The New York Oracle Users Group
Fall General Meeting – September 14, 2016

How can I Find My Data Security Blind Spots?

Ulf Mattsson, Chief Technology Officer, Compliance Engineering
umattsson@complianceengineers.com
www.complianceengineers.com

Ulf Mattsson

Inventor of more than 25 US Patents

Industry Involvement

PCI DSS - PCI Security Standards Council

- Encryption & Tokenization Task Forces, Cloud & Virtualization SIGs

IFIP - International Federation for Information Processing

- WG 11.3 Data and Application Security

CSA - Cloud Security Alliance

ANSI - American National Standards Institute

- ANSI X9 Tokenization Work Group

NIST - National Institute of Standards and Technology

- NIST Big Data Working Group

User Groups

- Security: ISACA & ISSA
- Databases: IBM & Oracle

National Institute of Standards and Technology

My work with PCI DSS Standards

Payment Card Industry Security Standards Council (PCI SSC)

1. PCI SSC Tokenization GuidelinesTask Force
2. PCI SSC Encryption Task Force
3. PCI SSC Point to Point Encryption Task Force
4. PCI SSC Risk Assessment SIG
5. PCI SSC eCommerce SIG
6. PCI SSC Cloud SIG
7. PCI SSC Virtualization SIG
8. PCI SSC Pre-Authorization SIG
9. PCI SSC Scoping SIG Working Group
10. PCI SSC Tokenization Products Task Force

DEVELOPER TRACK: Data-Centric Security Key to Cloud and Digital Business

Paper: Data-Centric Security Key to Cloud and Digital Business Mar 17, 2016

The rapid rise of cloud databases, storage and applications has led to unease among adopters over the security of their data. Whether it is data stored in a public, private or hybrid cloud, or used in third party SaaS applications, companies have good reason to be concerned. The biggest challenge in this interconnected world is merging data security with data value and productivity. If we are to realize the benefits promised by these new ways of doing business, we urgently need a data-centric strategy to protect the sensitive data flowing through these digital business systems.

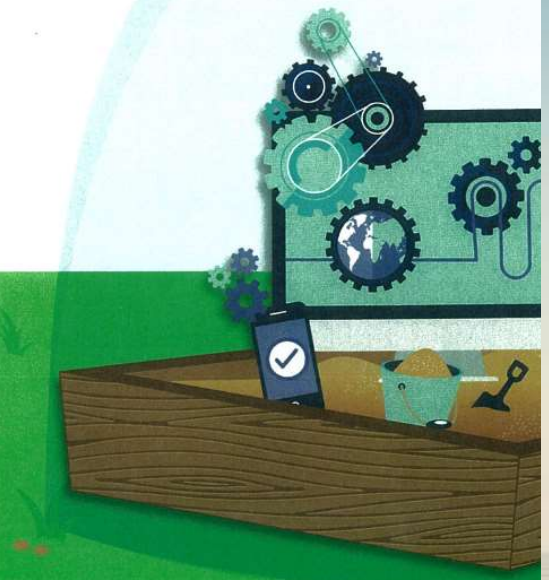
Ulf Mattsson

ISACA® Journal

Volume 6, 2014

WWW.ISACA.ORG

Cybersecurity



Featured articles:

How Zero-trust Network Security Can Enable Recovery From Cyberattacks

Leveraging Industry Standards to Address Industrial Cybersecurity Risk

Bridging the Gap Between Access and Security in Big Data

And more...

ISACA®
Trust in, and value from, information systems

ISACA® Journal

Emerging and Evolving IT Risk

Feature

Choosing the Most Appropriate Data Security Solution for an Organization

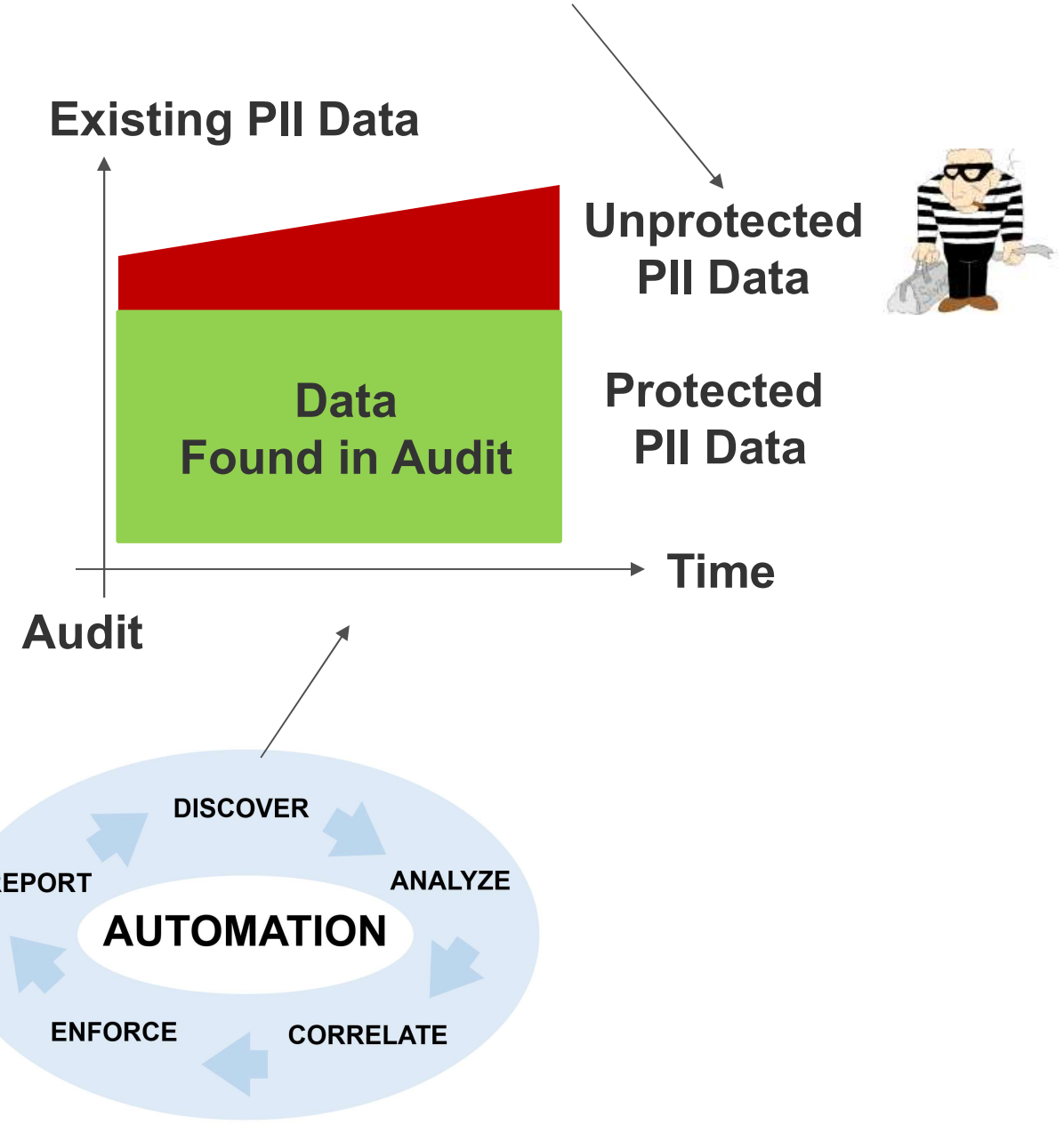
Ulf Mattsson is the chief technology officer of Protegrity, a leader in enterprise data security management, where he created the architecture of the Protegrity Data Security Platform. He is considered one of the founding fathers

With the rising cost and increasing frequency of data security breaches, companies are starting to reevaluate how they protect their data. External

to put in the time and effort necessary to access sensitive data.

Staying ahead of the bad guys is not an easy

How can I Find My Blind Spots?



COMPLIANCE ENGINEERING
Security & Compliance Solutions

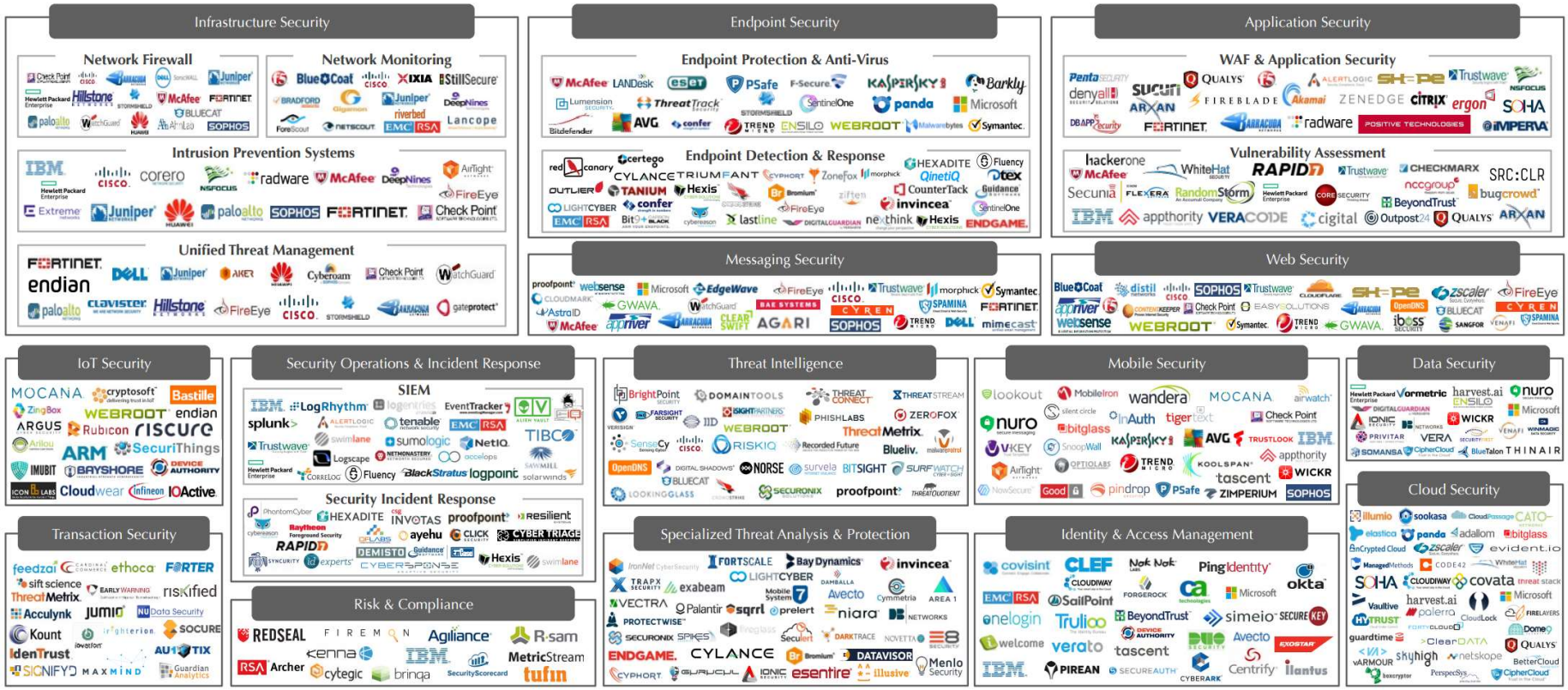
Every Day, we Create 2.5 Quintillion Bytes of Data

