

ELCA for
Client name
Date



Data Governance Event – 6th February 2018 – Geneva - Warwick Hôtel

Keep your data safe and be compliant via a 360° approach

Nagib Aouini – Head of Cyber Security / Blockchain

Agenda

- 1 — Why data breaches will continue to occur
- 2 — What is Data Governance
- 3 — How to comply with regulations with an effective data governance
- 4 program
- 5 — 360° Data Security Approach
- 6 — Q&A

Data breaches stories

Top Data Breaches in 2017

USER *****

PASS *****



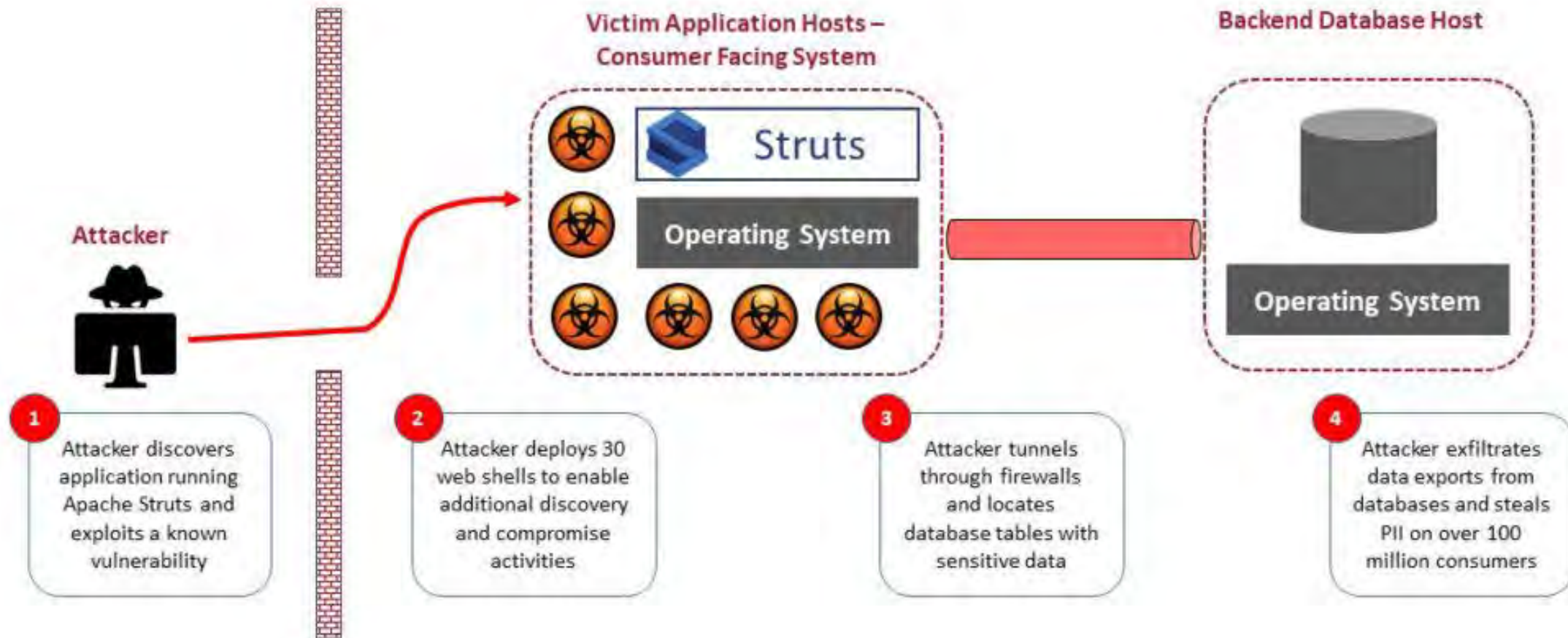
A low-angle shot of a modern glass skyscraper, identified as the Equifax building. The building's facade is composed of numerous rectangular glass panels reflecting the sky. A large, semi-transparent red rectangular box is superimposed over the middle section of the building. Inside this box, the text "MASSIVE DATA BREACH HITS 143 MILLION AMERICANS" is written in a bold, white, sans-serif font. At the bottom right of the image, the word "EQUIFAX" is visible in large, red, three-dimensional block letters mounted on a metal structure.

