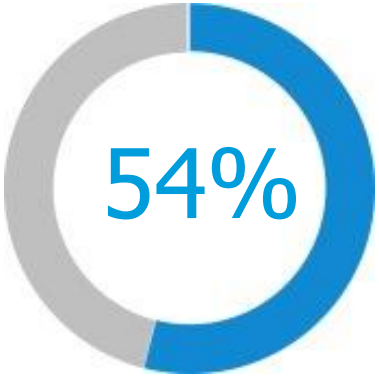
ORGANIZATIONS ARE MOST WORRIED ABOUT DATA ON

40% **CLOUD**

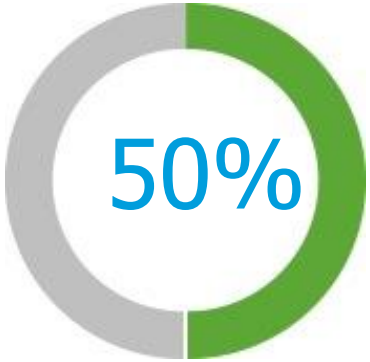
39% **MOBILE**

38% **DATABASES**

HOW ARE ORGANIZATIONS
ADDRESSING THE THREAT?



INCREASING SPENDING



NOW MAKE PREVENTING DATA BREACHES A TOP SPENDING PRIORITY

47% **INCREASING DATA AT REST DEFENSES**

TOP IT SPENDING PRIORITIES

COMPLIANCE IS LAST FOR THE FIRST TIME

50% PREVENTING A DATA BREACH INCIDENT

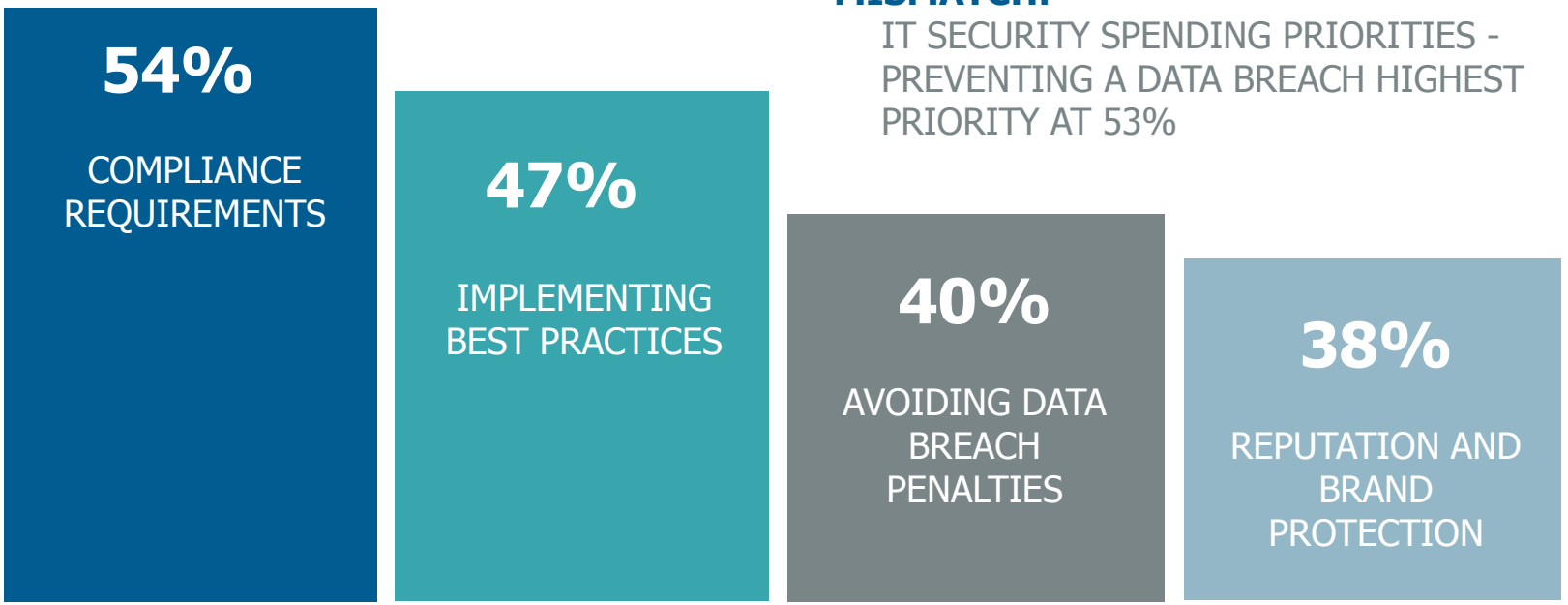
44% PROTECTION OF CRICAL IP

41% PROTECTION OF FINANCES AND OTHER ASSETS

32% FULFILLING REQUIREMENTS FROM CUSTOMERS, PARTNERS AND PROSPECTS

