

Data Protection, Security and Privacy Risks – On-premise & Cloud



Ulf Mattsson
ulf@ulfmattsson.com

Ulf Mattsson

- Previously Head of **Innovation** at TokenEx and **Chief Technology Officer** at Atlantic BT, Compliance Engineering, and Protegrity, and **IT Architect** at IBM
- Products and Services:**
 - Data Encryption, Tokenization, Data Discovery, Cloud Application Security Brokers (**CASB**), Web Application Firewalls (**WAF**), Robotics, and Applications
 - Security Operation Center (**SOC**), Managed Security Services (**MSSP**), and Security Benchmarking/Gap-analysis for Financial Industry
- Inventor** of more than 70 issued US Patents and developed **Industry Standards** with ANSI X9 and PCI SSC

Quantum Computing Risk Study
Informative Report

Approved American National Standard
ANSI
American National Standard
for Financial Services
ANSI X9.141–2020
Financial Services
Data Security Breach
Part 1: Data Protection

Approved American National Standard
ANSI
Payment Card Data —
Part 1: Using Encryption Methods

Approved American National Standard
ANSI
Payment Card Data —
Part 2: Implementing Post-Authorization
Tokenization Systems

Approved American National Standard
ANSI
Format-Preserving Encryption – Part 4

Accredited Standards Committee X9 Inc.
Financial Industry Standards
A Technical Accredited Financial Institution

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY
Dec 2019
Data Security: On Premise or in the Cloud
By Ulf Mattsson – ISSA member, New York Chapter

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY
May 2020
Data Privacy: De-Identification Techniques
By Ulf Mattsson – ISSA member, New York Chapter

This article discusses emerging data privacy techniques, standards, and examples of applications implementing different use cases of de-identification techniques. We will discuss different attack scenarios and practical balances between privacy requirements and operational requirements.

Abstract
The data privacy landscape is changing. There is a need for privacy models in the current landscape of the increasing numbers of privacy regulations and privacy breaches. Privacy methods use models and it is important to have

EU GDPR
Sweden. The Data Act, a national data protection law, went into effect in 2018.
1970, Germany passed the first national data protection law, first data protection law in the world.
The New York Privacy Act was introduced in 2019.
Brazil passing a comprehensive data protection regulation similar to GDPR.
GDPR's impact is expected to impact 12% of the world's population.



Payment Card Industry (PCI)
Security Standards Council (SSC):

1. Tokenization Task Force
2. Encryption Task Force, Point to Point Encryption Task
3. Risk Assessment SIG
4. eCommerce SIG
5. Cloud SIG, Virtualization SIG
6. Pre-Authorization SIG, Scoping SIG Working Group

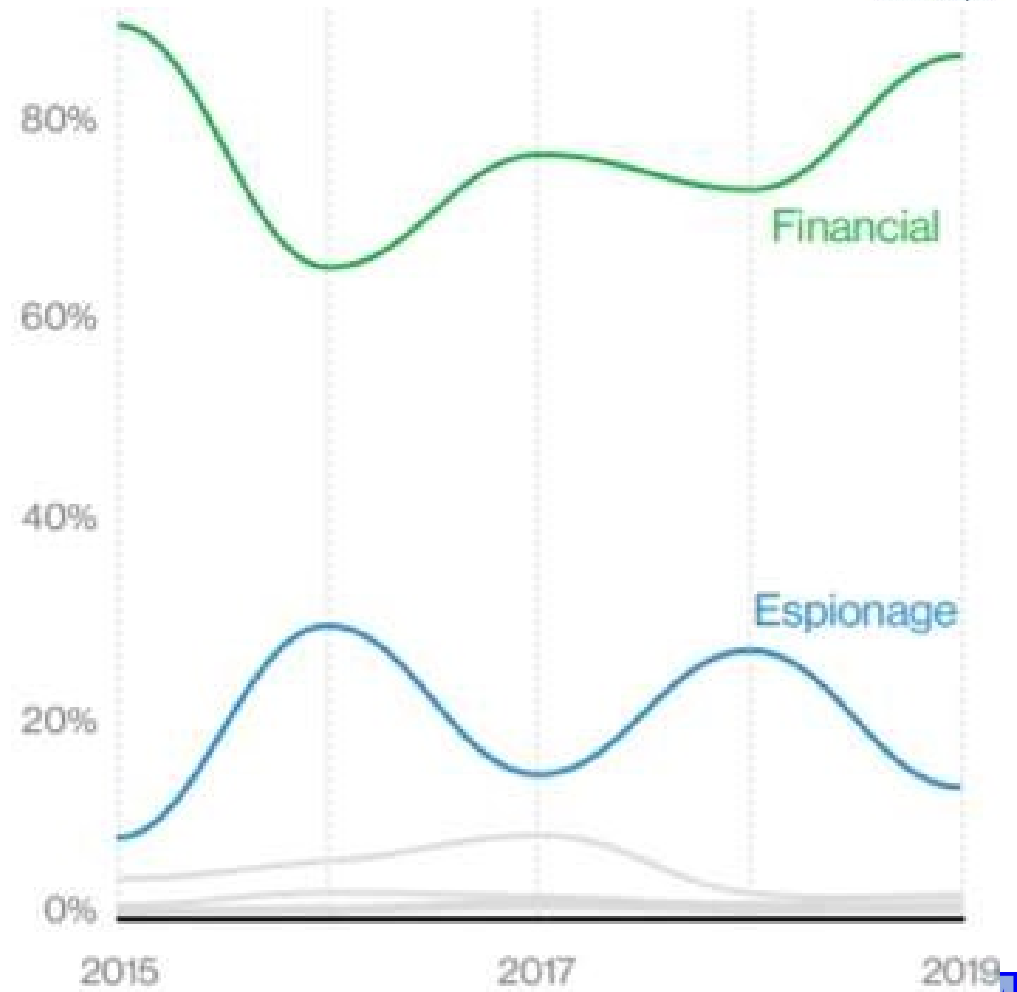
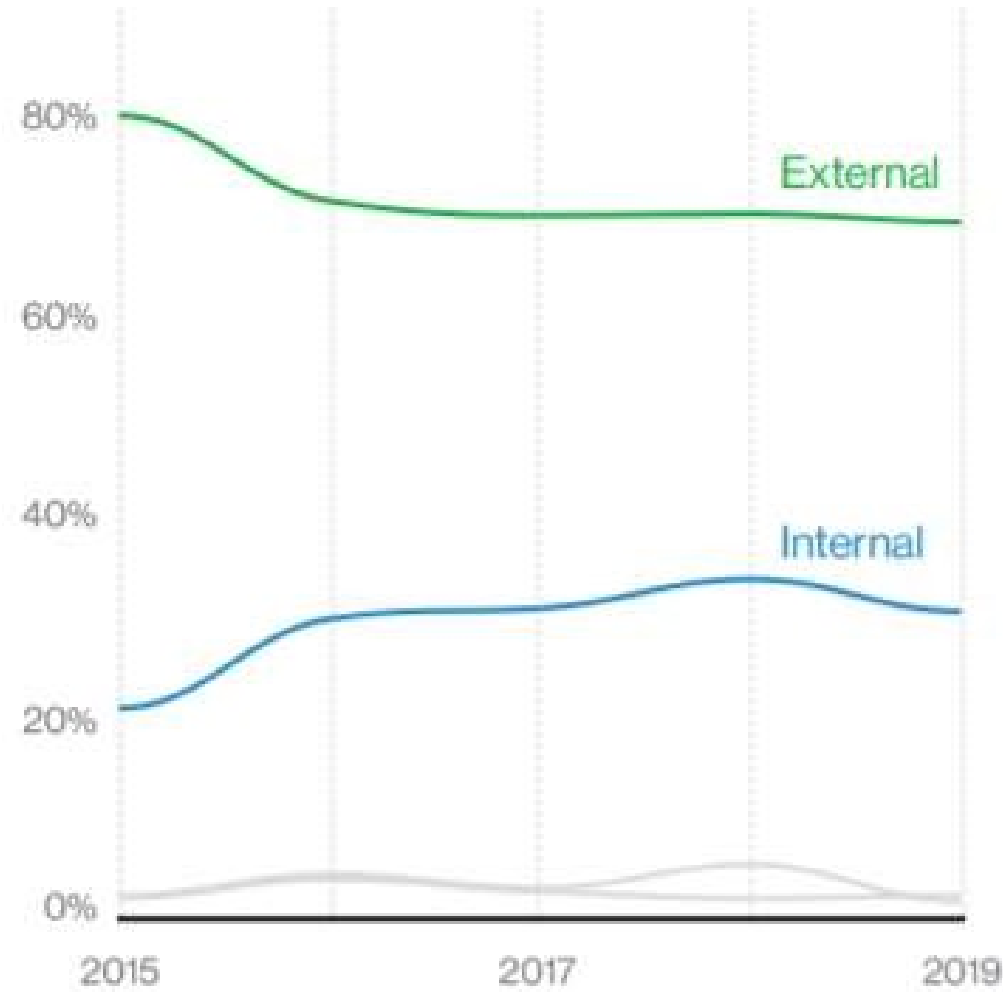
ISACA JOURNAL May 2020

Practical Data Security and Privacy for GDPR and CCPA

Author: Ulf Mattsson
Date Published: 13 May 2020

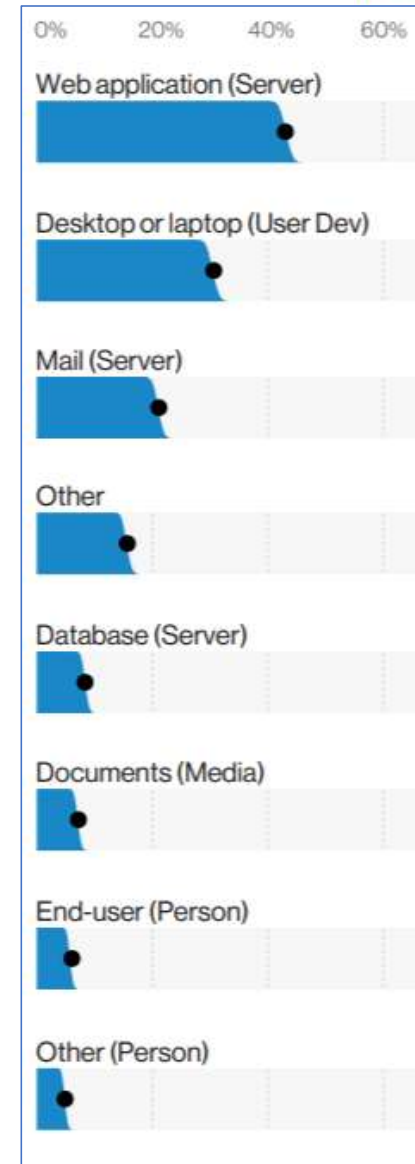
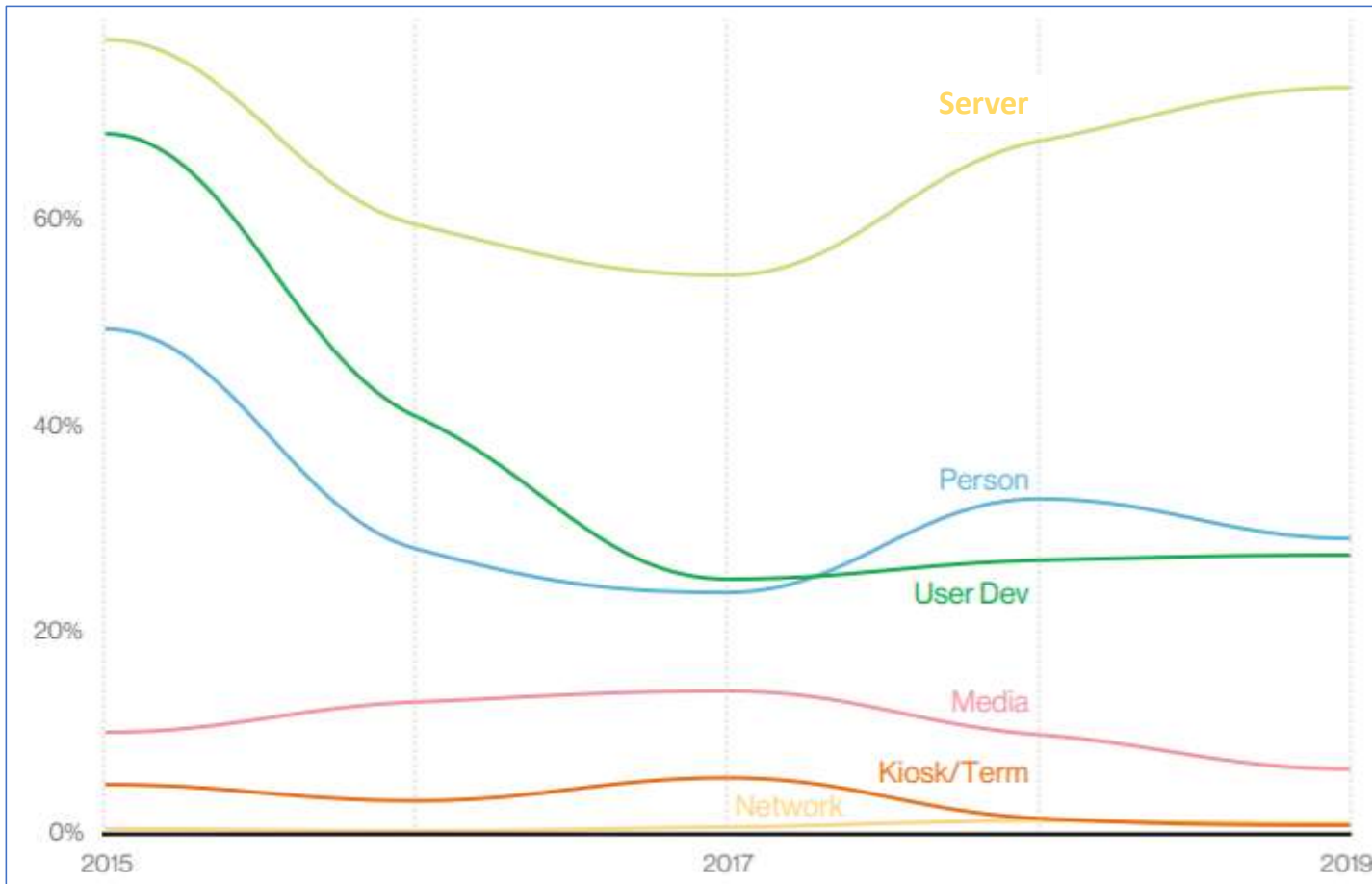
With sensitive data residing everywhere and the breach epidemic growing, the need for advanced data security solutions has become even more critical. Compliance with regulations such as the EU General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), US State California Consumer Privacy Act...

Actors in breaches

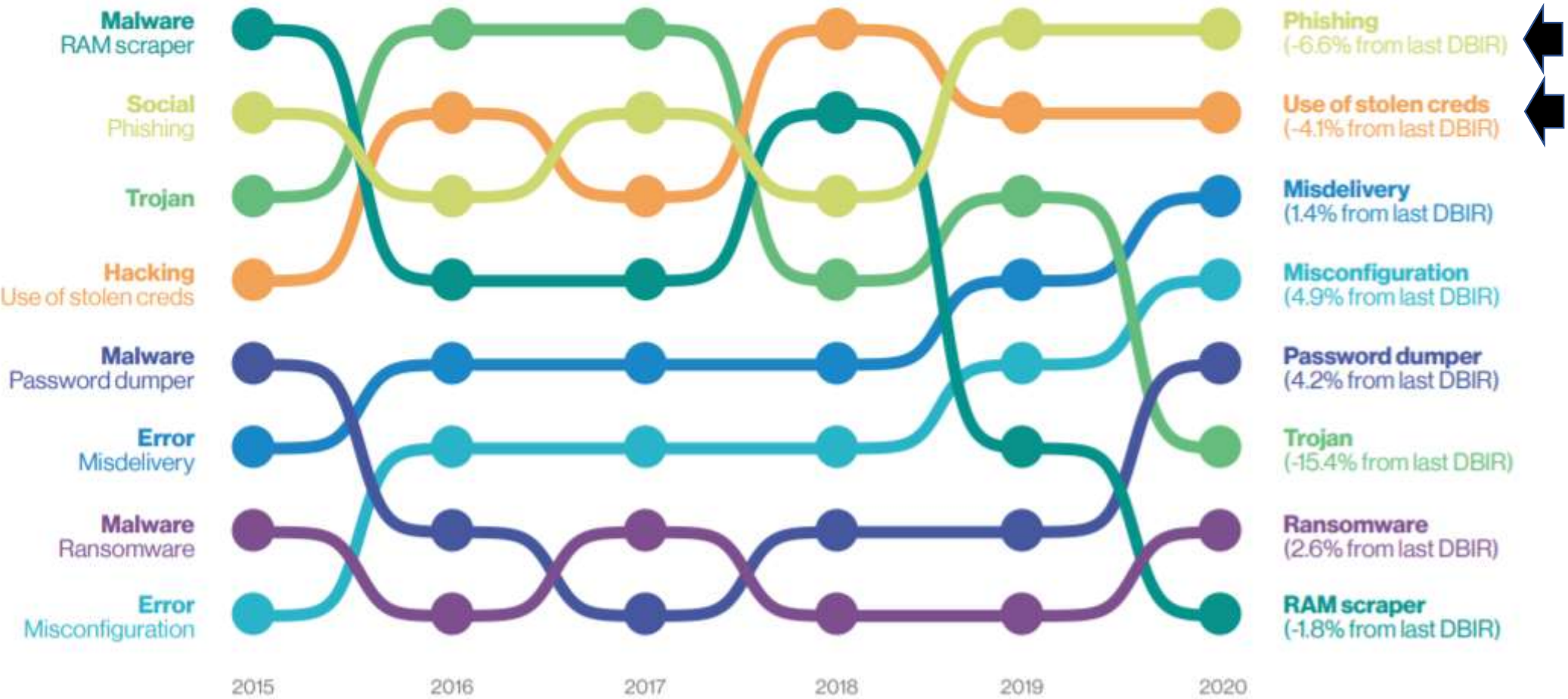


Assets in breaches

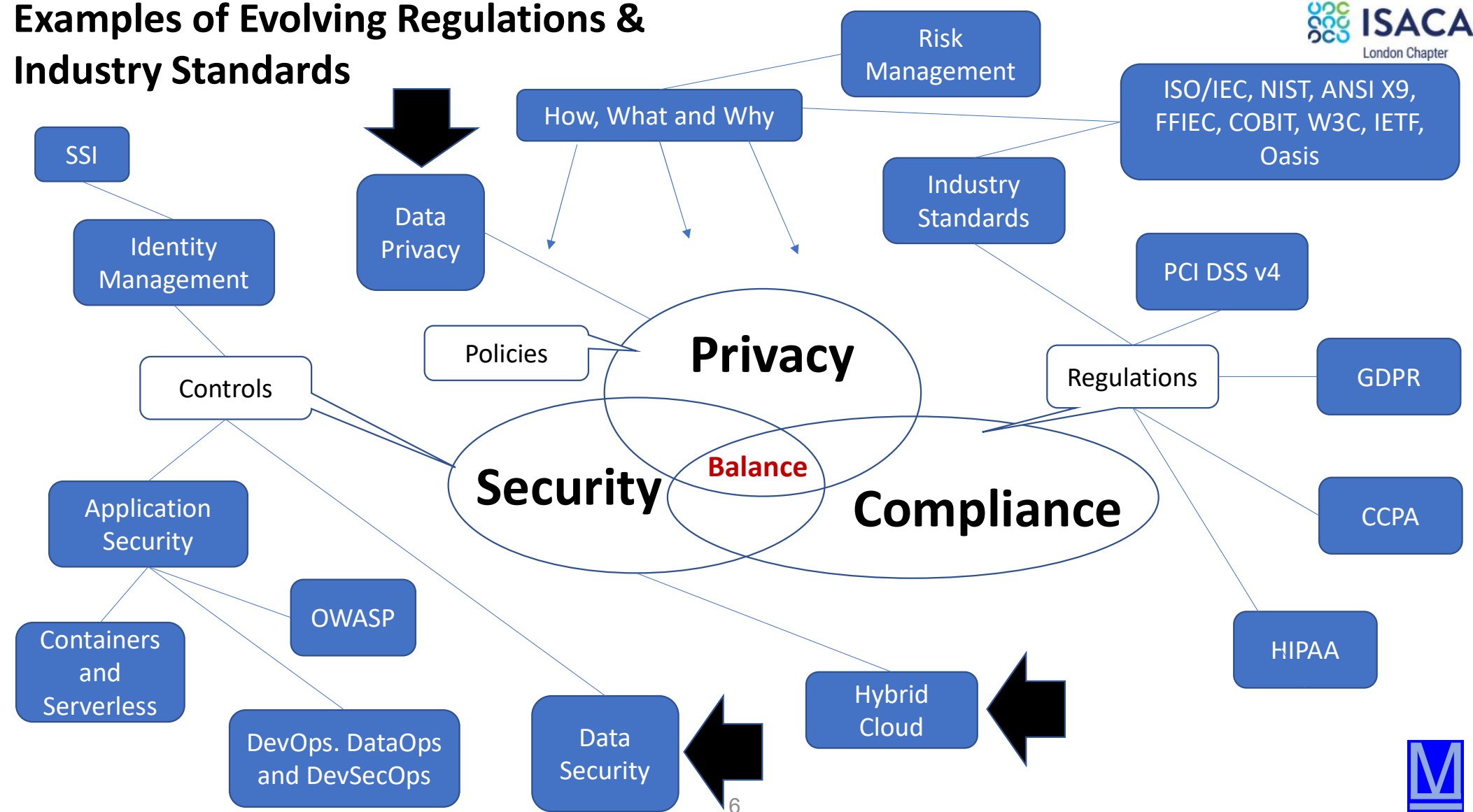
- **On-premises assets are still 70%** in our reported breaches dataset.
- **Cloud assets were involved in about 24% of breaches.**
 - **Email or web application server 73% of the time.**



