New York Oracle Users Group, Inc.

Data-Centric Security Key to Cloud and Digital Business

Ulf Mattsson, CTO
Compliance Engineering
umattsson@complianceengineers.com

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Ulf Mattsson, CTO Compliance Engineering

- Cloud Security Alliance (CSA)
- PCI Security Standards Council
  - Cloud & Virtualization SIGs
  - Encryption Task Force
  - Tokenization Task Force
- IFIP
  - WG 11.3 Data and Application Security
  - International Federation for Information Processing
- ANSI X9
- ISSA & ISACA

Agenda

- Exponential growth of data generation
  - New business models fueled by Big Data, cloud computing and the Internet of Things
  - Creating cybercriminal's paradise
- Challenge in this interconnected world
  - Merging data security with data value and productivity.
- Urgently need a data-centric strategy
  - Protect the sensitive data flowing through digital business systems
- Solutions to bring together data insight & security
  - Safely unlock the power of digital business

Are you ready for a big change revolution?

Source: www.firstpost.com

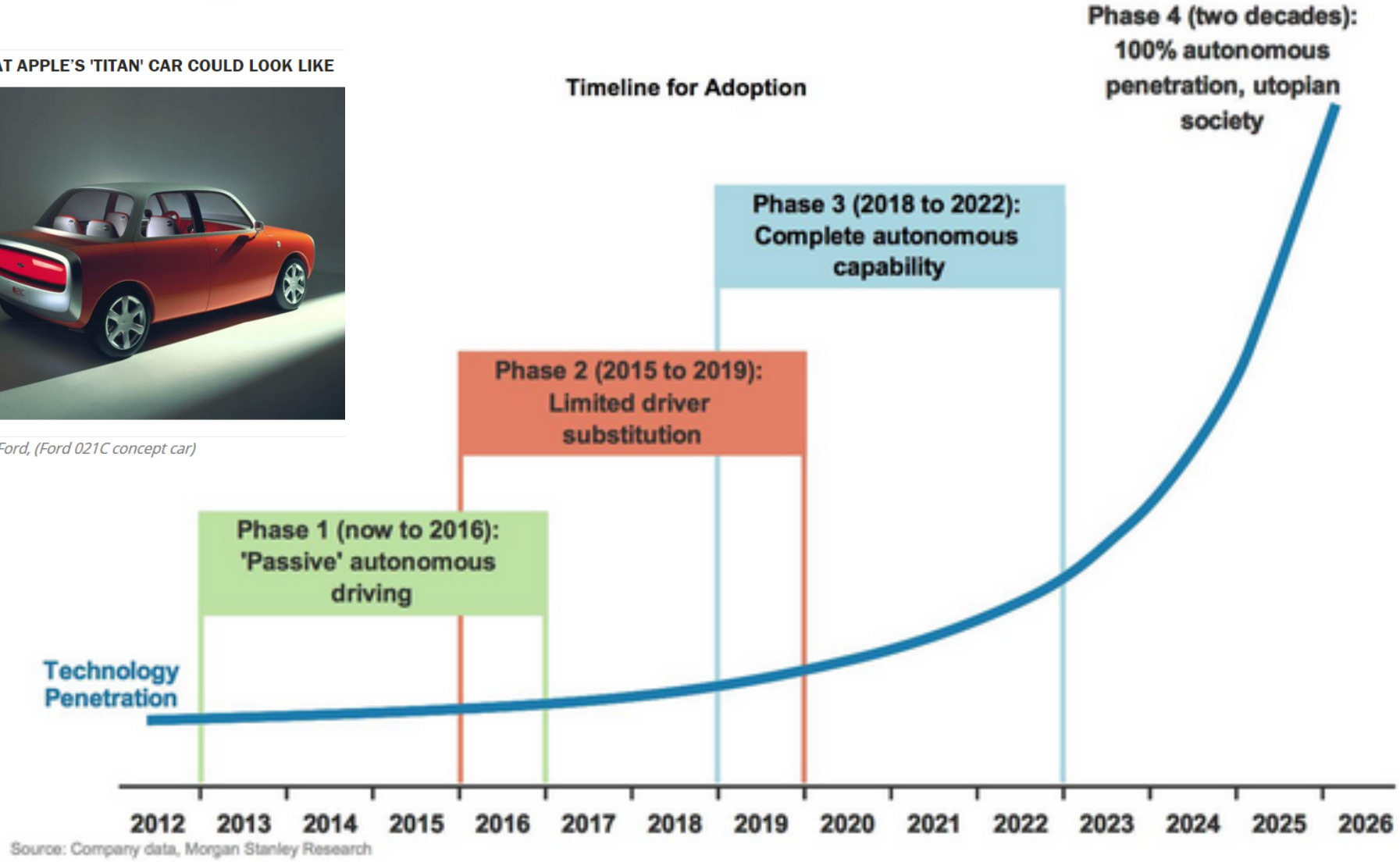
A Changing Landscape 2018 - 2020

- By 2018, digital business will require 50% fewer business process workers and 500% more key digital business jobs, compared with traditional models
- By 2018, the total cost of ownership for business operations will be reduced by 30% through smart machines and industrialized services
- By 2020, developed world life expectancy will increase by a half-year due to the widespread adoption of wireless health monitoring technology

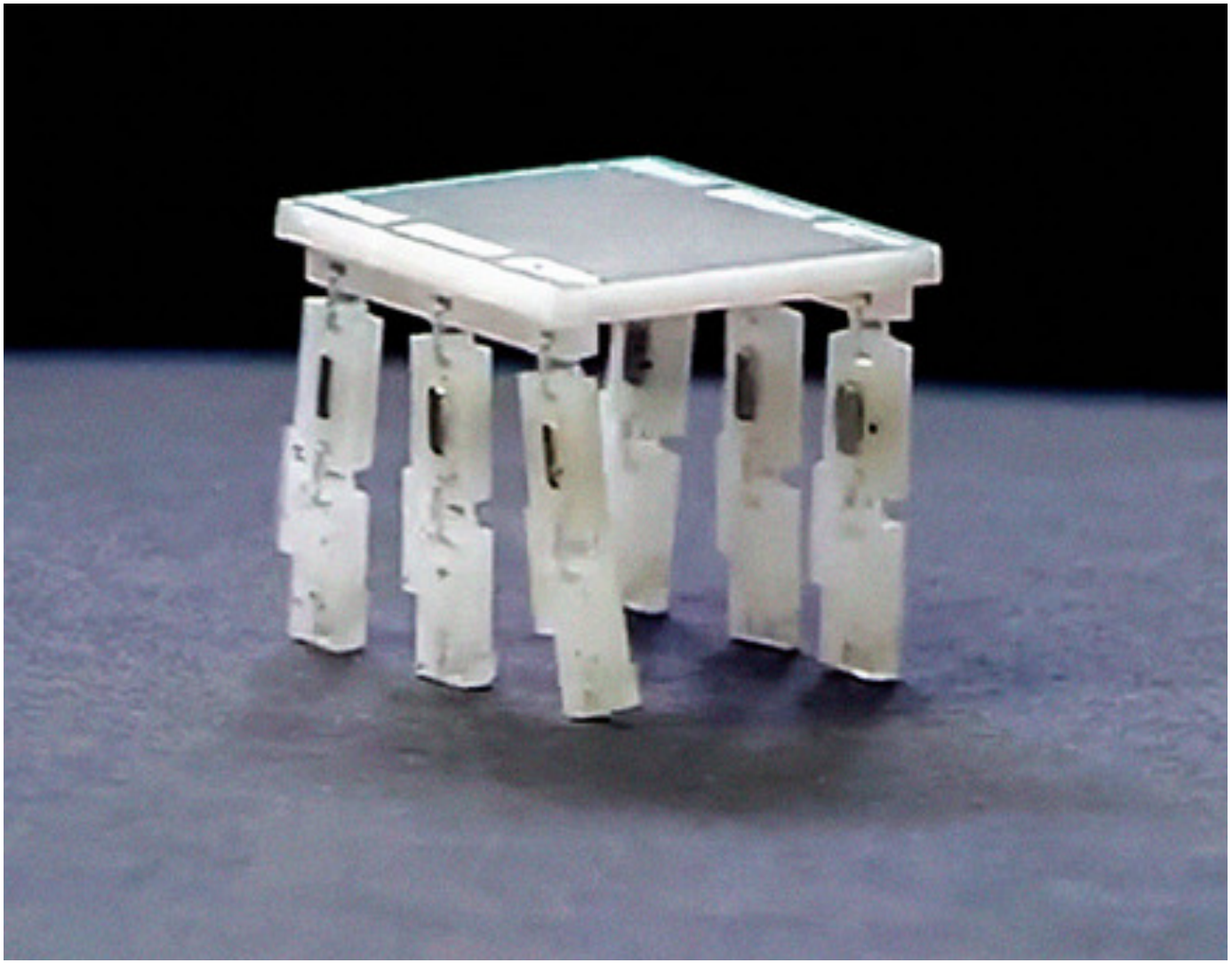
Source: Gartner – Top 10 Strategic Predictions for 2015 and Beyond: Digital Business Is Driving 'Big Change', Oct 2014

Self Driving Cars: Are We at the Cusp of a Revolutionary Change?

Image Source: Ford, (Ford 021C concept car)



Micro-robots, the size of a grain of rice

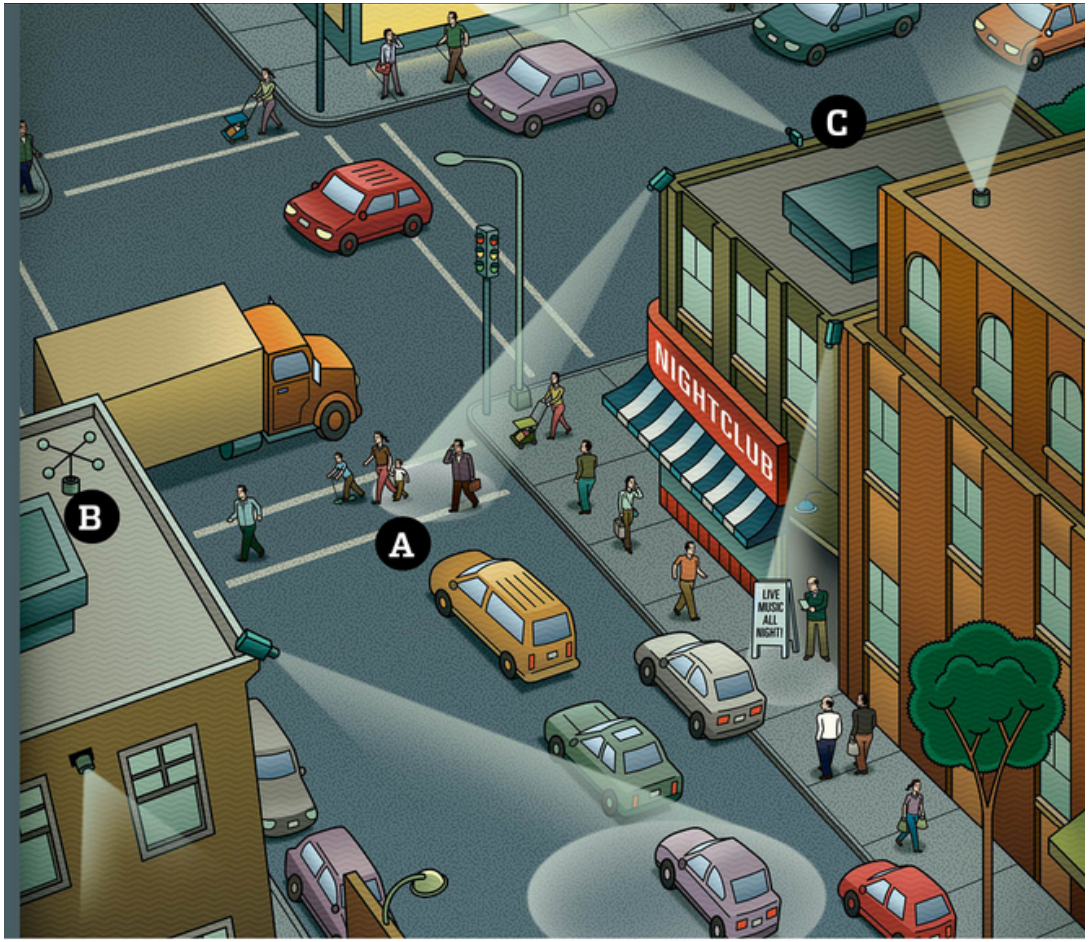


Source: www.ted.com/talks/sarah_bergbreiter

AVATAR - The Internet Of Things?

Source: thesocietypages.org/socimages/2009/12/28/on-avatar-the-movie-spoiler-alert/

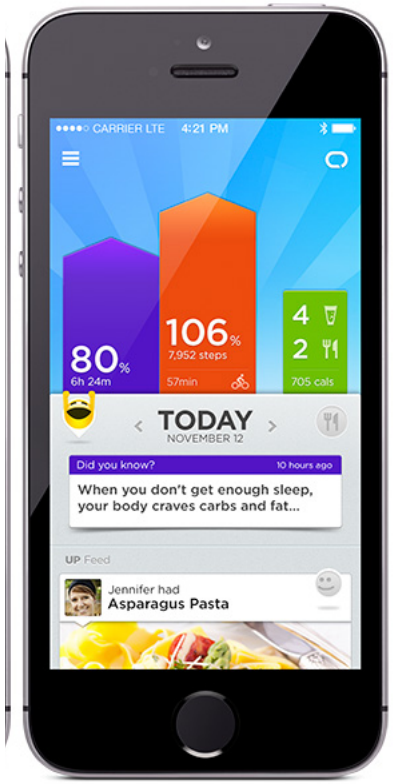
They're Tracking When You Turn Off the Lights



Sensors to capture data on environmental conditions including sound volume, wind and carbon-dioxide levels, as well as behavioral data such as pedestrian traffic flow

Source: Wall Street Journal

Jawbone Tracks Your Sleep Patterns



Source: Bogard, "the Internet of me."