90% of the Data in the World today has been Created in the Last Two Years

Source: https://www.ibm.com/software/data/bigdata/what-is-big-data.html
IBM

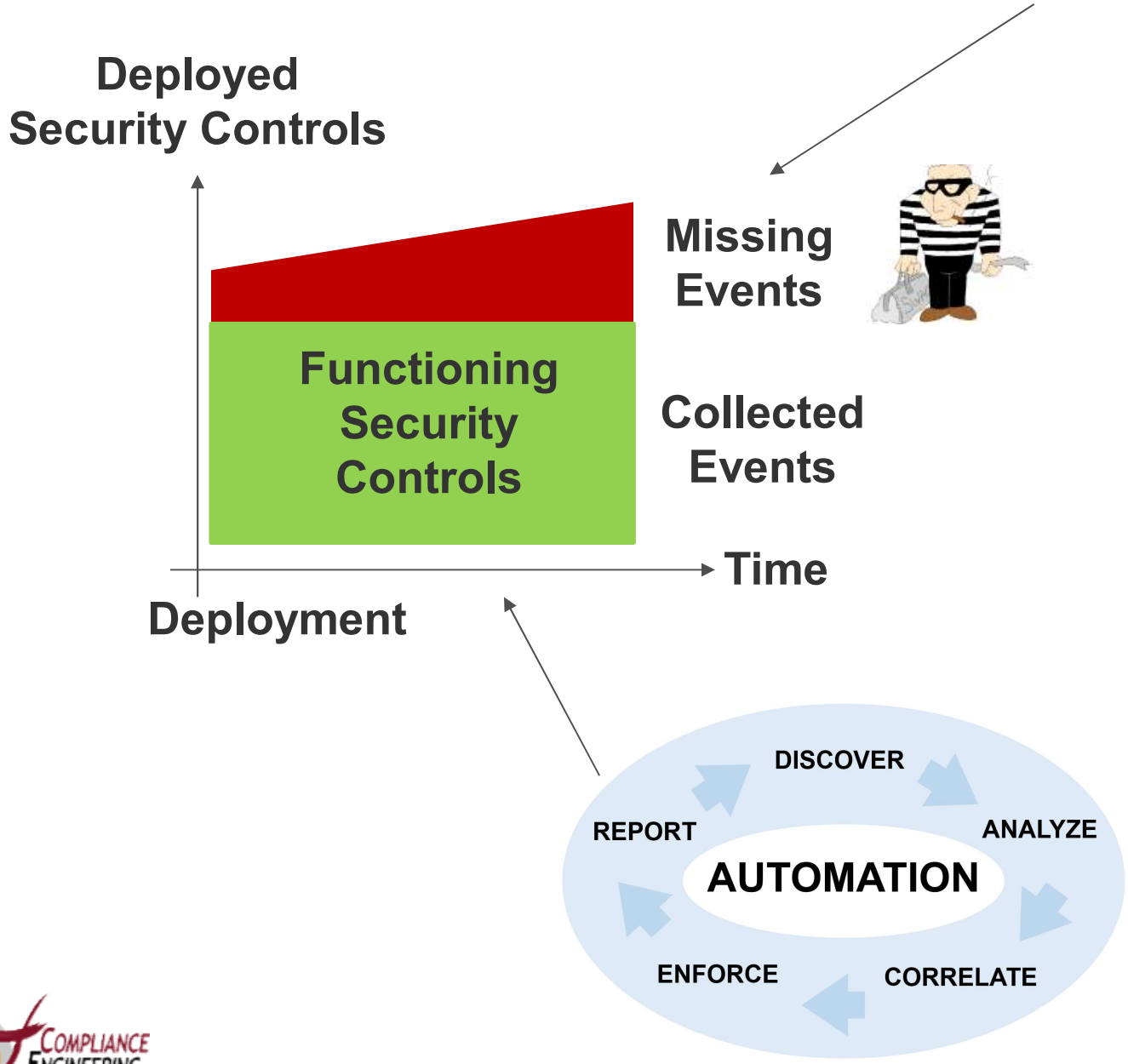
COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Enterprises may have 50 Security Control Systems

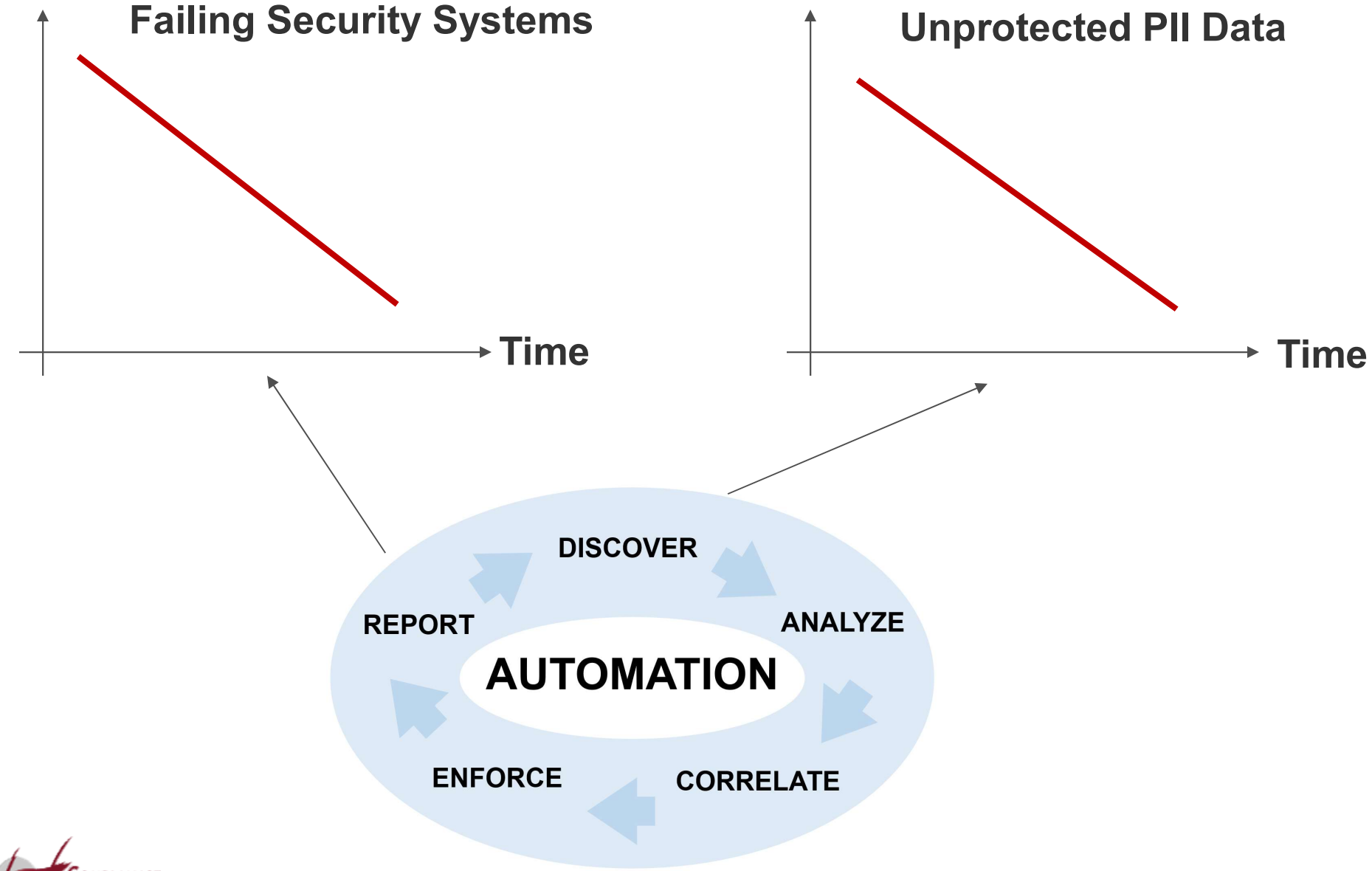


Source: Momentum Partners.

How can I Find My Blind Spots?



Generating Key Security Metrics



Business RISK

Remediation Management - Example

Are you compliant?

Are your controls really active & covering all your sensitive data?

RA	Asset	Controls	Inherent Risk	Residual Risk	Residual Qualitative	Regulatory Risk
CRM RA 2015	CRM	97.47	2.37	31.50	Medium	High
Online B2B Web Services RA 2015	Online B2B Web Services	97.47	1.31	28.30	Low	Low
SAP RA 2015	SAP	97.47	8.81	50.80	Medium	Medium
Crossbow RA 2015	Crossbow	97.47	2.94	33.20	Medium	High
HR+ RA 2014	HR+	97.47	0.35	25.40	Low	Low
IT Alert RA 2014	IT Alert	97.47	1.25	28.10	Low	Low
eTrader RA 2014	eTrader	97.47	10.95	57.20	Medium	High
Feed RA 2013	Feed	97.47	15.45	70.70	High	High

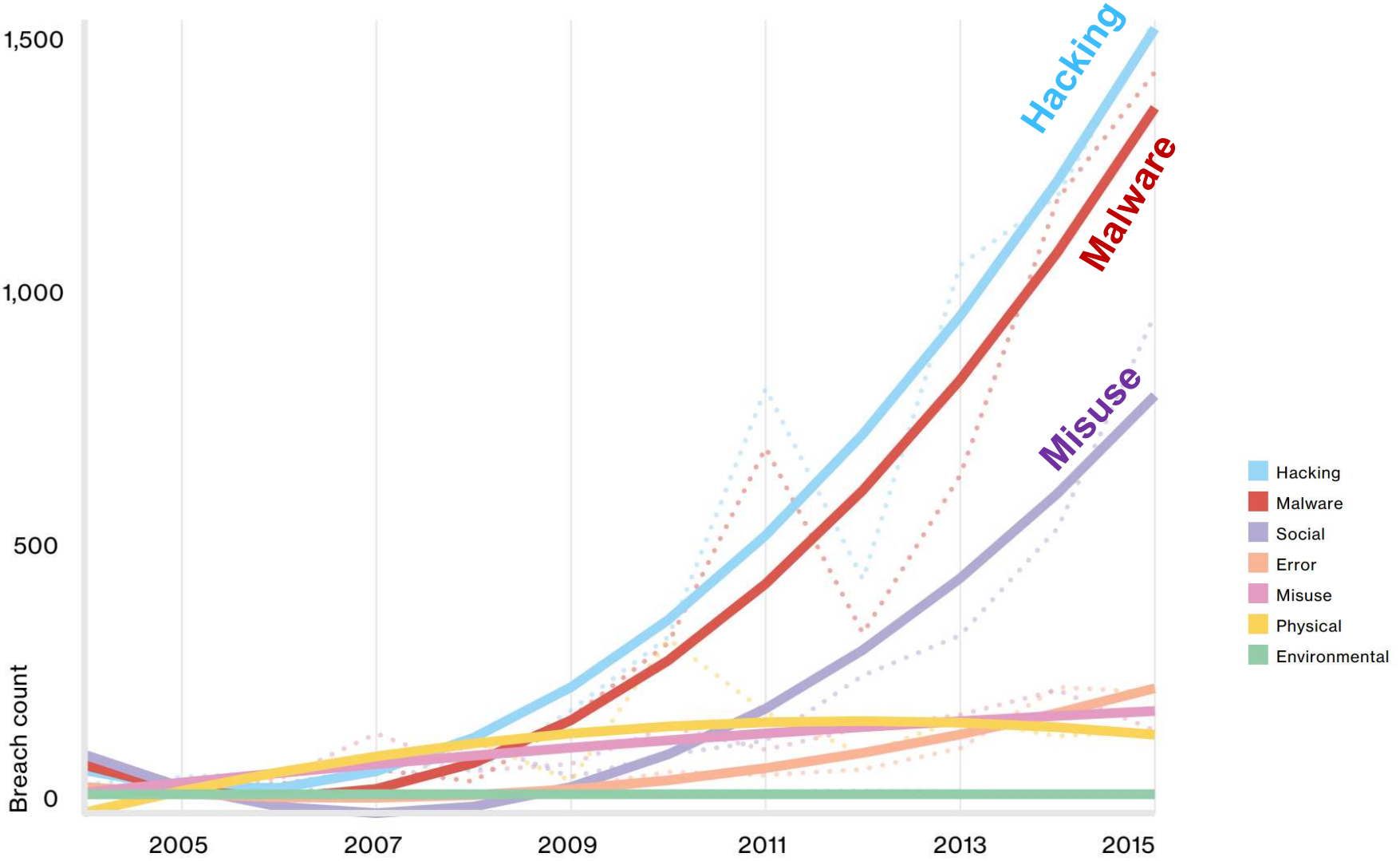
Are Breaches on the Rise?