32% FULFILLING COMPLIANCE REQUIREMENTS AND PASSING AUDITS

EXCEPT FOR HEALTHCARE



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

IT's Dirty Little Secret

Information Technology's Dirty Little Secret

30

100

1

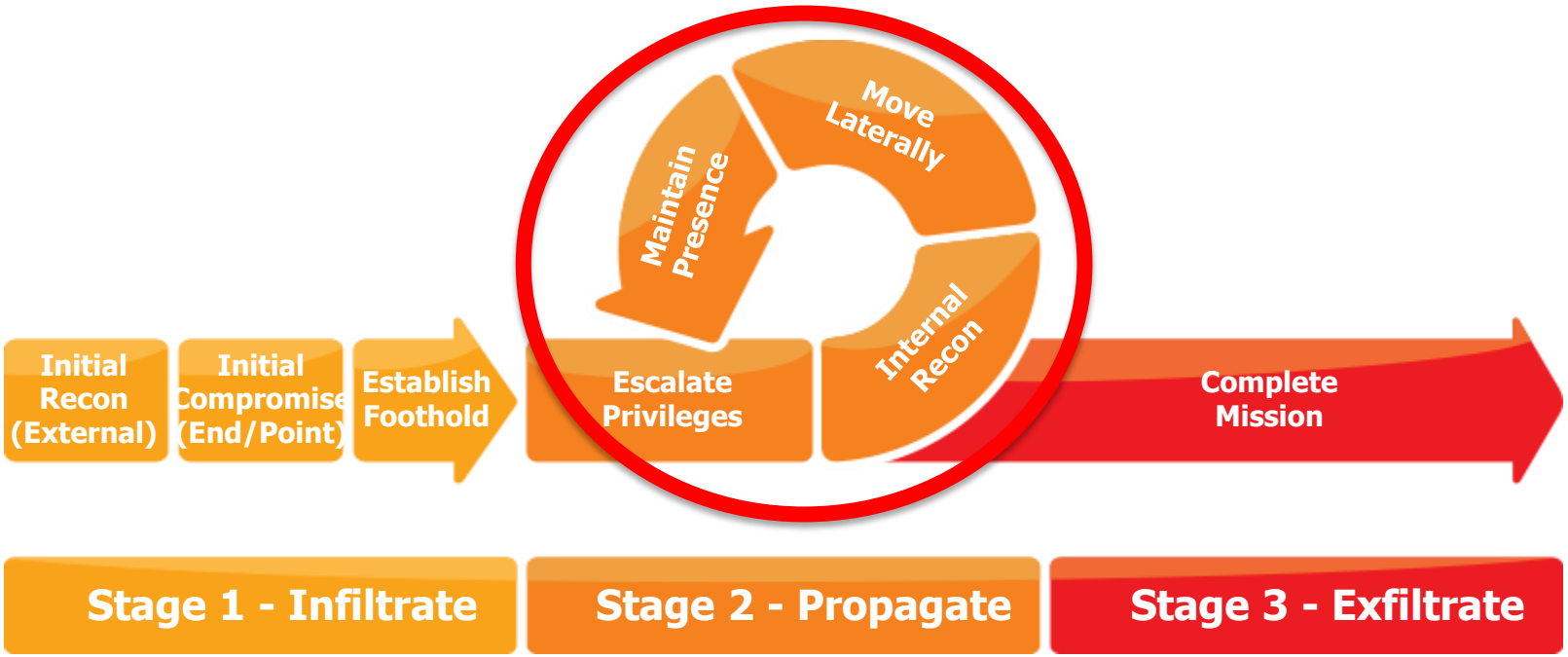
Information Technology's Dirty Little Secret

30+ Years super users have been managing our servers, their configurations, and data.

100% Super users have 100% access to all data in the systems they manage.

1 It only takes 1 compromised/rogue user to cause havoc.

Why is privilege so important?

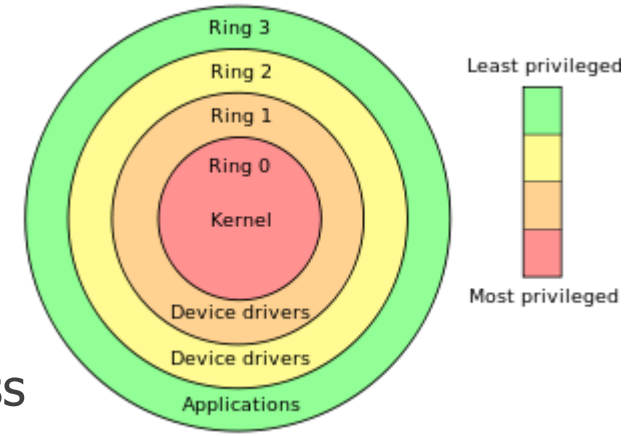


!