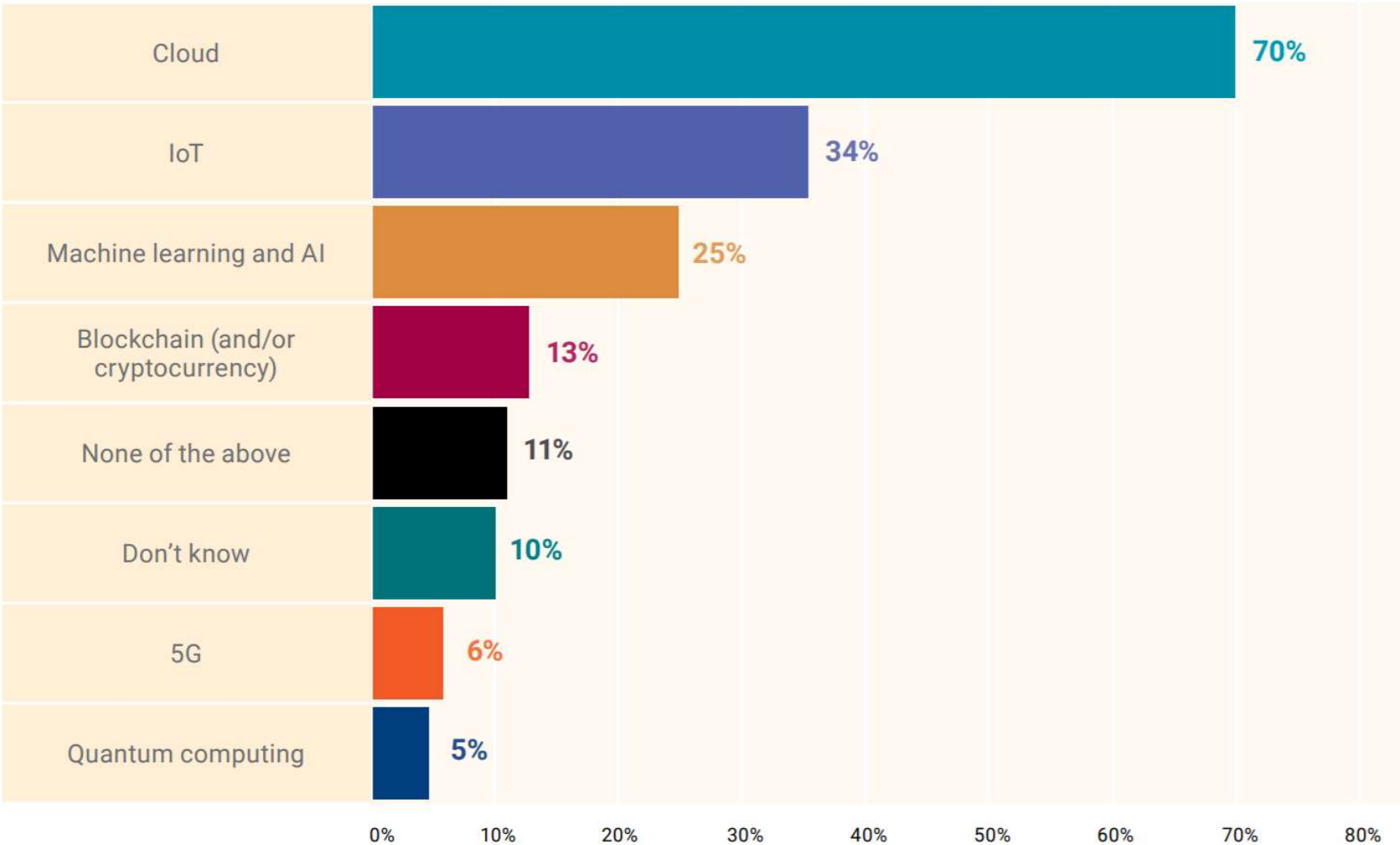
Action varieties in breaches



Examples of Evolving Regulations & Industry Standards

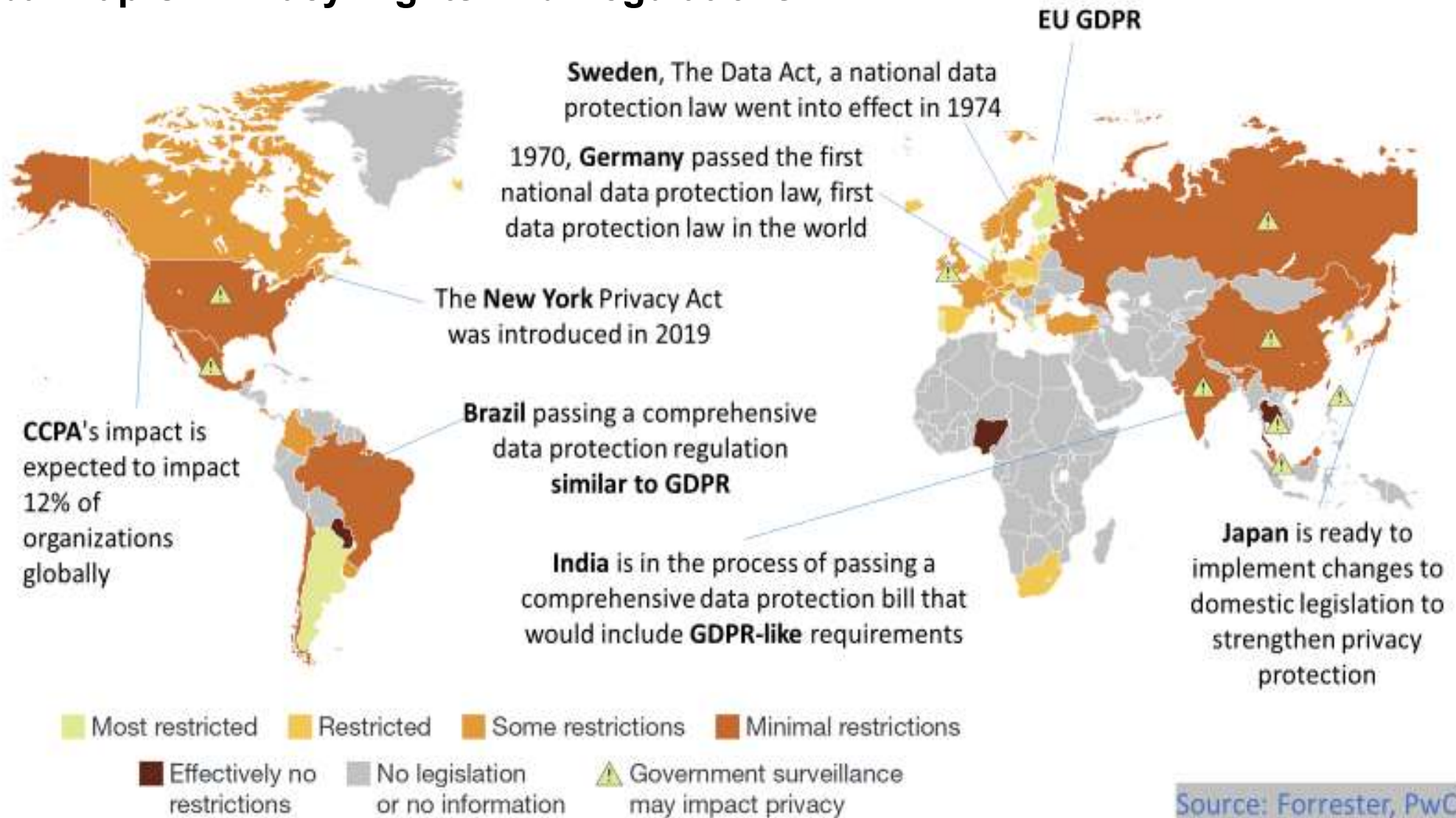


Emerging Technologies that Increase Risk



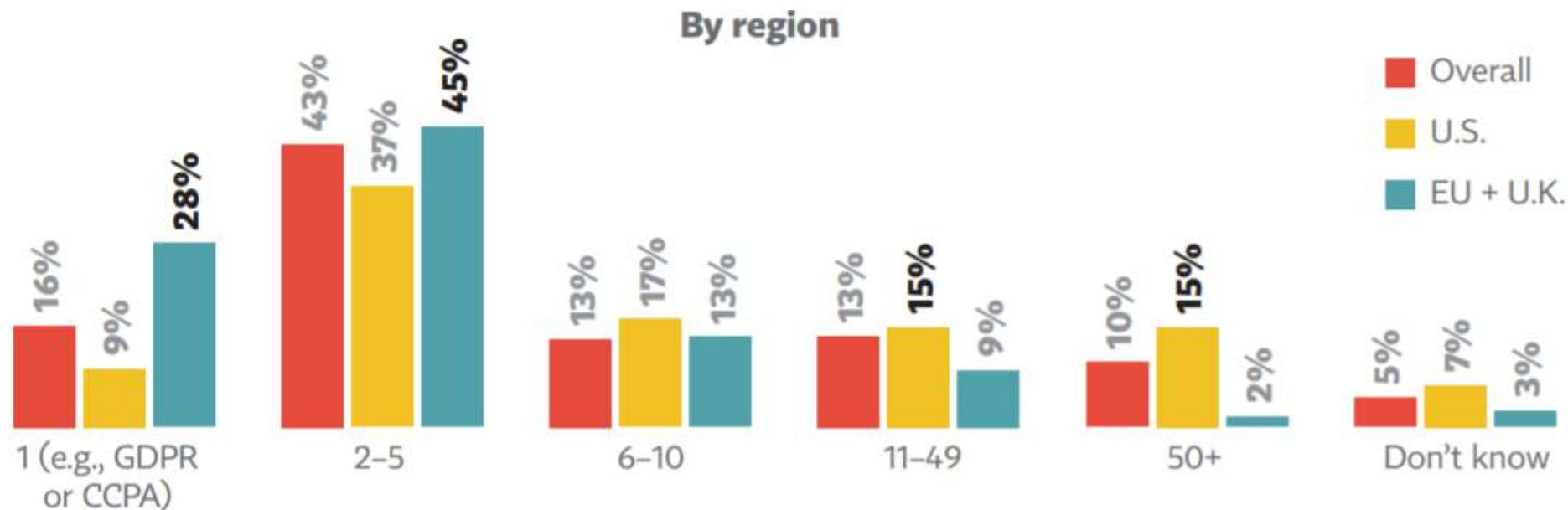
Source:
www.isaca.org

Global Map Of Privacy Rights And Regulations



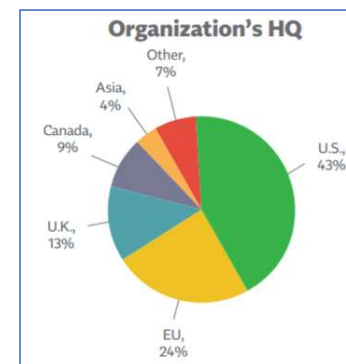
Source: Forrester, PwC

How many privacy laws are you complying with?



General Data Protection Regulation (EU) 2016/679 (**GDPR**) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.


California Consumer Privacy Act (**CCPA**) is a bill that enhances privacy rights and consumer protection for residents of California, United States.



Legal and regulatory risks are exploding



>600 Laws Globally



80 New Laws in 2019

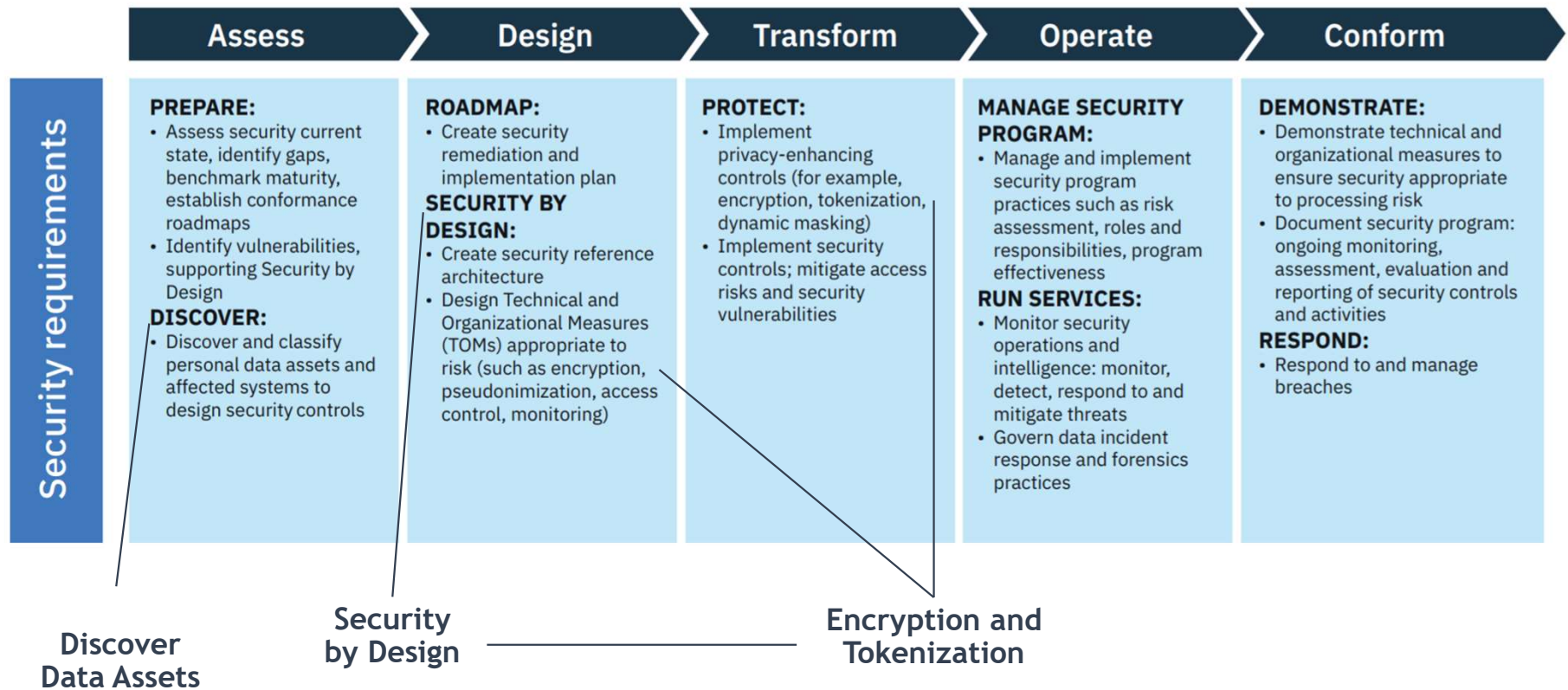


More Complex Rules

Category	North America	Latin America	EMEA	Asia Pacific	Totals
Comprehensive Data Protection		1	4	2	7
GDPR Implementation			9		9
Information Security	9		1	3	13
Health Privacy	4		2		6
Financial Privacy	5				5
Education Privacy	3				3
Breach	11	1			12
Privacy Rights	3	1		1	5
Other	8	1	9	2	20
Totals for 2019	43	4	25	8	80



GDPR Security Requirements – Encryption and Tokenization

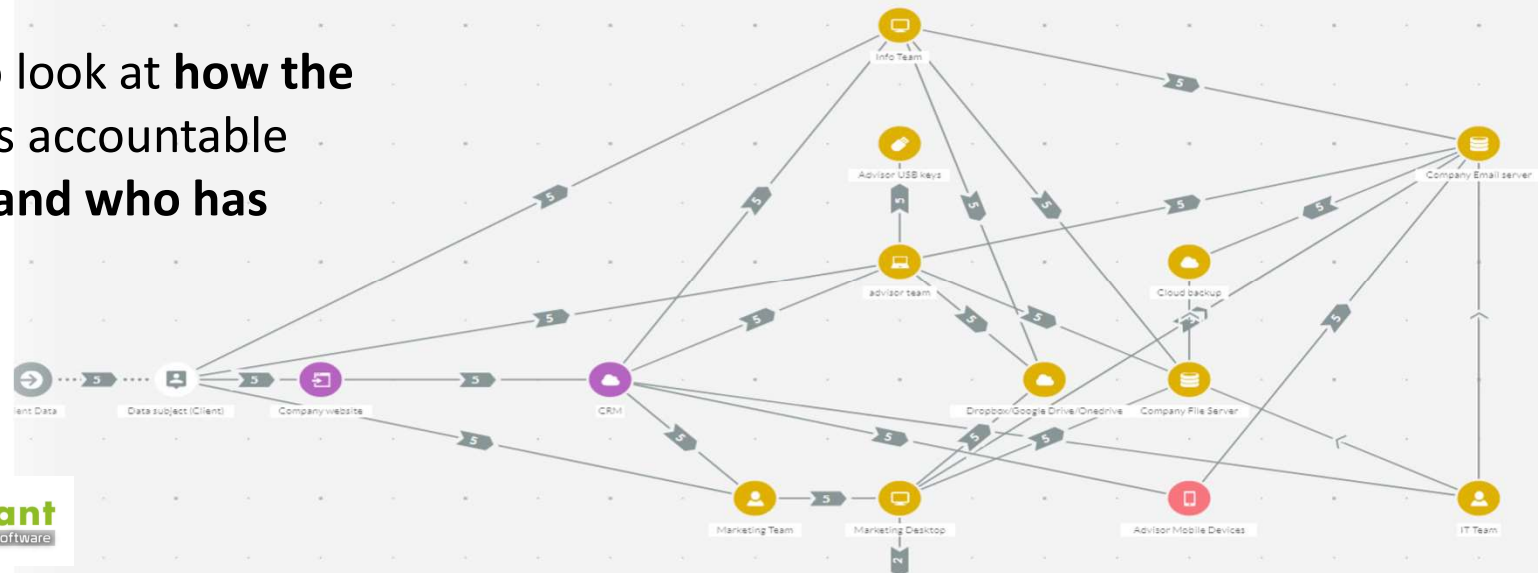


Data flow mapping under GDPR

- If there is not already a **documented workflow** in place in your organisation, it can be worthwhile for a team to be sent out to identify how the data is being gathered.
- This will enable you to see how your **data flow is different from reality** and **what needs to be done to amend this**.

If an organisation's theory about how its **data is flowing is different from the reality**, you **have a breach and could be fined**.

The organisation needs to look at **how the data was captured**, who is accountable for it, **where it is located** and **who has access**.



Scan Result

Source: BigID

 **26.47K** Pii Records Found

 **59** Query Risk Score

Summary

Geographic visualization of data location and flow for the DPO/CPO/CISO/CDO

Summary risk score based on parameters company tracks both aggregate and based on search (ie query)