Novus Ordo Seclorum - A New Order of the Ages

89% of Breaches had a Financial or Espionage motive

Source: Verizon 2016 Data Breach Investigations Report, Apr 26, 2016

Increasing Number of Breaches



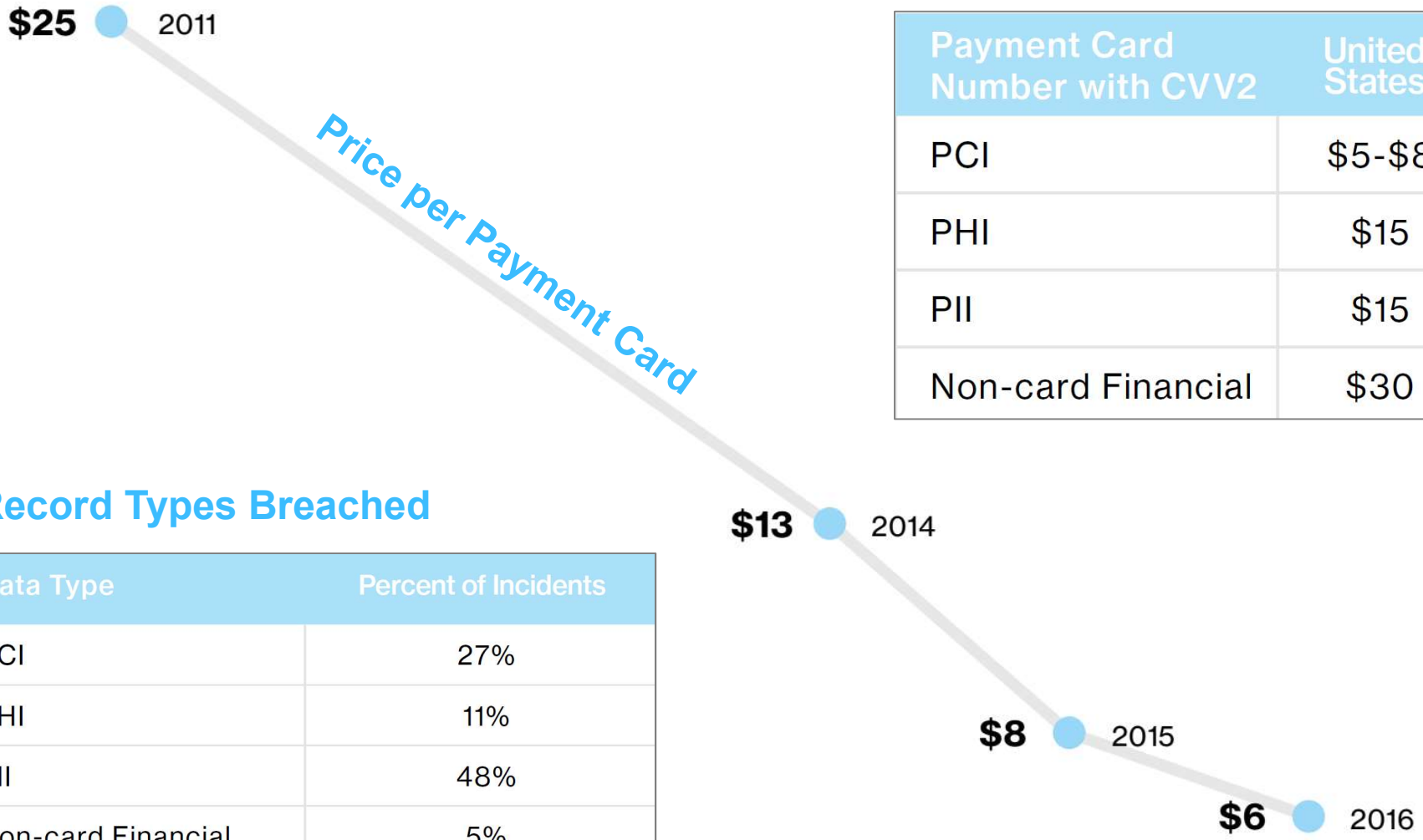
Source: Verizon 2016 Data Breach Investigations Report

Which Data is Breached?

PII Record are Attractive

Market Price per Record

Payment Card Number with CVV2	United States
PCI	$5-$8
PHI	$15
PII	$15
Non-card Financial	$30



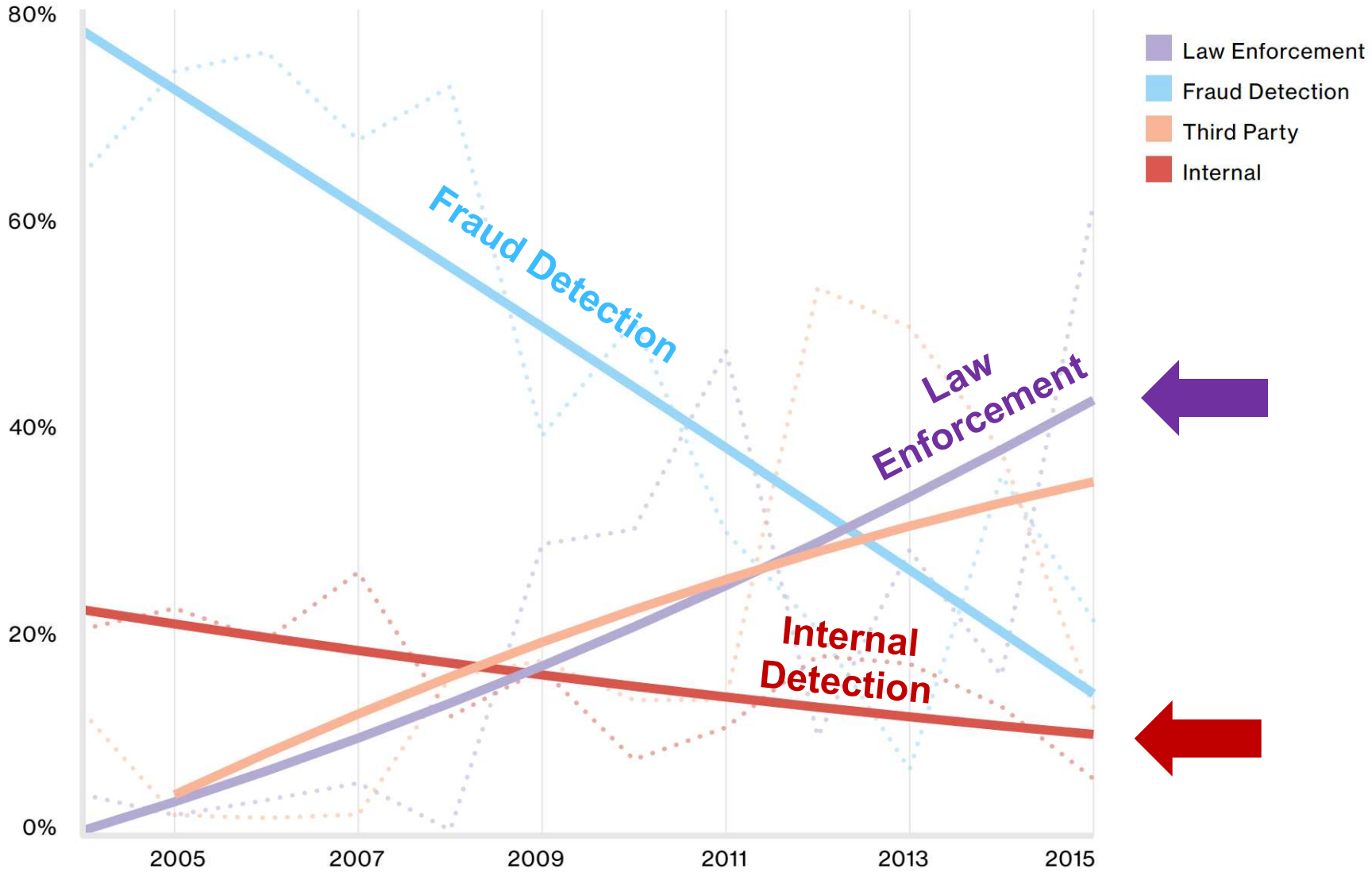
Record Types Breached

Data Type	Percent of Incidents
PCI	27%
PHI	11%
PII	48%
Non-card Financial	5%

Source: Verizon 2016 Data Breach Investigations Report

How are Breaches Detected?

Law Enforcement will Discover Your Breach – Not You



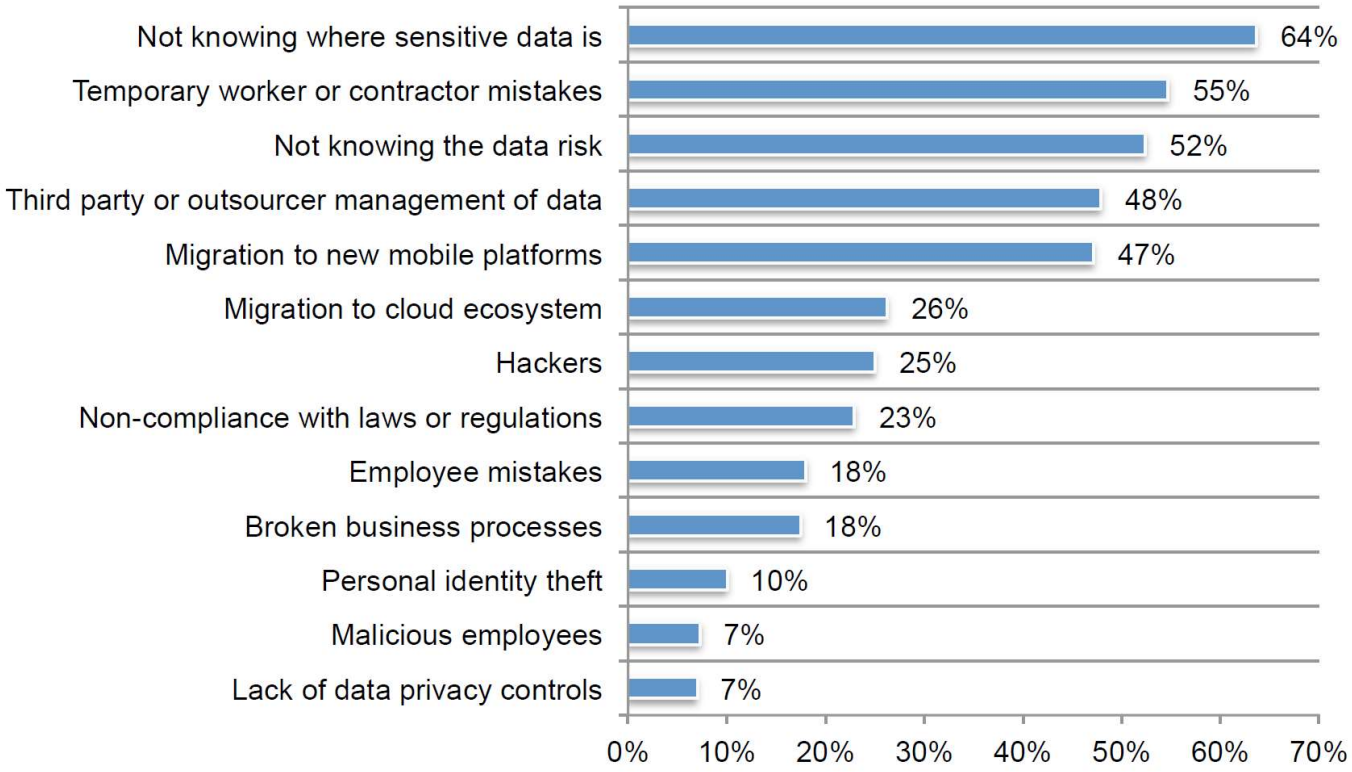
Source: Verizon 2016 Data Breach Investigations Report

Not Knowing Where Sensitive Data Is

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Not Knowing Where Sensitive Data Is

Figure 2. With respect to your organization's state of data security, what keeps you up at night?
Four choices permitted



Source: The State of Data Security Intelligence, Ponemon Institute, 2015

Are You Ready for the New Requirements of PCI-DSS V3.2?

The new requirements introduced in PCI DSS will be considered best practices until 31 January 2018.
Starting 1 February 2018 they are effective as requirements.

PCI Security Standards Council™

COMPLIANCE ENGINEERING
Security & Compliance Solutions

New PCI DSS 3.2 Standard – Data Discovery

- PCI DSS **v2**
  - **Mentioned data flow** in “Scope of Assessment for Compliance with PCI DSS Requirements.”
- PCI DSS **v3.1**
  - Added **data flow** into a **requirement**.
- PCI DSS **v3.2**
  - Added **data discovery** into a **requirement**.

Source: PCI DSS 3.2 Standard: data discovery (A3.2.5, A3.2.5.1, A3.2.6) for service providers

PCI-DSS
and Beyond

COMPLIANCE ENGINEERING
Security & Compliance Solutions

How can we Find Methods to Quickly and Accurately Discover all PII?

Do you need agents for this?

Can we apply machine learning to better deal with SSN false positives?