Samsung engineers are working on wearable for early stroke detection

Source: Early Detection Sensor and Algorithm Package (EDSAP)

FTC Wants a Trusted, Secure Internet of Things

The Federal Trade Commission (FTC) Looking At Apple HealthKit

Source: www.cio-today.com

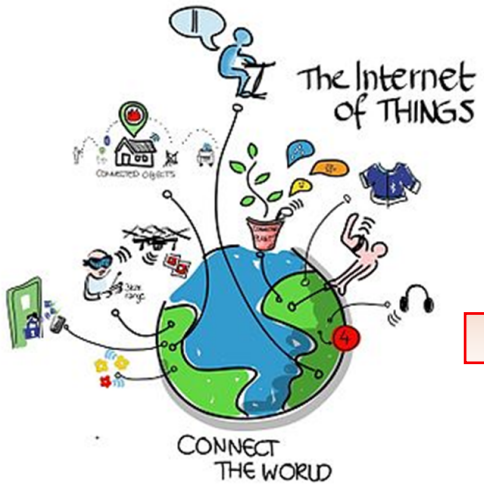
Security Threats of Connected Medical Devices

- The Department of Homeland Security
  - Investigating 2 dozen cases of suspected cyber security flaws in medical devices that could be exploited
  - Can be detrimental to the patient, creating problems such as instructing an infusion pump to overdose a patient with drugs or forcing a heart implant to deliver a deadly jolt of electricity
  - Encrypt medical data that's stored
- PricewaterhouseCoopers study
  - $30billion annual cost hit to the U.S. healthcare system due to inadequate medical-device interoperability

www.computing.co.uk/ctg/opinion/2390029/security-threats-of-connected-medical-devices#

IoT is a Paradise for Hackers

- Almost 90 percent of the devices collect personal information such as name, address, date of birth, email, credit card number, etc.
- Un-encrypted format on to the cloud and big data, thus endangering the privacy of users



Source: wikipedia.org

Source: HP Security Research

90% of world's data generated over last two years

- 26 billion devices on the Internet of Things by 2020 (Gartner)
- 15 Billion existing devices connected to the internet (Intel)
- Not adequately protected at the device level
  - Cannot wait for a new generation of secure devices to be developed
- Require robust and layered security controls

In 2015, ecosystems will transform fragmented wearables market

(Source: Validic)

Cloud Security

95% of cloud security failures will be the customer's fault

Gartner®

Source: Gartner

Sensitive Data in the Cloud

Ponemon INSTITUTE

82%

Of organizations currently (or plan to) transfer sensitive/confidential data to the cloud in next 24 mo.

Compliance Engineering
Security & Compliance Solutions

Lack of Cloud Confidence

Ponemon INSTITUTE

2/3

Number of survey respondents that either agree or are unsure that cloud services used by their organization are NOT thoroughly vetted for security

Compliance Engineering
Security & Compliance Solutions

Data Breach: Cloud Multiplier Effect

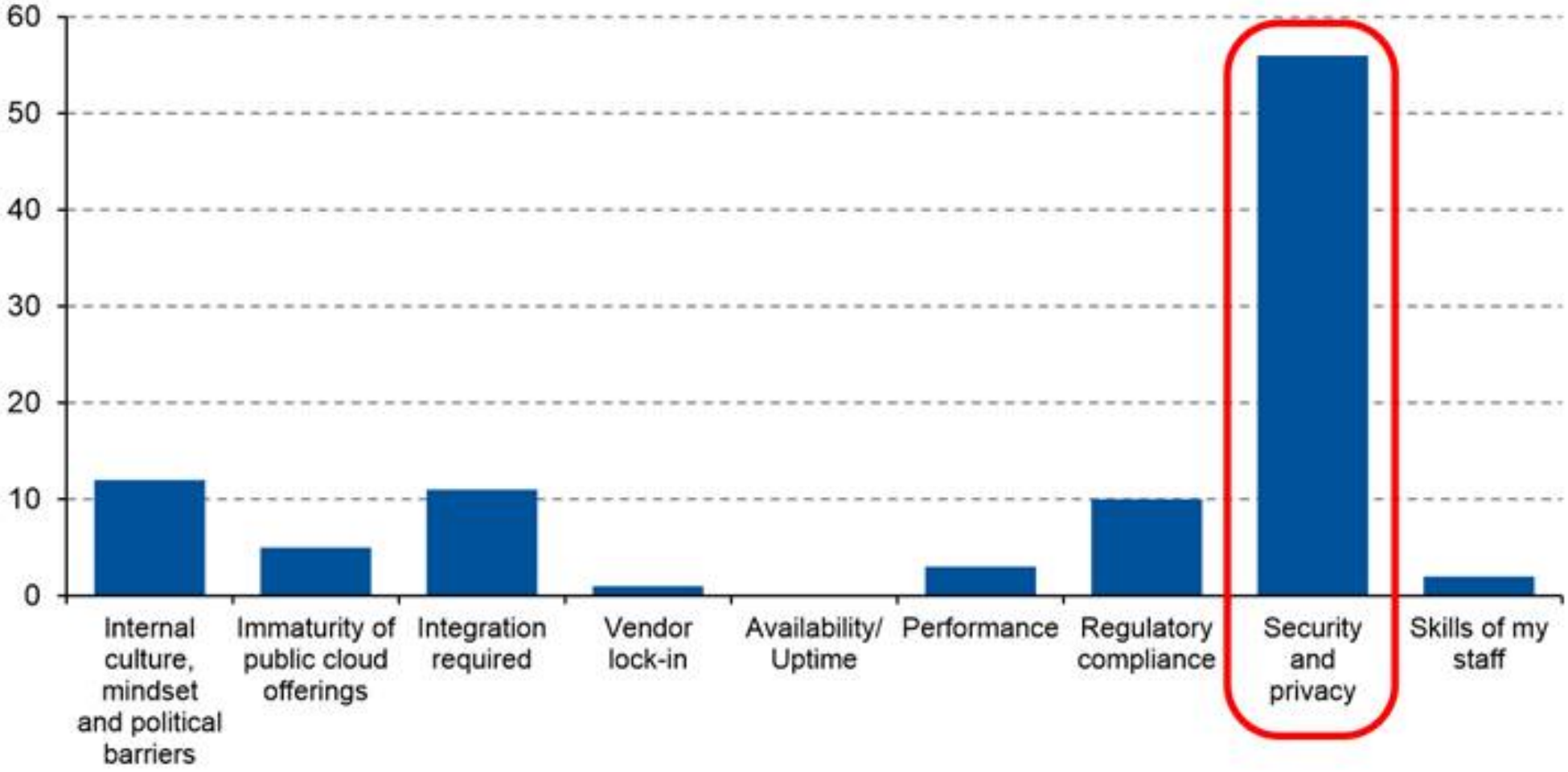
Ponemon INSTITUTE

2x

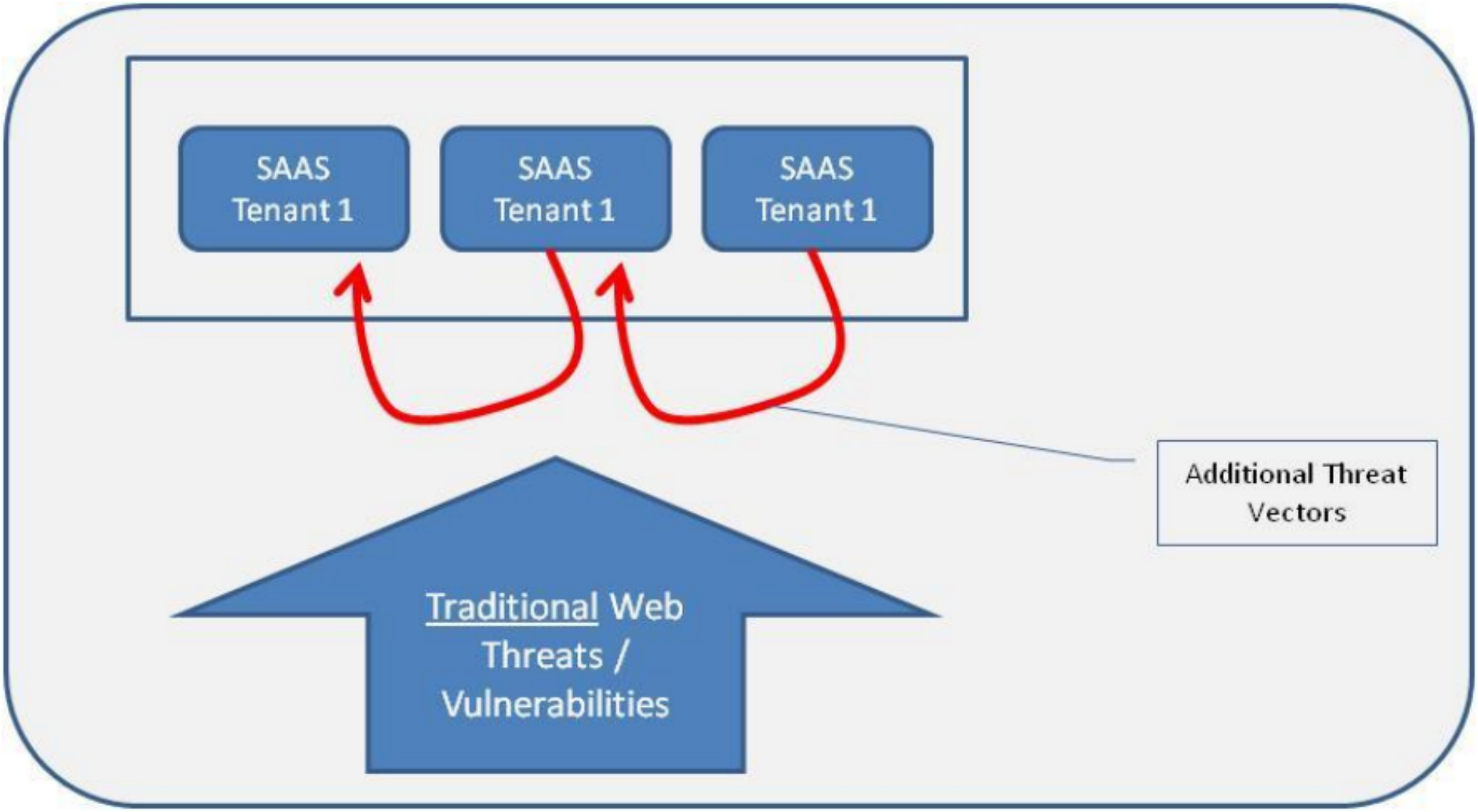
A data breach in the cloud can be 2x more costly. 66 percent of respondents say their organization's use of cloud resources diminishes its ability to protect confidential or sensitive information and 64 percent believe it makes it difficult to secure business-critical applications

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

What Is Your No. 1 Issue Slowing Adoption of Public Cloud Computing?



Threat Vector Inheritance



Data Security Holding Back Cloud Projects

38%
Loss of control over IT services.

28%
Concern over business continuity and disaster recovery.

73%
Concern about security of data.

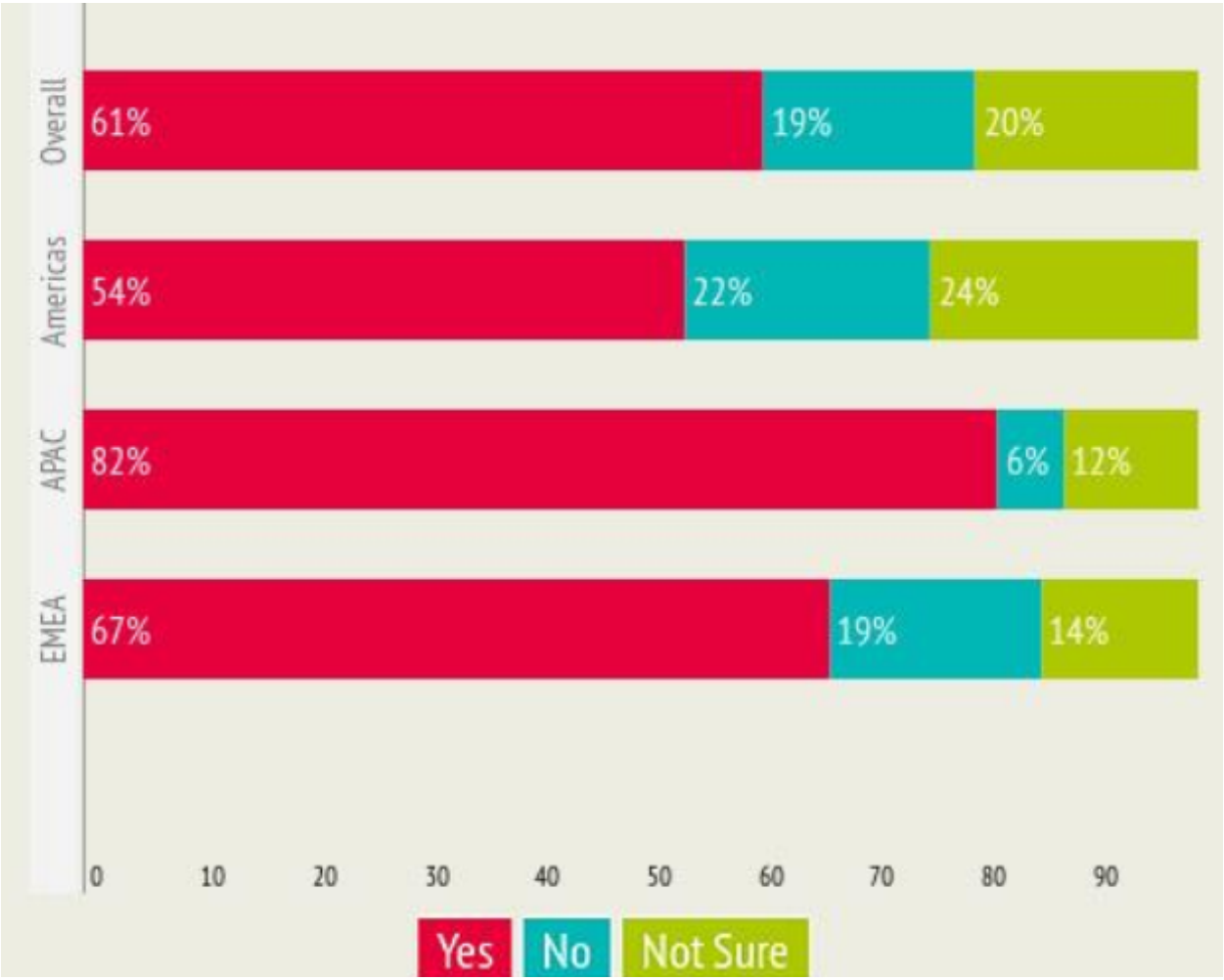
38%
Concern about regulatory compliance.

34%
Knowledge and experiences of both IT and business managers.

30%
Concern over compromised accounts and or insider threats.