Identities

data monitored

☆ TOP 5

 **3811**

Attributes

discovered

☆ TOP 5

 **4**

Systems

storing personal information

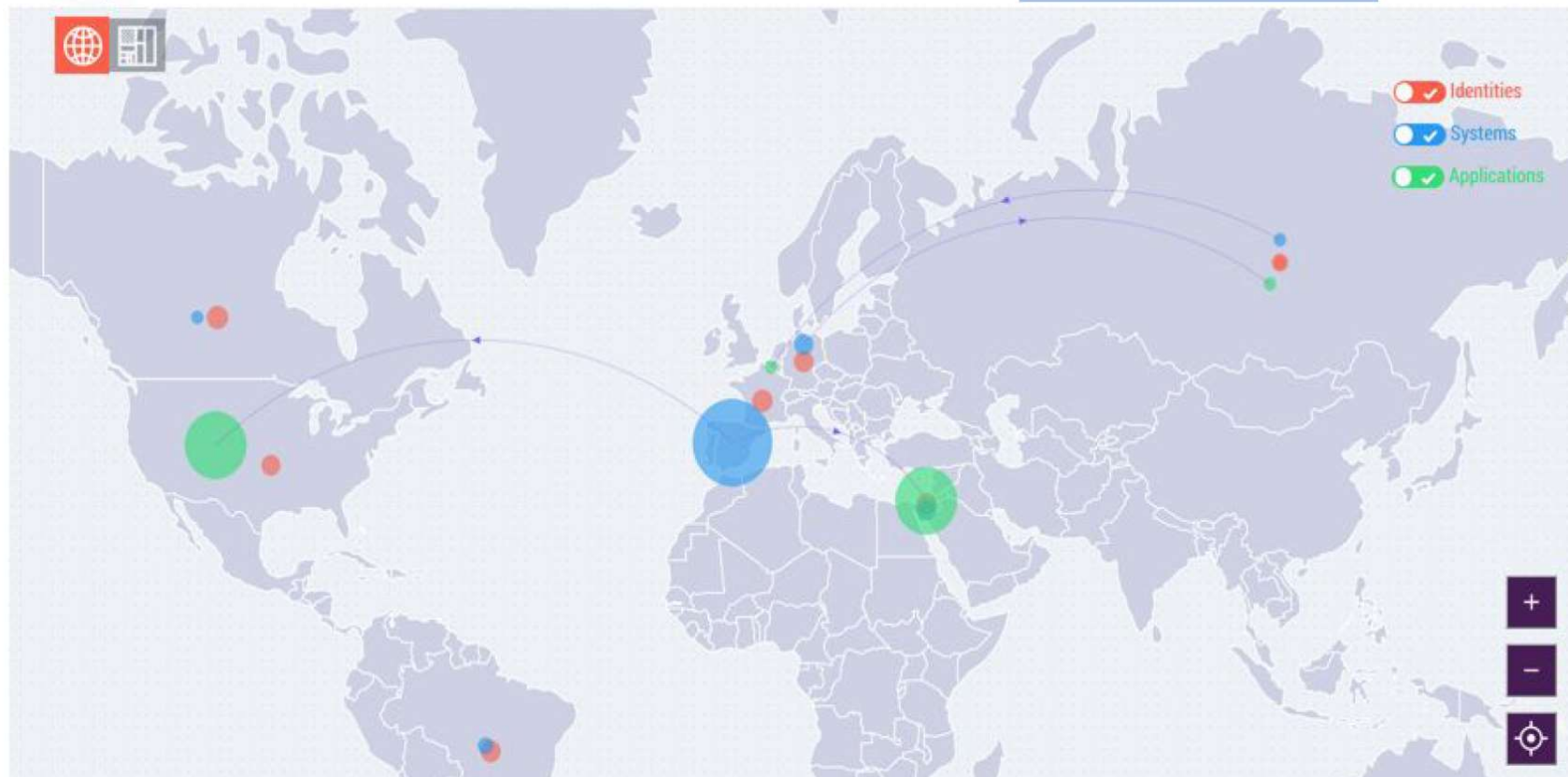
☆ TOP 5

 **11**

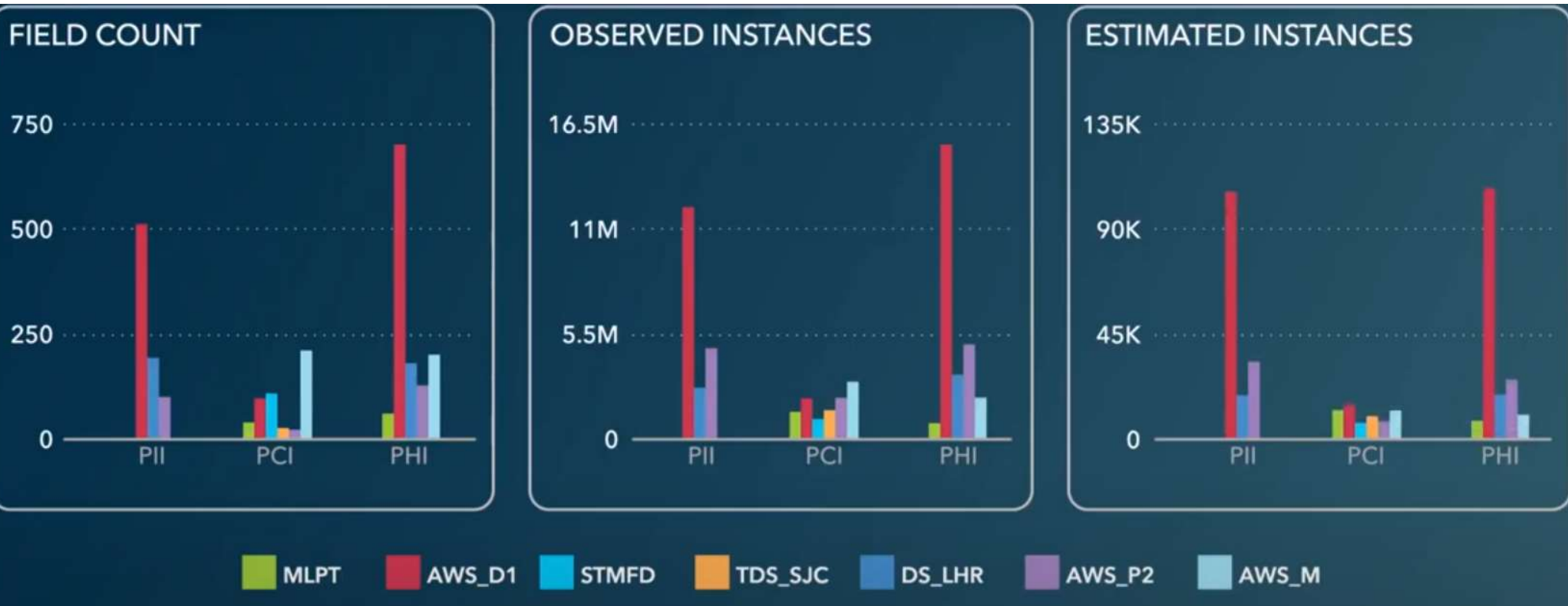
Applications

accessing personal information

☆ TOP 5



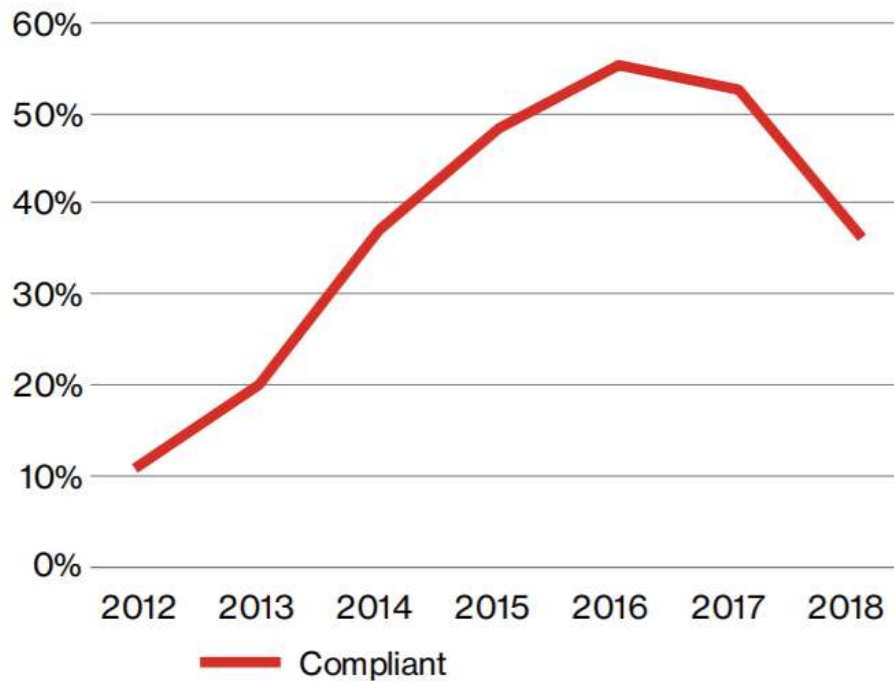
See security improvement and track sensitive data



Protecting Sensitive Data

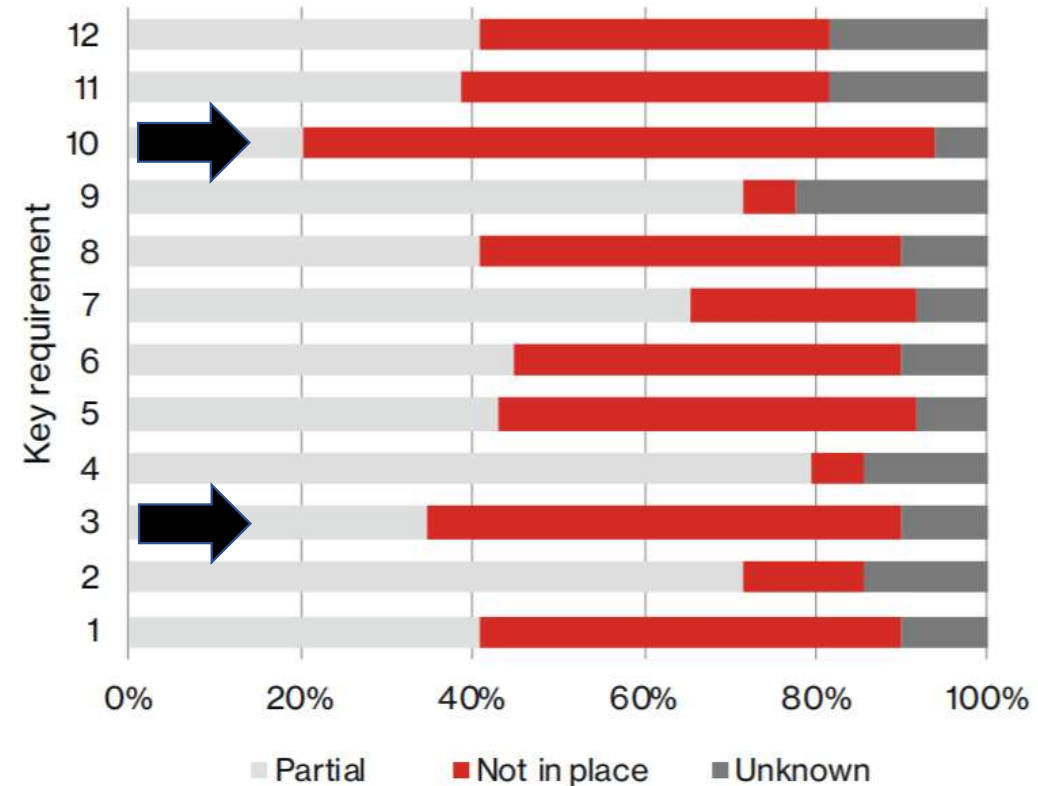
PCI DSS Compliance Issues with breached organizations and PCI DSS v4

Sustainability trends



PCI DSS v4 adds a customized approach

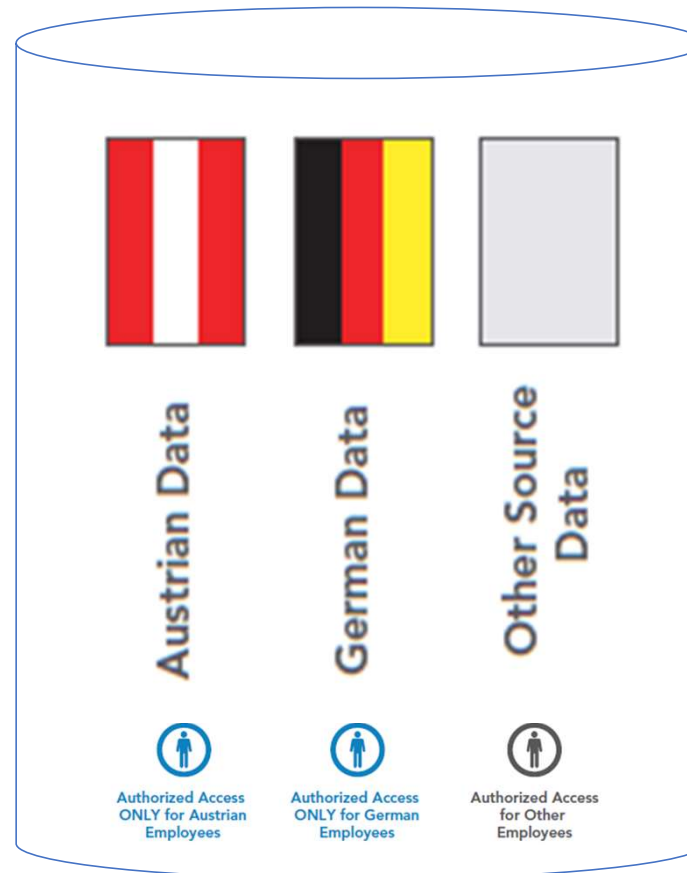
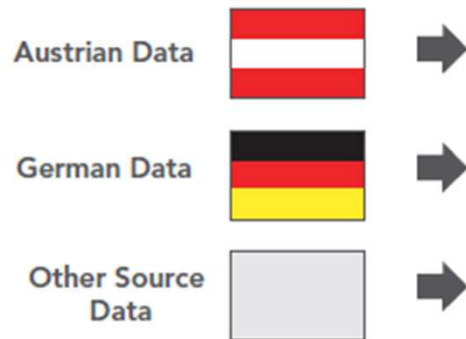
- Meeting the **security intent** of PCI DSS by **using security approaches that may be different than traditional PCI DSS requirements**.
- **Compensating controls** will be **removed**



- **PCI DSS Requirement 3** is addressing protecting cardholder data.
- **PCI DSS Requirement 10** is addressing network security and access.

Example of Cross Border Data-centric Security

Data sources



Complete policy-enforced de-identification of sensitive data across all bank entities

Data Warehouse In Italy

- **Protecting Personally Identifiable Information (PII)**, including names, addresses, phone, email, policy and account numbers
- **Compliance** with EU Cross Border Data Protection Laws
- Utilizing Data **Tokenization**, and centralized policy, key management, auditing, and reporting


☰

THE WALL STREET JOURNAL.

How Coronavirus Is Eroding Privacy

Technology to track and monitor individuals aims to slow pandemic, but raises concerns about government overreach



 **European nations** monitor citizen movement by **tapping telecommunications** data that they say conceals individuals' identities.

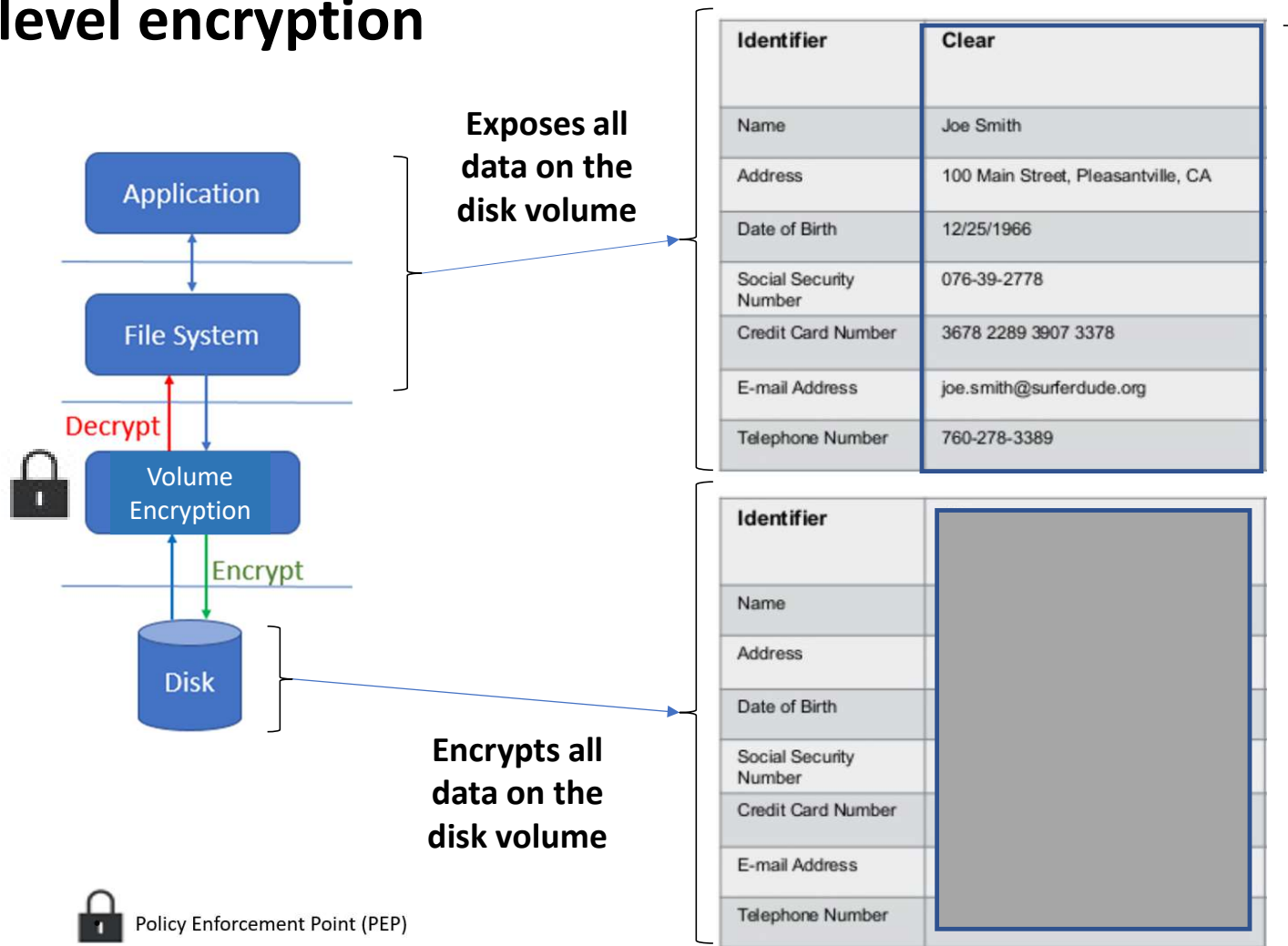
American officials are drawing **cellphone location data** from mobile **advertising firms** to **track the presence of crowds**—but not individuals. **Apple Inc.** and Alphabet Inc.'s **Google** recently announced plans to launch a **voluntary app** that health officials can use to **reverse-engineer sickened patients' recent whereabouts**—provided they agree to provide such information.

The extent of tracking hinges on a series of tough choices: **Make it voluntary or mandatory?** Collect personal or **anonymized data?** **Disclose information** publicly or privately?

In Western **Australia**, lawmakers approved a bill last month to install **surveillance gadgets in people's homes** to monitor those placed under **quarantine**. Authorities in **Hong Kong and India** are using **geofencing** that draws virtual fences around **quarantine** zones. They monitor digital signals from **smartphone or wristbands** to deter rule breakers and nab offenders, who **can be sent to jail**. **Japan's** most popular messaging **app beams health-status questions to its users** on behalf of the government.

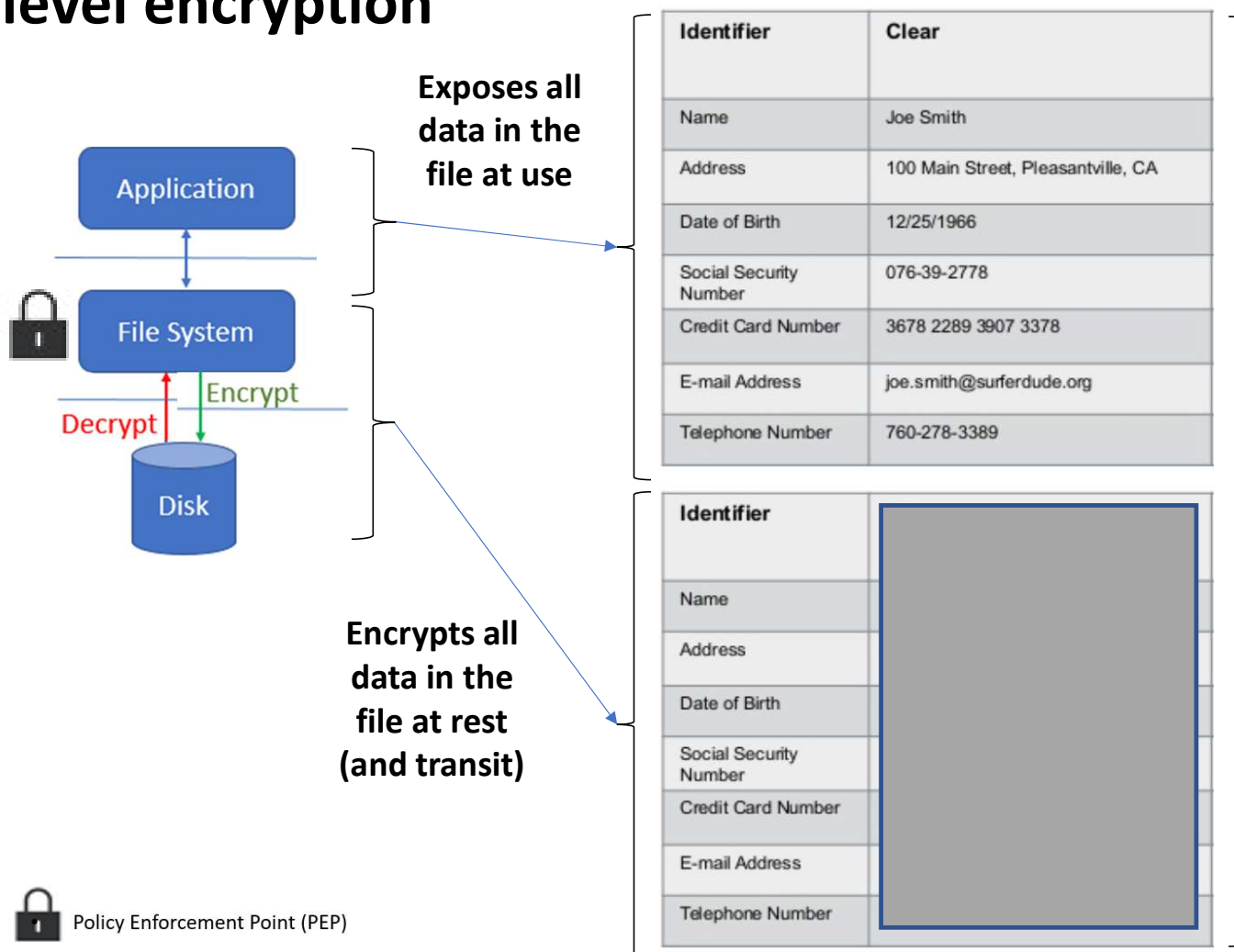
<http://dataprotection.link/Zn1Uk#https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028>

Example of disk level encryption



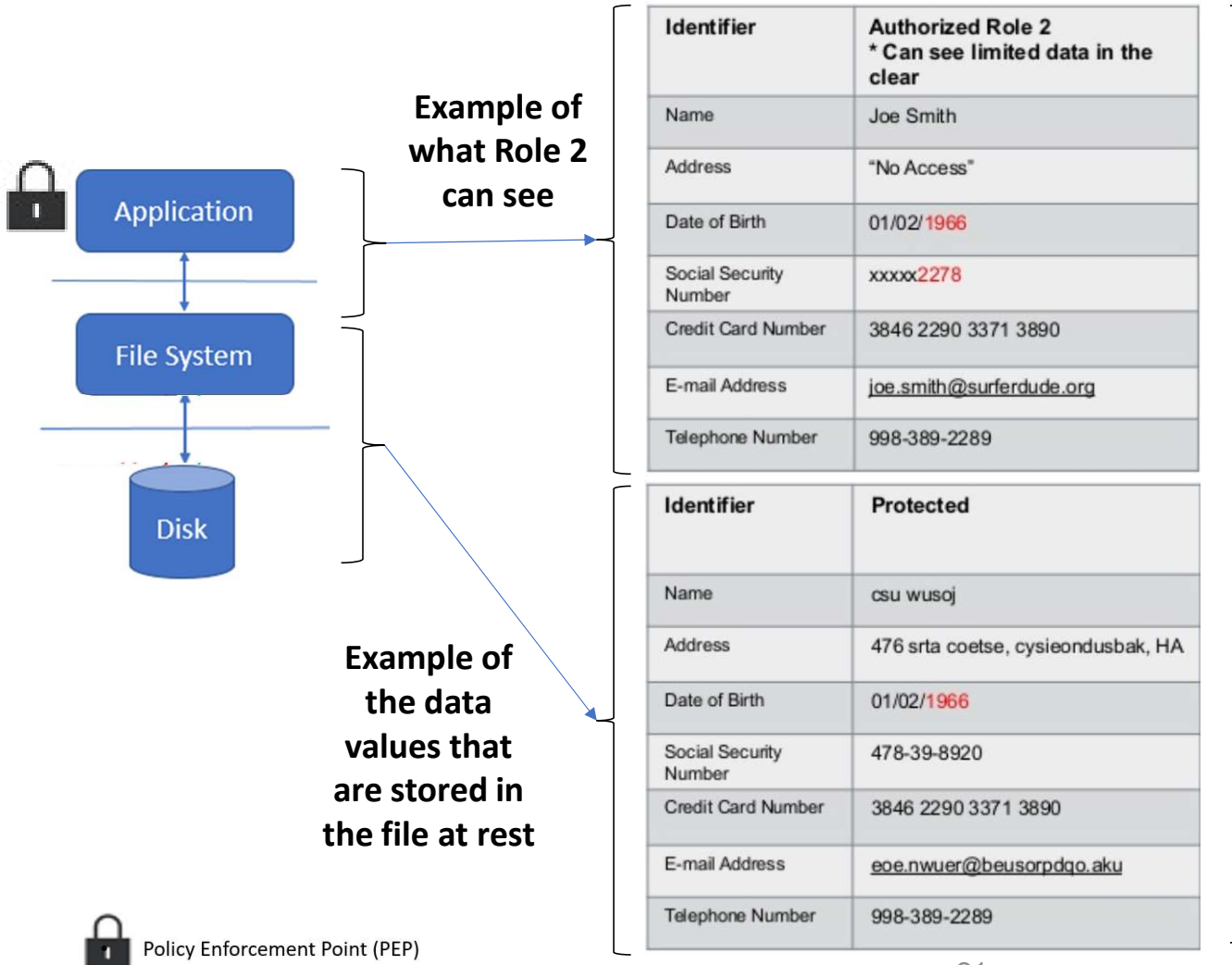
- "All or nothing" approach
- Does NOT secure file contents in use