Please look at the LinkedIn group “Enterprise Data Discovery” at

https://www.linkedin.com/groups/8563068

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Information Security, Worldwide, 2014-2020

The information security market is estimated to have grown 13.9% in revenue in 2015 with the IT **security outsourcing segment recording the fastest growth (25%).**

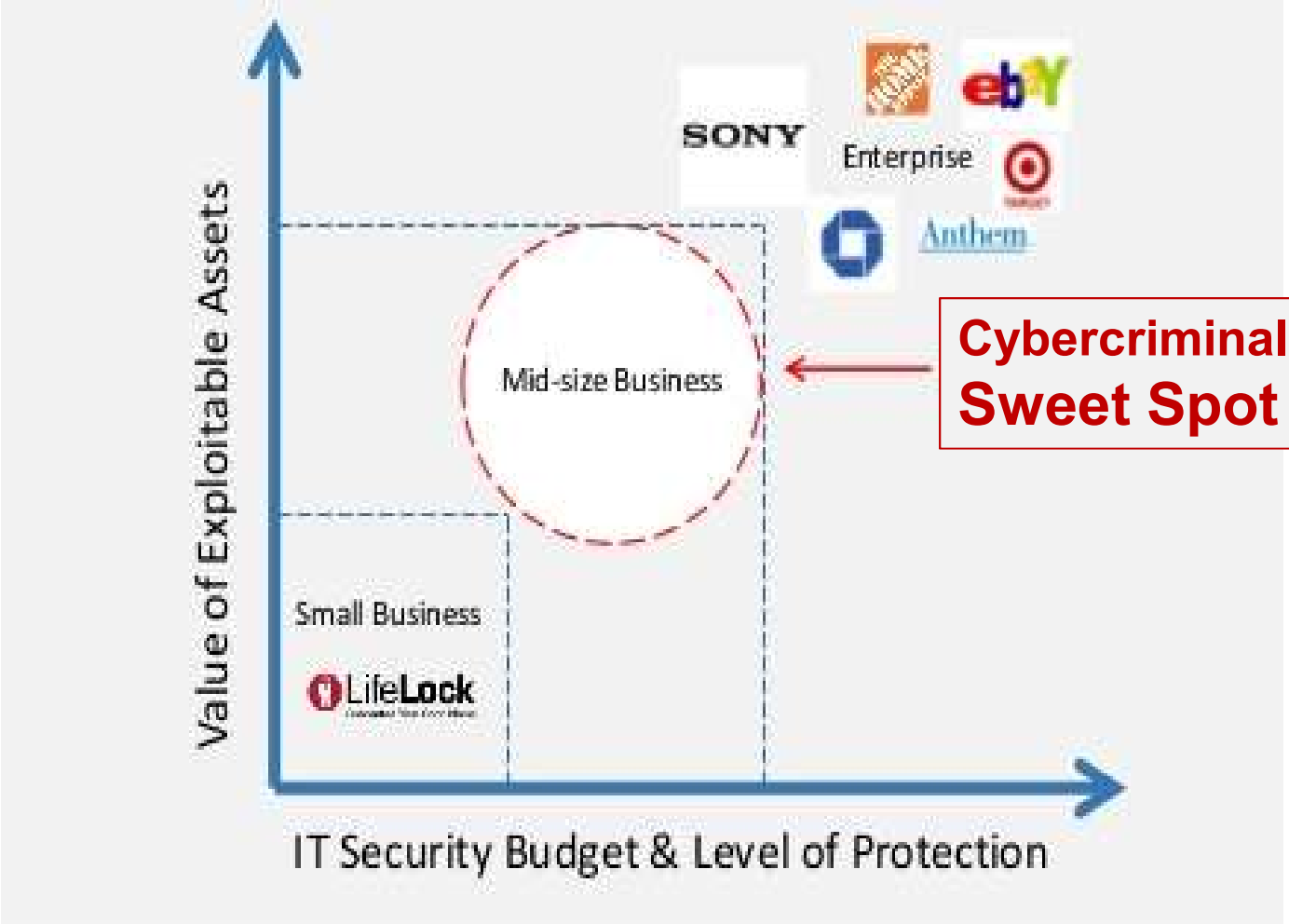
Gartner®

Source: Gartner Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

The Cybercriminal Sweet Spot

Cybercrime Trends and Targets



Source: calnet

Do We have the Skills Required?

Problematic and Increasing Shortage of Cybersecurity Skills

- 46 percent of organizations say they have a “problematic shortage” of cybersecurity skills in 2016
- By comparison, 28 percent of organizations claimed to have a “problematic shortage” of cybersecurity skills in 2015
- That means we’ve seen an 18 percent year-over-year increase

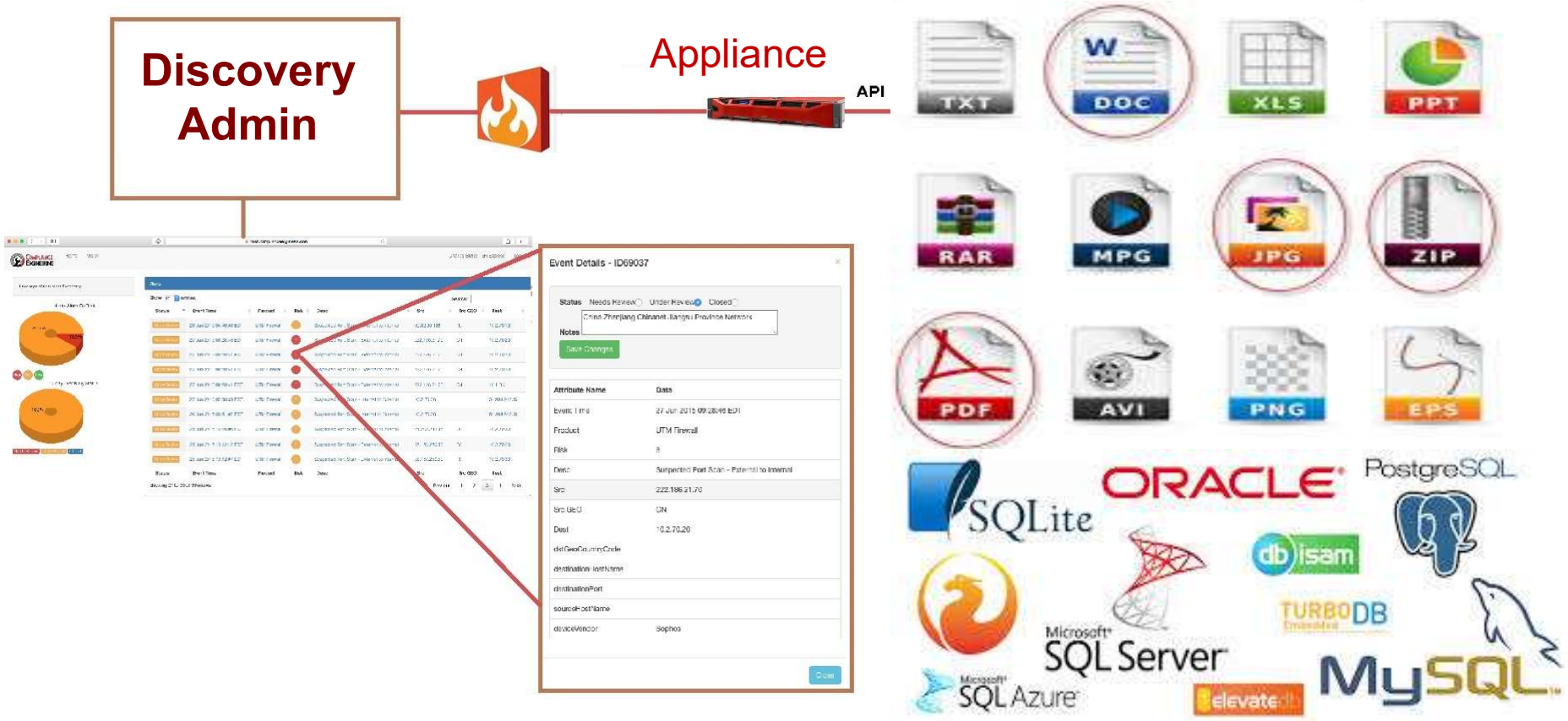
Source: EDG and Network World | May 10, 2016

NETWORKWORLD FROM IDG

EDG Research & Consulting

Compliance Engineering
Security & Compliance Solutions

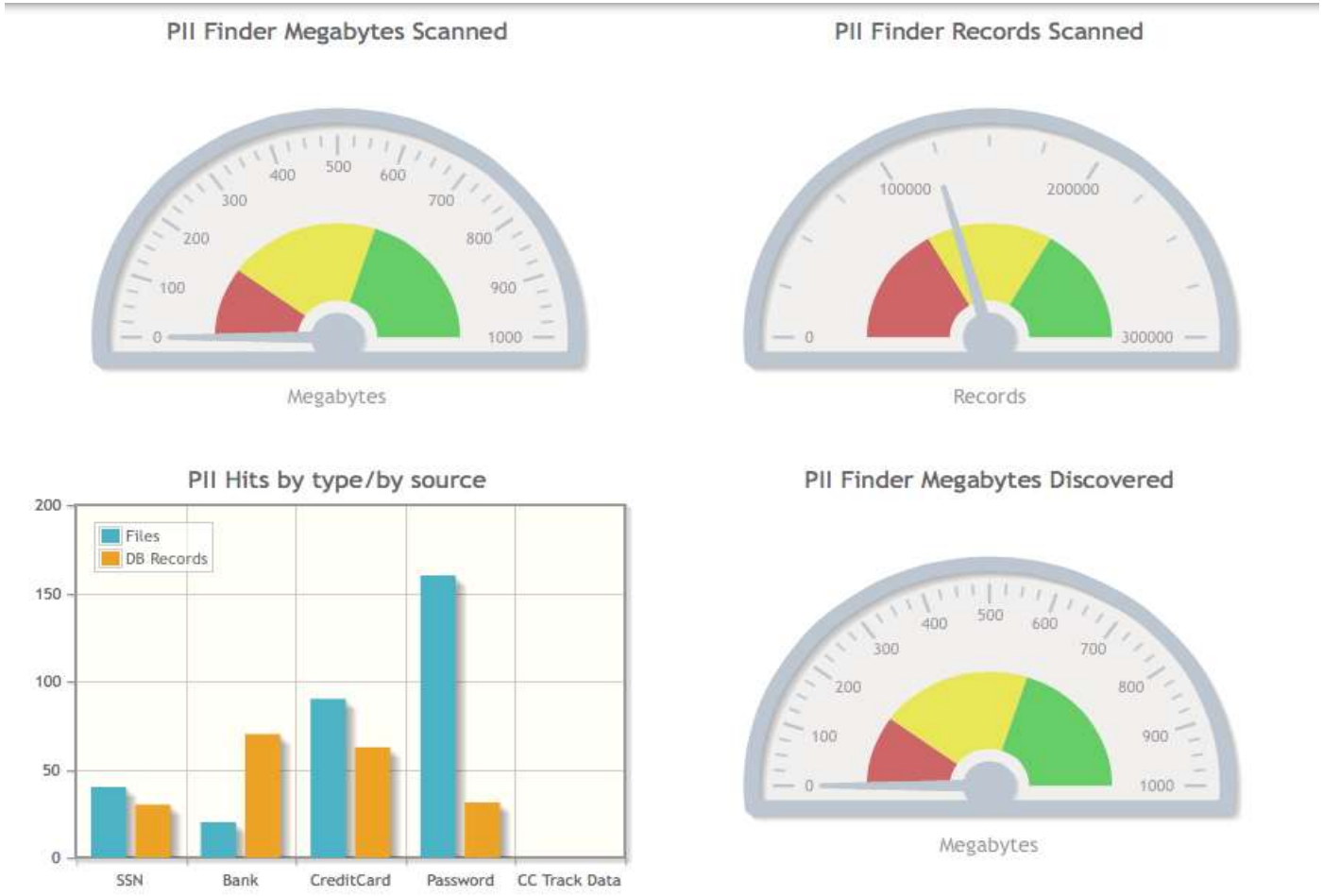
Discovery Deployment Example



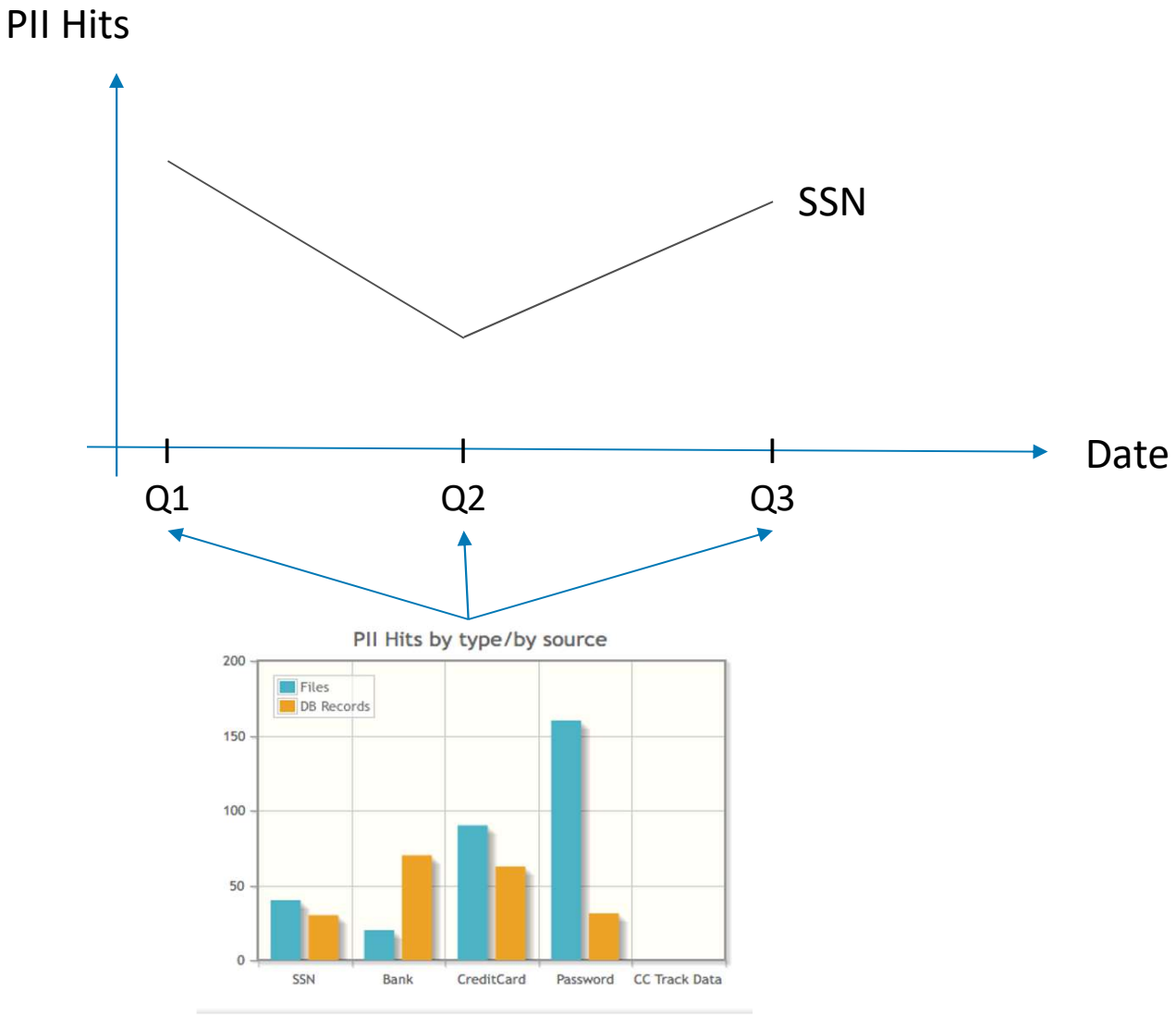
Example of Customer Provisioning:

- Virtual host to load Software or Appliance
- User ID with “Read Only” Access
- Firewall Access

Report Example



PII Hits Over Time - Metrics



PCI DSS 3.2 – Security Control Failures

PCI DSS 3.2 include 10.8 and 10.8.1 that outline that service providers need to detect and **report on failures of critical security control** systems.