Source: Cloud Adoption Practices & Priorities Survey Report January 2015

Security of Data in Cloud at Board-level



Source: Cloud Adoption Practices & Priorities Survey Report January 2015

High-profile Cyber Attacks

Ponemon INSTITUTE

49% recommended Database security

40% of budget still on Network security only

19% to Database security

Conclusion: Organizations have traditionally spent money on network security and so it is earmarked in the budget and requires no further justification

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

CHALLENGE

How can we Secure Data in the new Perimeter-less Environments?

SOLUTION

Fine Grained Data Security

Gartner®

Data–Centric Audit and Protection (DCAP)

Organizations that have not developed data-centric security policies to coordinate management processes and security controls across data silos need to act

By 2018, data-centric audit and protection strategies will replace disparate siloed data security governance approaches in 25% of large enterprises, up from less than 5% today

Gartner®

Source: Gartner – Market Guide for Data – Centric Audit and Protection (DCAP), Nov 21 2014

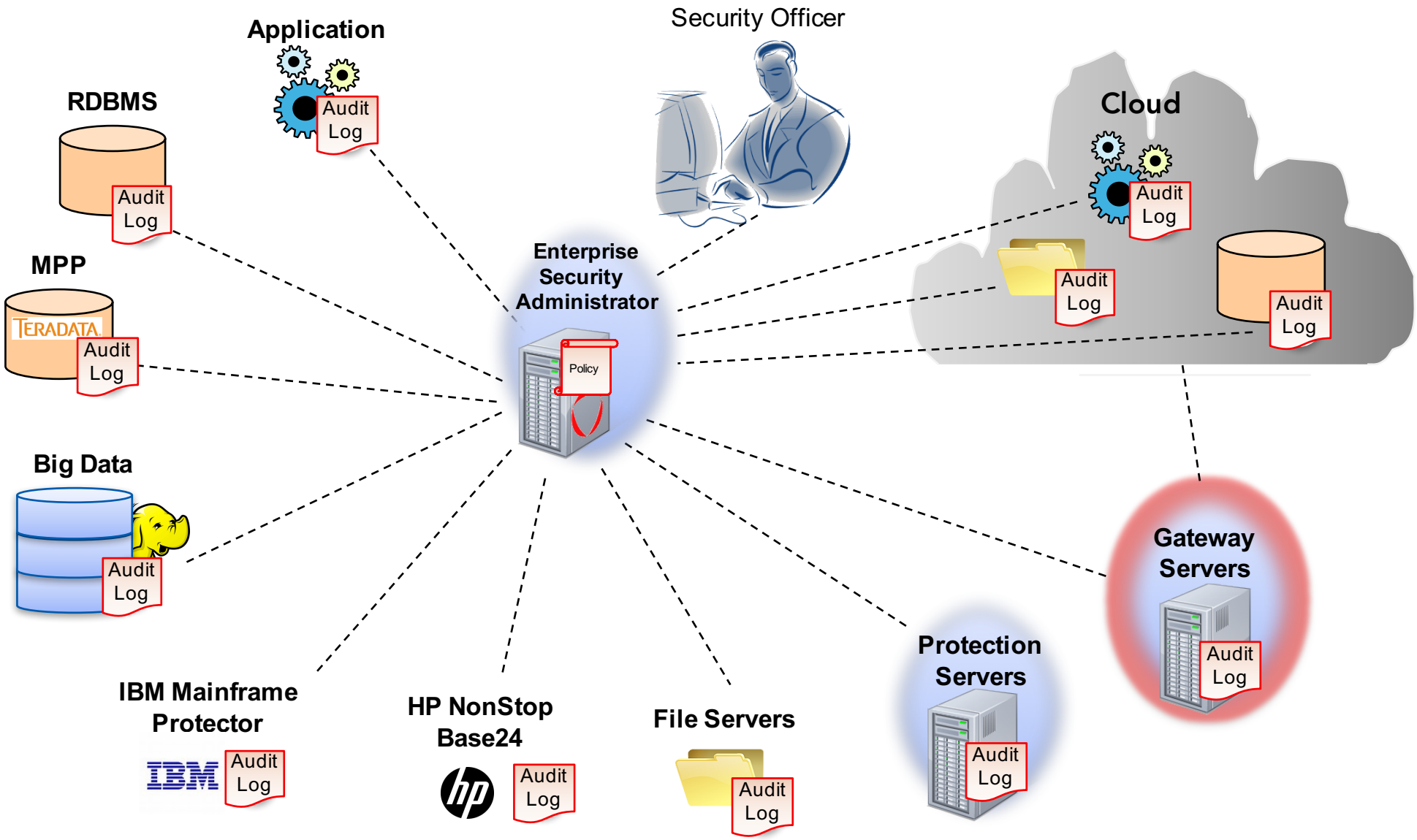
Data–Centric Audit and Protection (DCAP)

- Centrally managed security policy
- Across unstructured and structured silos
- Classify data, control access and monitoring
- Protection – encryption, tokenization and masking
- Segregation of duties – application users and privileged users
- Auditing and reporting

Gartner®

Source: Gartner – Market Guide for Data – Centric Audit and Protection (DCAP), Nov 21 2014

Centralized Policy Management - Example



Enterprise Data Security Policy

What — What is the sensitive data that needs to be protected.

How — How you want to protect and present sensitive data. There are several methods for protecting sensitive data.

Who — Who should have access to sensitive data and who should not. Security access control.

When — When should sensitive data access be granted to those who have access. Day of week, time of day.

Where — Where is the sensitive data stored? This will be where the policy is enforced.

Audit — Audit authorized or un-authorized access to sensitive data.

Securing Cloud Data

Data-Centric Protection Increases Security in Cloud Computing

- **Rather than making the protection platform based, the security is applied directly to the data**
- **Protecting the data wherever it goes, in any environment**
- Cloud environments by nature have more access points and cannot be disconnected
- Data-centric protection reduces the reliance on controlling the high number of access points

Clouds Are Secure: Are You Using Them Securely?

- Through 2020, **95% of cloud security failures will be the customer's fault.**

- By year-end 2018, 50% of organizations with more than 2,500 users will use a cloud access security broker (CASB) product to control SaaS usage, up from less than 5% today.

- By 2020, **85% of large enterprises will use a CASB** product, up from less than 5% today.

Gartner®

Source: Gartner

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

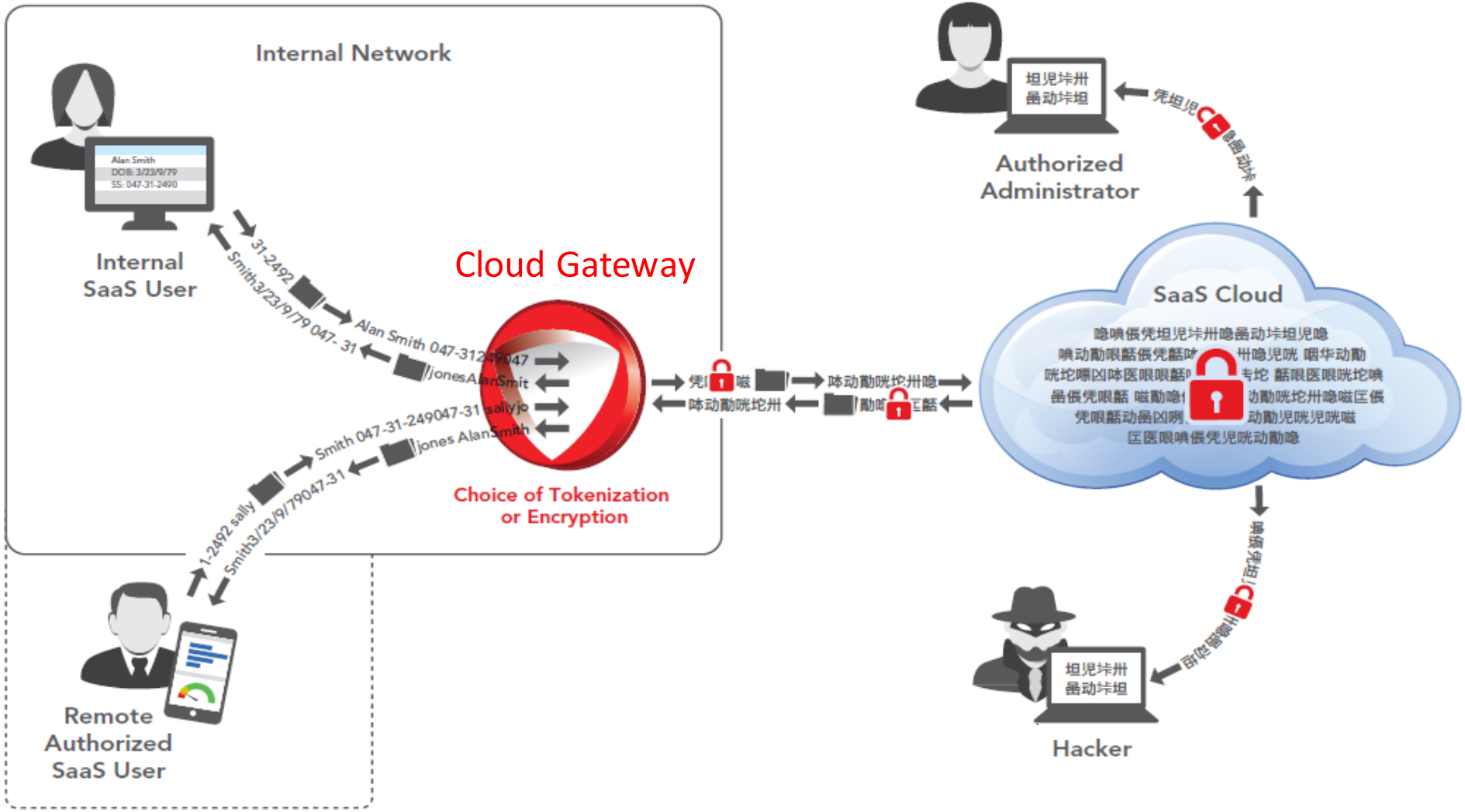
Cloud Security

- Gartner released the report "Simplify Operations and Compliance in the Cloud by Protecting Sensitive Data" in June 2015 that highlighted key challenges as "cloud increases the risks of noncompliance through unapproved access and data breach."
- The report recommended CIOs and CISOs to address data residency and compliance issues by "applying encryption or tokenization," and to also "understand when data appears in clear text, where keys are made available and stored, and who has access to the keys."
- Another recent Gartner report concluded that "Cloud Data Protection Gateways" provides a "High Benefit Rating" and "offer a way to secure sensitive enterprise data and files."