Example of file level encryption



- "All or nothing" approach
- Does NOT secure file contents in use
- OS File System Encryption
- HDFS Encryption
- Secures data at rest and in transit

Reduce risk by field level protection



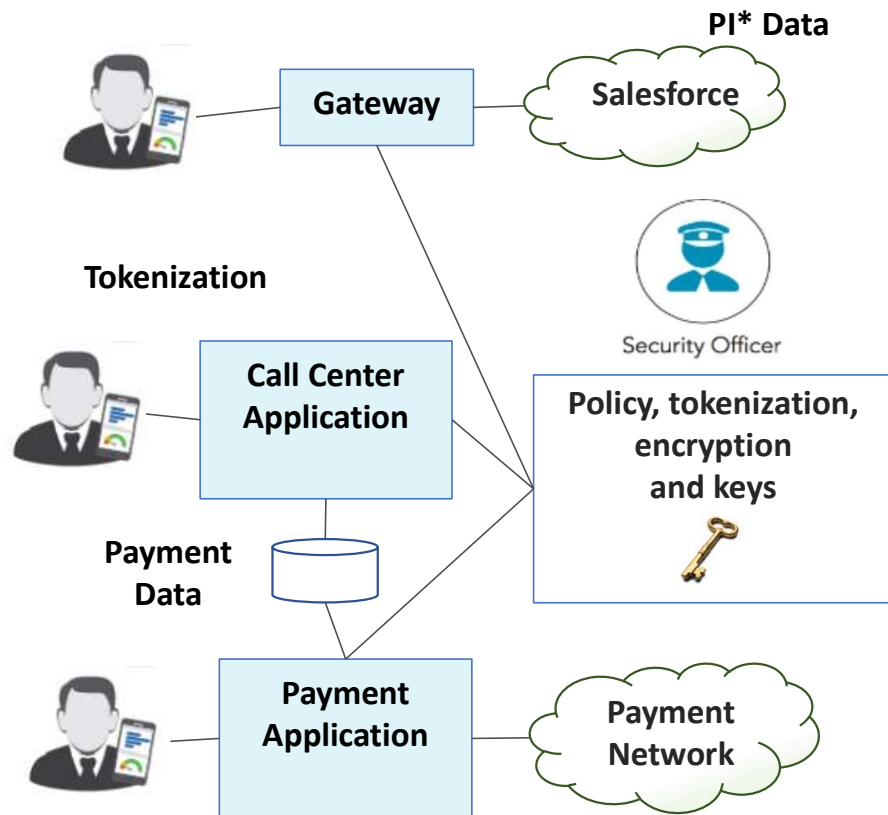
Reduce risk by **not exposing the full data value** to applications and users that only need to operate on a limited representation of the data



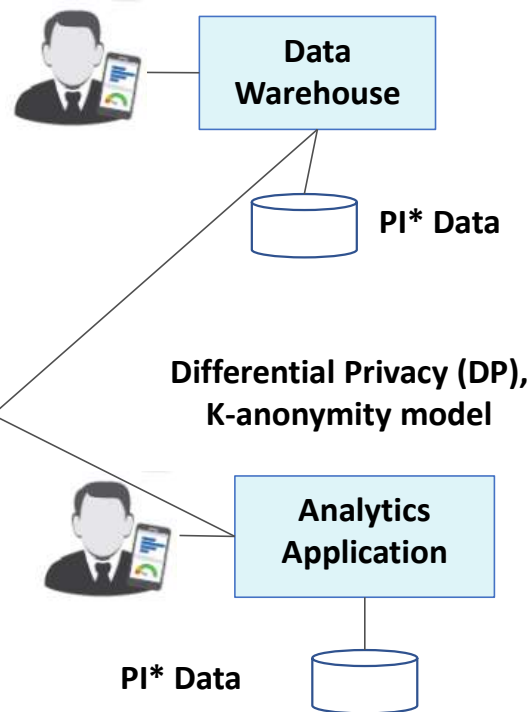
- At the individual field level
- Fine Grained Protection Methods:
 - Vaultless Tokenization
 - Encryption
 - Format Preserving Encryption
 - Masking/Data Obfuscation
- Data is protected wherever it goes (even In-Use)
- Business intelligence analytics capability retained (80%-90% of analytics performed on data in protected form)

Use-cases of some de-identification techniques

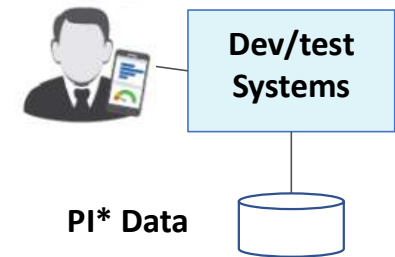
Format Preserving Encryption (FPE)



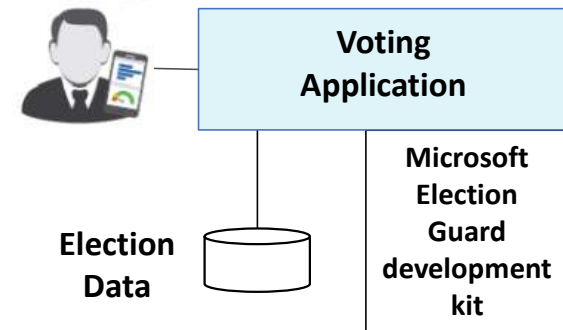
Vault-less tokenization (VLT)



Masking



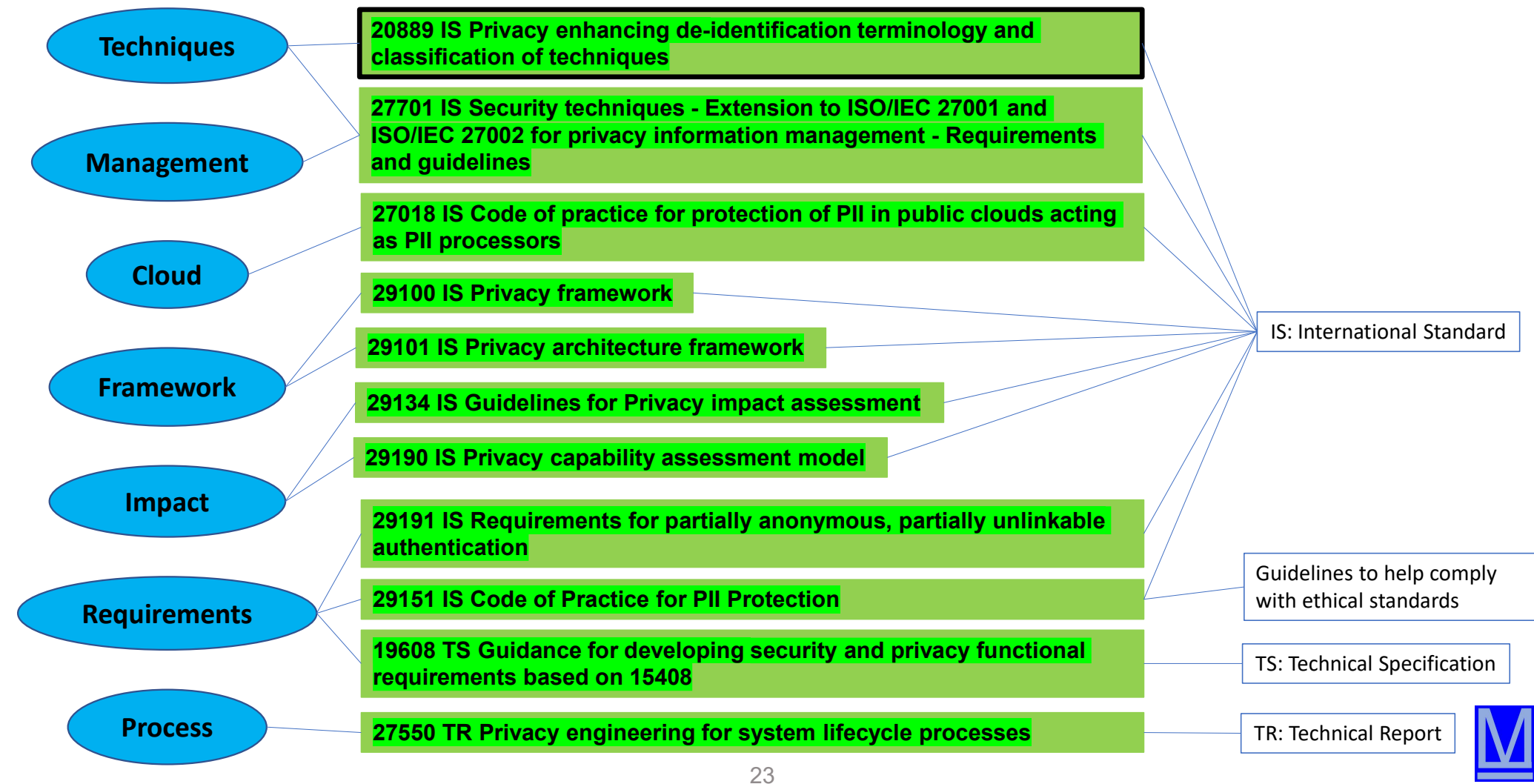
Homomorphic Encryption (HE)



*: **PI Data** (Personal information) means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household according to CCPA

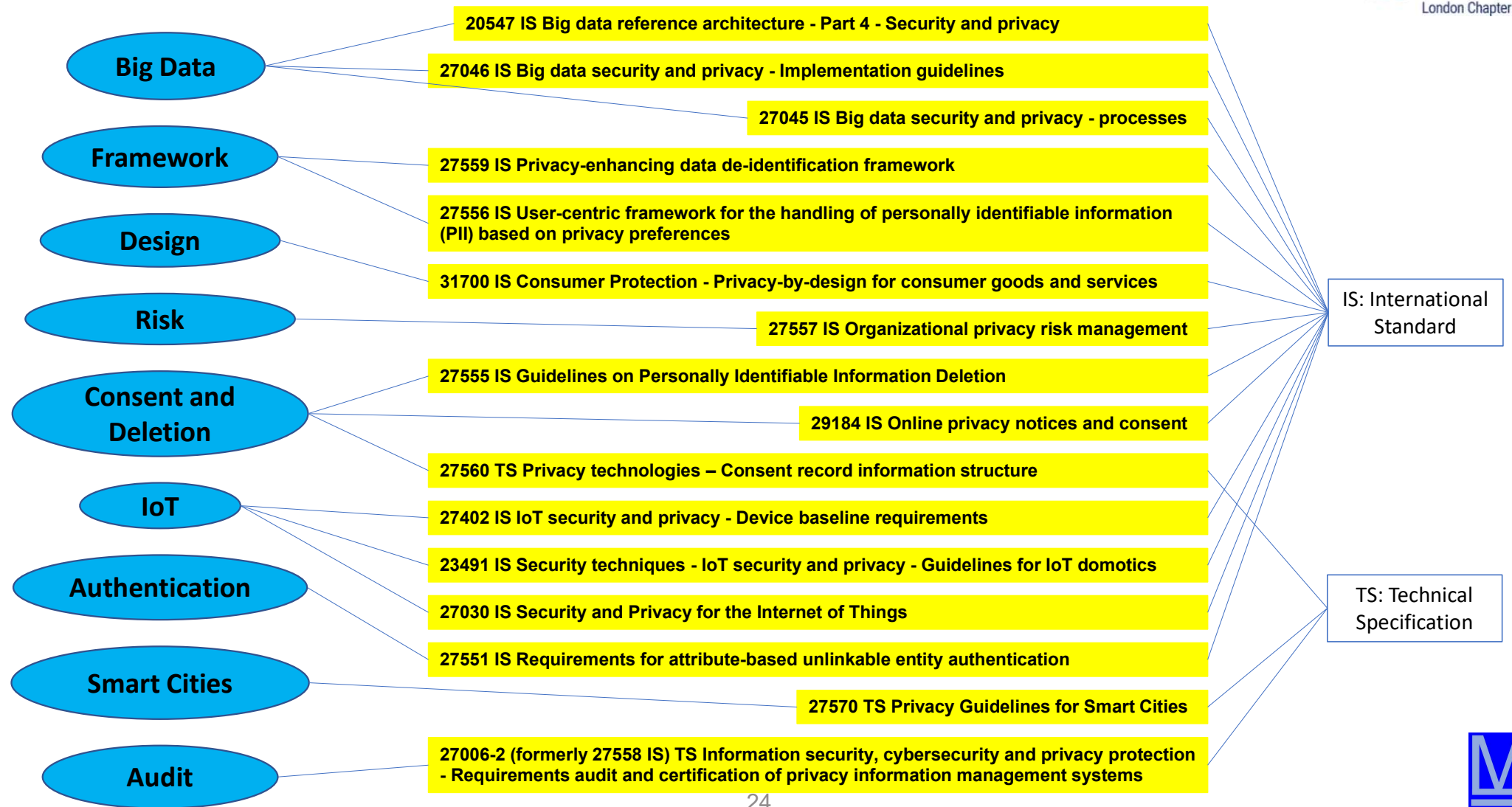
Privacy Standards

11 Published International Privacy Standards (ISO)



Privacy Standards

16 International Privacy Standards in development (ISO)



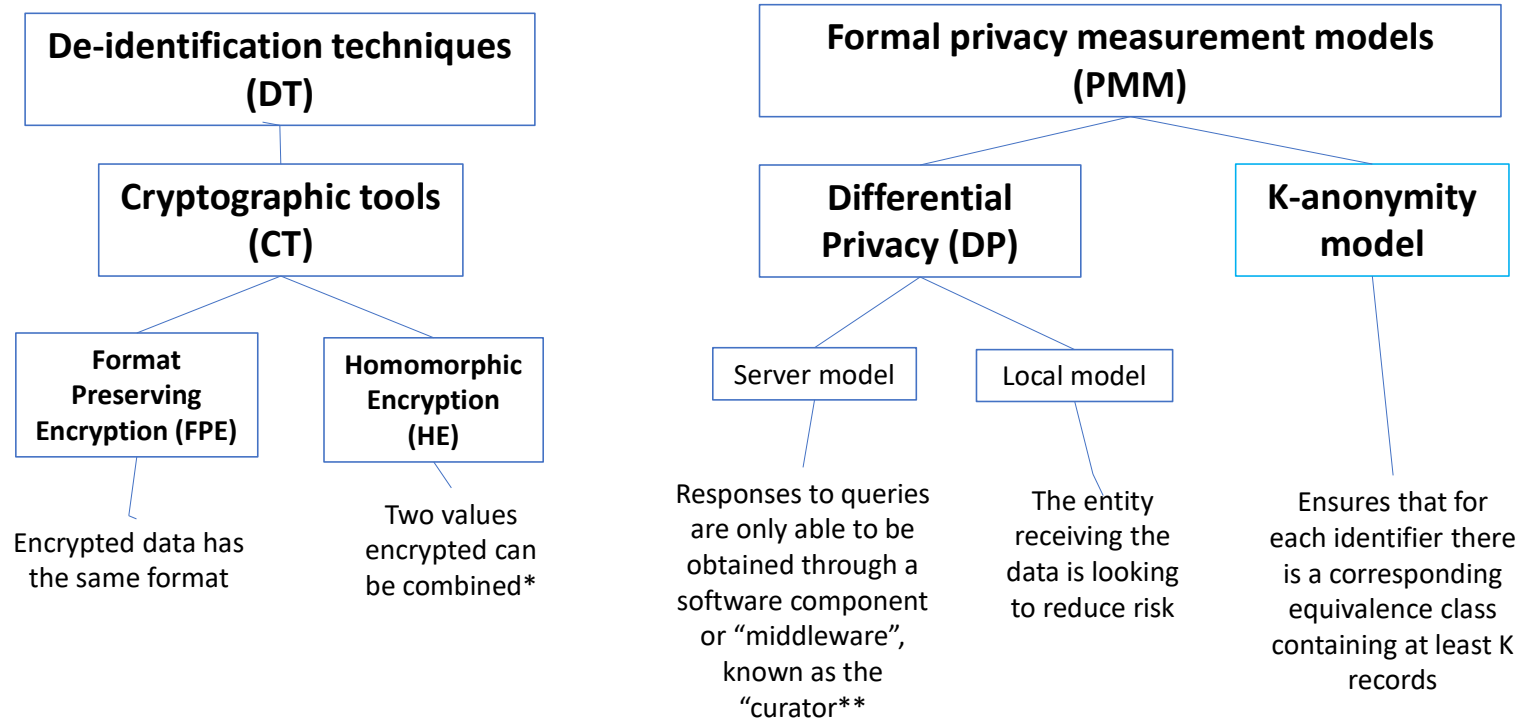
Data protection techniques: Deployment on-premises, and clouds

Privacy enhancing data de-identification terminology and classification of techniques			Data Warehouse	Centralized	Distributed	On-premises	Public Cloud	Private Cloud
De-identification techniques	Tokenization	Vault-based tokenization		y				y
		Vault-less tokenization	y	y	y	y	y	y
	Cryptographic tools	Format preserving encryption		y	y	y	y	y
		Homomorphic encryption			y		y	
	Suppression techniques	Masking	y	y	y	y	y	y
		Hashing	y	y	y	y	y	y
Formal privacy measurement models	Differential Privacy	Server model	y	y	y	y	y	y
		Local model	y	y	y	y	y	y
	K-anonymity model	L-diversity	y	y	y	y	y	y
		T-closeness	y	y	y	y	y	y



ISO Standard for Encryption and Privacy Models

- Privacy enhancing data de-identification terminology and classification of techniques



*: Multi Party Computation (MPC)

** : Example Apple and Google

Examples of data de-identification

Source data:

Last name	Balance	Age	Gender
Folds	93791	23	m
...

Output data:

Generalization

Generalization

Pseudonymization

Rounding

Aggregation/Binning

Field	Privacy Action (PA)	PA Config	Variant Twin Output
Balance	Nearest Unit Value	Thousand	94000

Source: INTERNATIONAL STANDARD ISO/IEC 20889, Privitar, Anonos

Source data:

Patient	Age	Gender	Region	Disease
173965429	57	Female	Hamburg	Gastric ulcer

Generalization

Generalization

Output data:

Patient	Age	Gender	Region	Disease
173965429	>50	Female	Germany	Gastric ulcer

Field	Privacy Action (PA)	PA Config	Variant Twin Output
Gender	Pseudonymise		AD-lks75HF9aLKSa

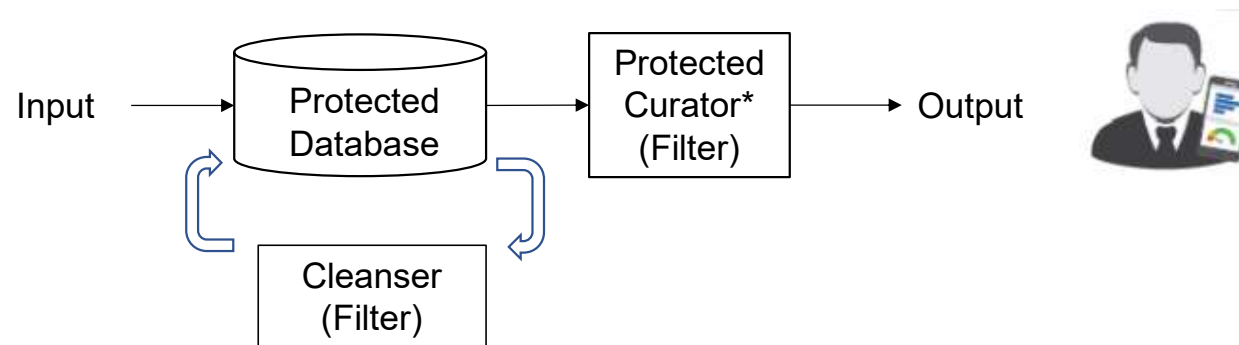
Field	Privacy Action (PA)	PA Config	Variant Twin Output
Age	Integer Range Bin	Step 10 + Pseud.	Age_KXYC
Age	Integer Range Bin	Custom Steps	18-25

Privacy Measurement Models

Privacy measurement models

Differential Privacy

Differential privacy is a model that provides mathematical guarantees that the probability distribution of the output of this analysis differs by a factor no greater than a specified parameter regardless of whether any data principal is included in the input dataset.