Common Requirement… Privilege

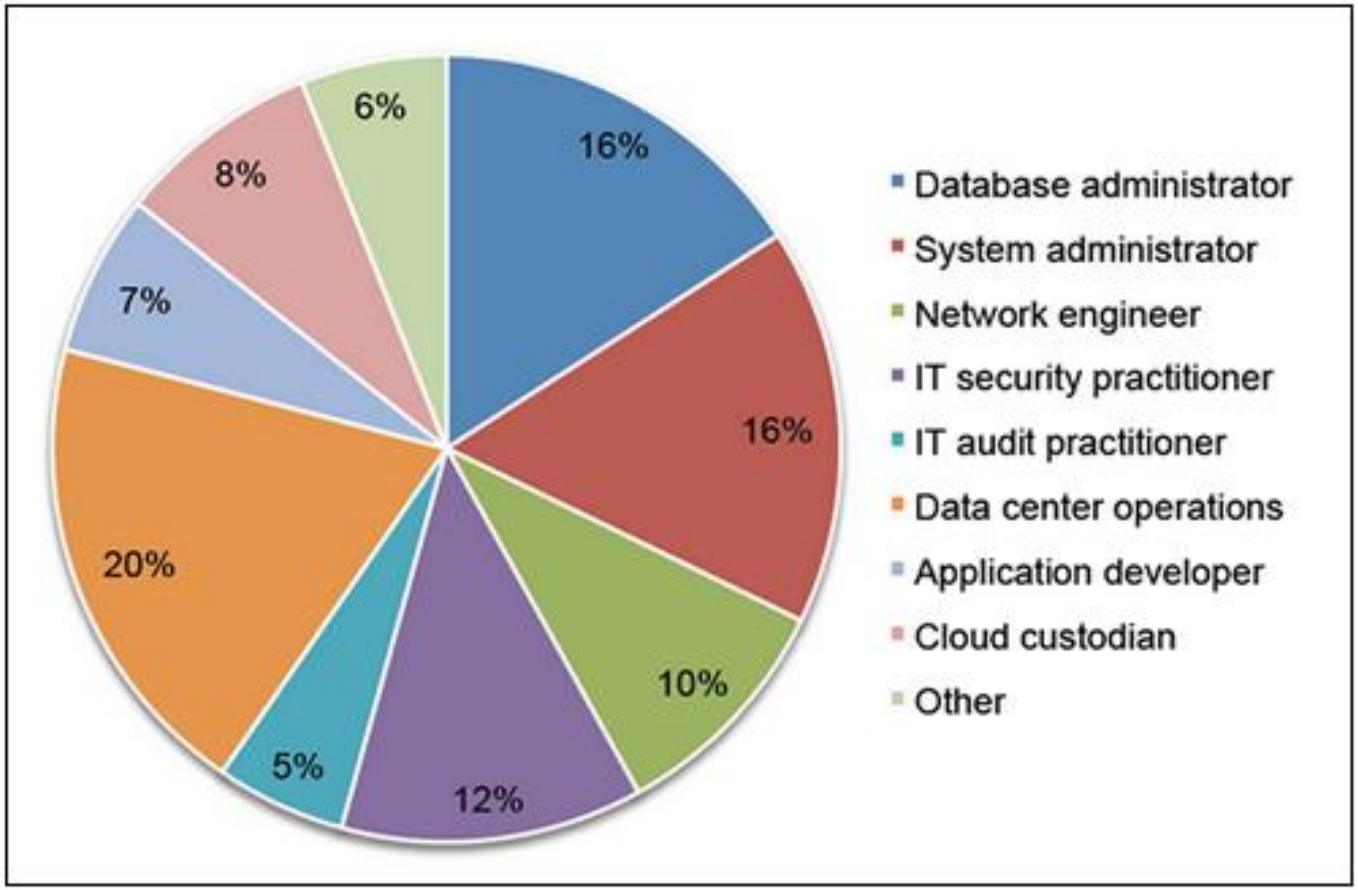
Establishing Some Terms

- **Privileged User**
  - Employees who use data and systems as part of their jobs
  - Executives who have more access than they should
  - Administrators who are the governors of the systems
- **Super User**
  - Account that leverages the ring-0 privilege
  - Examples: root, administrator, SYSTEM
- **Ring-0**
  - The kernel process who has complete access to all resources



http://en.wikipedia.org/wiki/Protection_ring

Who are the Privileged Users?