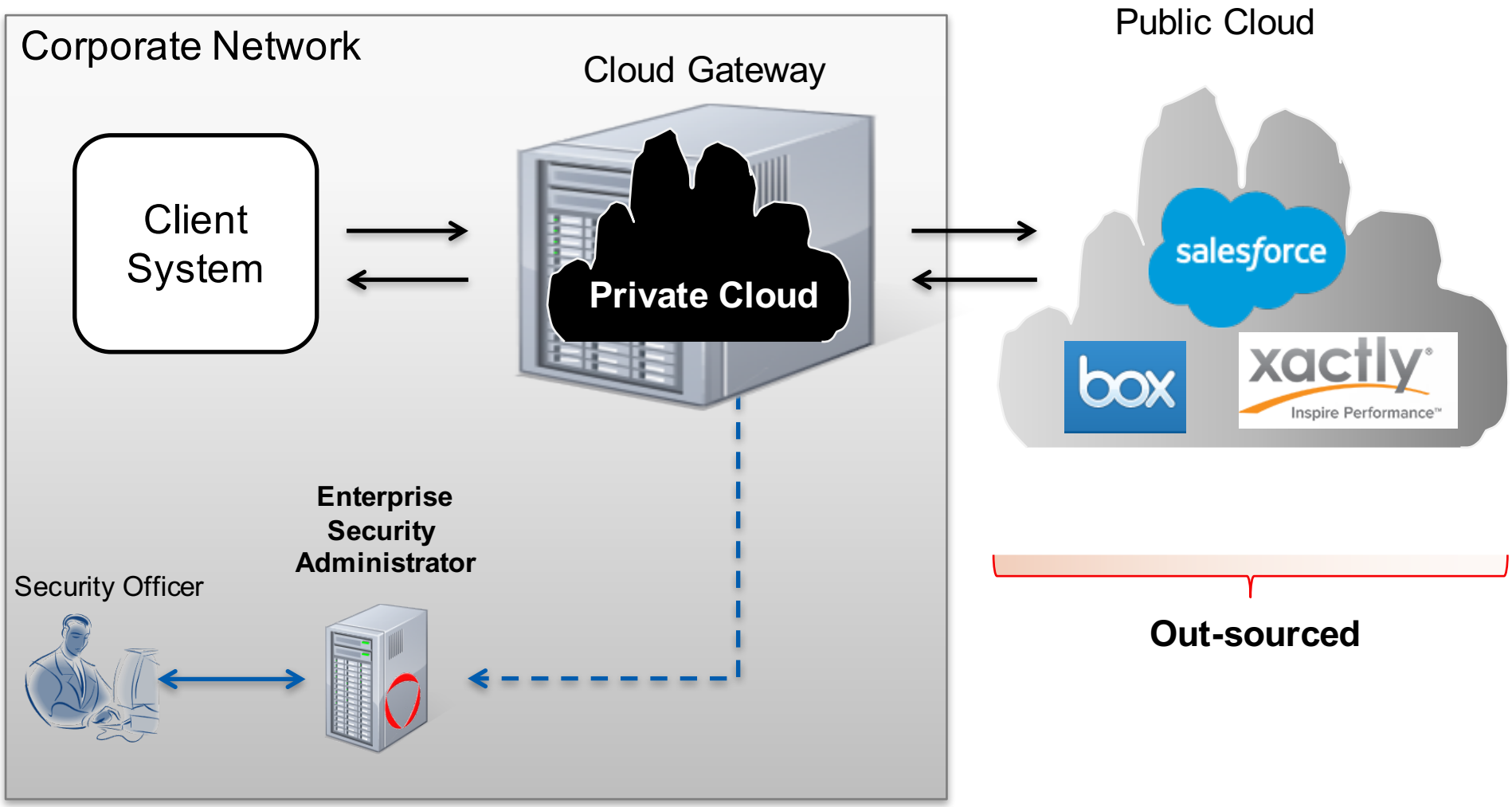
Gartner®

Source: Gartner – xxxx

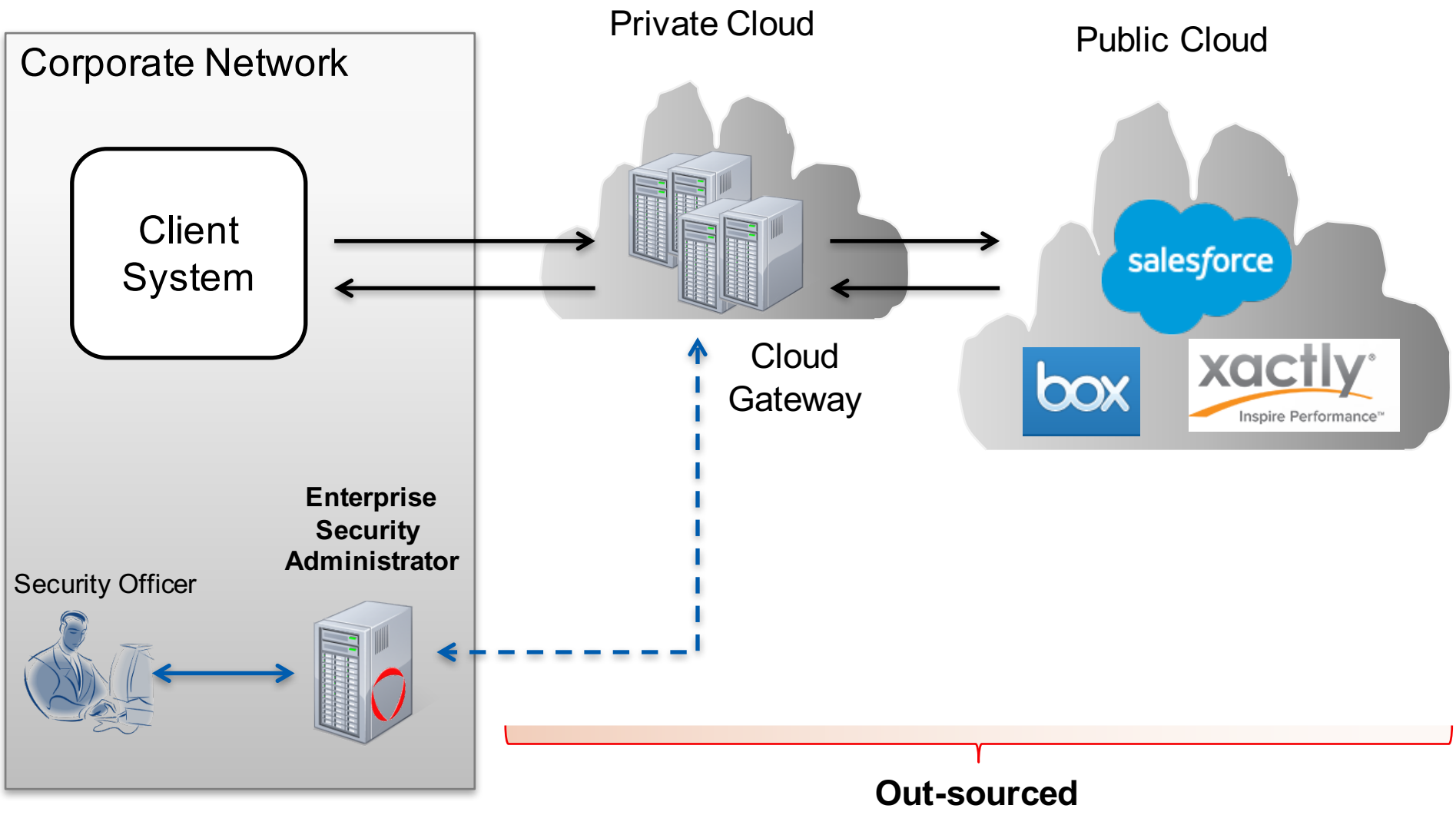
Protect the Entire Flow of Sensitive Data



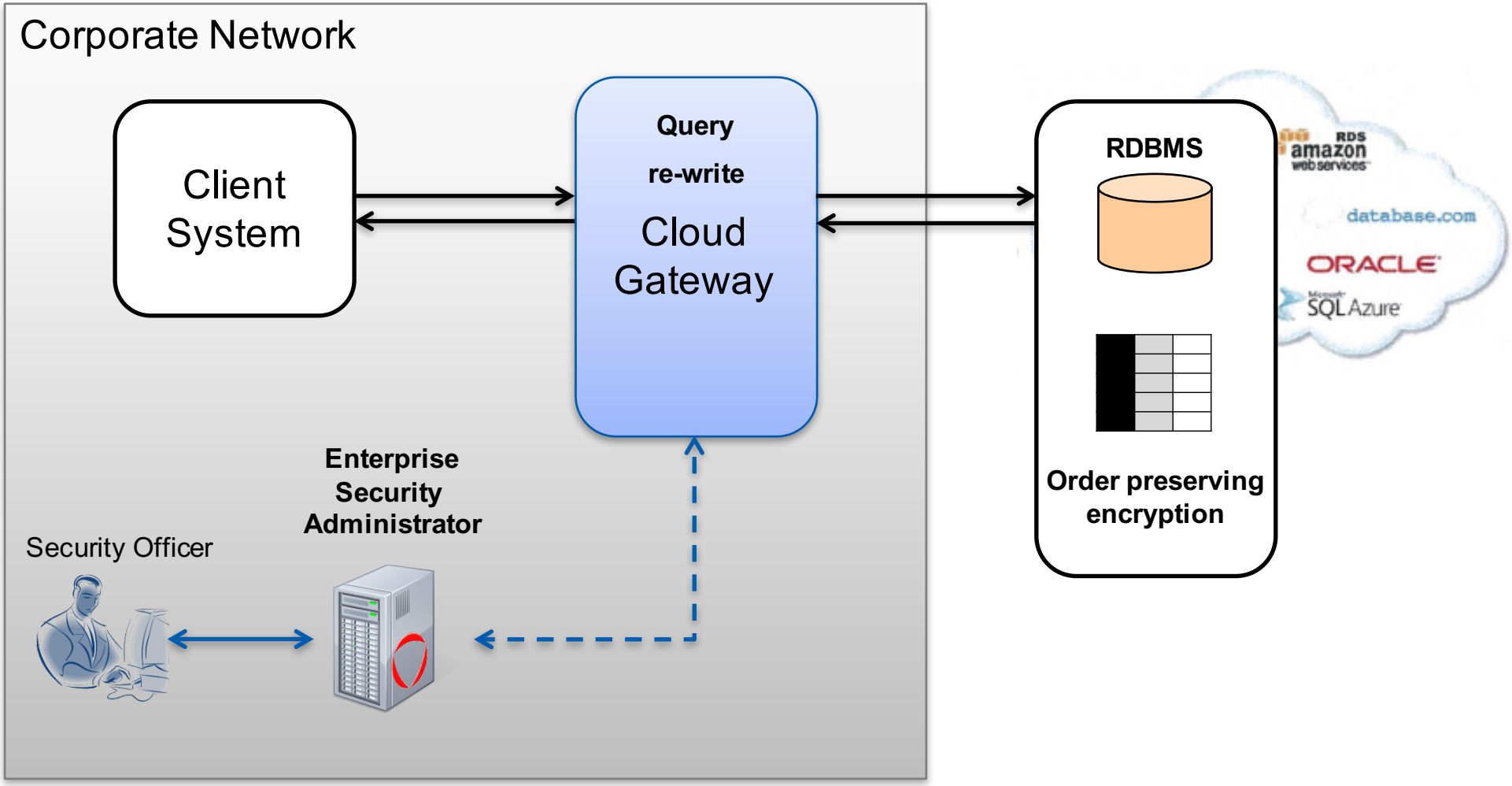
Security Gateway Deployment – Hybrid Cloud



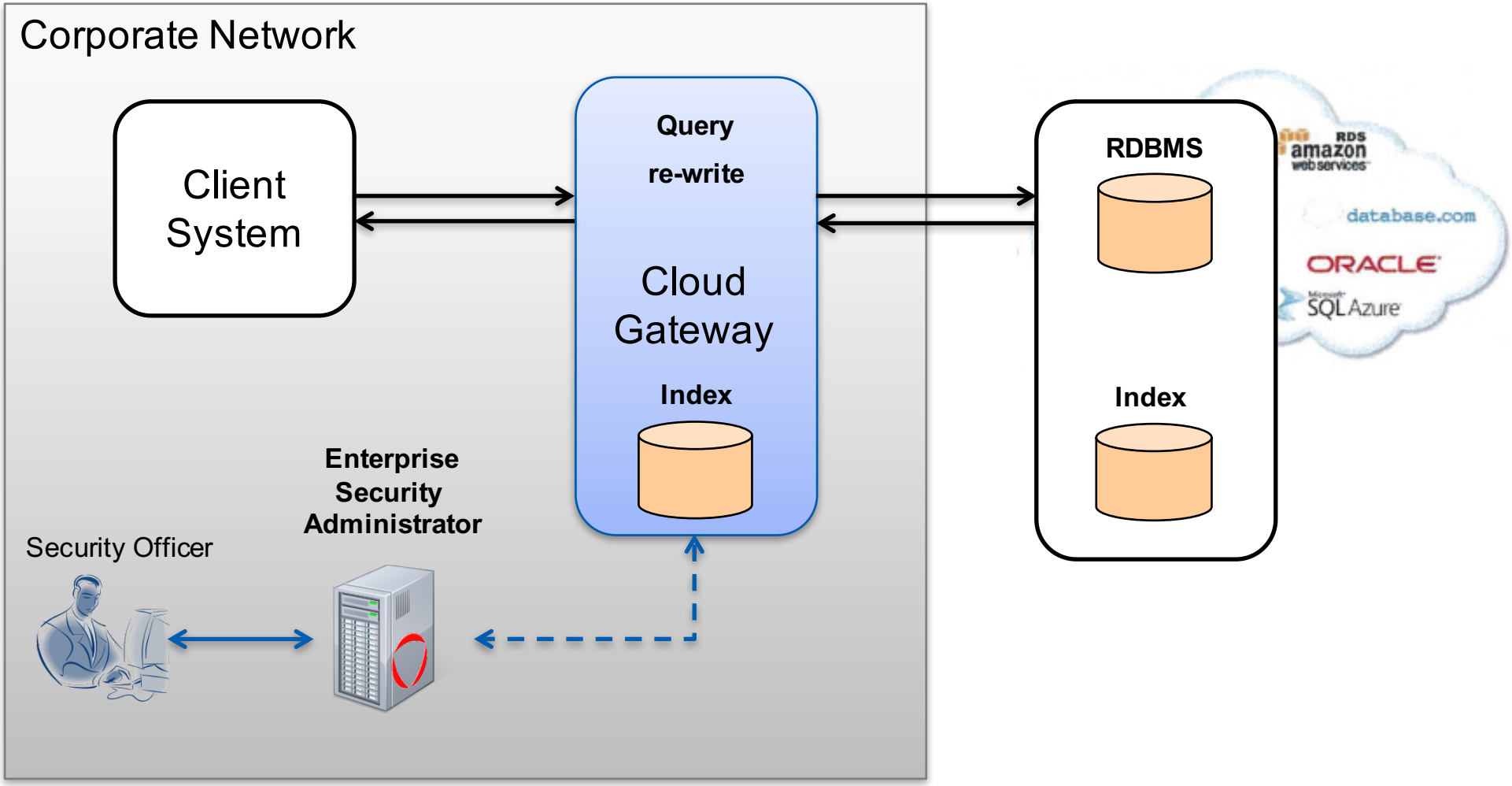
Security Gateway Deployment – Hybrid Cloud



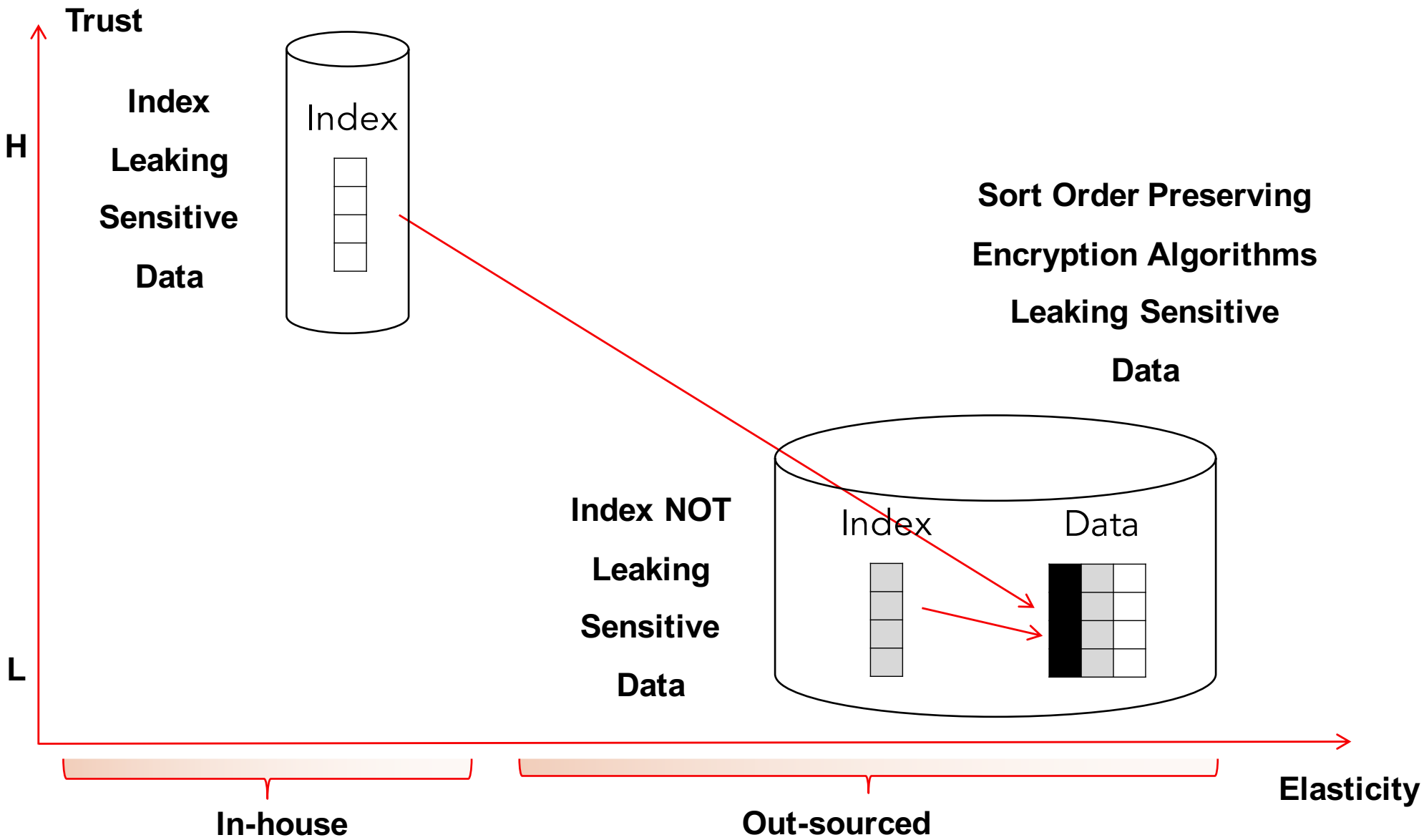
Security Gateway – Searchable Encryption