PCI Security Standards Council CTO Troy Leach explained

- "without formal processes to detect and alert to critical security control failures as soon as possible, the window of time grows that **allows attackers to identify a way to compromise the systems and steal sensitive data** from the cardholder data environment."
- "While this is a new requirement only for service providers, we **encourage all organizations to evaluate the merit of this control** for their unique environment and adopt as good security hygiene."

You may have a Blind Spot during an Attack

How do you know that all the agents are up and running and delivering critical SIEM data after all configurations changes you have done over the years?

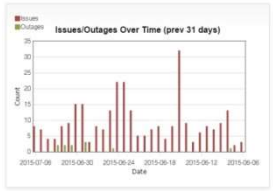
Or you may have a blind spot potentially during an attack. Will this impact your compliance posture?

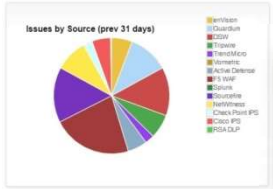
Are you paying licenses for agents that are not working?

Please look at the LinkedIn group “Managing Security Control Systems” at https://www.linkedin.com/groups/8559877

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

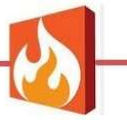
Example - Report on Failures of Critical Security controls



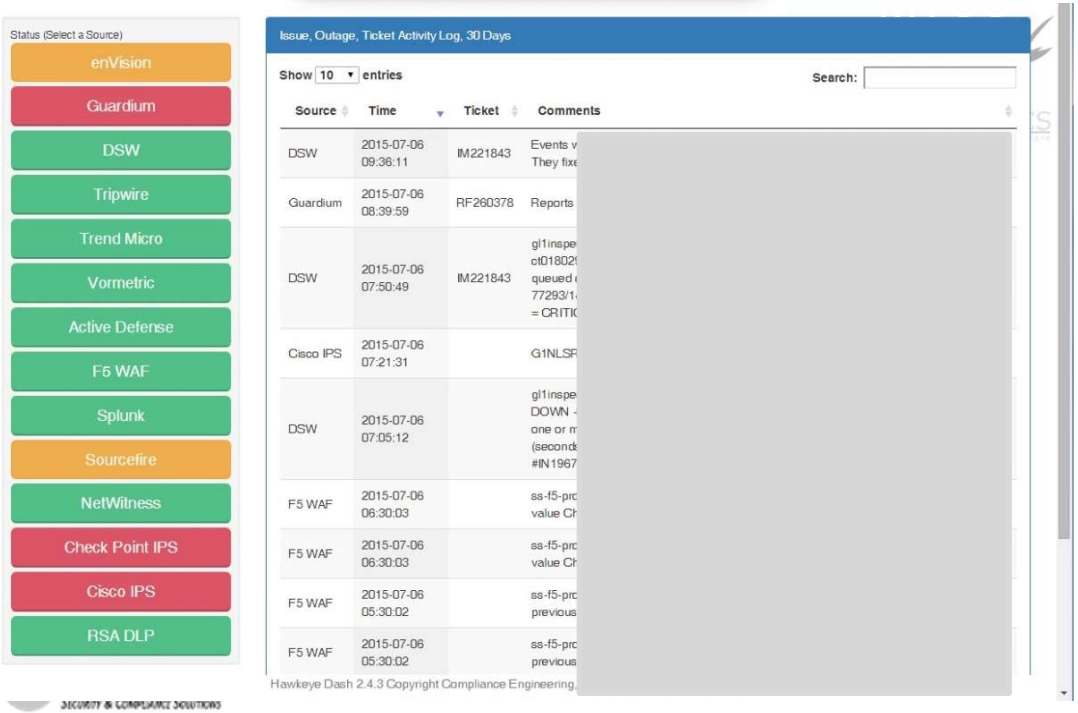


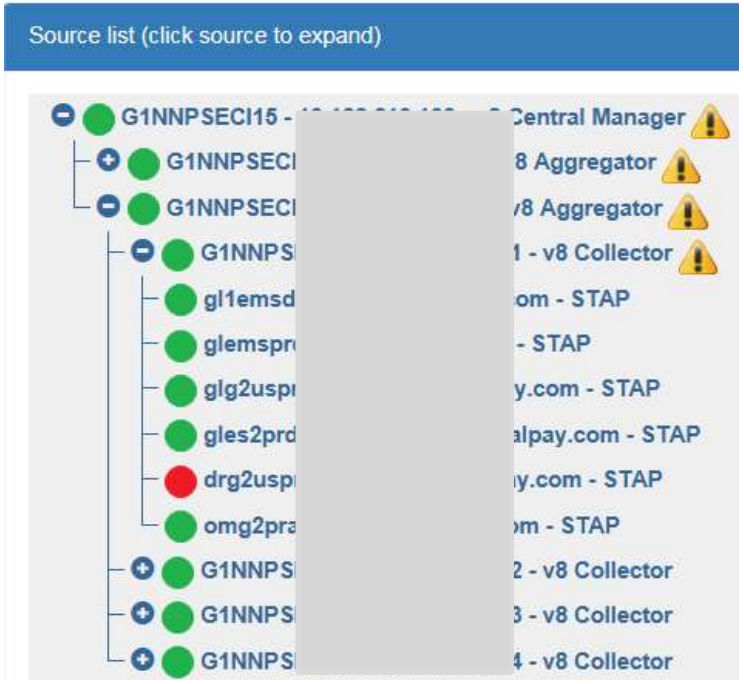
Management

Environment

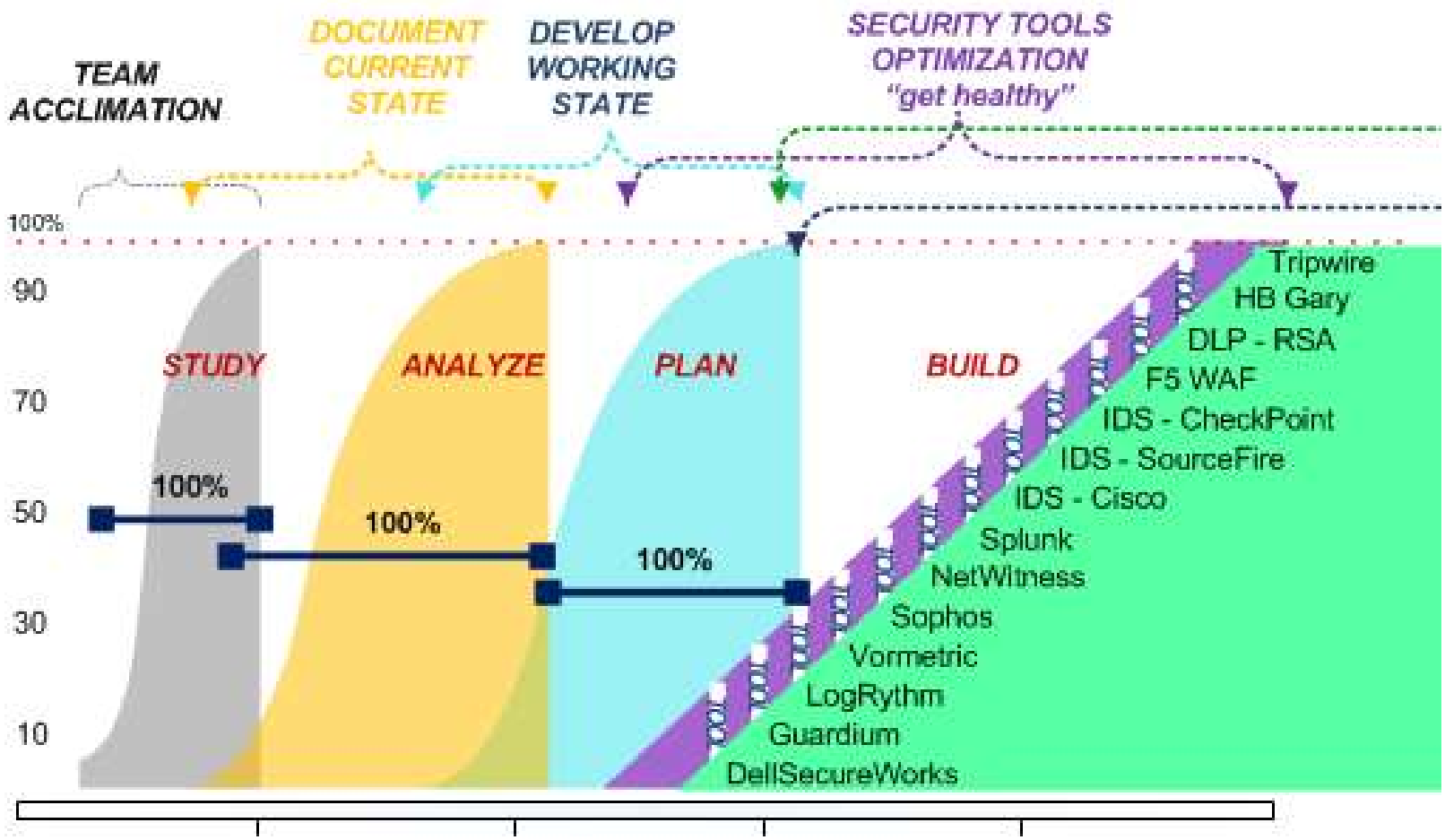


API

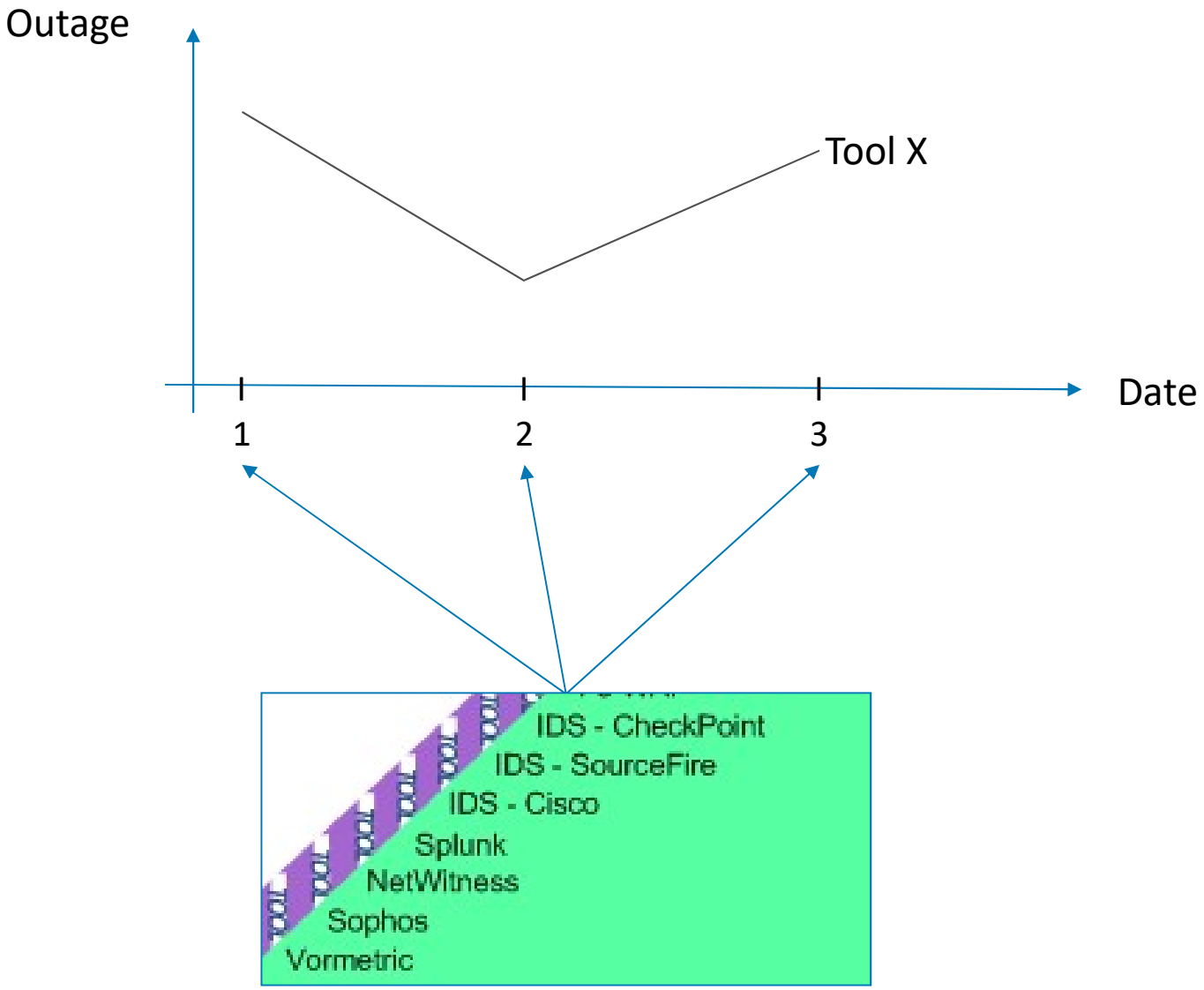




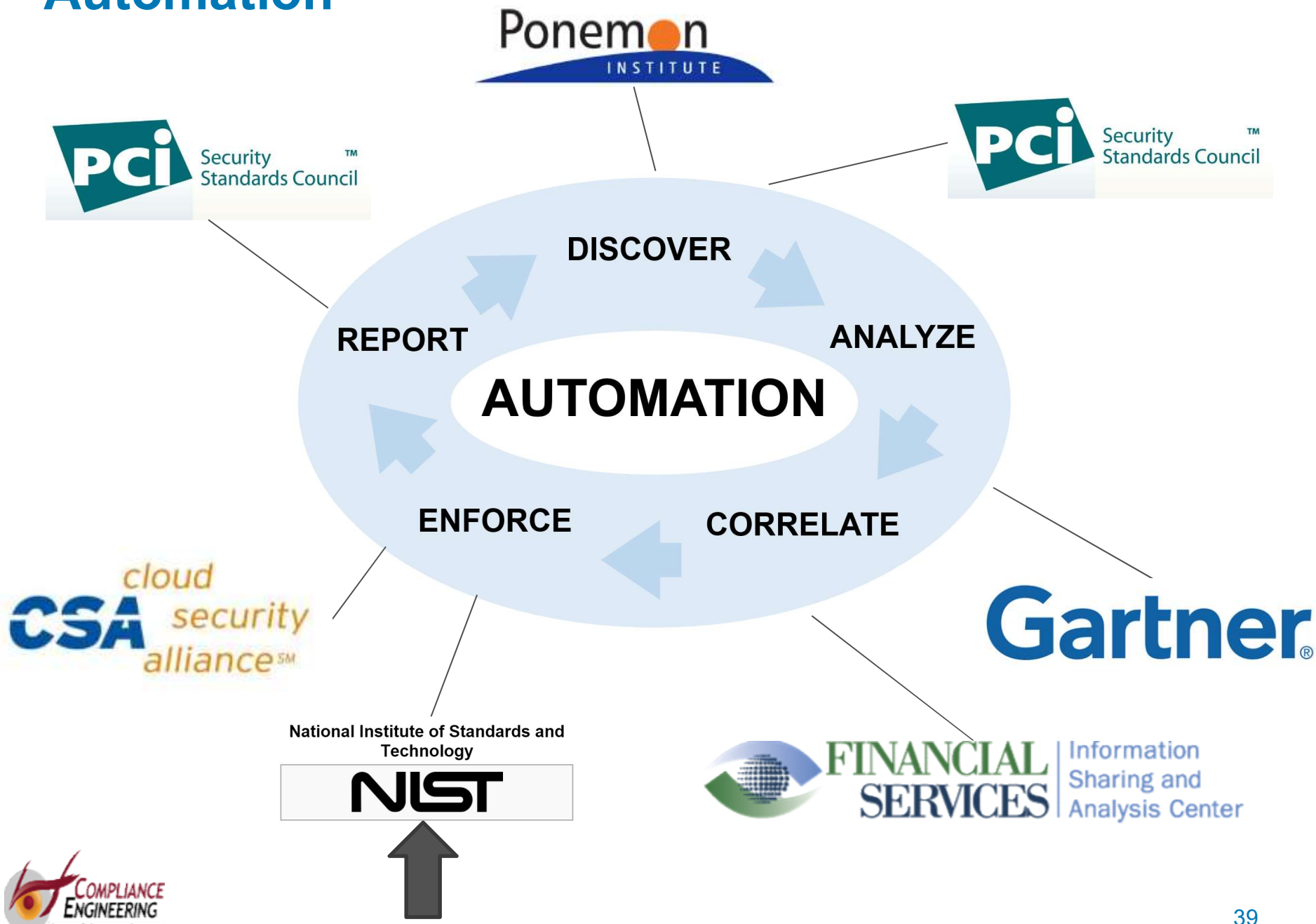
Managed Tools Security Services - Example



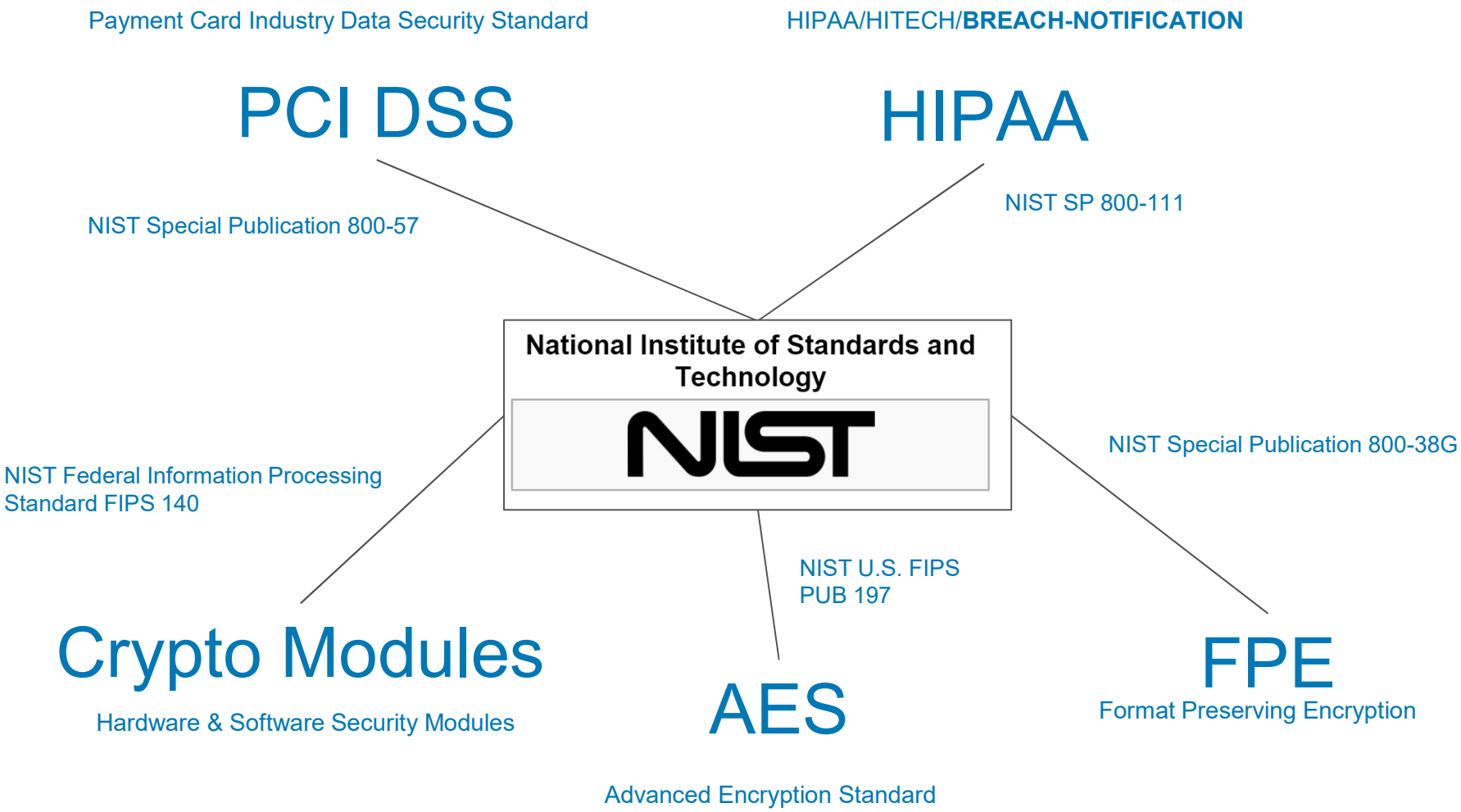
Managed Tools Security Services - Metrics



Automation


Ponemon INSTITUTE
PCI Security Standards Council
PCI Security Standards Council
DISCOVER
ANALYZE
CORRELATE
ENFORCE
REPORT
AUTOMATION
cloud security alliance
CSA
Gartner
National Institute of Standards and Technology
NIST
FINANCIAL SERVICES Information Sharing and Analysis Center
COMPLIANCE ENGINEERING

NIST - Increasing Relevance



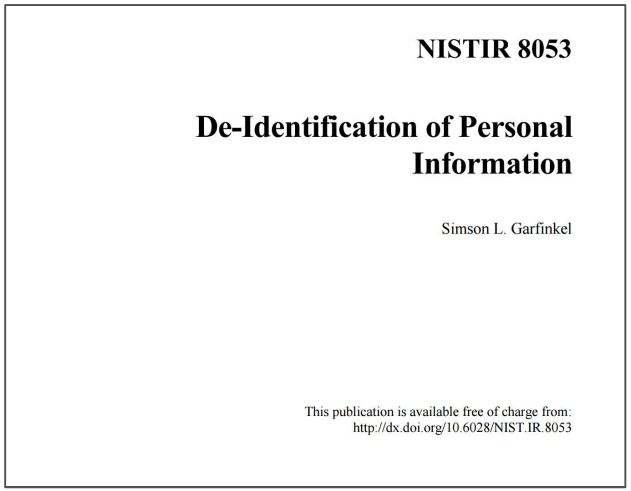
Need for Masking Standards

Many of the current techniques and procedures in use, such as the HIPAA Privacy Rule's Safe Harbor de-identification standard, are **not firmly rooted in theory**.

There are **no widely accepted standards** for testing the effectiveness of a de-identification process or gauging the utility lost as a result of de-identification.