*: Example: Apple

Differential privacy model

Differential privacy is a formal privacy measurement model that, if incorporated in the **design of a particular statistical analysis**, provides mathematical **guarantees that the probability distribution of the output** of this analysis **differs by a factor no greater than a specified parameter** regardless of whether **any** particular data principal **is included** in the input dataset.

- a **mathematical definition of privacy** which posits that, for the outcome of any statistical analysis distribution independent of whether any given data principal is added to or removed from the dataset; and
- a **measure of privacy** that enables monitoring of cumulative privacy loss and setting of a **“budget” for loss** limit.

When adequately implemented and used, provide a mathematically proven guarantee of privacy.

The design and construction of a differentially private algorithm requires appropriate **expertise** in the field of **probability and statistics**, and of the **theory of differential privacy**.

Differentially private algorithms are built by **adding** a certain amount of “random **noise**” that is generated **from a carefully** selected probability distribution, such that the desired **usefulness** of data is **preserved**.

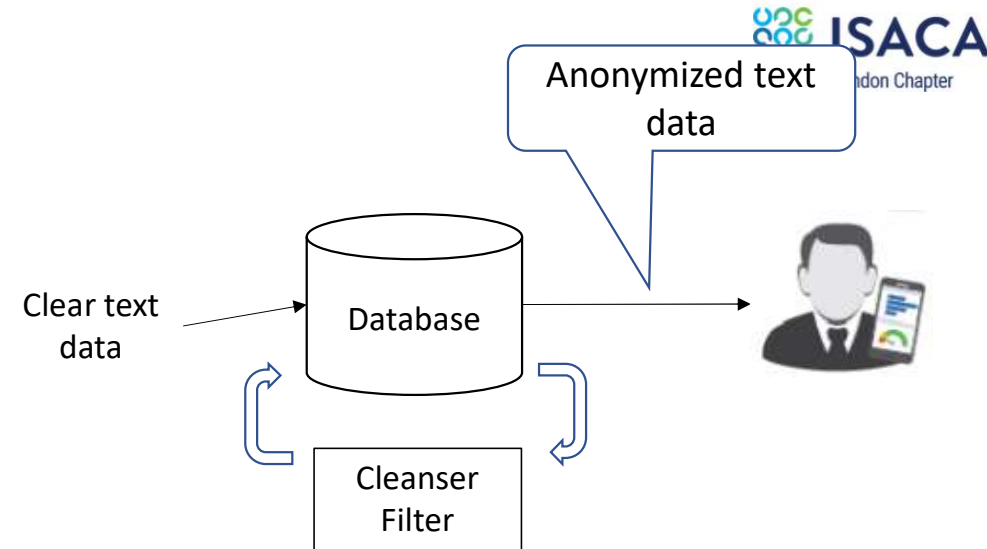
NOTE For detailed treatment of these and other relevant topics on the subject, see [9], [45] and [15]. And Annex E

Privacy measurement models

K-anonymity model

The k-anonymity model that ensures that **groups** smaller than k individuals **cannot be identified**.

- Queries will **return at least k number of records**. K-anonymity is a formal privacy measurement model that ensures that for each identifier there is a corresponding equivalence class containing at least K records.



Some of the **de-identification techniques** can be used either independently or **in combination** with each other to **satisfy the K-anonymity model**.

Suppression techniques, generalization techniques, and **microaggregation*** can be applied to different types of attributes in a dataset to achieve the desired results.

*: **Microaggregation replaces all values** of continuous attributes **with their averages** computed in a certain algorithmic way.

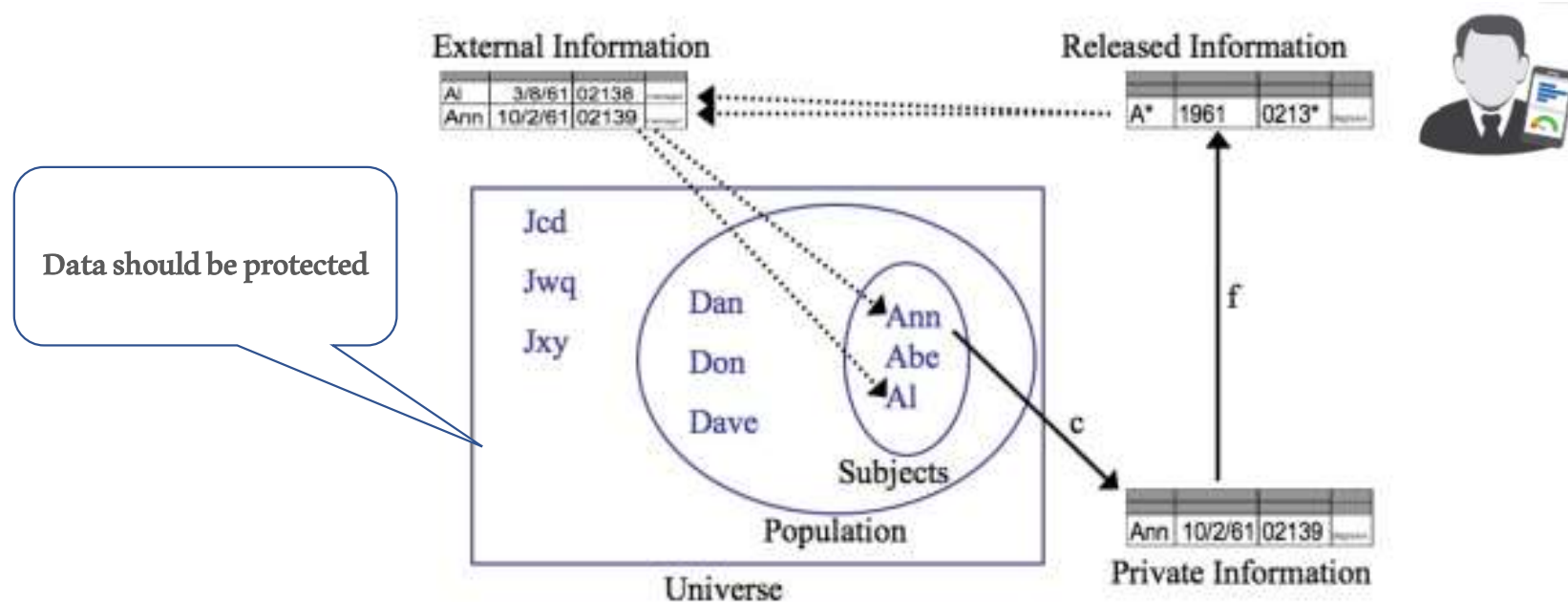
Privacy measurement models

K-anonymity model

The k-anonymity can thwart the ability to link field-structured databases


Given person-specific field-structured data, produce a release of the data with **scientific guarantees that the individuals who are the subjects of the data cannot be reidentified** while the data remain practically useful.

A release provides k-anonymity if the data for **each person cannot be distinguished from at least k-1 individuals** whose data also appears in the release



Source: INTERNATIONAL STANDARD ISO/IEC 20889

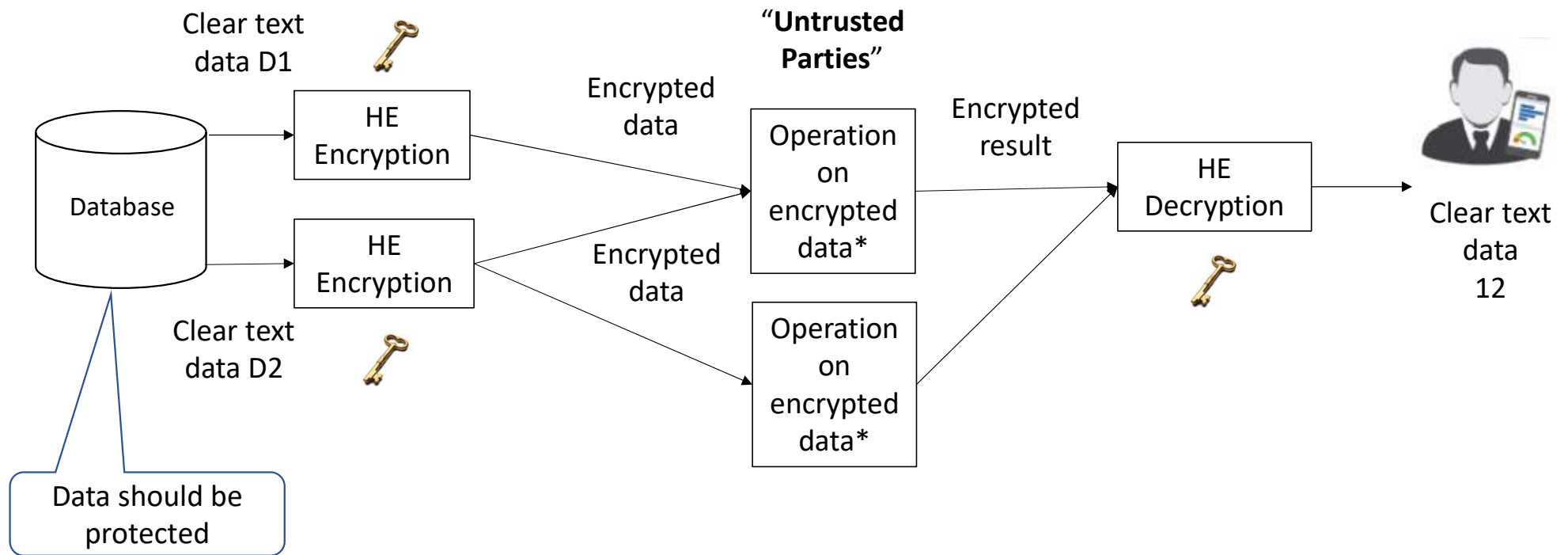
Risk reduction and truthfulness of standardized de-identification techniques and models

Technique name		Use Case / User Story	Data protected in			Data truthfulness at record level	Applicable to types of attributes	 Reduces the risk of		
			Transit	Use	Storage			Singling out	Linking	Inference
Pseudonymization	Tokenization	Protects the data flow from attacks	Yes	Yes	Yes	Yes	Direct identifiers	No	Partially	No
Cryptographic tools	Deterministic encryption	Protects the data when not used in processing operations	Yes	No	Yes	Yes	All attributes	No	Partially	No
	Order-preserving encryption	Protects the data from attacks	Partially	Partially	Partially	Yes	All attributes	No	Partially	No
	Homomorphic encryption	Protects the data also when used in processing operations	Yes	Yes	Yes	Yes	All attributes	No	No	No
Suppression	Masking	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Local identifiers	Yes	Partially	No
	Local suppression	Protects the data in analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	Partially	Partially	Partially
	Record suppression	Removes the data from the data set	Yes	Yes	Yes	Yes	All attributes	Yes	Yes	Yes
	Sampling	Exposes only a subset of the data for analytical applications	Partially	Partially	Partially	Yes	All attributes	Partially	Partially	Partially
Generalization	Generalization	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	Partially	Partially	Partially
	Rounding	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	No	Partially	Partially
	Top/bottom coding	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	No	Partially	Partially
Randomization	Noise addition	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	No	Identifying attributes	Partially	Partially	Partially
	Permutation	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	No	Identifying attributes	Partially	Partially	Partially
	Micro aggregation	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	No	All attributes	No	Partially	Partially
Privacy models	Differential privacy	Protects the data in analytical applications	No	Yes	Yes	No	Identifying attributes	Yes	Yes	Partially
	K-anonymity	Protects the data in analytical applications	No	Yes	Yes	Yes	Quai identifiers	Yes	Partially	No

Source: INTERNATIONAL STANDARD ISO/IEC 20889

Encryption and Tokenization

Homomorphic Encryption (HE)

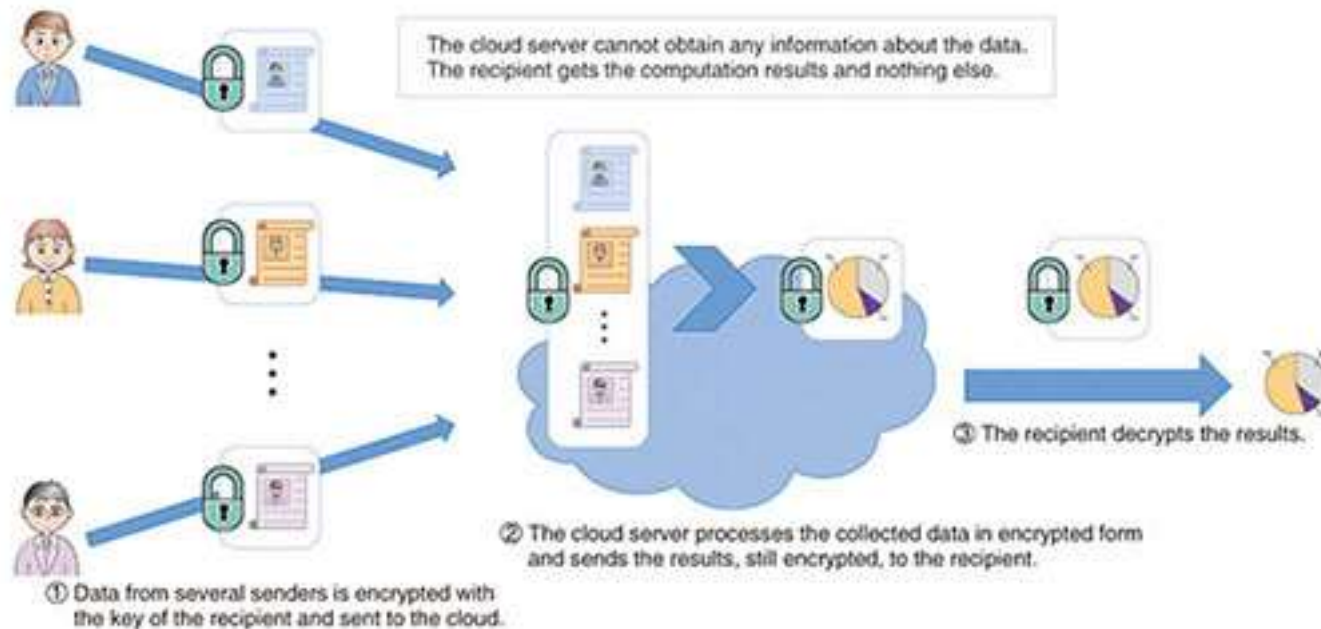


Homomorphic Encryption (HE)

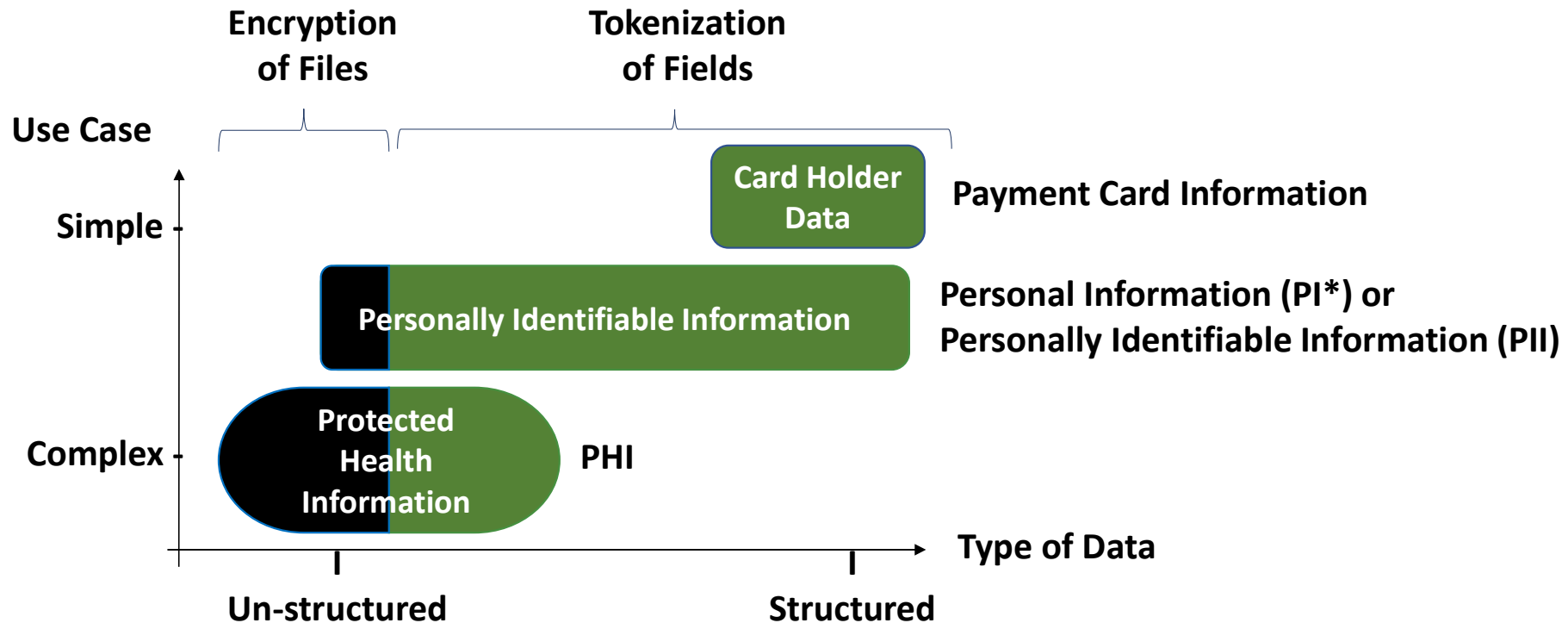
Anonymous data processing with fully homomorphic encryption

Anonymous data processing involves **multiple users sending some sensitive data to a cloud server**, where it is aggregated, stripped of identifying information, and analyzed, typically to extract some statistical information, which is then delivered to the final recipient.

- The security requirement is that the cloud **server must learn nothing about the content of users' data**, and the **recipient must obtain only the anonymized results** of the statistical analysis, and, no **information on individual users**.



How to protect different types of data with encryption and tokenization

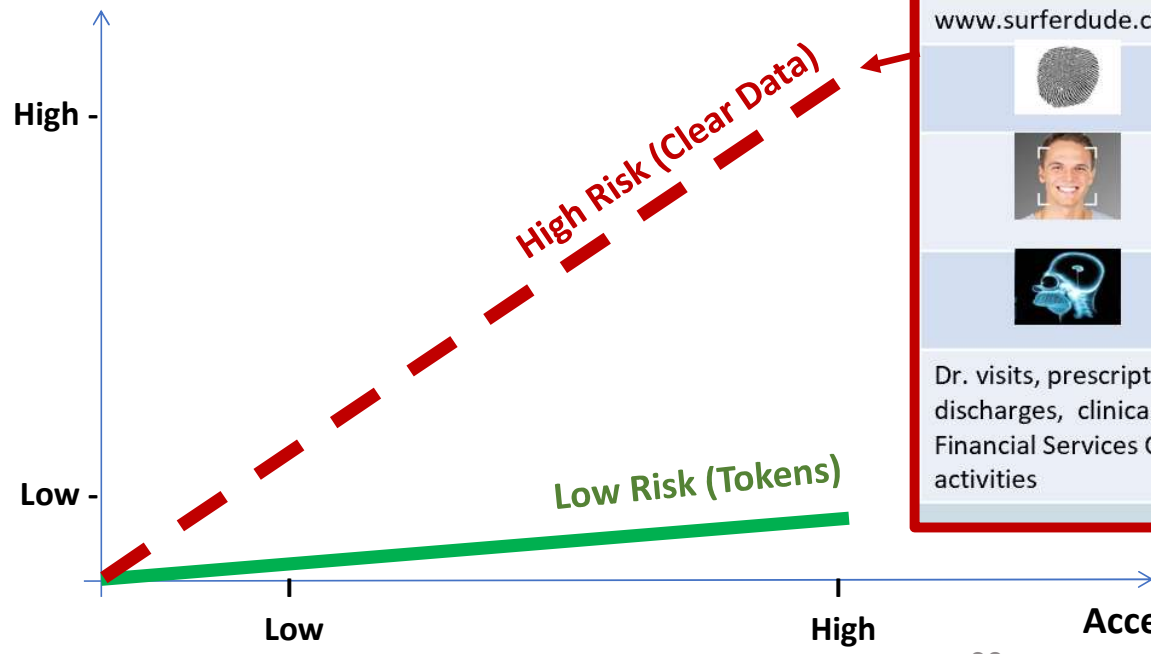


*: California CCPA

Risk, productivity and access to more data fields



User Productivity



Real Data
Joe Smith
100 Main Street, Pleasantville, CA
12/25/1966
760-278-3389
joe.smith@surferdude.org
076-39-2778
3678 2289 3907 3378
www.surferdude.com



Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities

Tokenized / Pseudonymized
csu wusoj
476 srta coetse, cysieondusbak, CA
01/02/1966
760-389-2289
eo.e.nwuer@beusorpdqo.org
076-28-3390
3846 2290 3371 3378
www.sheyinctao.com
Encrypted
Encrypted
Encrypted
Protection methods can be equally applied to the actual data, but not needed with de-identification



Example of Cross Border Data-centric Security using Tokenization

Data should be protected

Data sources



Security Officer

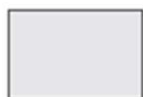
Austrian Data



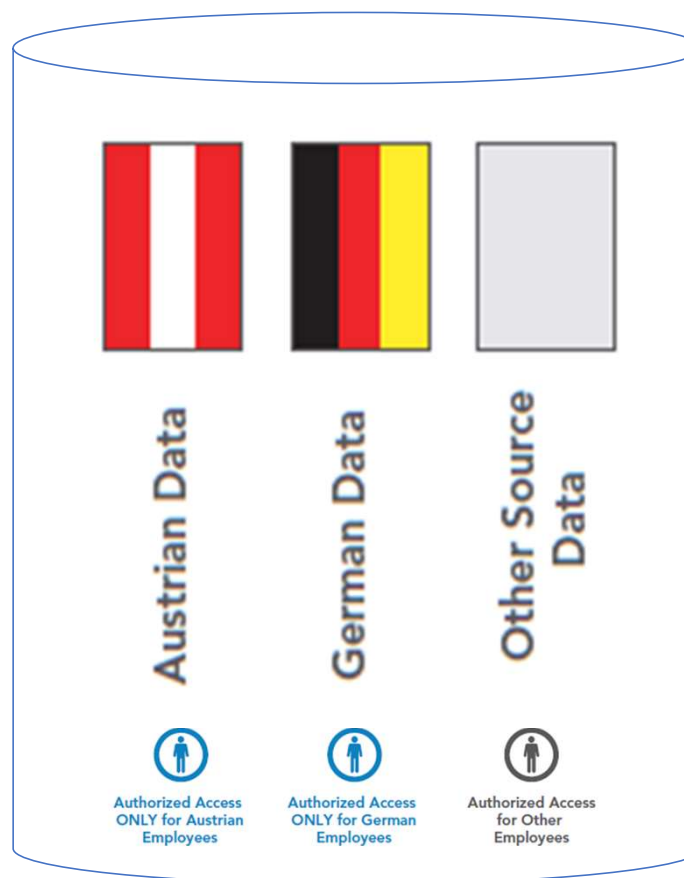
German Data



Other Source Data



- **Protecting Personally Identifiable Information (PII)**, including names, addresses, phone, email, policy and account numbers
- **Compliance** with EU Cross Border Data Protection Laws
- Utilizing Data **Tokenization**, and centralized policy, key management, auditing, and reporting