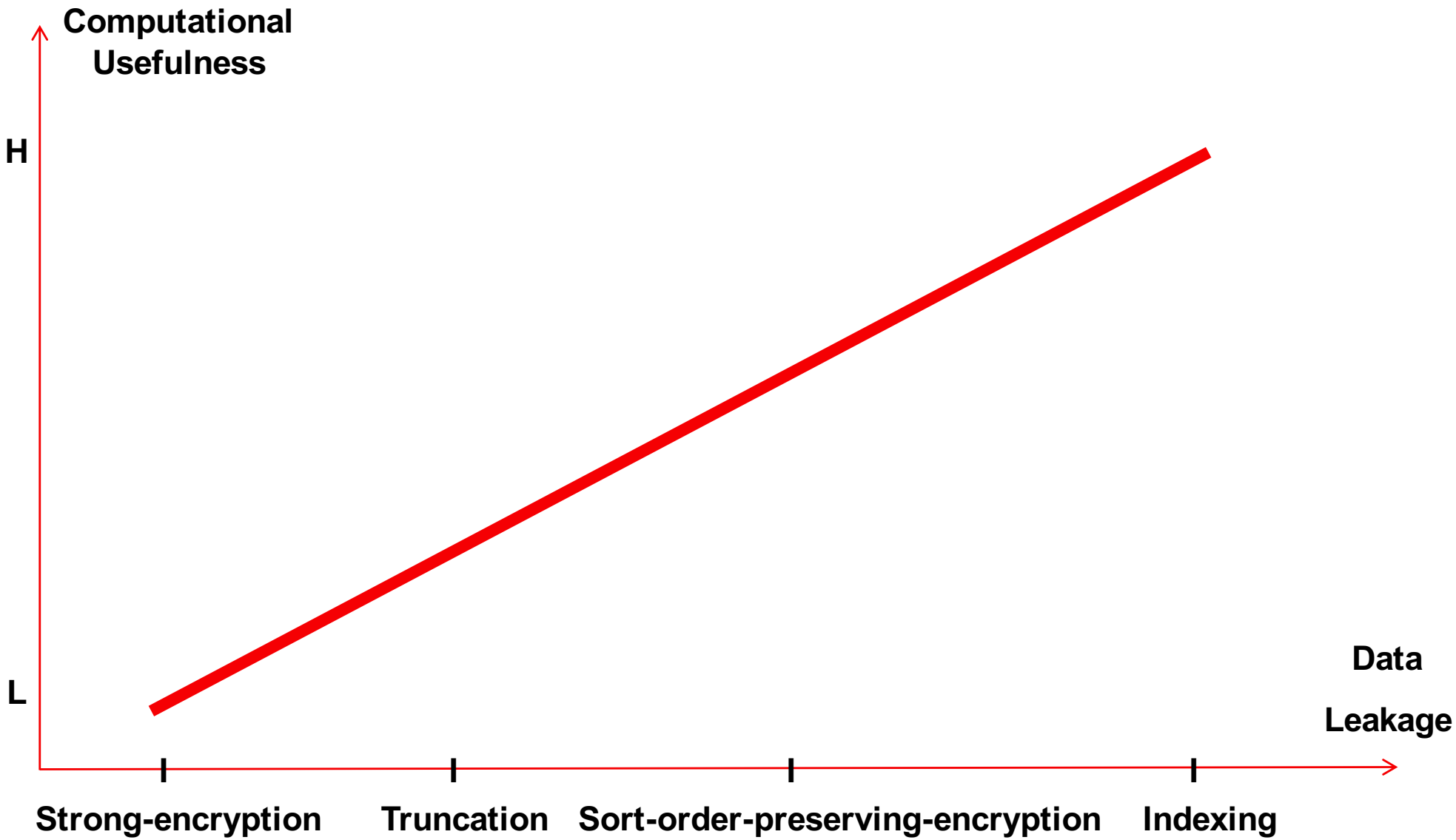
Security Gateway – Search & Indexing



Risk Adjusted Data Leakage

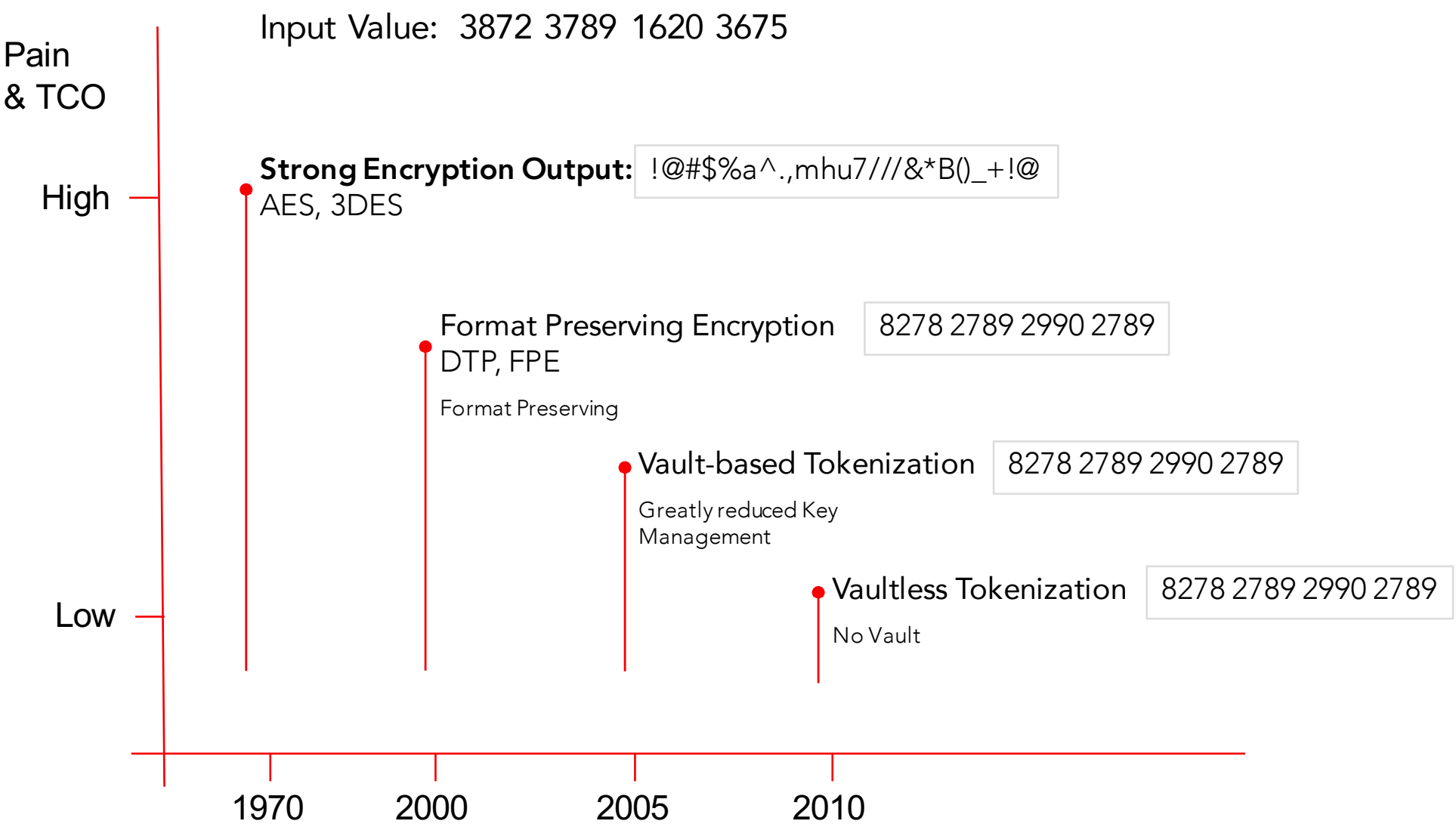


Risk Adjusted Storage – Data Leaking Formats



Comparing Fine Grained Data Protection Methods

Reduction of Pain with New Protection Techniques

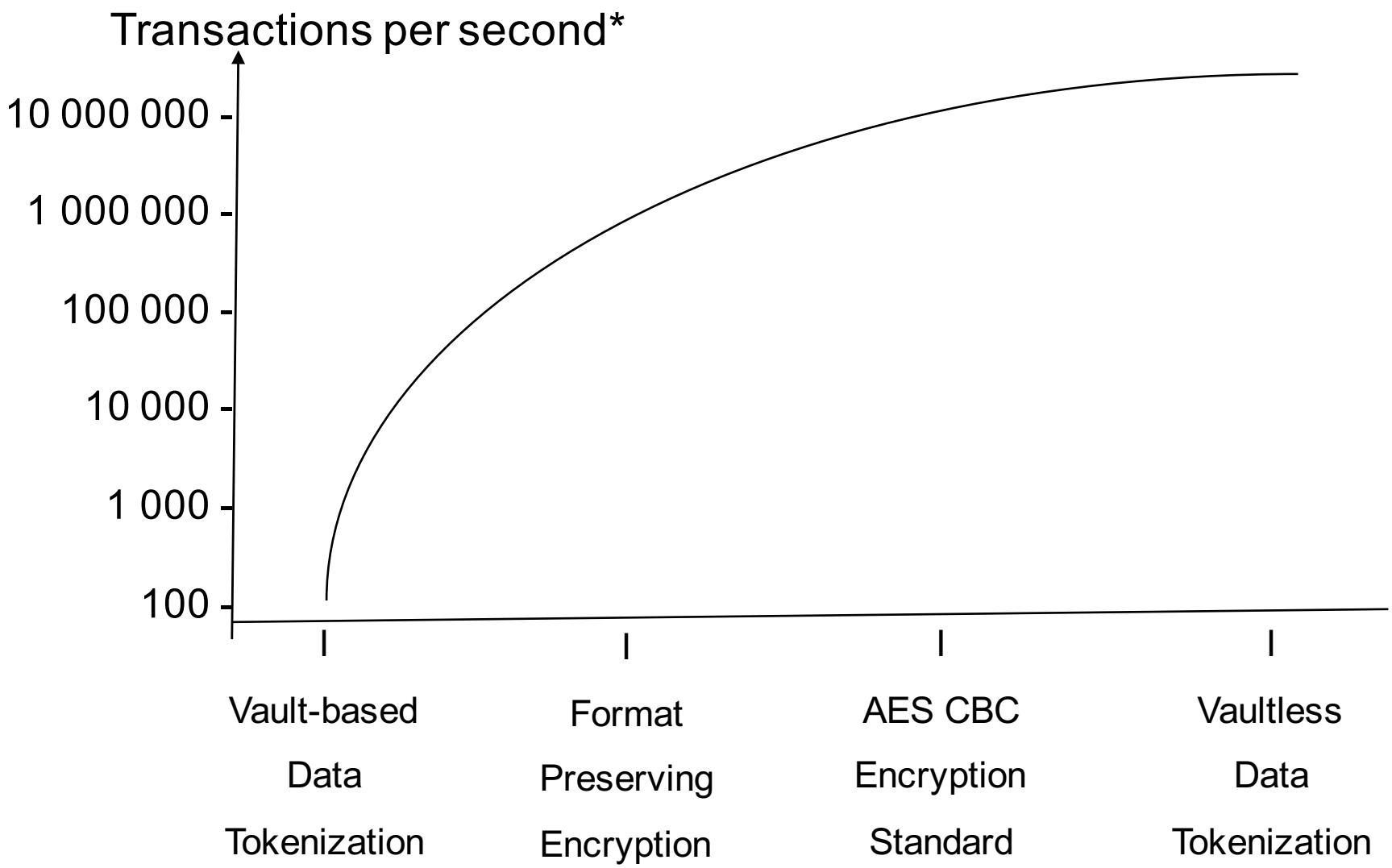


Cloud Gateway - Requirements Adjusted Protection

Data Protection Methods	Scalability	Storage	Security	Transparency
System without data protection	●	●	○	●
Weak Encryption (1:1 mapping)	◔	◔	◕	◔
Searchable Gateway Index (IV)	◒	◒	●	●
Vaultless Tokenization	◔	●	●	◔
Partial Encryption	◕	●	◔	◔
Data Type Preservation Encryption	◕	●	◔	◔
Strong Encryption (AES CBC, IV)	◒	◒	●	◕

Best ● ◔ ◒ ◕ ○ Worst

Speed of Fine Grained Protection Methods



*: Speed will depend on the configuration

What is Data Tokenization?