National Institute of Standards and Technology

NIST



NISTIR 8053

De-Identification of Personal Information

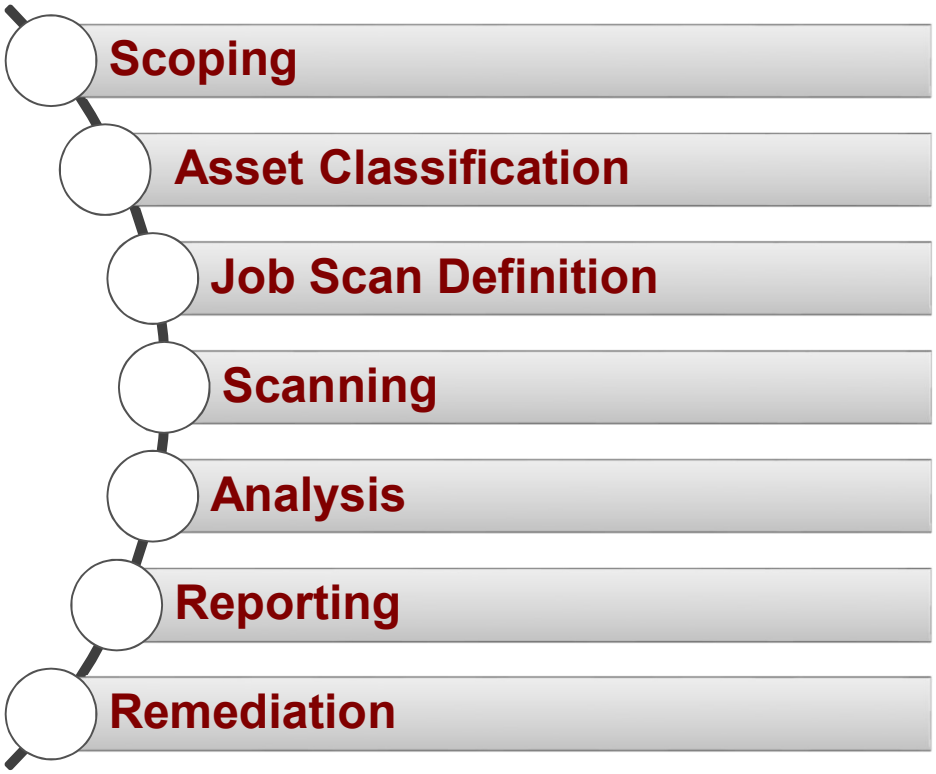
Simson L. Garfinkel

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8053

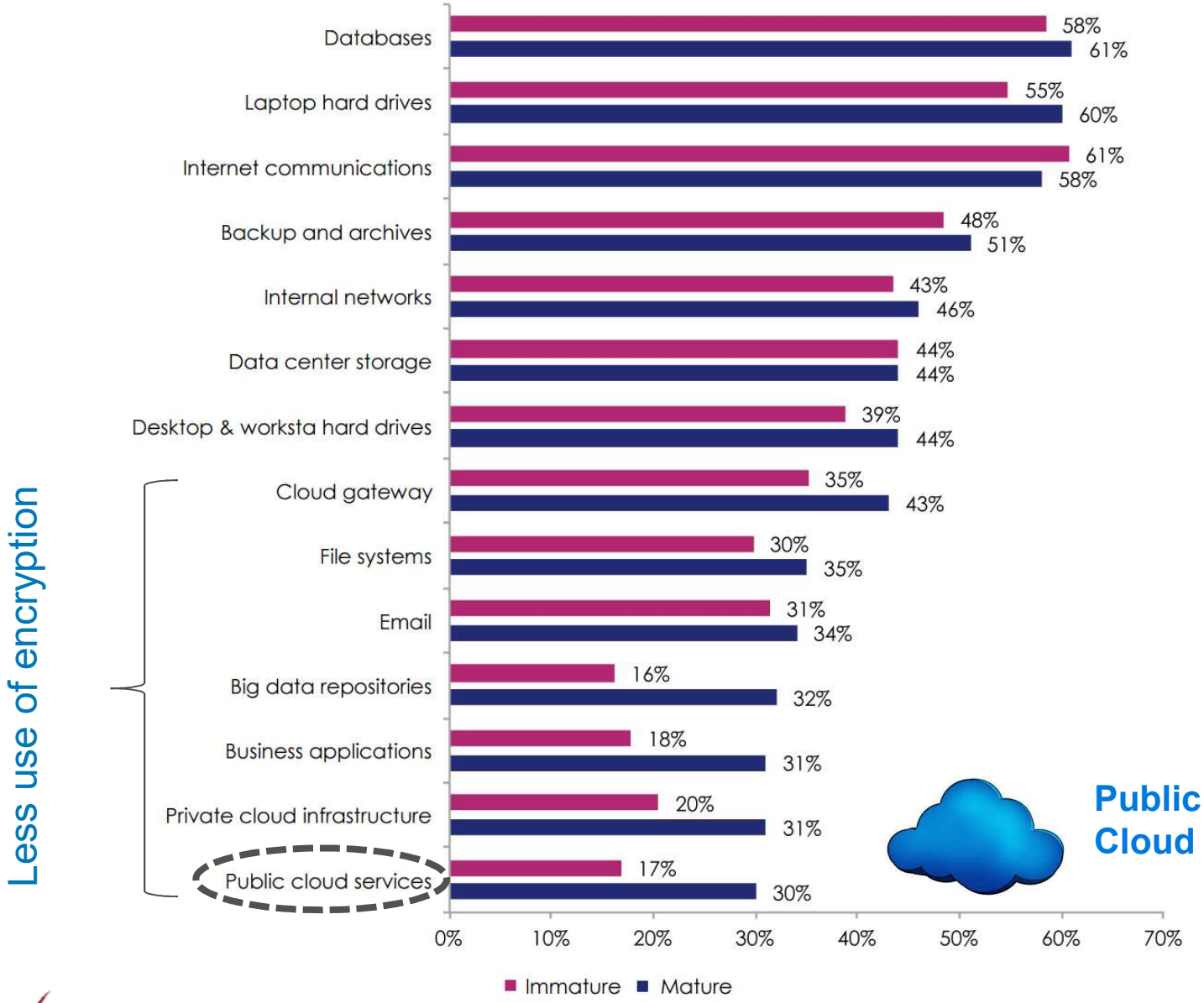
COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

PCI DSS 3.2 Requirement - Discovery

Example of A Discovery Process



Encryption Usage - Mature vs. Immature Companies



Source: Ponemon - Encryption Application Trends Study • June 2016

Data-Centric Protection Increases Security

- Rather than making the protection platform based, the **security is applied directly to the data**, protecting it **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

Cloud Providers Not Becoming Security Vendors

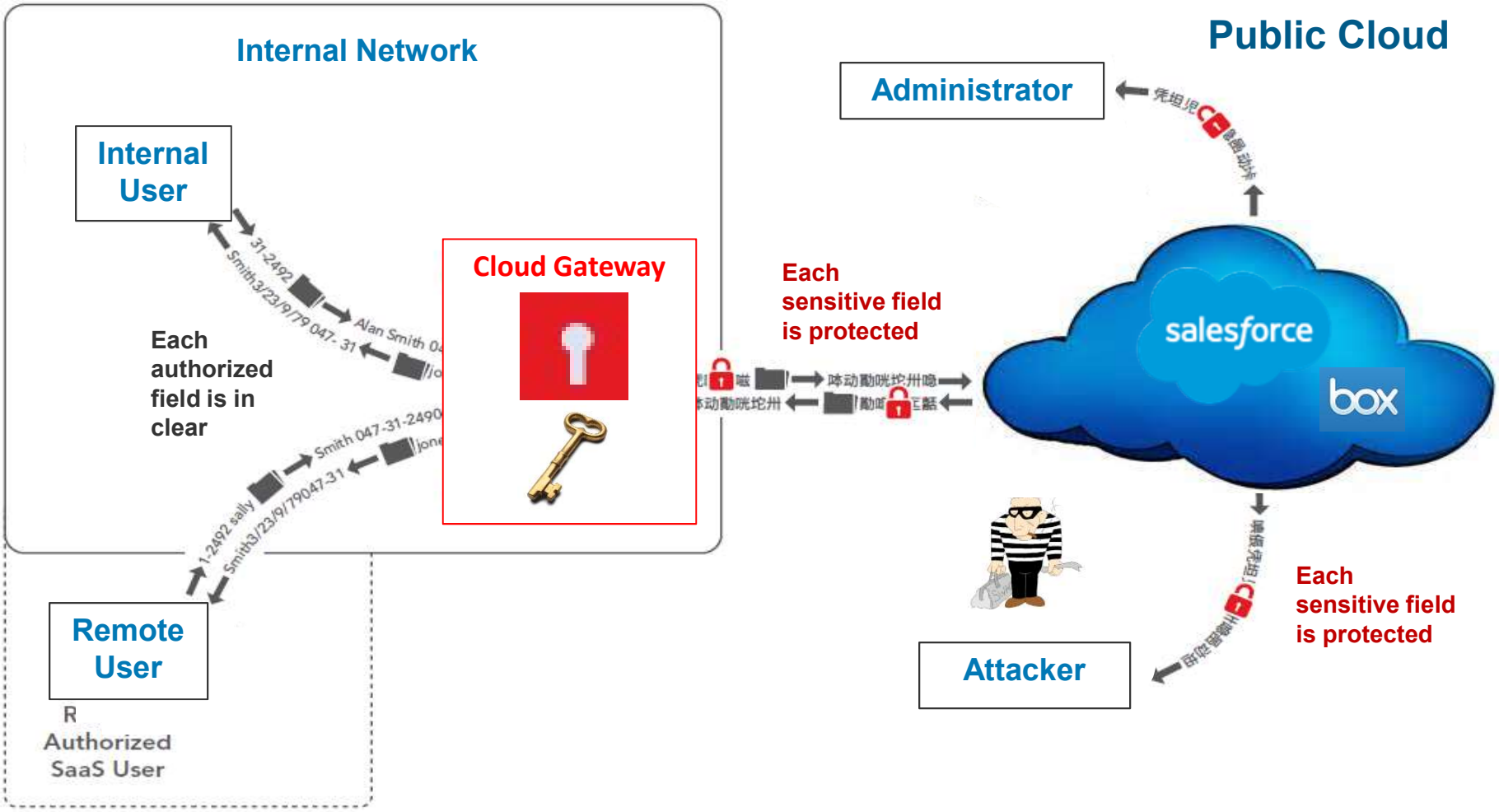
- There is great demand for security providers that can offer orchestration of security policy and controls that span not just multicloud environments but also **extend to on-premises infrastructure**
- Customers are starting to realize that the responsibility for mitigating **risks associated with user behavior lies with them and not the CSP** — driving them to evaluate a strategy that allows for incident detection, response and remediation capabilities in cloud environments

Source: Gartner: Market Trends: Are Cloud Providers Becoming Security Vendors? , May 2016

Gartner®

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Protect Sensitive Cloud Data - Example



Data Security Agents, including encryption, tokenization or masking of fields or files (at transit and rest)

Cloud Providers Not Becoming Security Vendors

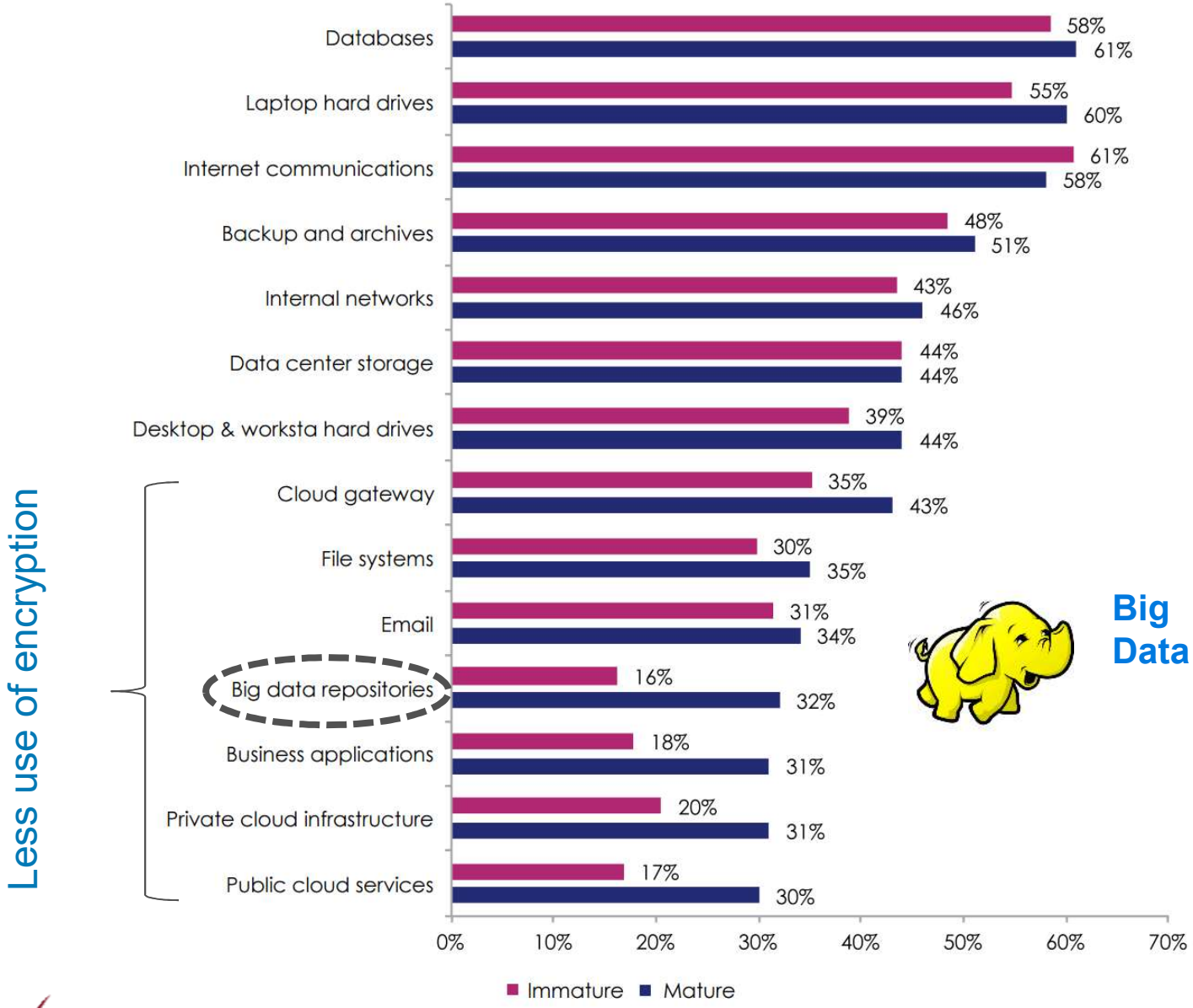
- There is great demand for security providers that can offer orchestration of security policy and controls that span not just multicloud environments but also **extend to on-premises infrastructure**
- Customers are starting to realize that the responsibility for mitigating **risks associated with user behavior lies with them and not the CSP** — driving them to evaluate a strategy that allows for incident detection, response and remediation capabilities in cloud environments