This chart illustrates the most common positions that require privileged access to sensitive data and networks (Ponemon Institute)

http://www.trustedcs.com/resources/whitepapers/RTN-PrivilegedUserAccessPUMA-RiskMitigationIIS2013-238WP.pdf

What is the issue?

- Superusers control the system, packages, patches, and data permissions
- The nature of the superuser is that they have full access to data accessible by the system.
- If a superuser is compromised or goes rogue, the impact can be severe, as they can destroy, steal, and manipulate.

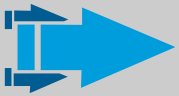
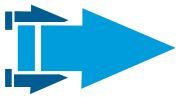
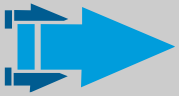
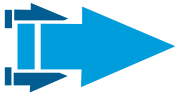
Traditional Controls for Super Users

- **Monitoring**
  - OS Level auditing, keystroke logging, etc…
- **Privileged Account Management**
  - Checkout account with single usage password
- **Policy based elevation**
  - Tools that allow a user to elevate to the superuser on a per command basis. sudo, powerbroker, etc…
  - They are good for saying who can do what as root. But does not control what root can do.

None of these controls stop the superuser…
Just how one becomes the superuser

How This Changes the Landscape

What proactive businesses are doing

Protect the least amount of data, mandated by compliance/audit		**Encrypt everywhere…**
Least amount of control mandated by compliance		**Importance of access controls and security intelligence**
Point Products with little to no enterprise strategy		**Solutions on an enterprise and cloud scale**
Operational Impact not forefront because scope was limited		**Broad-based deployment puts operational impact in forefront**