Fine Grained Data Security Methods

Tokenization and Encryption are Different

Used Approach	Cipher System (Encryption)	Code System (Tokenization)
Cryptographic algorithms	●	
Cryptographic keys	●	
Code books		●
Index tokens		●

Source: McGraw-HILL ENCYPLOPEDIA OF SCIENCE & TECHNOLOGY

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Significantly Different Tokenization Approaches

Property	Vault-based: Dynamic	Vault-based: Pre-generated	Vaultless
Footprint	Large, Expanding	Large, Static	Small, Static
Replication	Complex replication required	No replication required	No replication required
Collisions	Prone to collisions	No collisions	No collisions
Latency / Performance	Will impact performance and scalability	Will impact performance and scalability Faster than the traditional dynamic approach	Little or no latency Fastest tokenization in the industry
Tokenizing many data categories	Potentially impossible	Potentially impossible	Can tokenize many data categories with minimal or no impact on footprint or performance

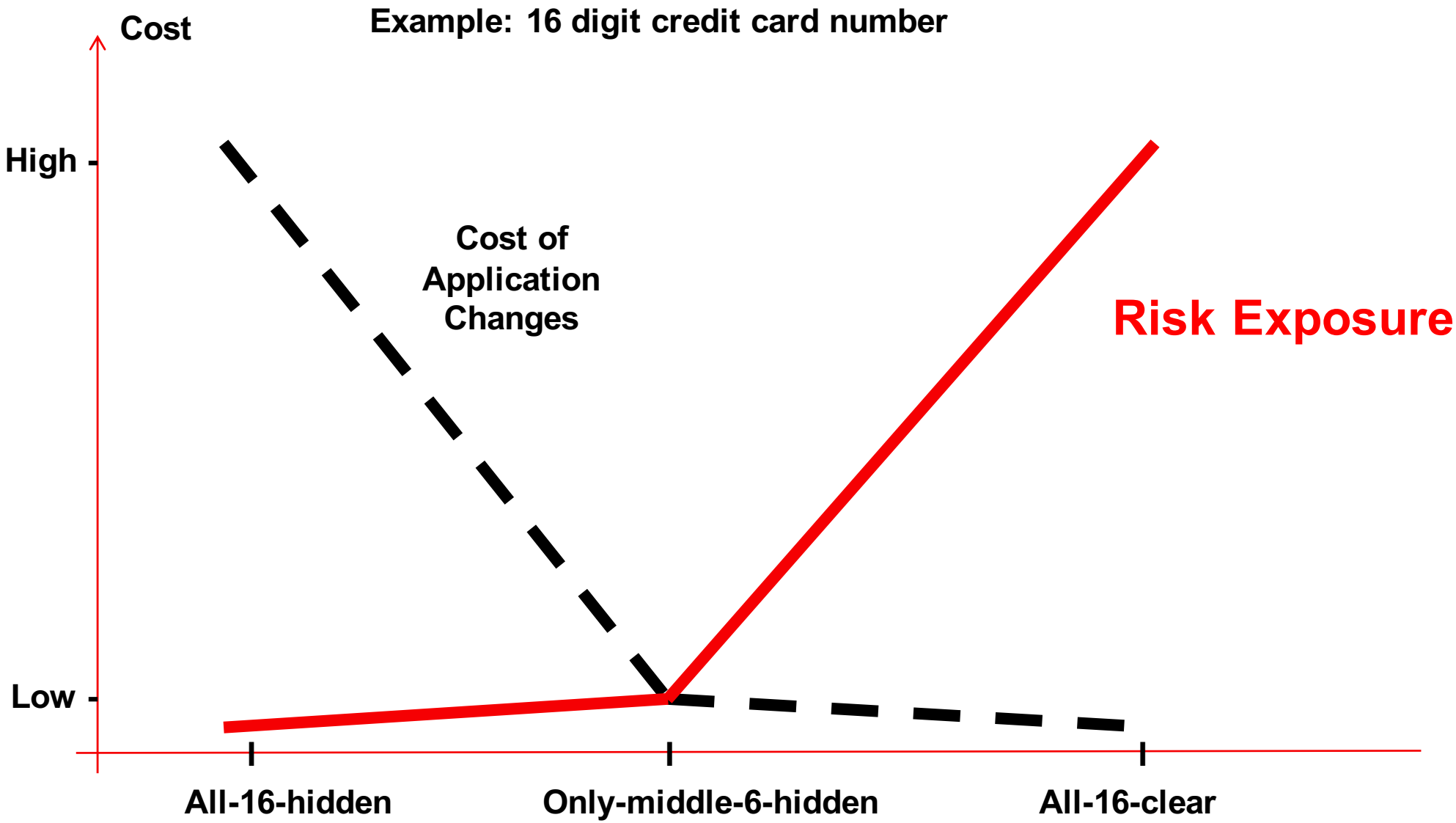
COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Examples of Protected Data

Field	Real Data	Tokenized / Pseudonymized
Name	Joe Smith	csu wusoj
Address	100 Main Street, Pleasantville, CA	476 srta coetse, cysieondusbak, CA
Date of Birth	12/25/1966	01/02/1966
Telephone	760-278-3389	760-389-2289
E-Mail Address	joe.smith@surferdude.org	eoe.nwuer@beusorpdqo.org
SSN	076-39-2778	076-28-3390
CC Number	3678 2289 3907 3378	3846 2290 3371 3378
Business URL	www.surferdude.com	www.sheyinctao.com
Fingerprint		Encrypted
Photo		Encrypted
X-Ray		Encrypted
Healthcare / Financial Services	Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities	Protection methods can be equally applied to the actual data, but not needed with de-identification

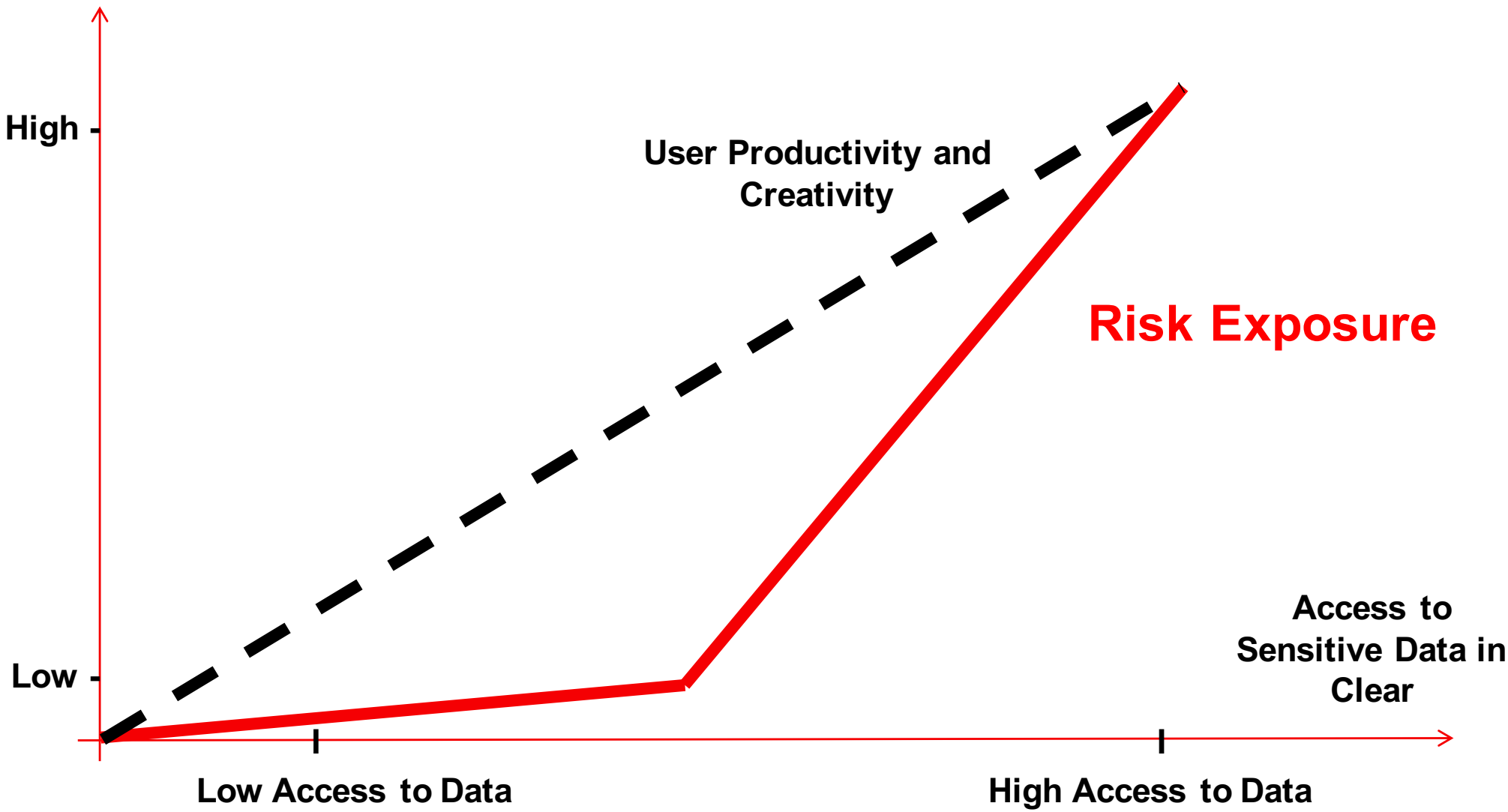
COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Partial Protection of Data Fields

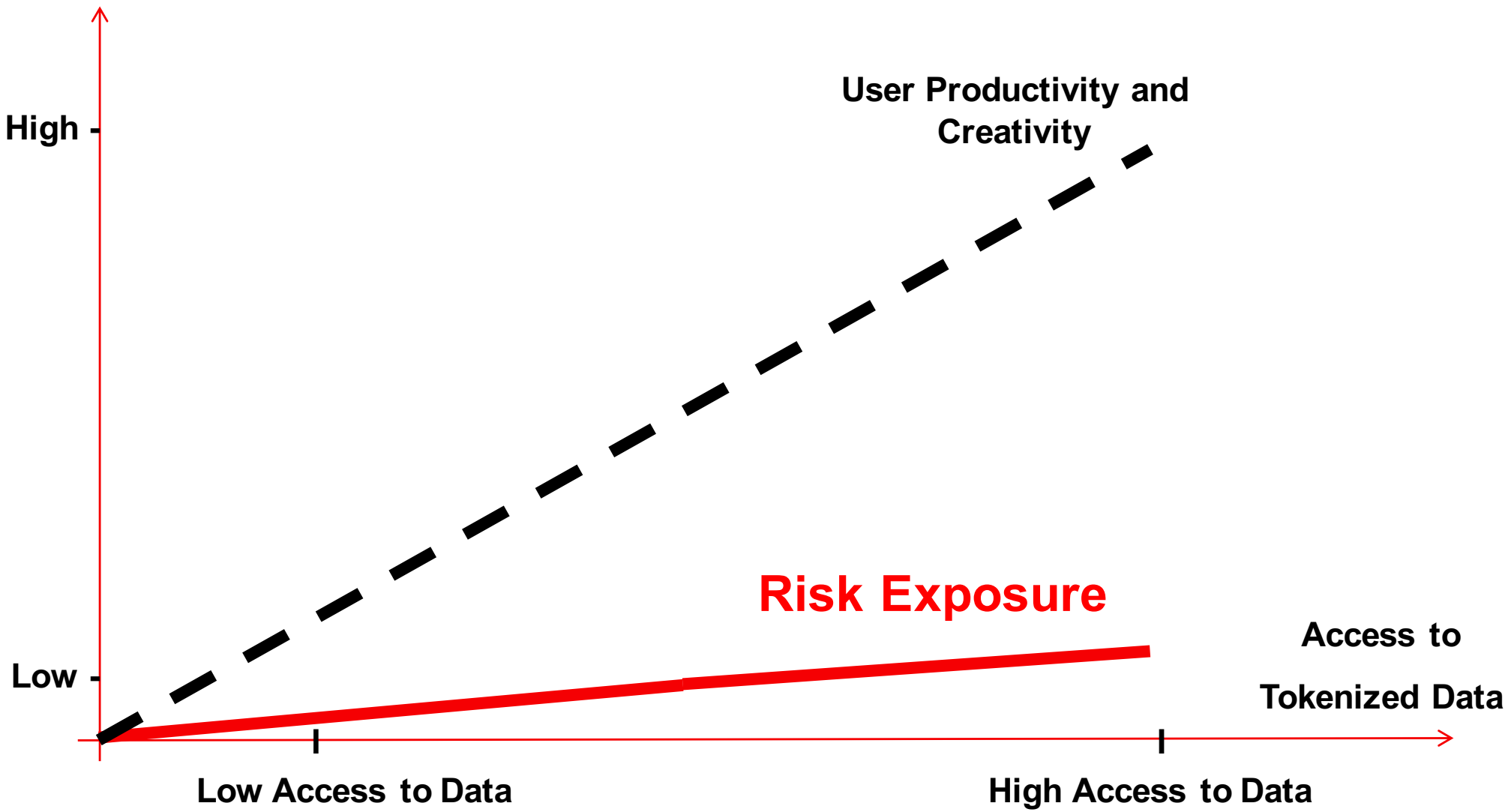


COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Traditional Access Control



Fine Grained Protection of Data Fields



COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Securing Big Data

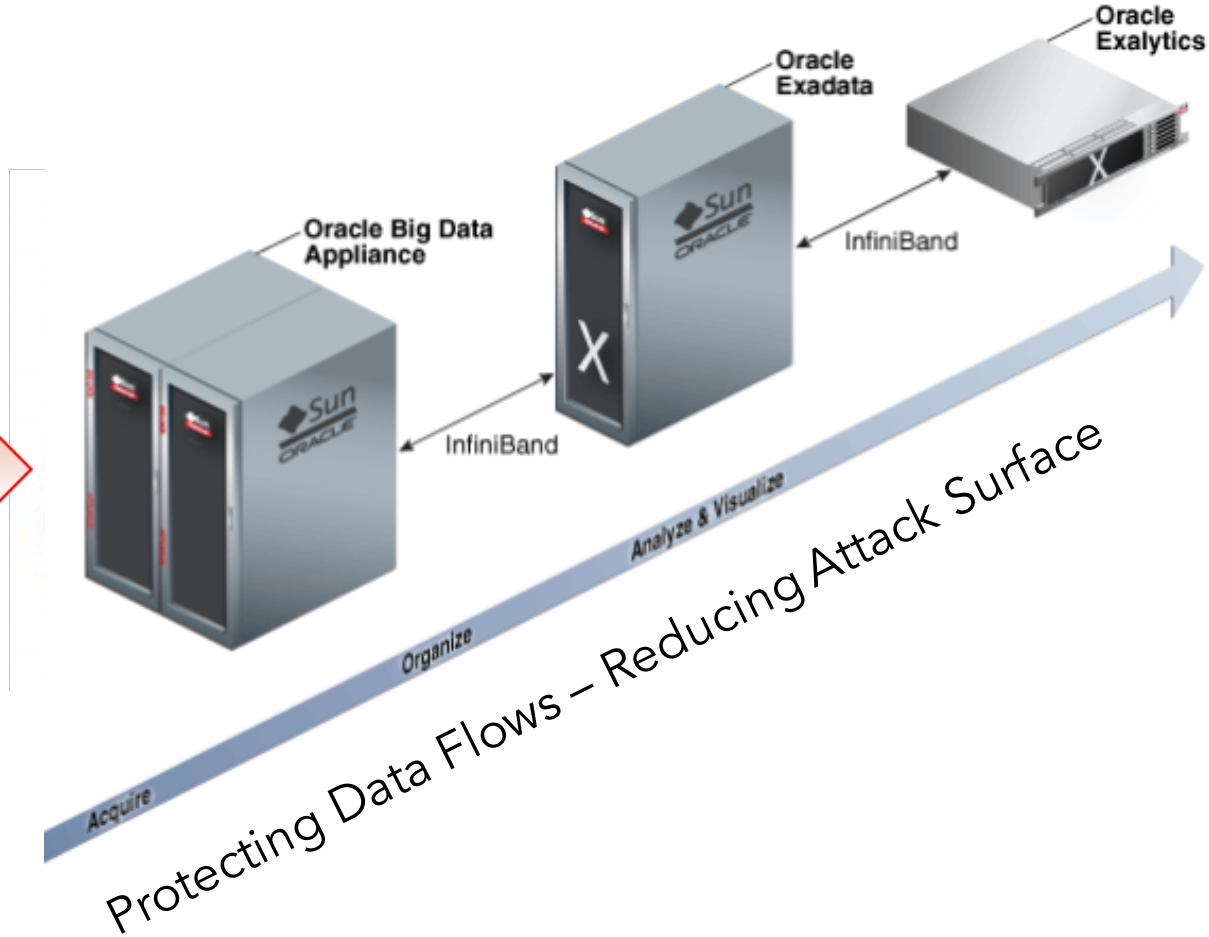
Big Data Needs a Data-Centric Security Focus