**MASSIVE DATA
BREACH HITS 143
MILLION AMERICANS**

EQUIFAX

The Equifax Breach

Story #1
Failed to implement a WAF
and vulnerability mgt



<https://baffle.io/the-threat/equifax-breach/>



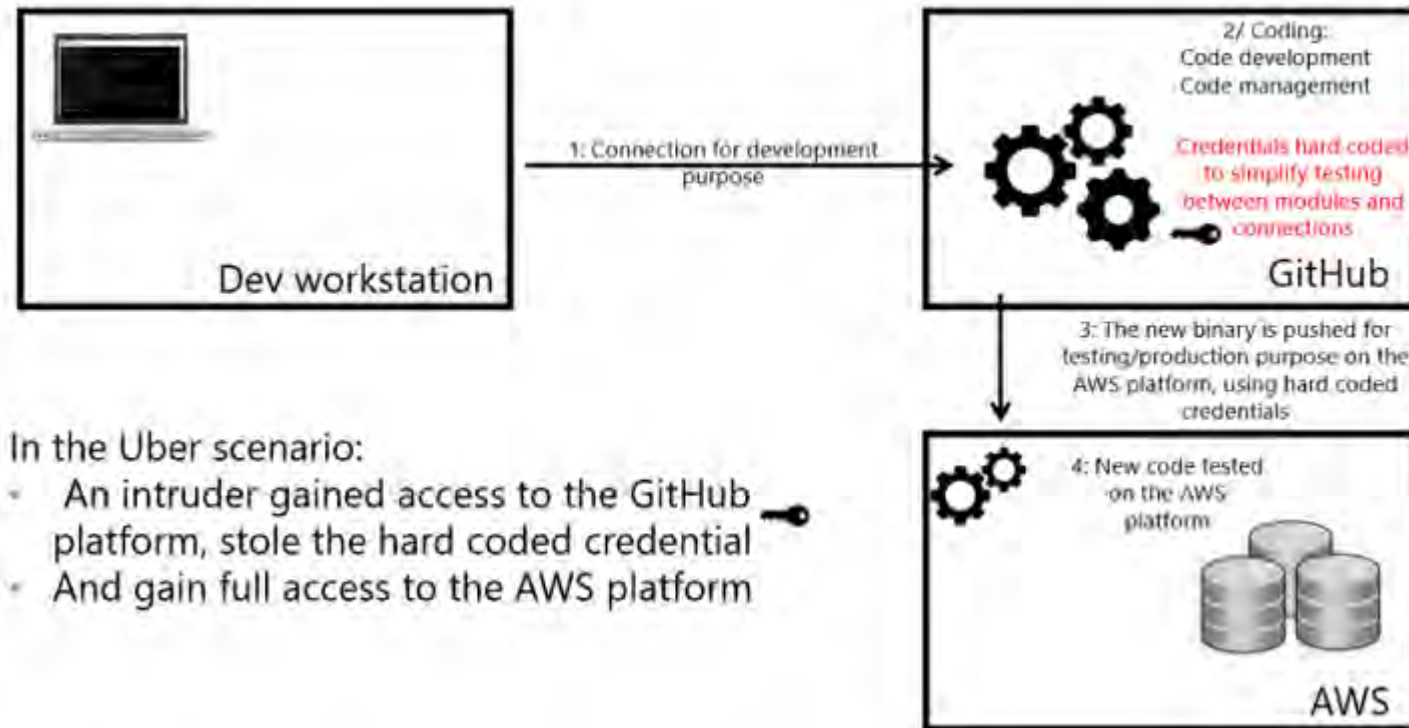
BREAKING NEWS

UBER HID CYBERATTACK THAT EXPOSED 57 MILLION PEOPLE

NIGHTLY
NEWS

How those breaches can happen