Widening Adoption of Encryption
to Defend Sensitive Business Data

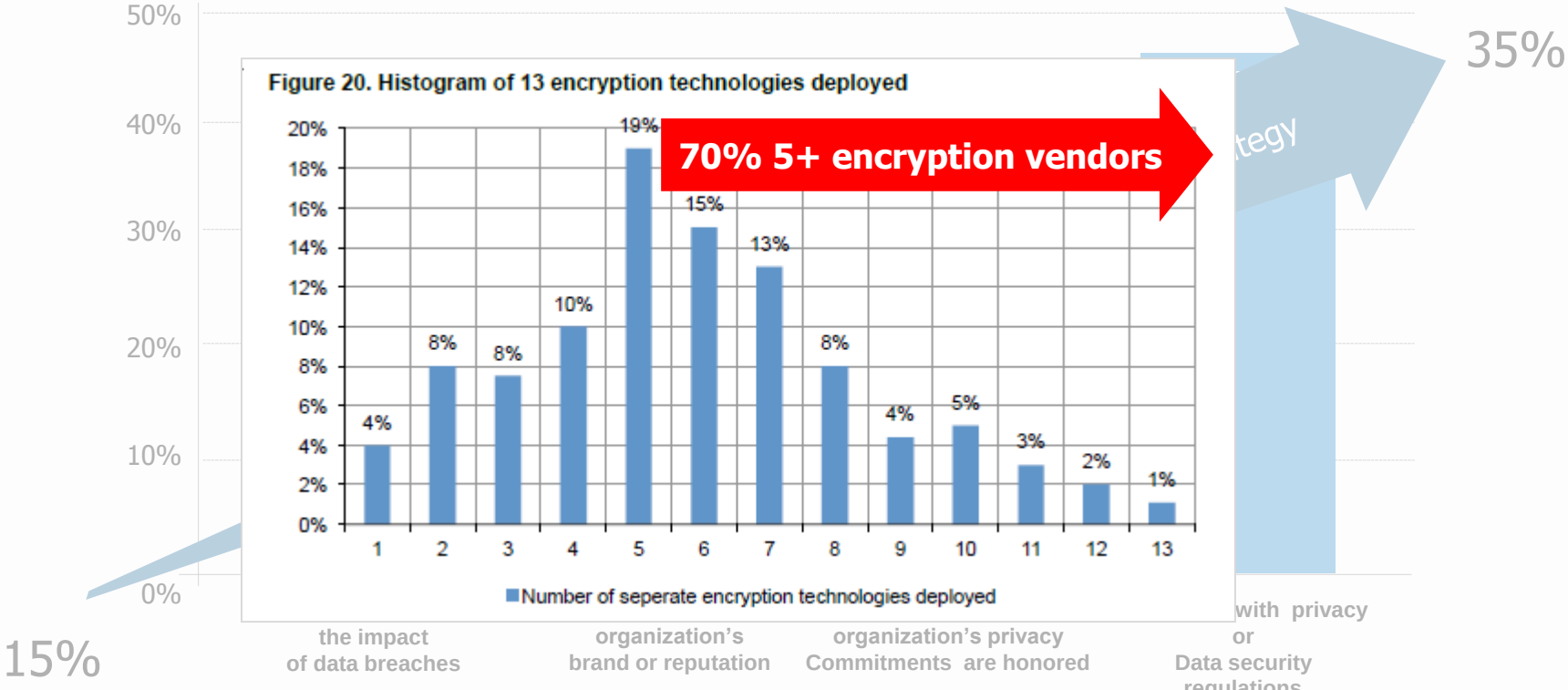


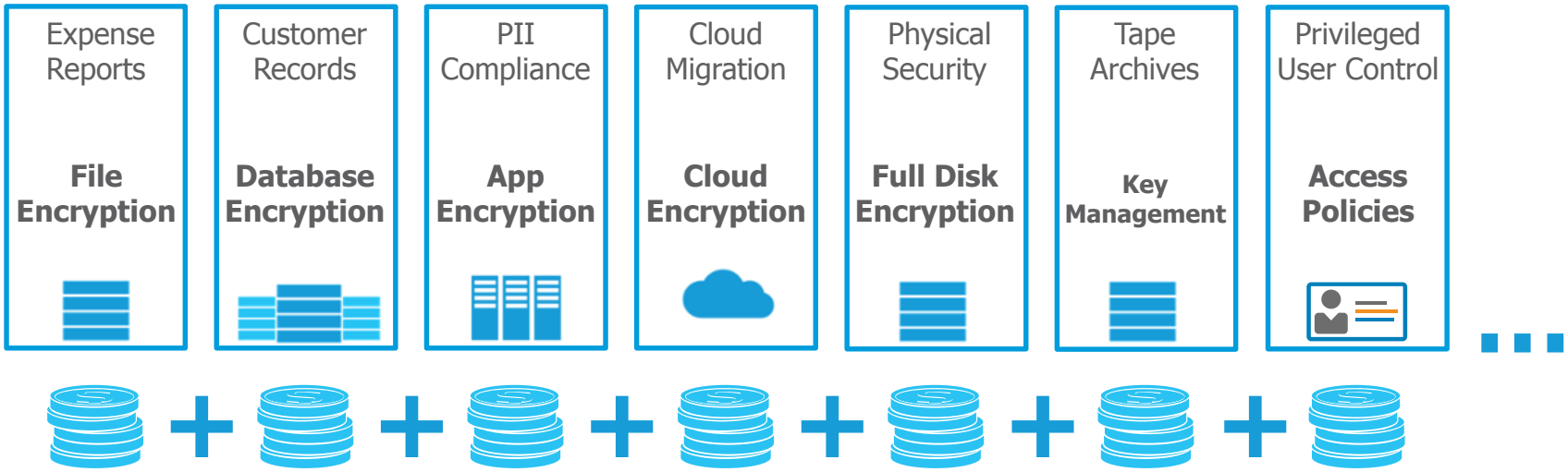
Figure 15. The main drivers for using encryption technology solutions

Ponemon INSTITUTE

Feb 2014

Data-at-Rest Security Survival Tactics

A disjointed, expensive collection of point products



Each use case requires individual infrastructure, management consoles and training.

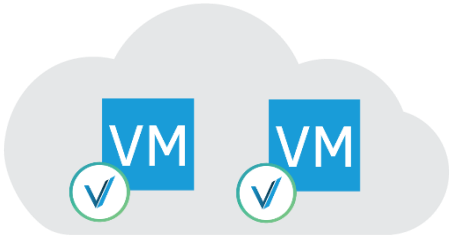
Complex – Inefficient - Expensive

One Platform – One Strategy

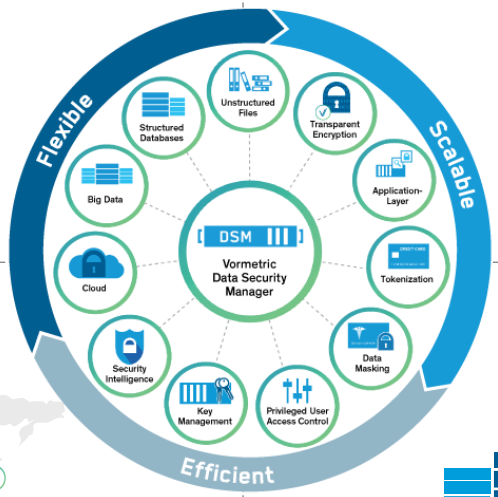
Data-at-rest security that follows your data