- CISOs should not treat big data security in isolation, but require policies that encompass all data
- New data-centric audit and protection solutions and management approaches are required
- Big data initiatives require data to move between structured and unstructured data silos, exposing incoherent data security policies that CISOs must address to avoid security chaos

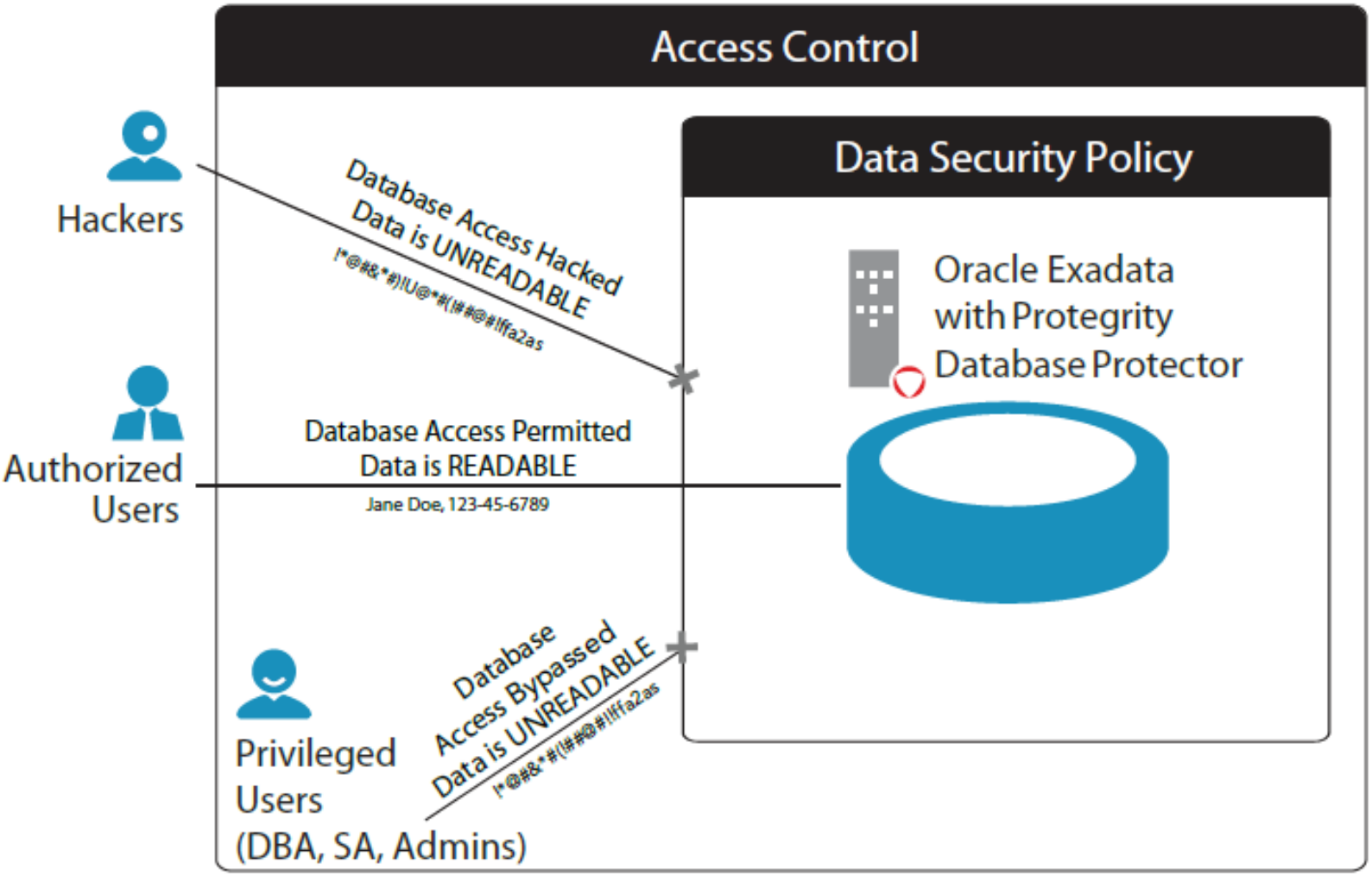
Gartner®

Source: Gartner – **Big Data Needs a Data-Centric Security Focus,** 2014

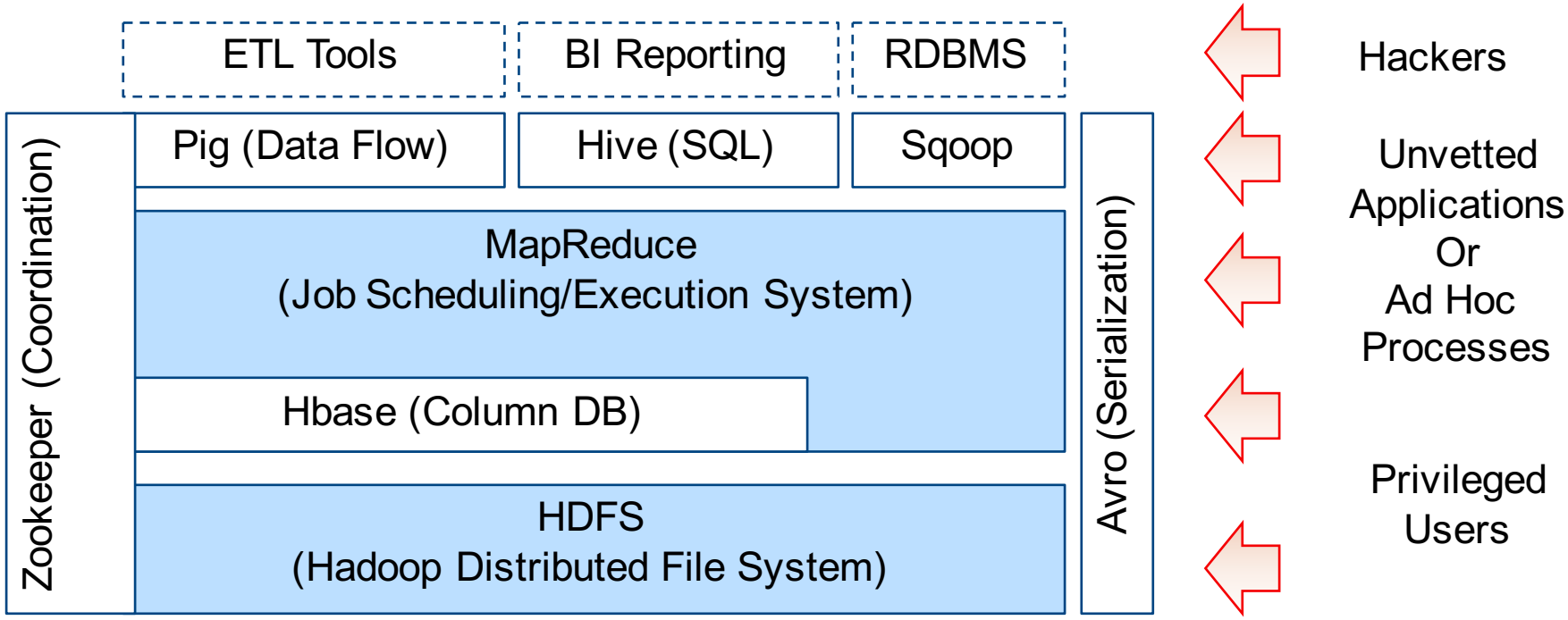
Oracle's Big Data Platform



Oracle's Exadata

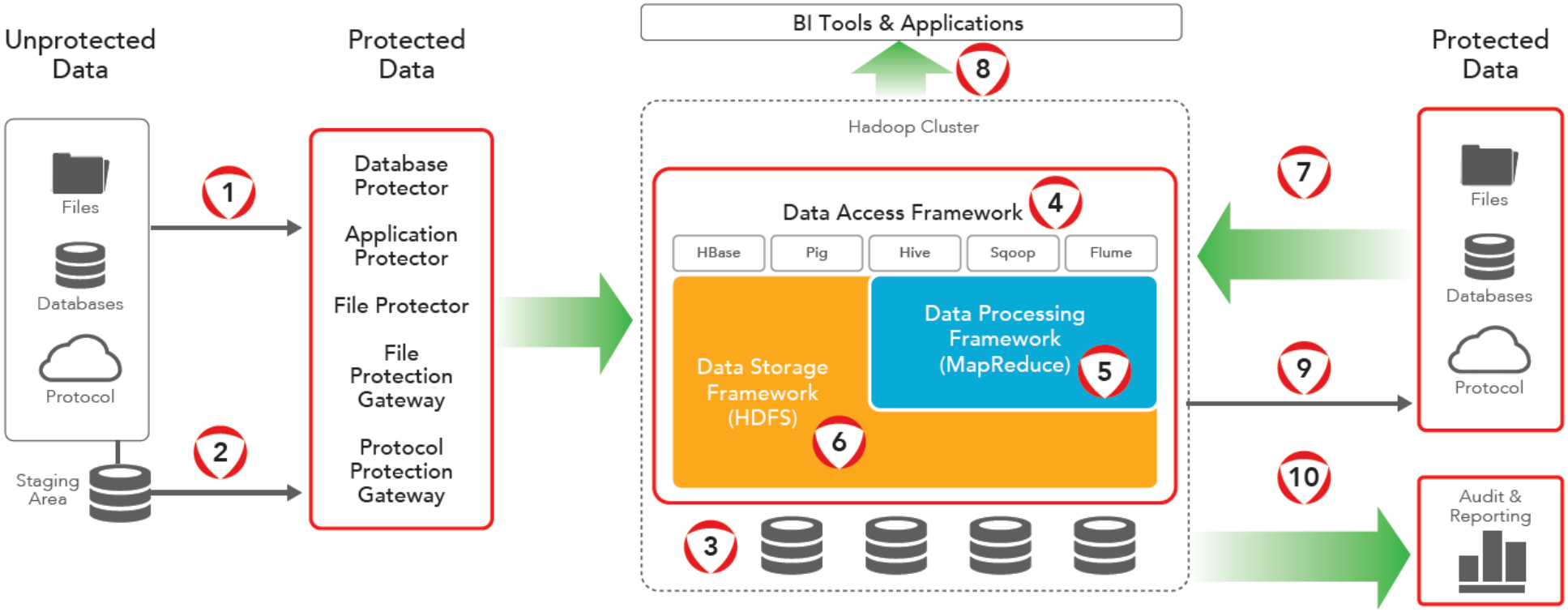


Many Ways to Hack Big Data



Source: http://nosql.mypopescu.com/post/1473423255/apache-hadoop-and-hbase

Securing Big Data

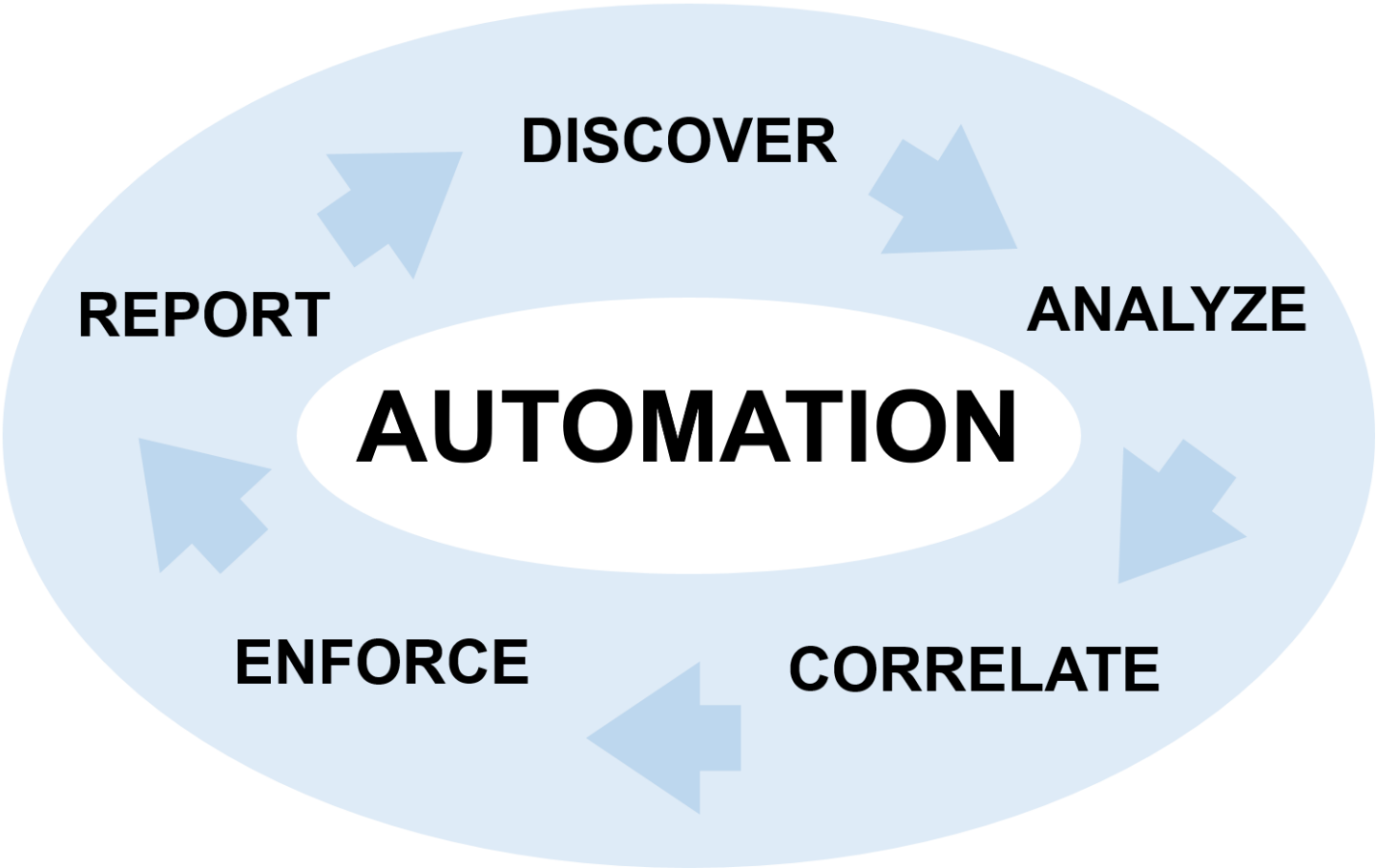


1. Data protection at database, application or file
2. Data protection in a staging area

3. Volume encryption in Hadoop
4. Hbase, Pig, Hive, Flume and Scope using protection API
5. MapReduce using protection API
6. File and folder encryption in HDFS
8. Export de-identified data