Story #2
Failed to implement
Two-Factor and Privileged ID Mgt



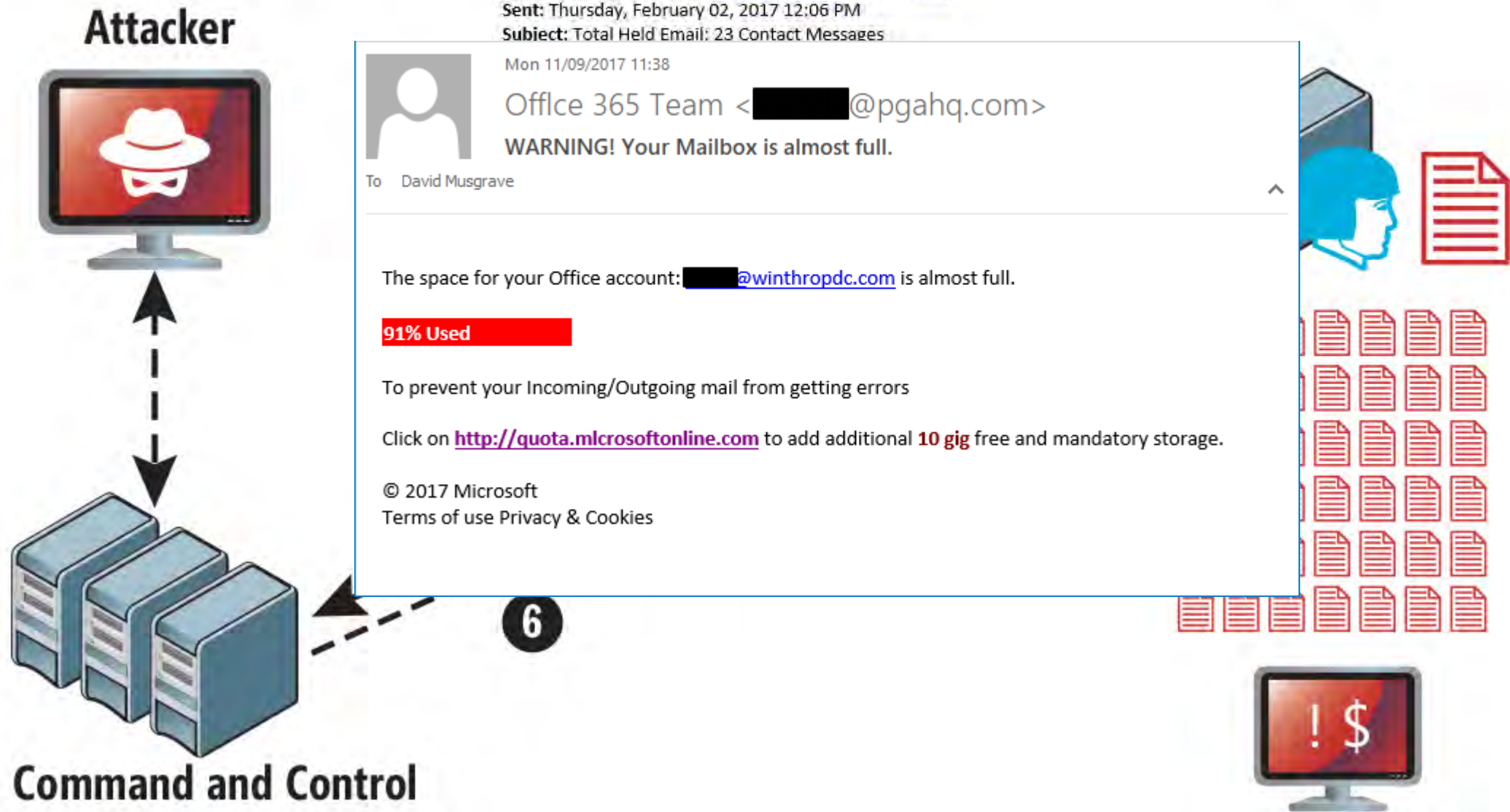
- The data of 57 million users has been stolen from Uber.
- Malicious intruders managed to gain access to a GitHub private coding site used by some Uber software engineers, find AWS credentials, and use them to steal private data.