Data Warehouse

Complete policy-enforced de-identification of sensitive data across all bank entities

Use Case - Compliance with cross-border and other privacy restrictions

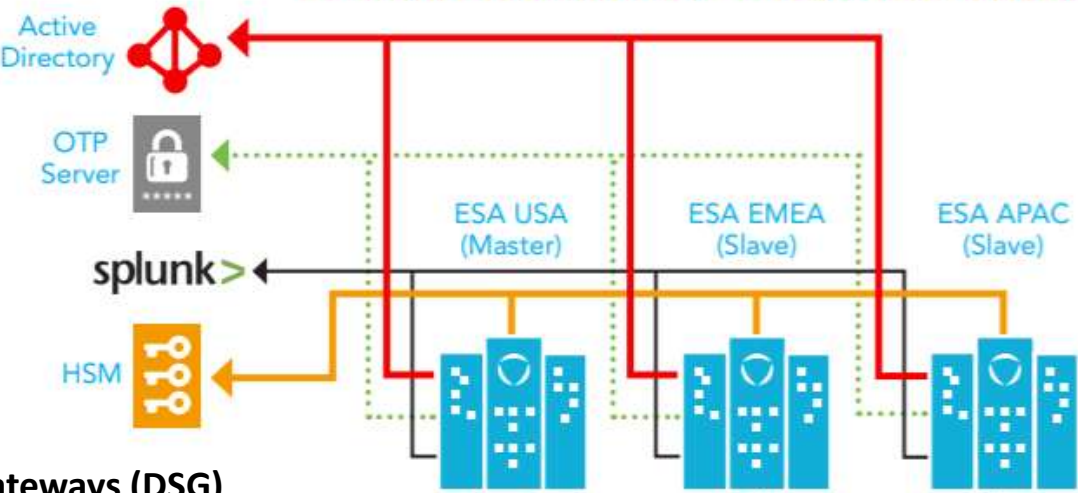
CENTRAL CONTROL (US) – LOCAL DATA MANAGEMENT

- Standard User Authentication
- Two Factor Authentication
- Log Analytics
- Key Management
- Security Policy Enforcement
- Protected Application Data



Security Officer

Central Security Manager (ESA)

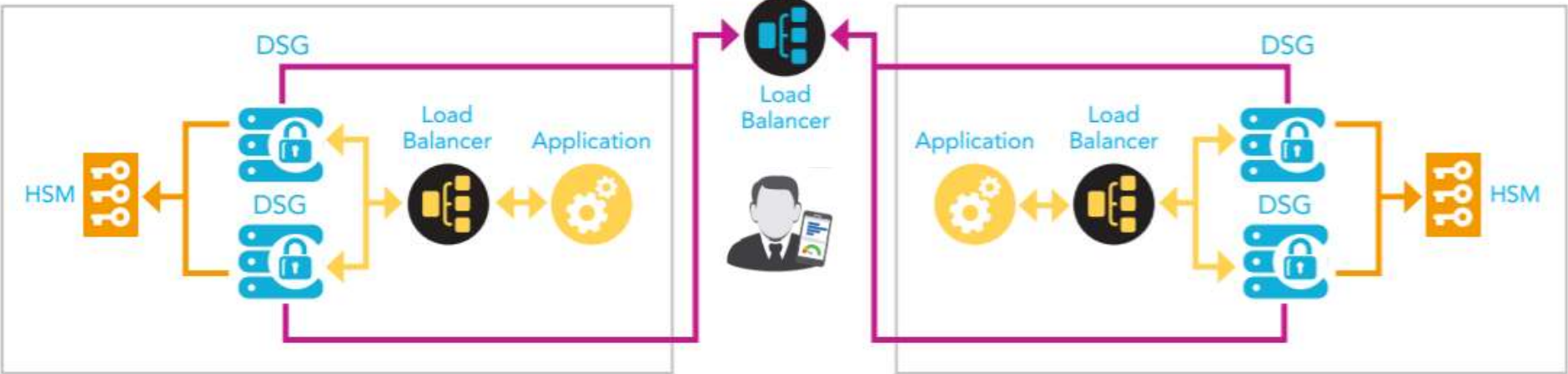


Local Data Security Gateways (DSG)

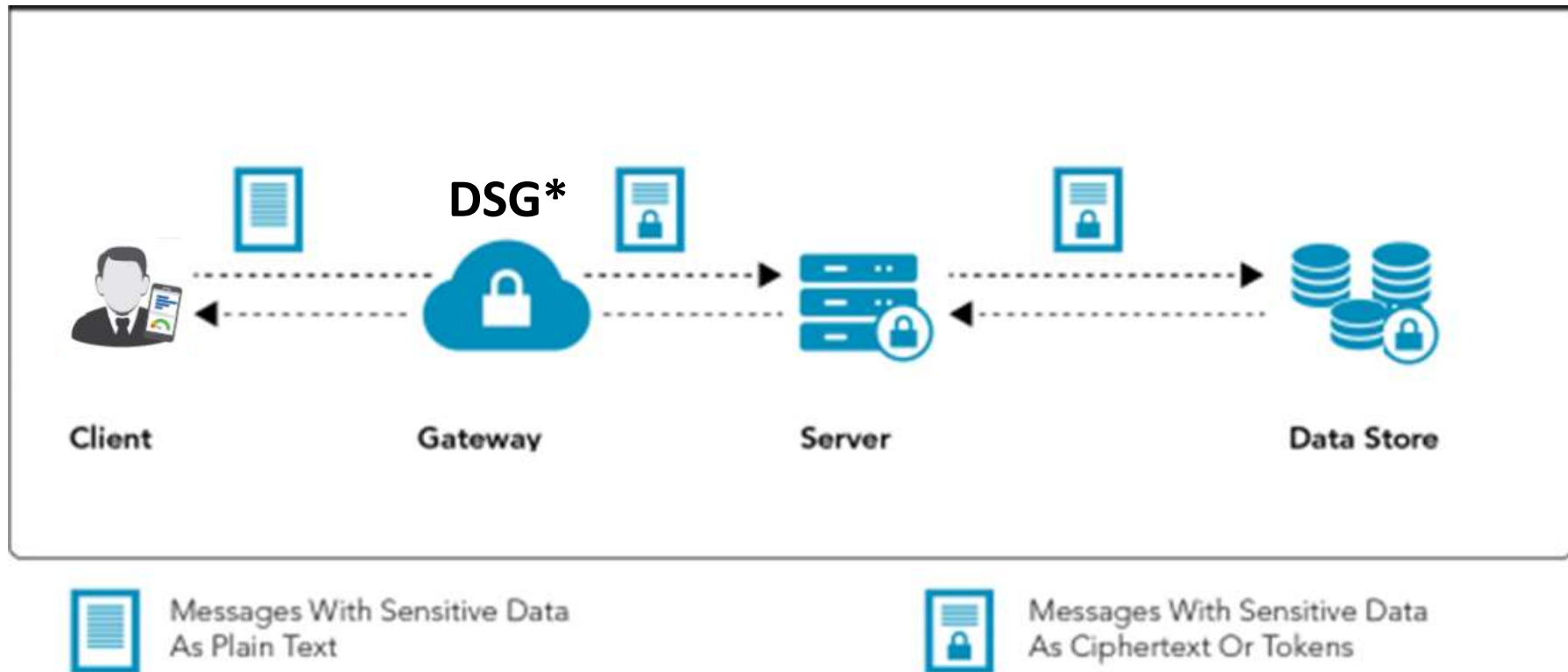
- 200 million users
- 160 countries

DOMAIN IN EMEA

DOMAIN IN APAC



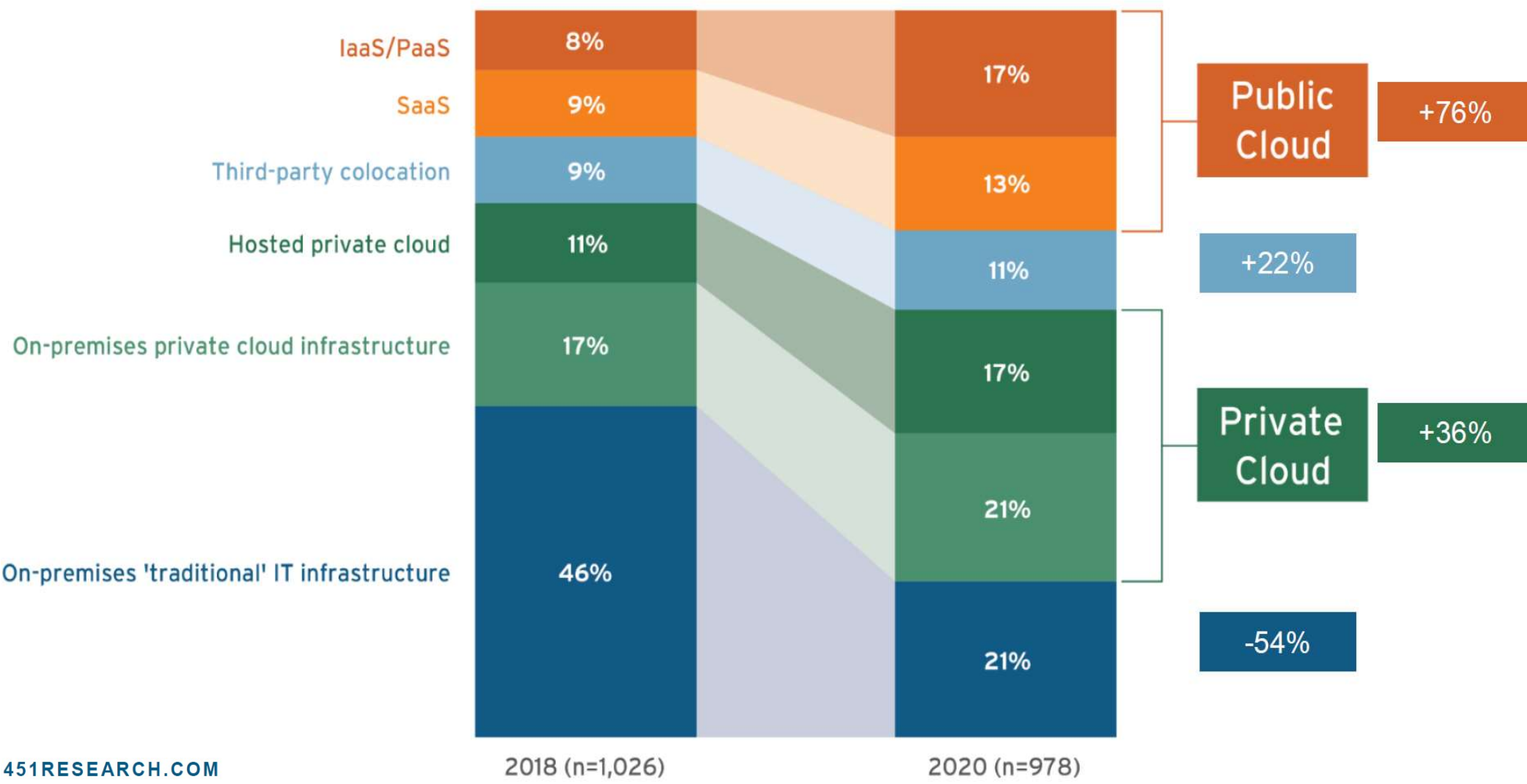
A Data Security Gateway (DSG) can turn sensitive data to Ciphertext or Tokens



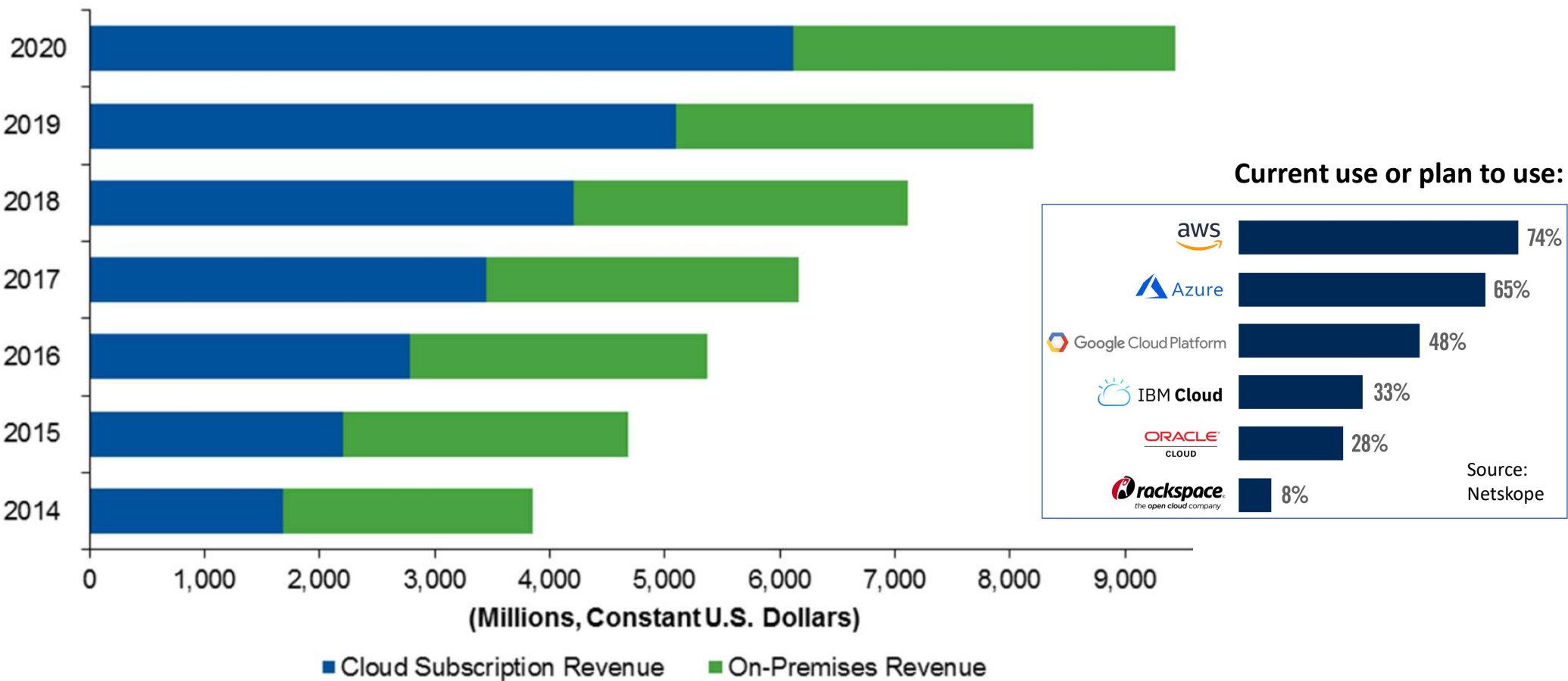
*: Example of supported protocols include HTTP, HTTPS, SFTP, SMTP and API utilizing web services or REST

Trends in Cloud Security

Cloud transformations are accelerating



Spending by Deployment Model, Digital Commerce Platforms, Worldwide



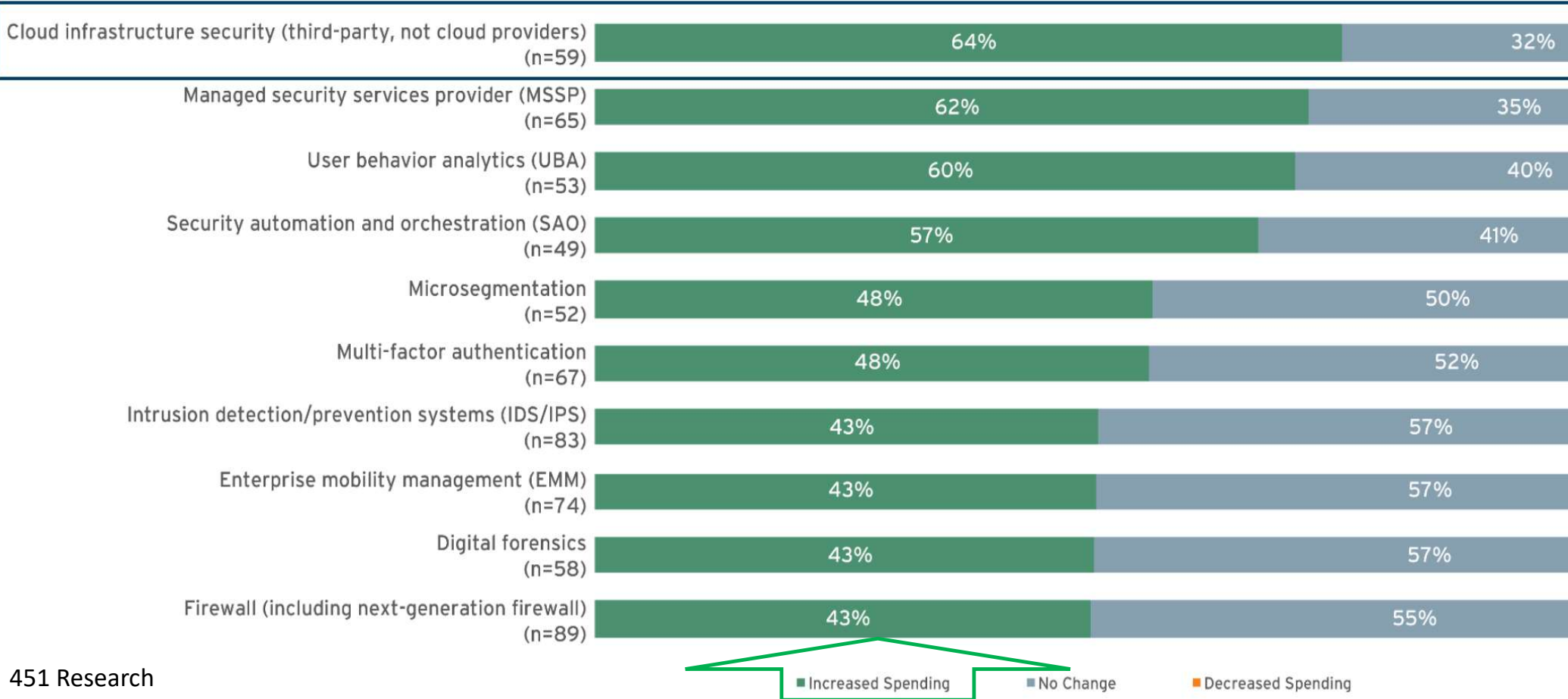
Source: Gartner



Securing Cloud Workloads – Greatest Increase in Spending

ANTICIPATED CHANGES IN SPENDING ON INFORMATION SECURITY TECHNOLOGIES IN NEXT 12 MONTHS

% of respondents



- “Active Directory”
- WAF
- SIEM
- Firewall
- Encryption
- Tokenization
- Key Management
- AV – Anti Virus
- Network Sec

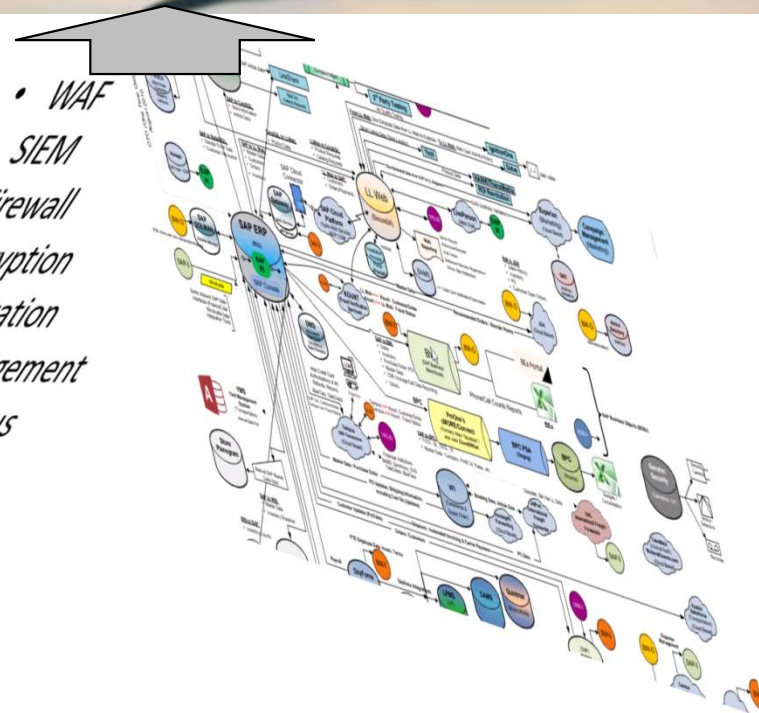
Public Cloud / Multi-cloud



**Security controls can be applied
On-premises or Cloud**

Active Directory, Load Balancers

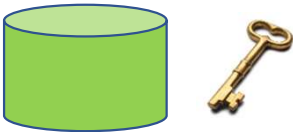
- WAF
- SIEM
- Firewall
- Encryption
- Tokenization
- Key Management
- AV – Anti Virus
- Network Sec
- And more



Shared responsibilities across cloud service models

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Network controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Host infrastructure	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Physical security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer

Cloud Customer Cloud Provider



The Customer is Responsible for the Data across all Cloud Service Models



Multi-Cloud Key Management considerations

Legal Compliance and Nation-State Attacks

- Many companies have **information that is attractive to governments** and intelligence services.
- Others worry that litigation may result in a **subpoena** for all their data.