7. Import de-identified data
9. Export identifiable data
10. Export audit s for reporting

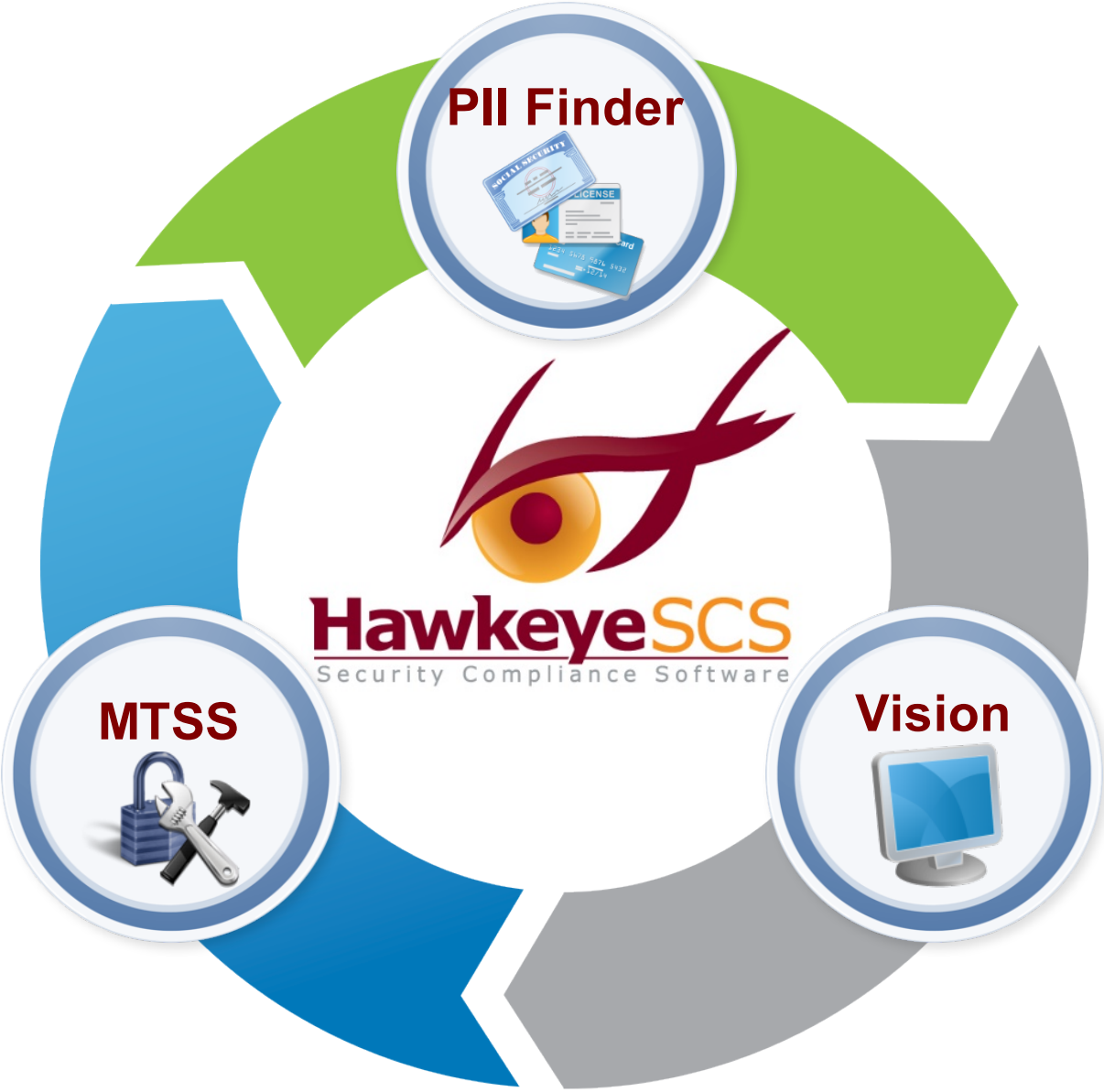
Critical Data Asset Discovery and Protection



Security Tools and Integrated Services

Software as a Service (SaaS) data discovery solution

Managed Tools Security Service



24/7 Eyes on Glass (EoG) monitoring, Security Operations Center (SOC)

Thank you!

Questions?

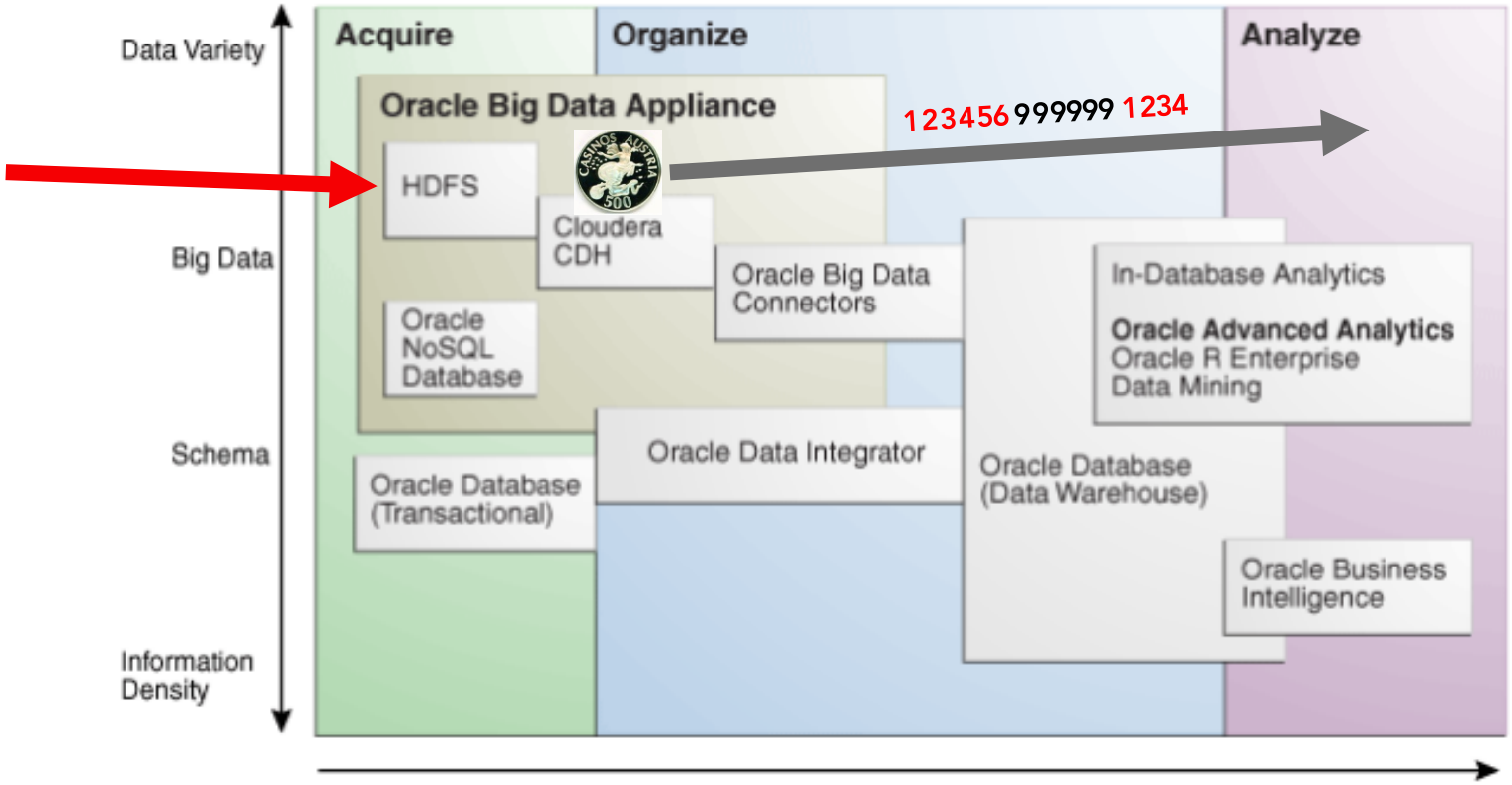
Ulf Mattsson, CTO
Compliance Engineering
umattsson@complianceengineers.com

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Tokenization Reducing Attack Surface

Tokenization on Each Node

123456 123456 1234



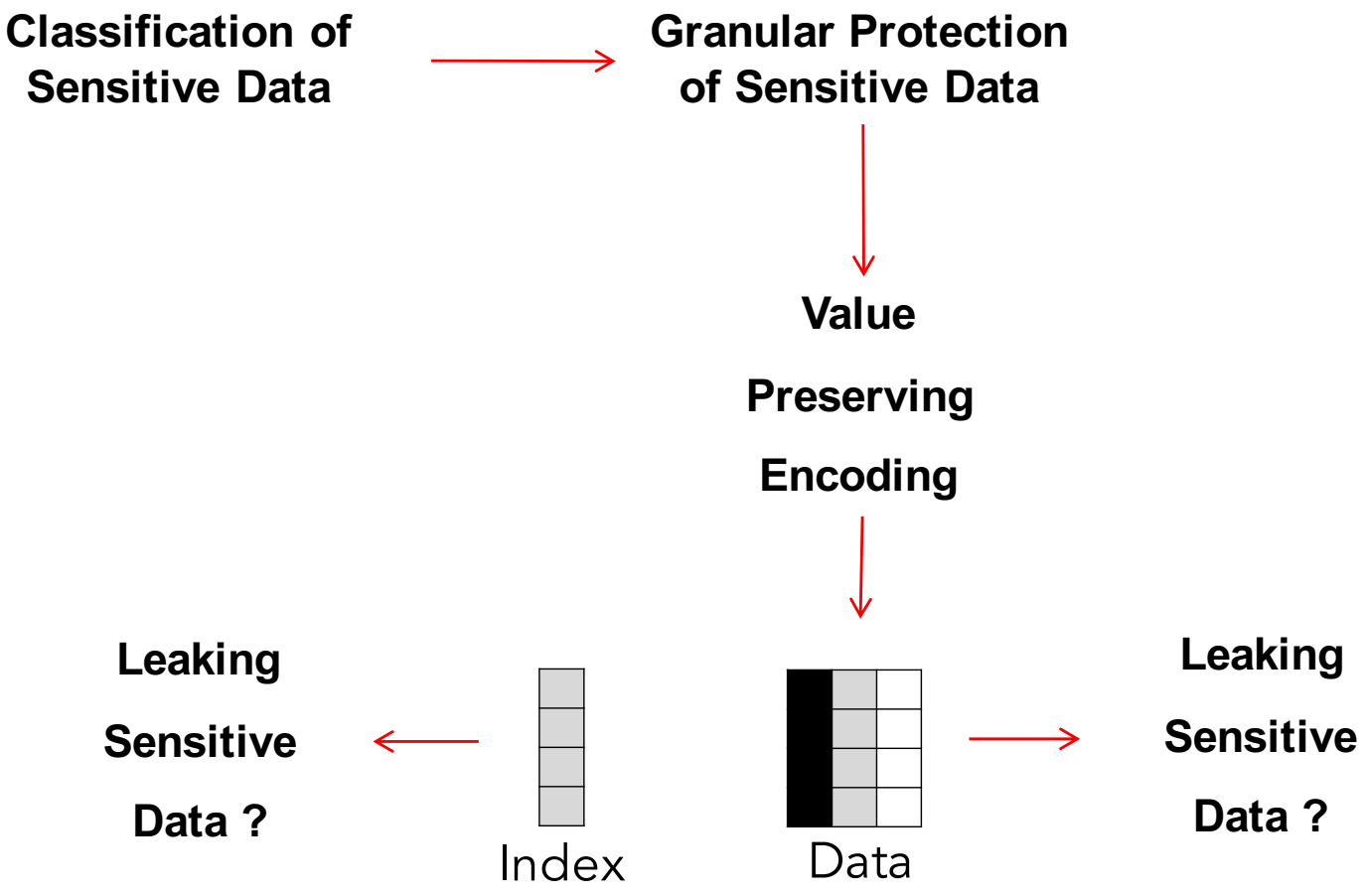
Security & Business Skills

InformationWeek

- The global shortage of technical skills in information security is by now well documented, but an equally concerning shortage of soft skills
- "I need people who understand that they are here to help the business make money and enable the business to succeed -- that's the bottom line. But it's very hard to find information security professionals who have that mindset," a CISO at a leading technology company told us

Source: www.informationweek.com/strategic-cio/enterprise-agility/the-security-skills-shortage-no-one-talks-about/a/d-id/1315690

Balancing Data Security & Utility



Summary

- Exponential growth of data generation
  - New business models fueled by Big Data, cloud computing and the Internet of Things
  - Creating cybercriminal's paradise
- Challenge in this interconnected world
  - Merging data security with data value and productivity.
- Urgently need a data-centric strategy
  - Protect the sensitive data flowing through digital business systems
- Solutions to bring together data insight & security
  - Safely unlock the power of digital business