Source: Gartner: Market Trends: Are Cloud Providers Becoming Security Vendors? , May 2016

Gartner®

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Encryption Usage - Mature vs. Immature Companies

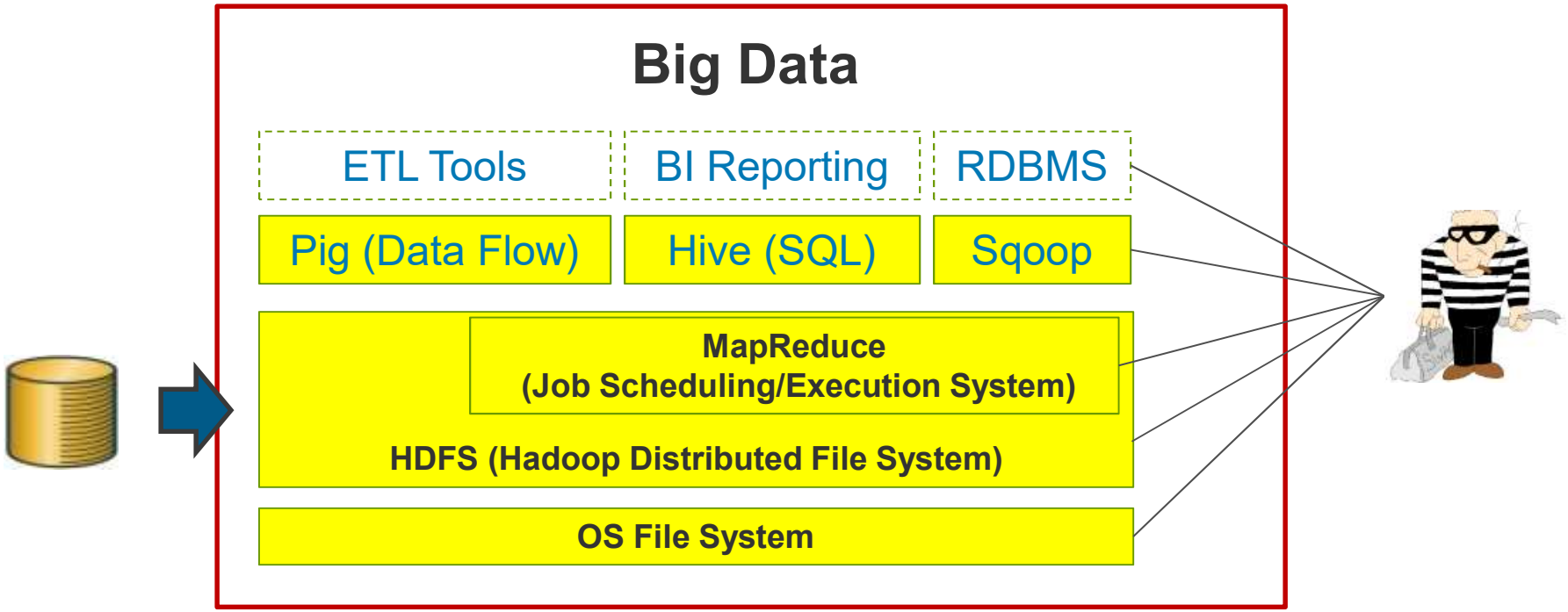


Ponemon INSTITUTE

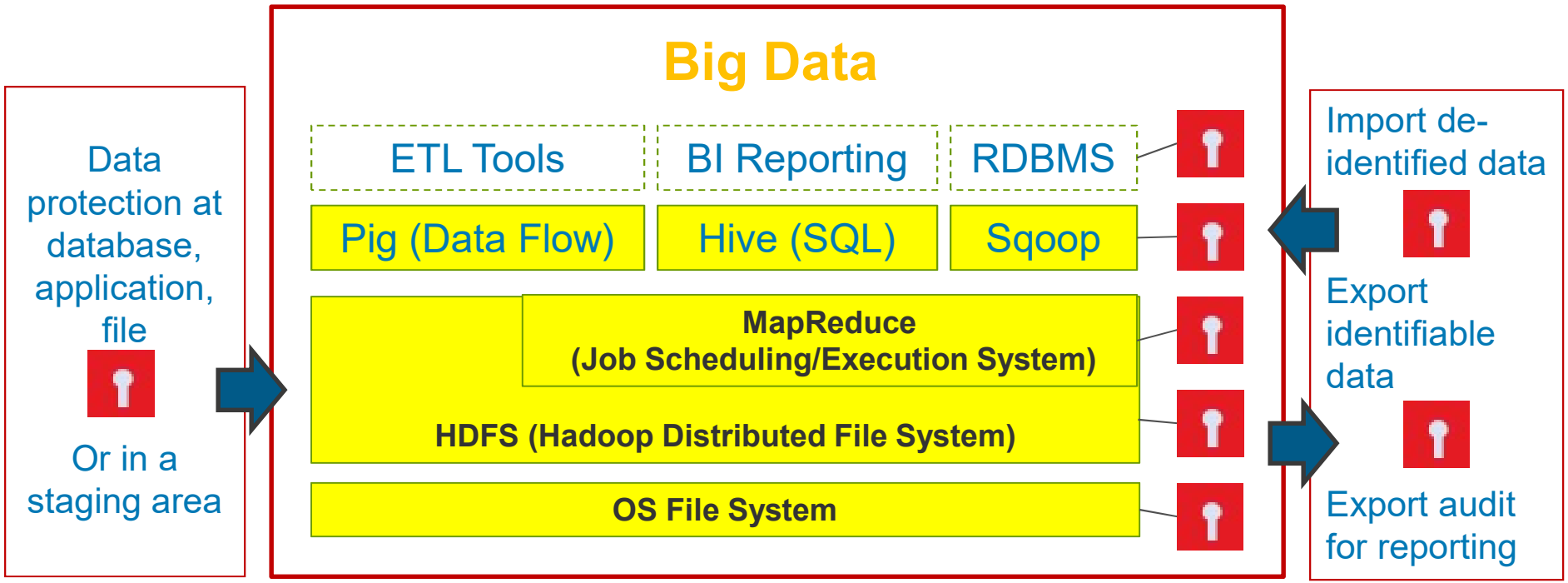
Big Data

Source: Ponemon - Encryption Application Trends Study • June 2016

Attacking Big Data



Securing Big Data – Examples of Security Agents

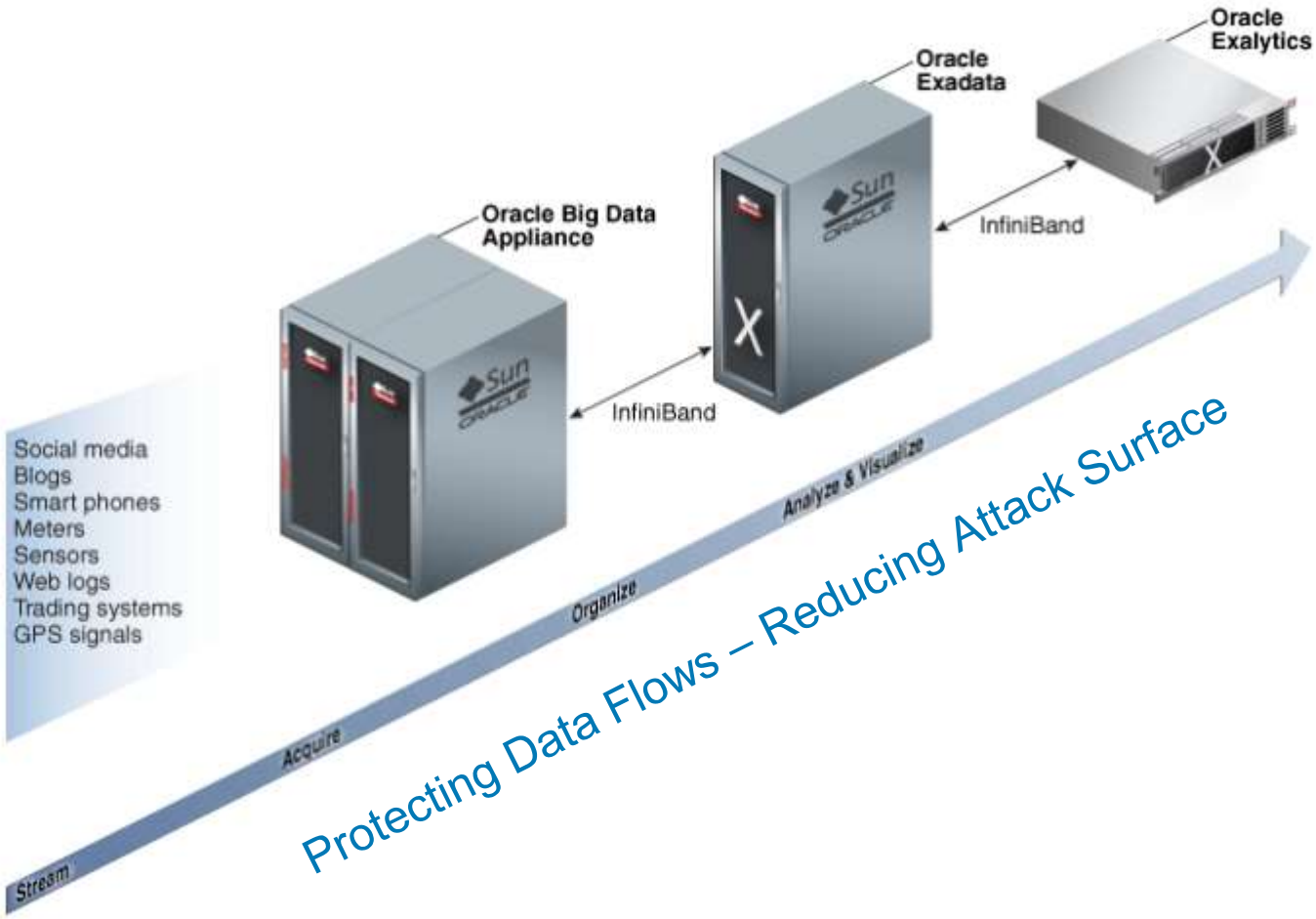


Data Security Agents, including encryption, tokenization or masking of fields or files (at transit and rest)

Oracle's Big Data Platform

123456 123456 1234

123456 999999 1234



COMPLIANCE ENGINEERING
Security & Compliance Solutions

CE Core Services

Compliance Assessments 10%

- PCI DSS & PA Gap
- HIPAA (2013 HITECH)
- SSAE 16-SOC 2&3*
- GLBA
- SOX
- FCRA
- FISMA
- SB 1385
- *ISO 27XXX*
- Security Posture Assessments (based on industry best practices)
- Internal compliance guidelines for suppliers or business partners
- BCP & DRP (SMB market)

Professional Security Services 30%

- Security Architecture
- Engineering/Operations
- Staff Augmentation
- Penetration Testing
  - Application Security and Secure Code SDLC
  - "Rugged Ops"
- Platform Baseline Hardening (M/F, Unix, Teradata, i-Series, BYOD, Windows)
- *IDM/IAM/PAM architecture*
- SIEM design, operation and implementation
- *Security Technology Support 365 (2011)*
- *eGRC Readiness & Deployment*

CE Security & Vendor Products 20%

- *CE Hawkeye PIIFinder Standalone 2016*
- *HP, RSA, IBM, Cisco, Centrify, Gemalto, Vormetric, Sophos…*
- 50+ Leading Products
- Data Loss Protection
- SIEM & Logging
- Identity and Access Management
- EndPoint Protection
- Network Security Devices
- Encryption
- Unified Threat
- Multi-factor Authentication
- 2 Hosted Data Centers SMB

Managed Security Services 40%

- *CE Hawkeye PIIFinder Data Exposure / Discovery SaaS*
- *Security Tool Sprawl*

CE Hawkeye MTSS

(Managed Tools Security Service

MSSP/SOC "EoG" (2013 1st Qtr.)

- Hawkeye Vision Hosted SIEM 365
- Data Center SOC
- IDM/IAM Security Administration
- Hawkeye PCI SOC Advantage Program
- Managed Vulnerability Scans
- Managed Penetration Testing

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Benefits of Managed Tool Security Service

Security controls in place and functioning.

Prepared to address information security when it becomes a Boardroom Issue

Visibility to measure ROI

Confidence in reduced risk of data loss, damaged share price, stolen IP, etc.

CIO
CTO
CISO

Ability to produce a positive return on capital investments in tools.

Cost reduction in (people, licenses, maintenance, etc.)

Reduced risk of breach and associated costs (financial, reputational, regulatory losses)

COMPLIANCE ENGINEERING
SECURITY & COMPLIANCE SOLUTIONS

Thank you!
Questions?

Ulf Mattsson, Chief Technology Officer, Compliance Engineering
umattsson@complianceengineers.com
www.complianceengineers.com