Jurisdiction

- Cloud service providers, especially IaaS vendors, offer **services in multiple countries**, often in more than one region, with **redundant data centers**.
 - This redundancy is great for resilience, but **regulatory concerns arises when moving data across regions** which may have different laws and jurisdictions.



Multi-Cloud Key Management considerations

Consistency

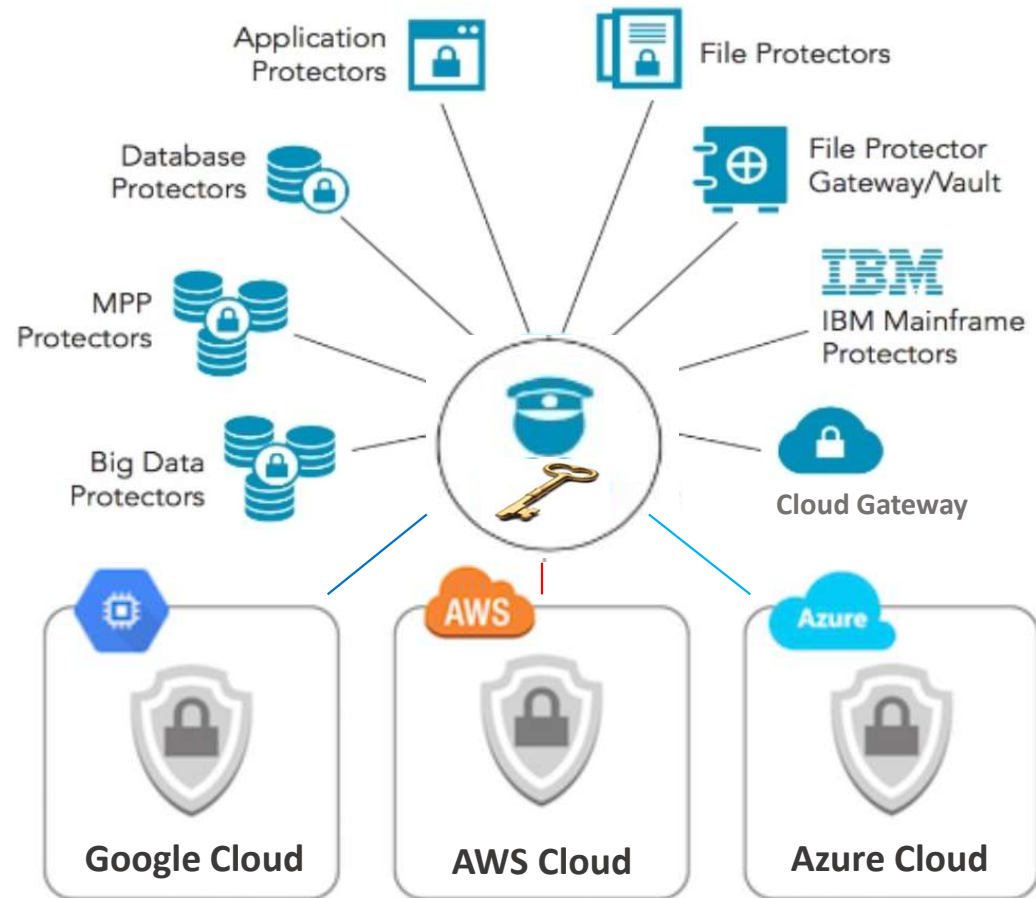
- Most firms are quite **familiar with their on-premises encryption and key management** systems, so they often prefer to leverage the **same tool and skills across multiple clouds**.
- Firms often adopt a “**best of breed**” cloud approach.

Trust

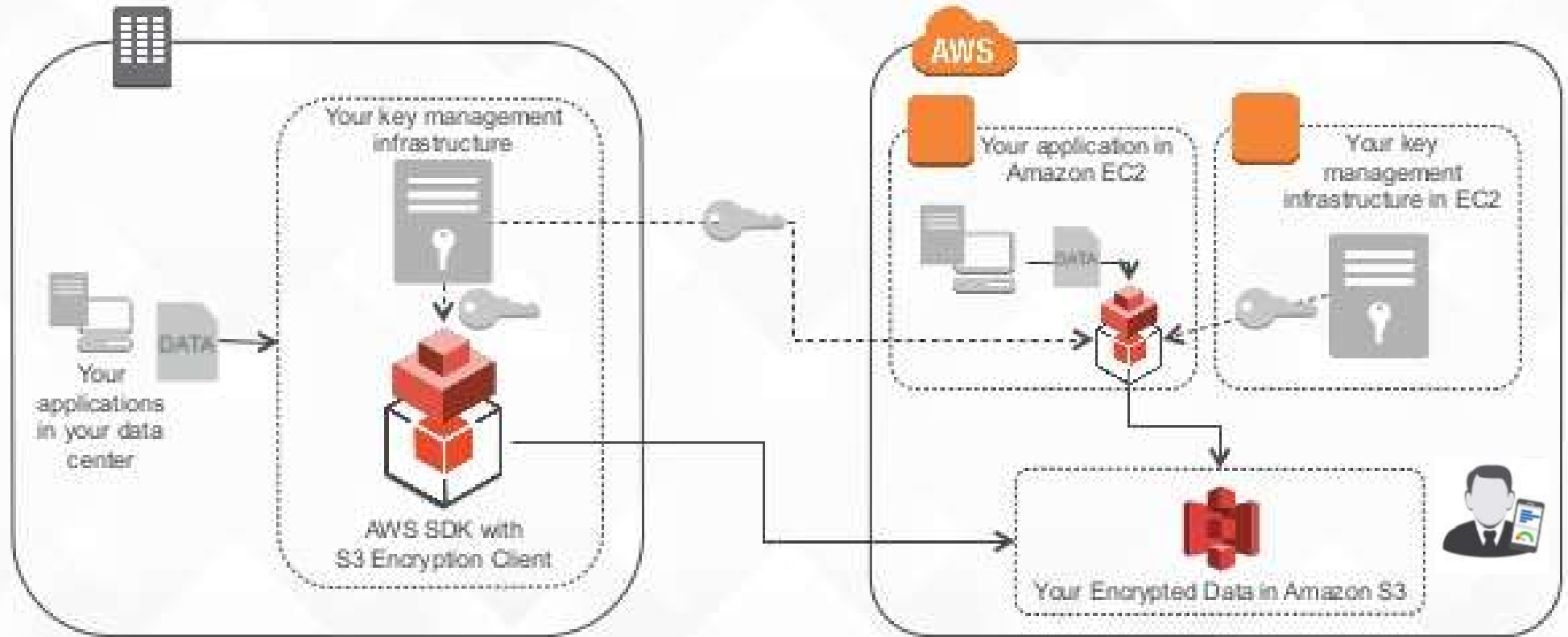
- Some customers simply **do not trust their vendors**.

Vendor Lock-in and Migration

- A common concern is **vendor lock-in**, and an inability to migrate to another cloud service provider.
 - Some native cloud encryption systems **do not allow customer keys to move outside the system**, and cloud encryption systems are based on proprietary interfaces.
 - The goal is to maintain **protection regardless of where data resides**, moving **between cloud vendors**.



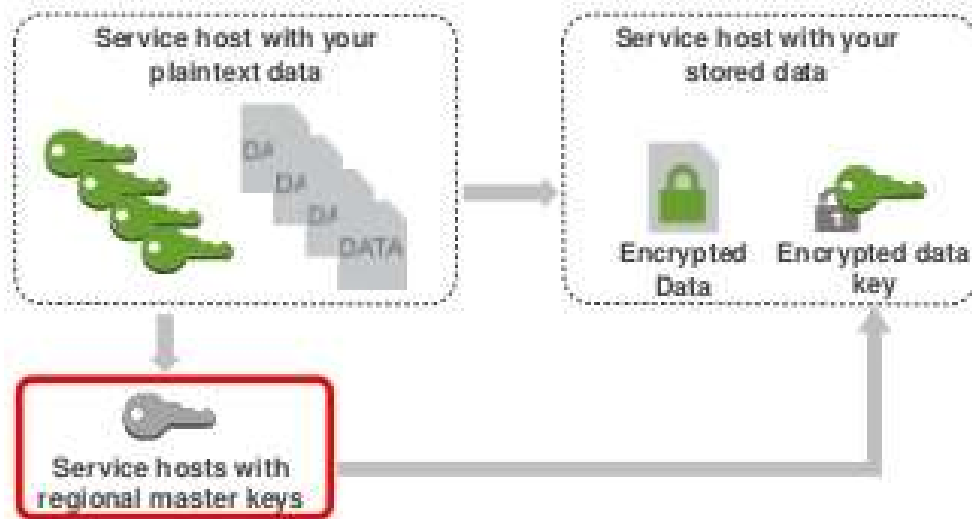
Amazon S3 client-side encryption



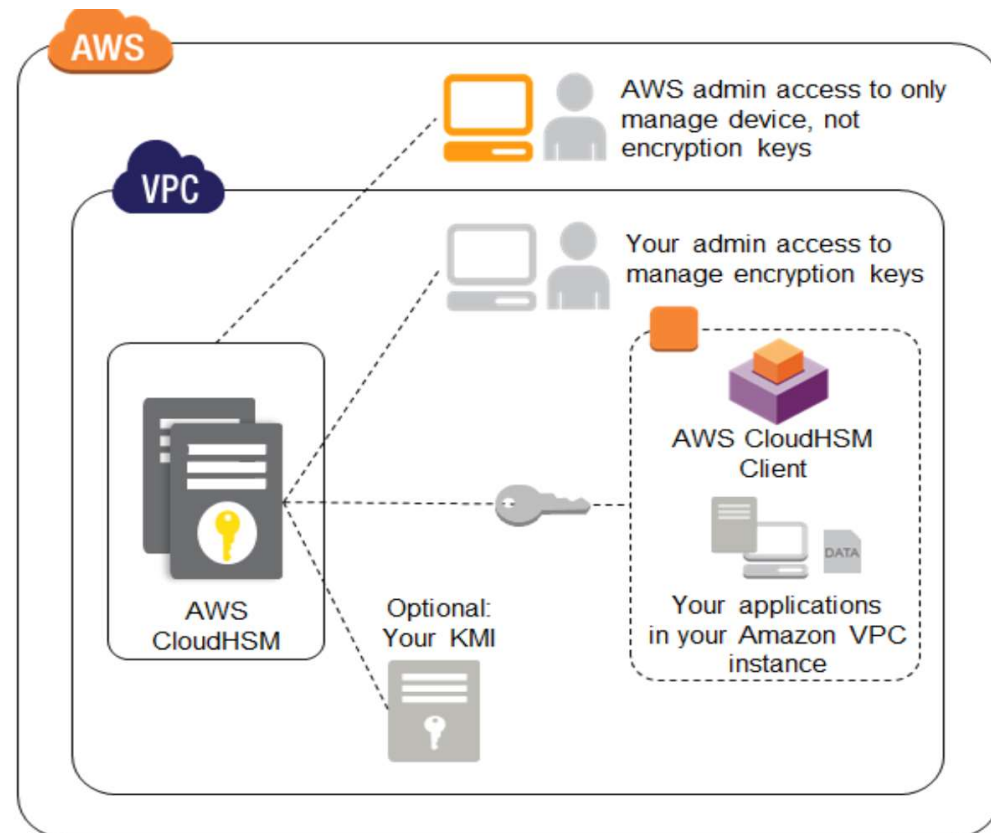
- Amazon S3 encryption and decryption takes place in the **EMRFS client** on your cluster.
- Objects are encrypted before being uploaded to Amazon S3 and decrypted after they are downloaded.
- The EMR (Elastic MapReduce) File System (**EMRFS**) is an implementation of HDFS that all Amazon EMR clusters use for reading and writing regular files from Amazon EMR directly to Amazon S3.

AWS encryption key management

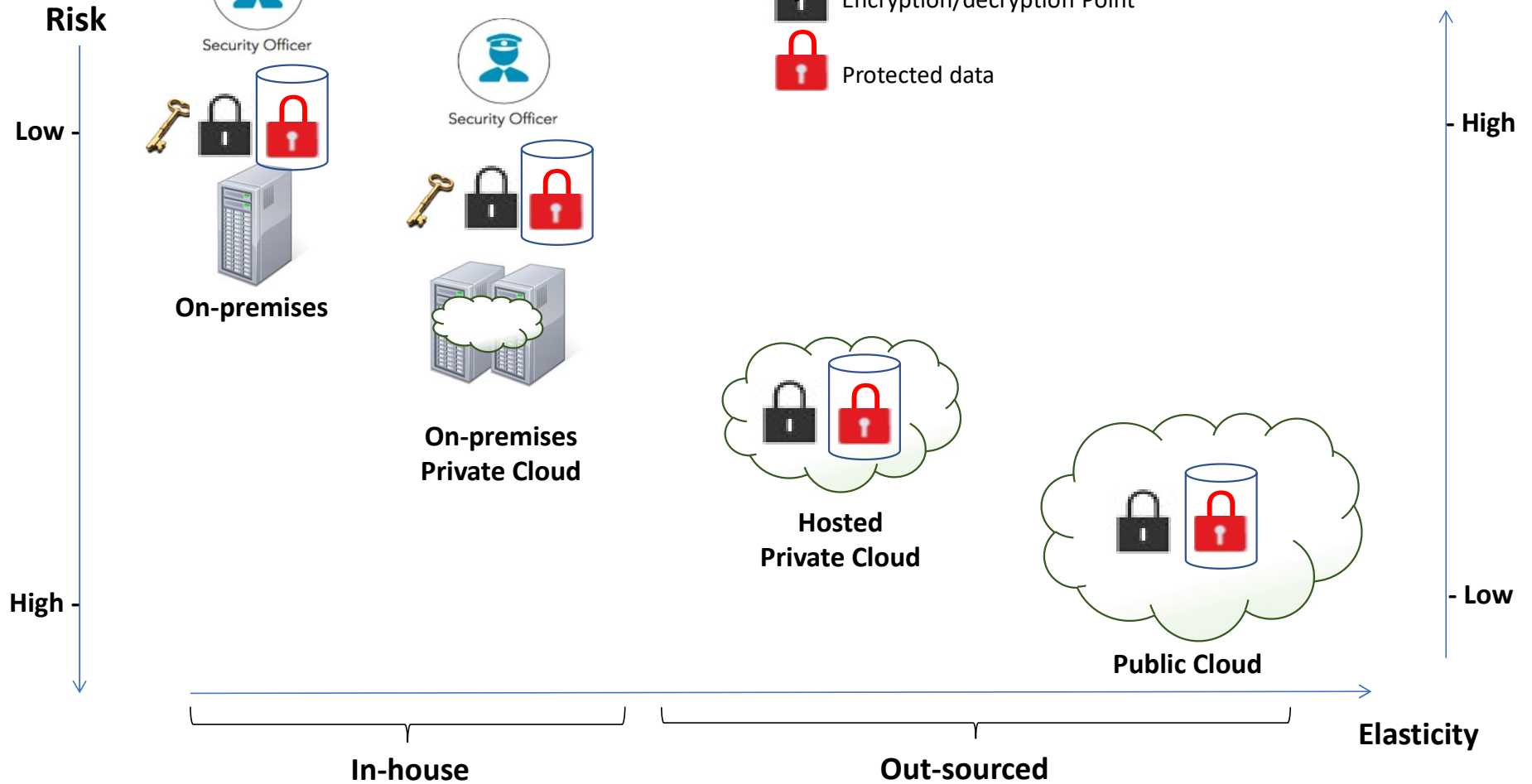
- AWS service generates unique 256-bit AES data key per object, archive, cluster or database
- Service uses regularly rotated, regional 256-bit AES master keys to encrypt data keys
- Your encrypted data key is stored with your encrypted data



- Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources
- Your virtual networking environment allows selection of your own IP address range, creation of subnets, and configuration



Computing Cost



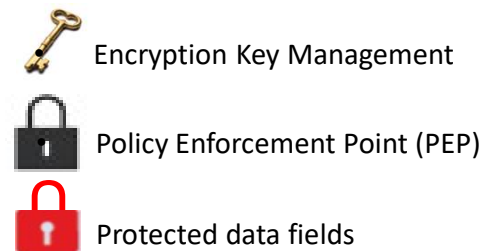
A Cloud Security Gateway (CASB) can protect sensitive data in Cloud (SaaS)

Separation of Duties



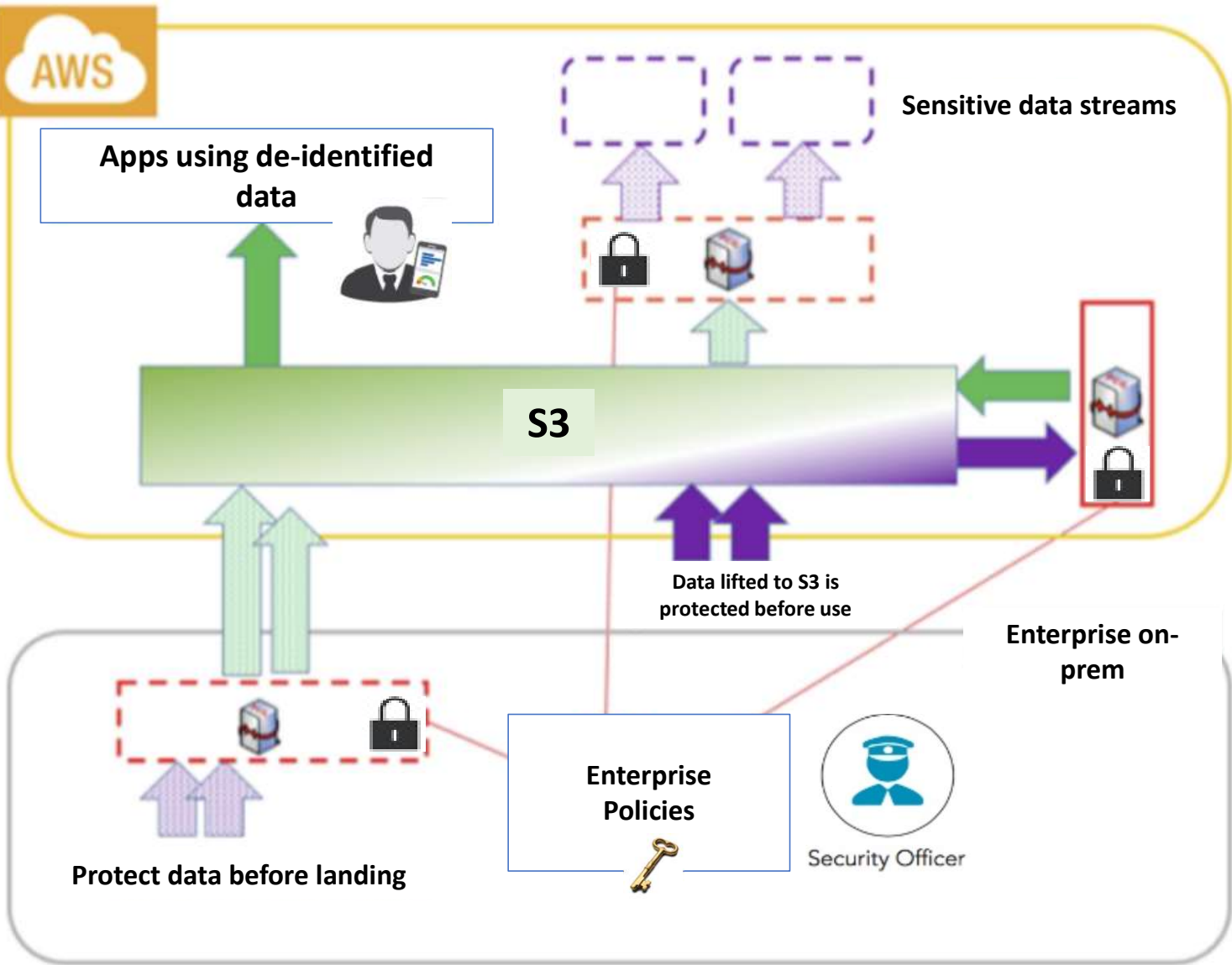
- Example of supported protocols include HTTP, HTTPS, SFTP, and SMTP
- Based on configuration instead of programming
- Secures existing web services or REST API calls
- See and control where sensitive data travels

1. Install the Cloud Security Gateway in your trusted domain
2. Select the fields to be protected
3. Start using Salesforce with enhanced security





Protection of data in AWS S3 with Separation of Duties

- Applications can use de-identified data or data in the clear based on policies
- Protection of data in AWS S3 before landing in a S3 bucket



Separation of Duties

-  Encryption Key Management
-  Policy Enforcement Point (PEP)