- Physical
- Virtual
- Outsourced

Enterprise Data Centers



Private, Public, Hybrid Clouds
SaaS, PaaS, IaaS



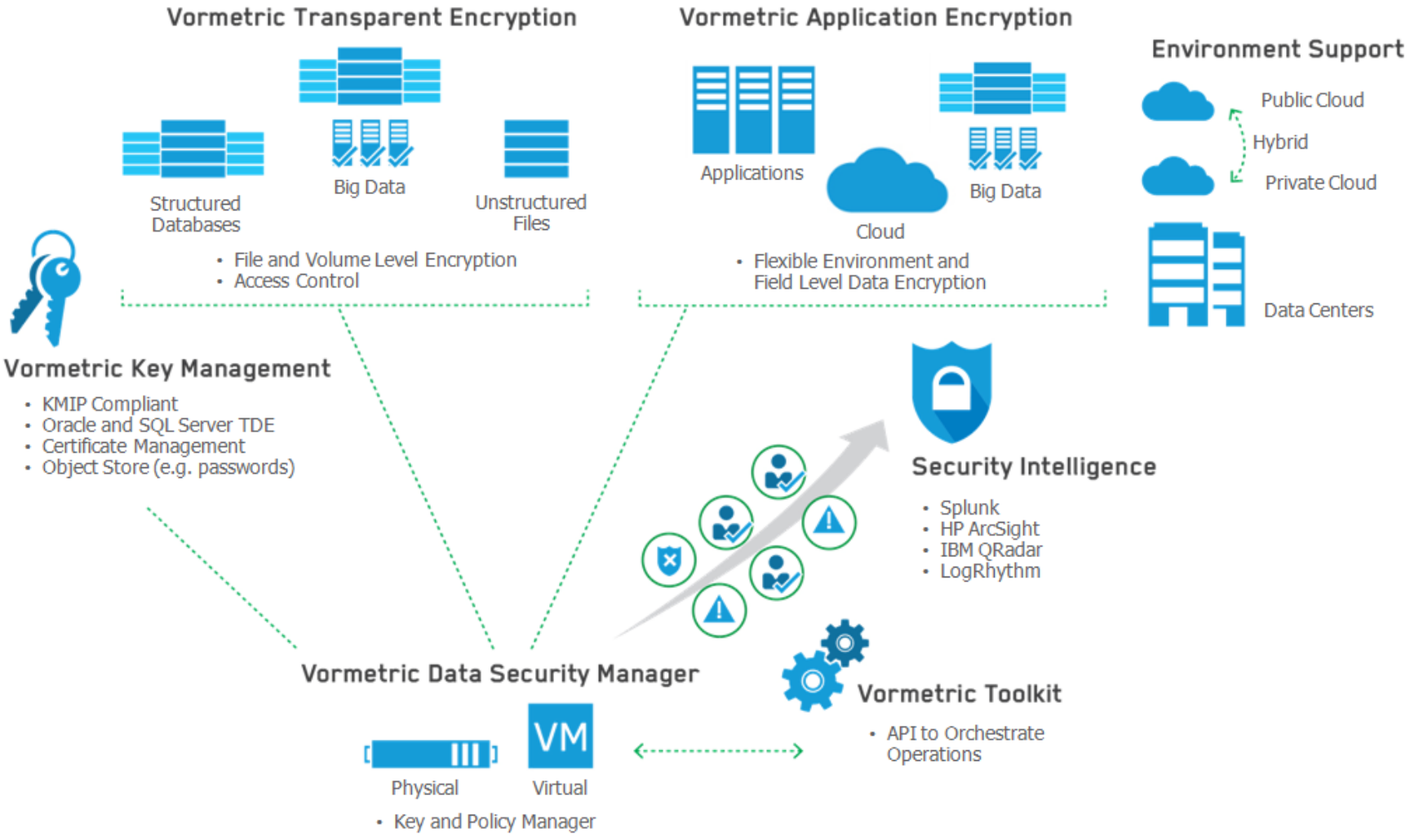
Remote Servers

- Sources
- Nodes
- Analytics

Big Data

Vormetric Data Security Platform

Single Platform



Transparent Encryption

- **Reasons:**
  - "I can't change this application/architecture."
  - "I need to be compliant ASAP."
  - "Privileged Users(System and Below) are a risk to my data."
- **Typical Use Cases**
  - Databases
  - Applications
  - Big Data
  - Unstructured Data

Application Encryption

- **Reasons**
  - "I need to blind the DBA"
  - "I need to encrypt/tokenise a limited number of objects"
  - "My developers are encrypting, but need to move the key out of the application"
- **Typical Use Cases**
  - Custom Applications
  - Tokenisation
  - Partnered ISVs – i.e. Mongo, Teradata

Key Management

- **Reasons**
  - "We have TDE already deployed, but are struggling with Key Management"
  - "My Storage provider has SED, yet I need centralised Key Management"
- **Typical Use Cases**
  - Oracle/MSSQL TDE
  - NAS with Self Encrypting Drives
  - KMIP Clients

Tokenization + Dynamic Data Masking

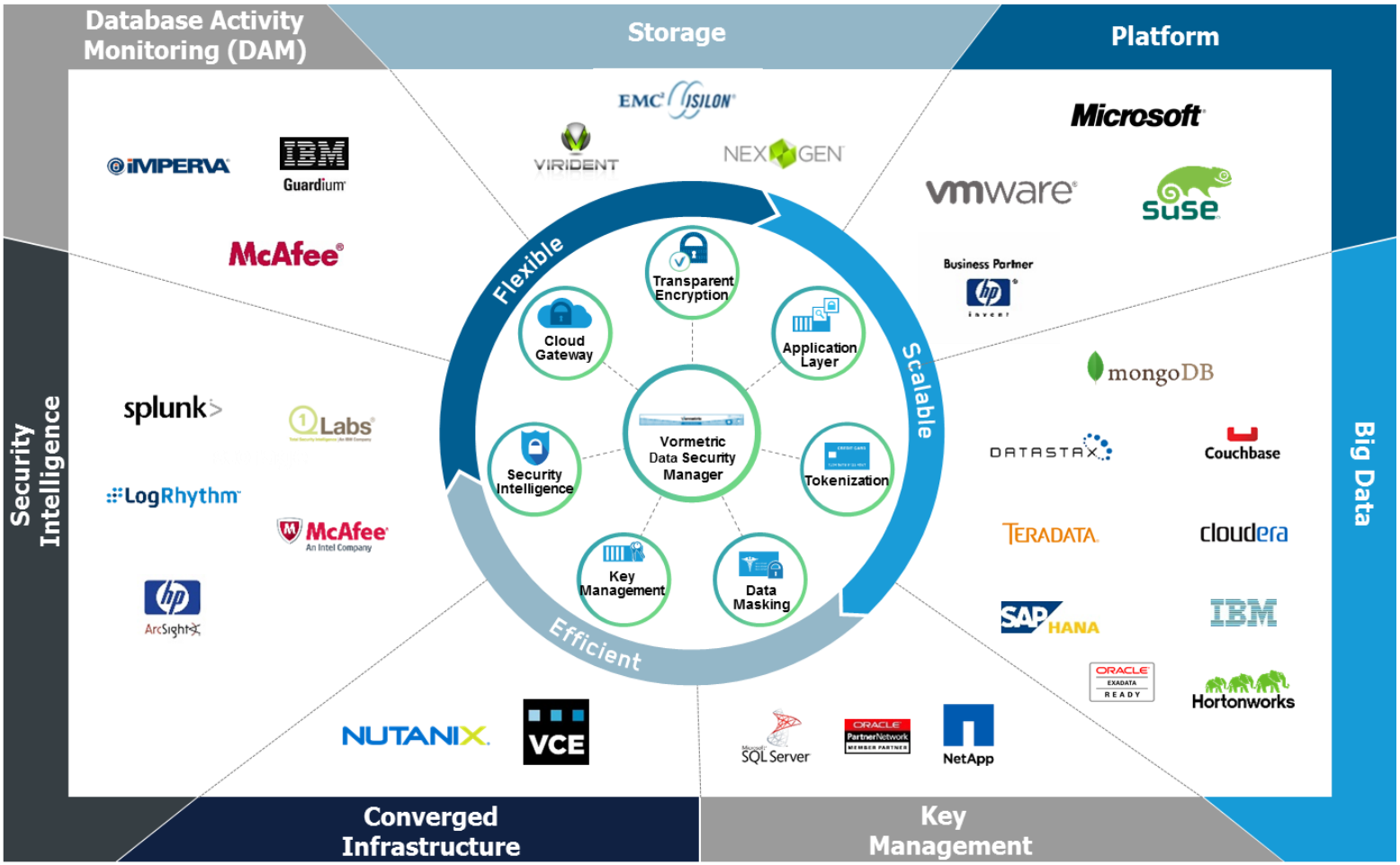
- **Reasons**
  - "PCI Scope reduction, please…"
  - "I need to redact, or replace the real data with compatible data."
  - "Anonymize data for Data Analytics"
- **Typical Use Cases**
  - CC Transaction Workflows
  - Big Data
  - Dynamic data view altering

Encryption as a Service

- **Larger Enterprises and Service Providers**
  - Standardizing on Encryption
  - They provide a menu to their "customers"
    - Transparent Encryption – "Encrypt with no change"
    - Application Encryption – "Design Crypto in"
    - Key Management – "Bring your own Crypto"
  - Centralize Encryption and Key Management Service
  - Benefits realized:
    - Less overall Cost
    - Standard Answers to the "how to encrypt" question