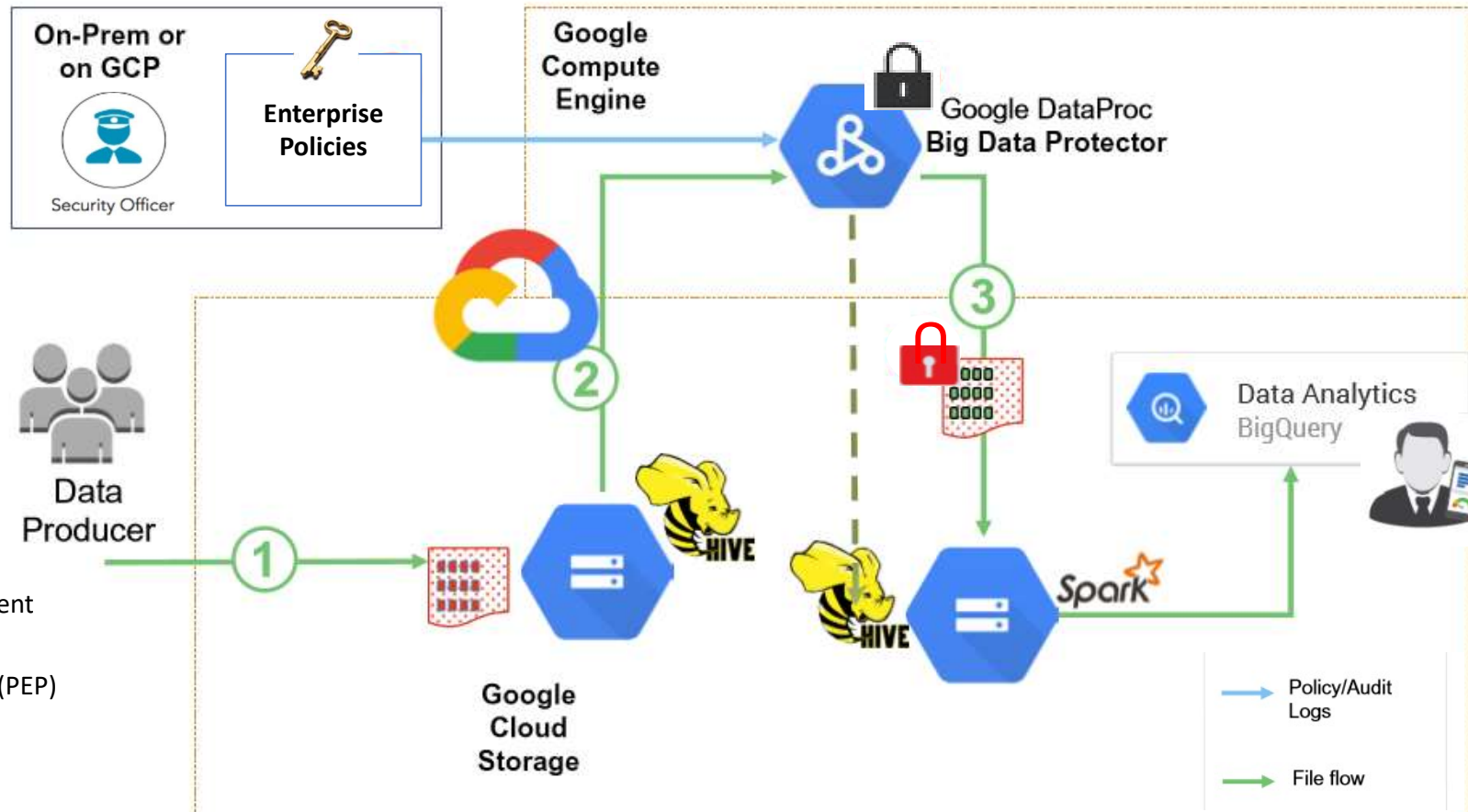
Big Data Protection with Granular Field Level Protection for Google Cloud

Big Data Protector
tokenizes or encrypts
sensitive data fields

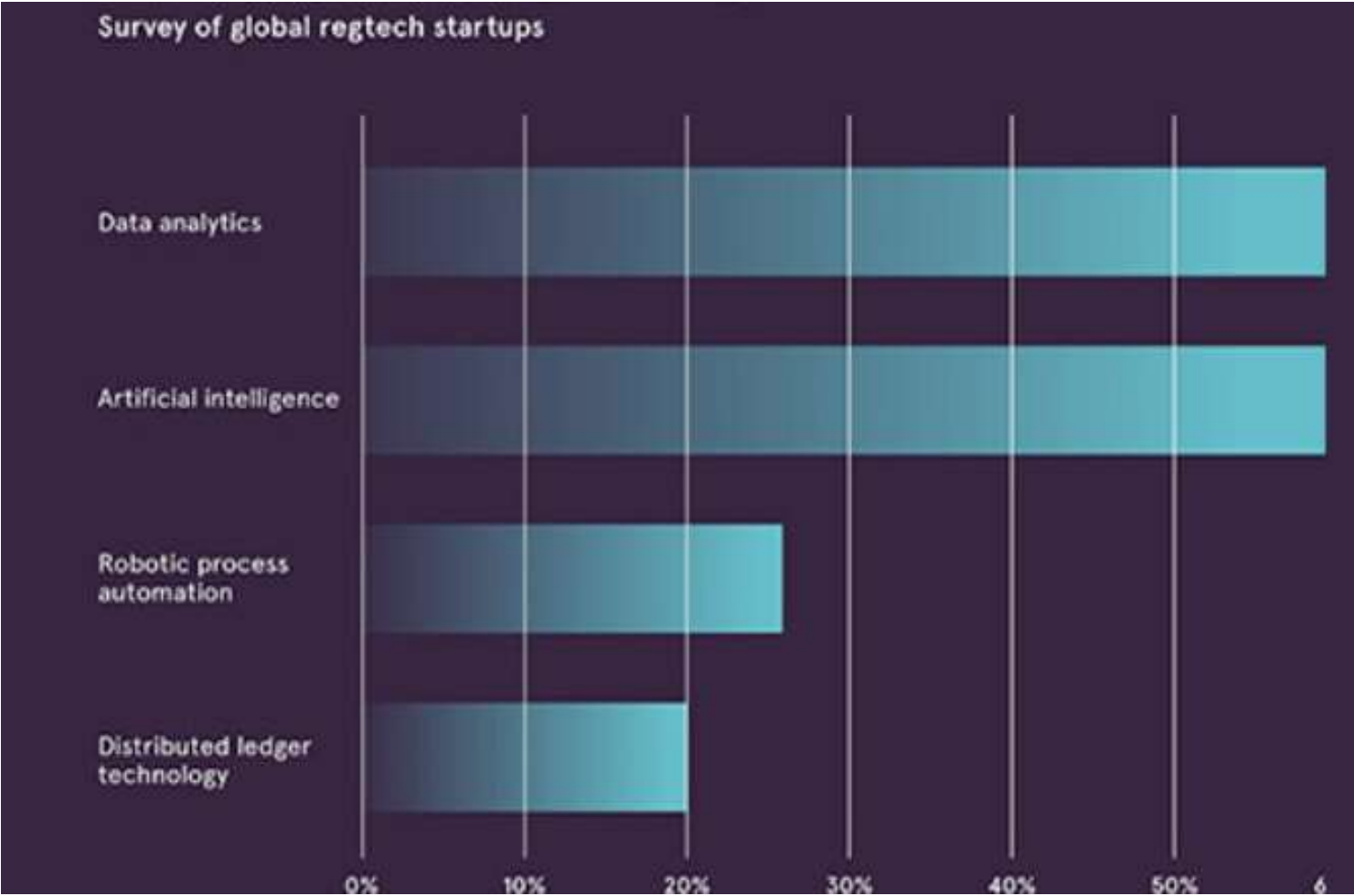


Separation of Duties

Policies may be managed
on-prem or Google Cloud
Platform (GCP)



Underlying Technology for RegTech Solutions



Source: medium, fintechnews



Shared platforms are most useful when built with digital technologies - Examples

Privacy Enhancing Technologies (PETs)

The market recently began exploring the use of PETs in KYC (e.g., FCA's July 2019 AML and Financial Crime TechSprint in London focused on applying examples of PETs to AML/KYC).^{2 3}

Homomorphic encryption (HE): Enables the processing of machine-to-machine encrypted data without the need to decrypt the data. Basically, HE allows data to remain encrypted while it is analyzed and processed.

Zero-knowledge proof (ZKP): Enables data to be verified without revealing the data itself. The technology can transform the way data is collected, used and transacted. ZKP uses the concept of a verifier and a prover. In each transaction, the prover can use the data without revealing the input or the computational process to the verifier.

Data Sharing Technologies

Digital Identity

Some shared platforms use biometrics and machine learning tools to establish, maintain and share digital identities of individuals or entities, while reducing friction for end users (e.g., India's Aadhaar).¹

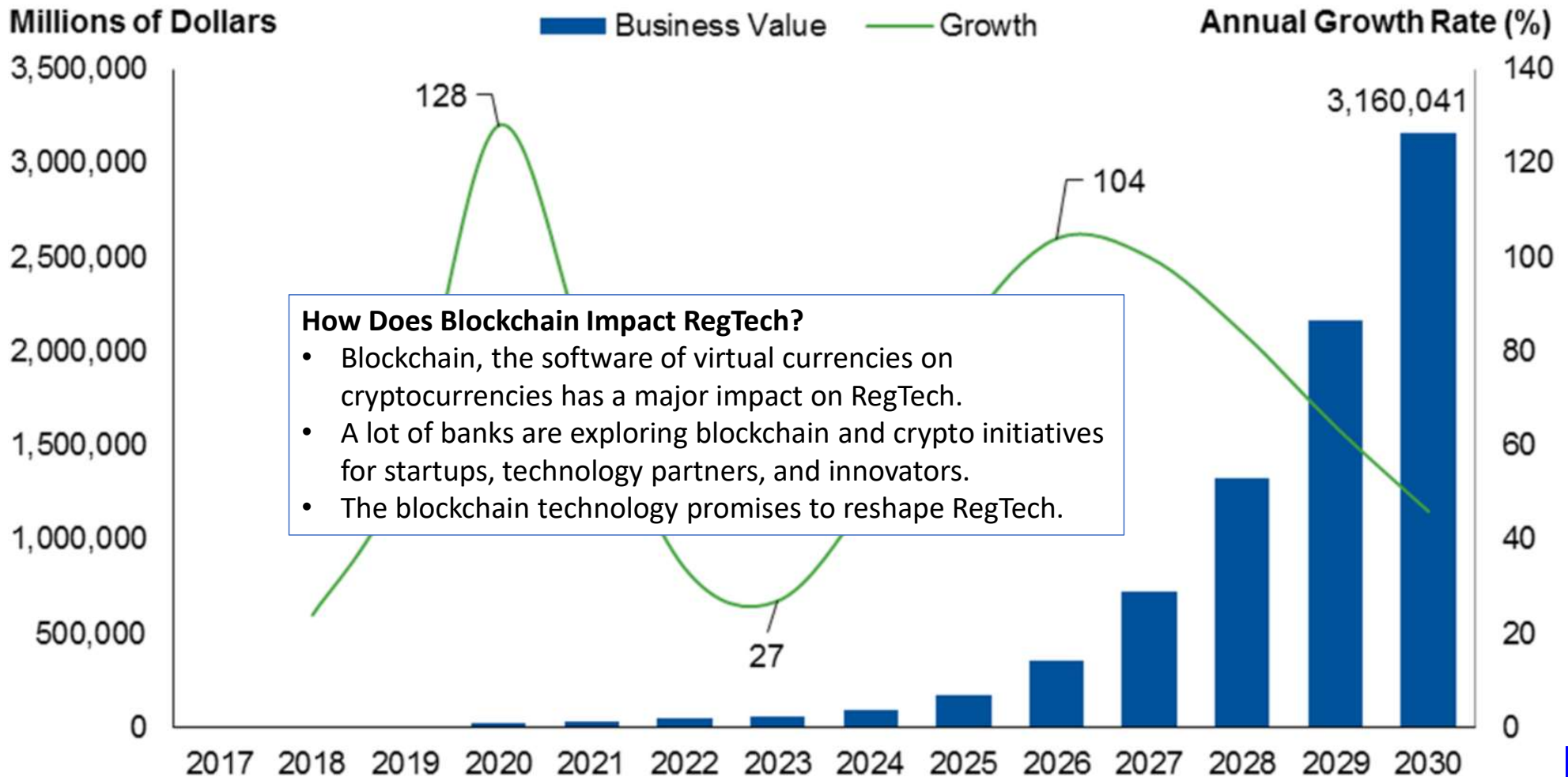
DLT, such as blockchain, underpins a secure ledger of digital events that is shared among all the parties participating in the events. Blockchain is bonded in nature, as each block can contain several transactions and has a unique proof of work attached. Together with the unique proof of work from the previous block, a chain effect is created, making it impossible to alter the information.⁴

DLT allows a high degree of data privacy and security while maintaining transparency through an audit trail of data changes. DLT uses smart contracts to help streamline roles and responsibilities in a shared platform.

Source: <https://regtechassociation.org/wp-content/uploads/2019/11/Protiviti-IRTA-Urgent-Call-KYC-Optimization-Final-Report.pdf>



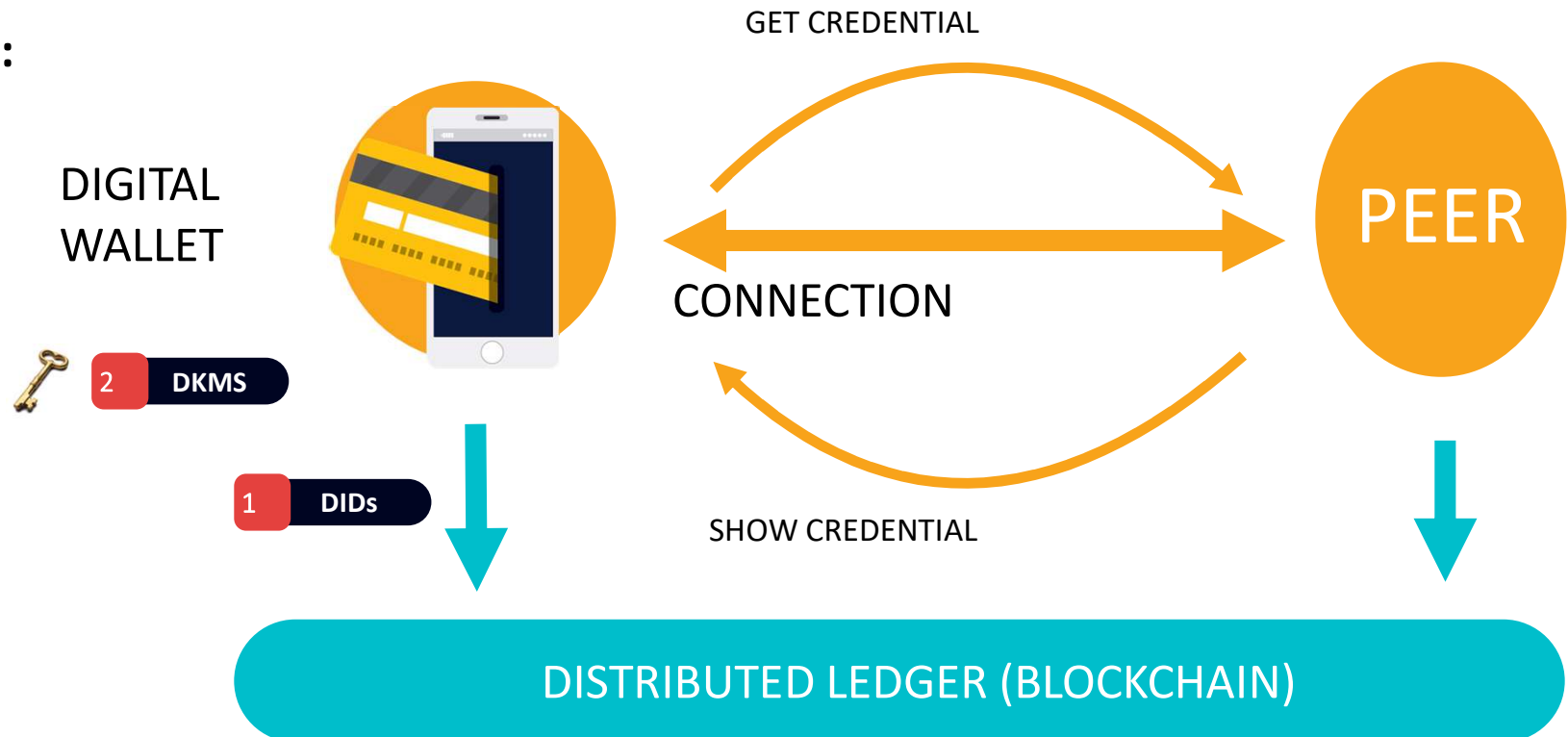
Gartner Forecast: Blockchain Business Value, Worldwide



Emerging De Jure Standards for Self-Sovereign Identity (SSI)

1. Verifiable Credentials, (W3C)
2. DID Auth, (IETF)
3. DKMS (Decentralized Key Management System), (OASIS)
4. DID (Decentralized Identifier), (W3C)

SSI Example:

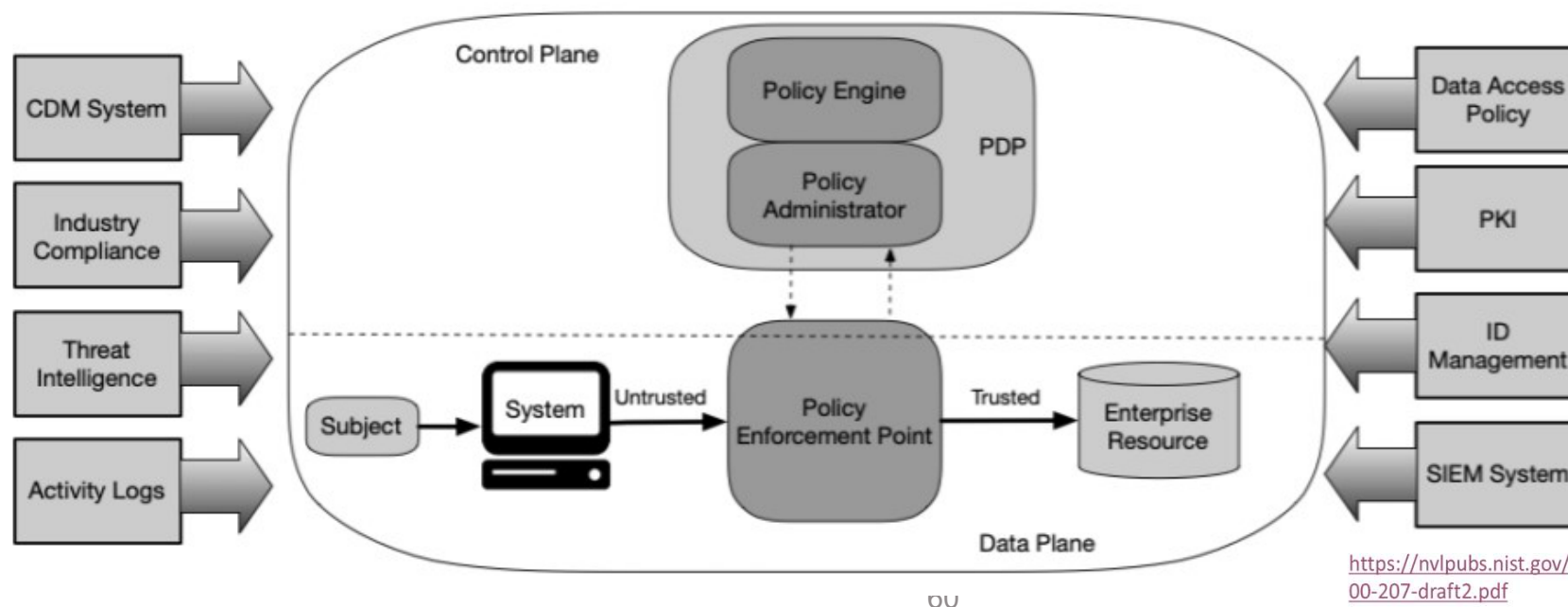


Source: sovrin



A zero trust architecture (US NIST, ANSI X9)

1. All data sources and computing services are considered **resources**.
2. All **communication is secured** regardless of network location.
3. Access to individual enterprise resources is granted on a **per-session** basis.
4. Access to resources is determined by **dynamic policy**—including the observable state of client identity, application, and other behavioral attributes.
5. The enterprise **monitors assets** to ensure that they remain in the **most secure state possible**.
6. All resource authentication and authorization are **dynamic and strictly enforced before access is allowed**.
7. The enterprise collects the **current state of network infrastructure** and communications.



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf>



References:

1. California Consumer Privacy Act, OCT 4, 2019, <https://www.csoonline.com/article/3182578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html>
2. CIS Controls V7.1 Mapping to NIST CSF, <https://dataprivacylab.org/projects/identifiability/paper1.pdf>
3. GDPR and Tokenizing Data, <https://tdwi.org/articles/2018/06/06/biz-all-gdpr-and-tokenizing-data-3.aspx>
4. GDPR VS CCPA, <https://wirewheel.io/wp-content/uploads/2018/10/GDPR-vs-CCPA-Cheatsheet.pdf>
5. General Data Protection Regulation, https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
6. IBM Framework Helps Clients Prepare for the EU's General Data Protection Regulation, <https://ibmsystemsmag.com/IBM-Z/03/2018/ibm-framework-gdpr>
7. INTERNATIONAL STANDARD ISO/IEC 20889, https://webstore.ansi.org/Standards/ISO/ISOIEC208892018?gclid=EAIaIQobChMIvI-k3sXd5gIVw56zCh0Y0QeeEAAYASAAEgLVKfD_BwE
8. INTERNATIONAL STANDARD ISO/IEC 27018, https://webstore.ansi.org/Standards/ISO/ISOIEC270182019?gclid=EAIaIQobChMlleWM6MLd5gIVFKSzCh3k2AxKEAAYASAAEgKbHvD_BwE
9. New Enterprise Application and Data Security Challenges and Solutions <https://www.brighttalk.com/webinar/new-enterprise-application-and-data-security-challenges-and-solutions/>
10. Machine Learning and AI in a Brave New Cloud World <https://www.brighttalk.com/webcast/14723/357660/machine-learning-and-ai-in-a-brave-new-cloud-world>
11. Emerging Data Privacy and Security for Cloud <https://www.brighttalk.com/webinar/emerging-data-privacy-and-security-for-cloud/>
12. New Application and Data Protection Strategies <https://www.brighttalk.com/webinar/new-application-and-data-protection-strategies-2/>
13. The Day When 3rd Party Security Providers Disappear into Cloud <https://www.brighttalk.com/webinar/the-day-when-3rd-party-security-providers-disappear-into-cloud/>
14. Advanced PII/PI Data Discovery <https://www.brighttalk.com/webinar/advanced-pii-pi-data-discovery/>
15. Emerging Application and Data Protection for Cloud <https://www.brighttalk.com/webinar/emerging-application-and-data-protection-for-cloud/>
16. Data Security: On Premise or in the Cloud, ISSA Journal, December 2019, ulf@ulfmattsson.com
17. Webinars and slides, www.ulfmattsson.com

Thank You!



Ulf Mattsson
ulf@ulfmattsson.com