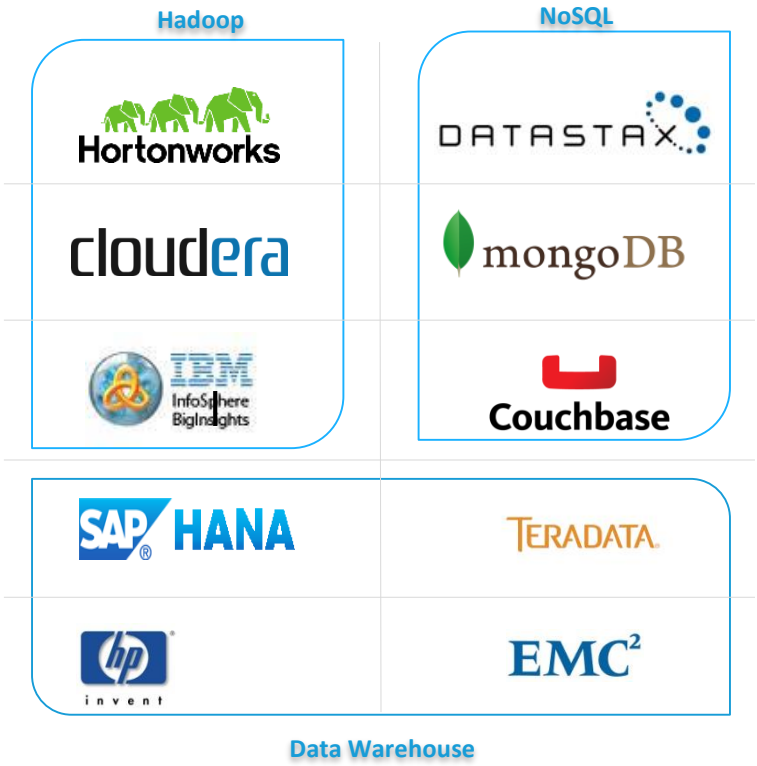
Partnerships and Certifications

Assures high performance and confidence



Follow The Big Data Adoption

World-Class Vendors Rely on Vormetric



"Vormetric gives our customers best in class security controls needed for compliance, data breach protection and for safeguarding critical intellectual property through powerful data-at-rest encryption."

Rod Hamlin
Vice President
Couchbase

Data Security as a Service Offerings

Vormetric Cloud Partners

CenturyLink™ | rackspace

QTS | Microsoft Azure

firehost SECURE CLOUD HOSTING | Google Cloud Platform

CloudHesive securing your enterprise in the cloud | IBM Cloud Managed Services

D+H | Pega Pegasystems Inc.

virtustream | amazon web services Partner Network

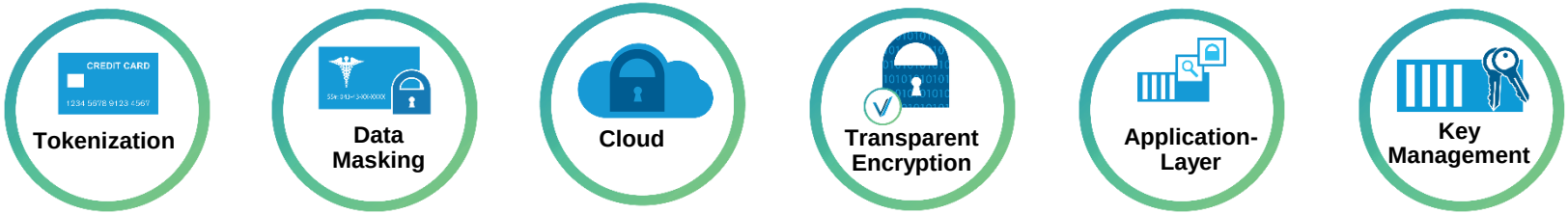
GNAX GLOBAL NET ACCESS | CIRRITY

> **"With Vormetric, we've added new capabilities to extend data security practices to our customer implementations across our managed cloud platform."**
>
> **John Engates**
> **CTO**
> rackspace

Vormetric Data Security Platform

Enterprise and cloud-scale data-at-rest security strategy

- **Flexible**
  - Enterprise-wide protection and compliance
  - History of delivering new use cases enabling secure innovation
- **Scalable**
  - Multi-operating systems across all server environments
  - Global scale with centralized control
- **Efficient**
  - High-performance, minimizes system resources
  - Operational simplicity through consistent deployment
- **Single Platform = Lower TCO**



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.*"