Microsoft Office 365 hit by ransomware



Behind the Attack – Locky Infection

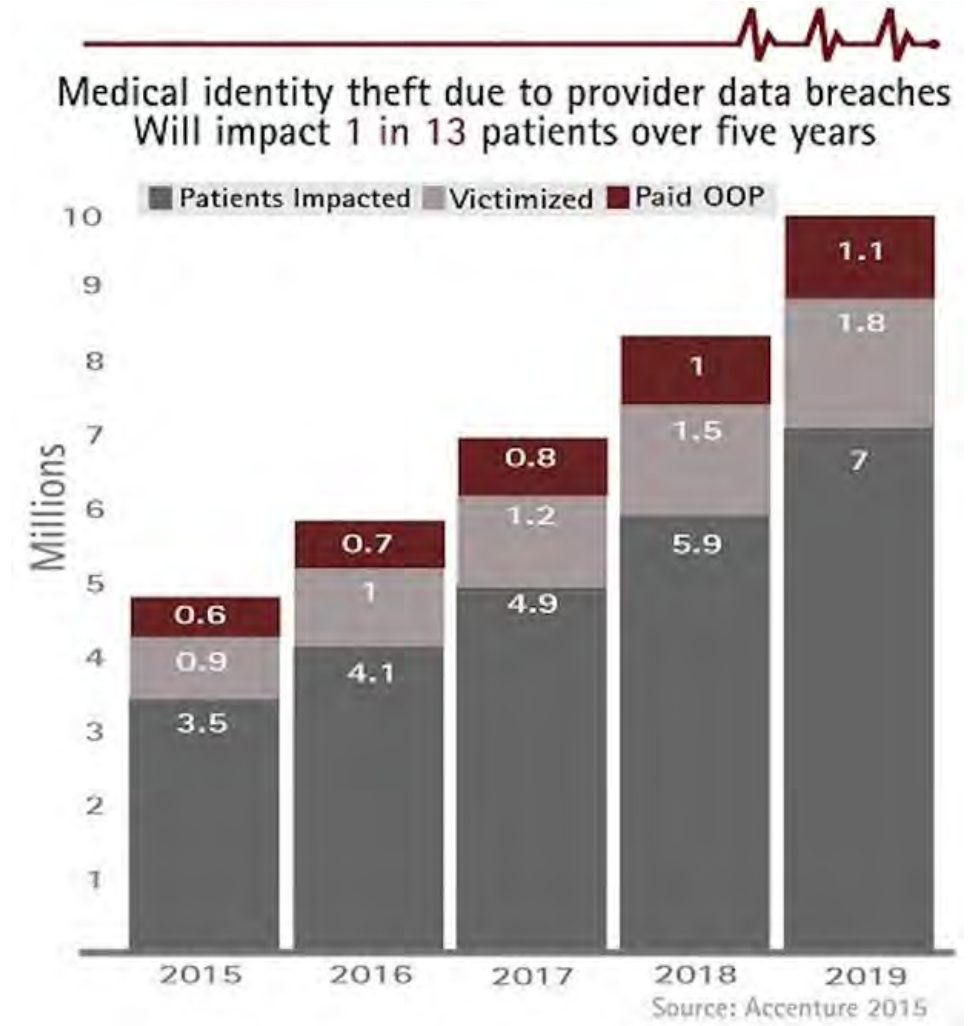


Threats to Healthcare IT systems

- Data stolen from a bank quickly becomes useless once the breach is discovered and passcodes **are changed**
- Data from the healthcare industry, which includes both personal identities and medical histories, **can live a lifetime**
- Healthcare IT and apps use are secured only with simple username / password with no password policy enforced
- Managing access control and putting strong security controls is challenging in healthcare environment because of “Need to work” principle (emergency access, doctors needs access to HER ...)

This data can be used to launch

Spear phishing scams, Identity theft, social engineering frauds ---





Use case study : Protecting a medical information system and electronic health record

Challenge: Development of a medical portal accross Switzerland allowing hospitals, doctors and patients to access medical information hosted on a CRM or Web app portal (even fat client via Citrix). This portal contains patient data that is protected by [Swiss law](#)

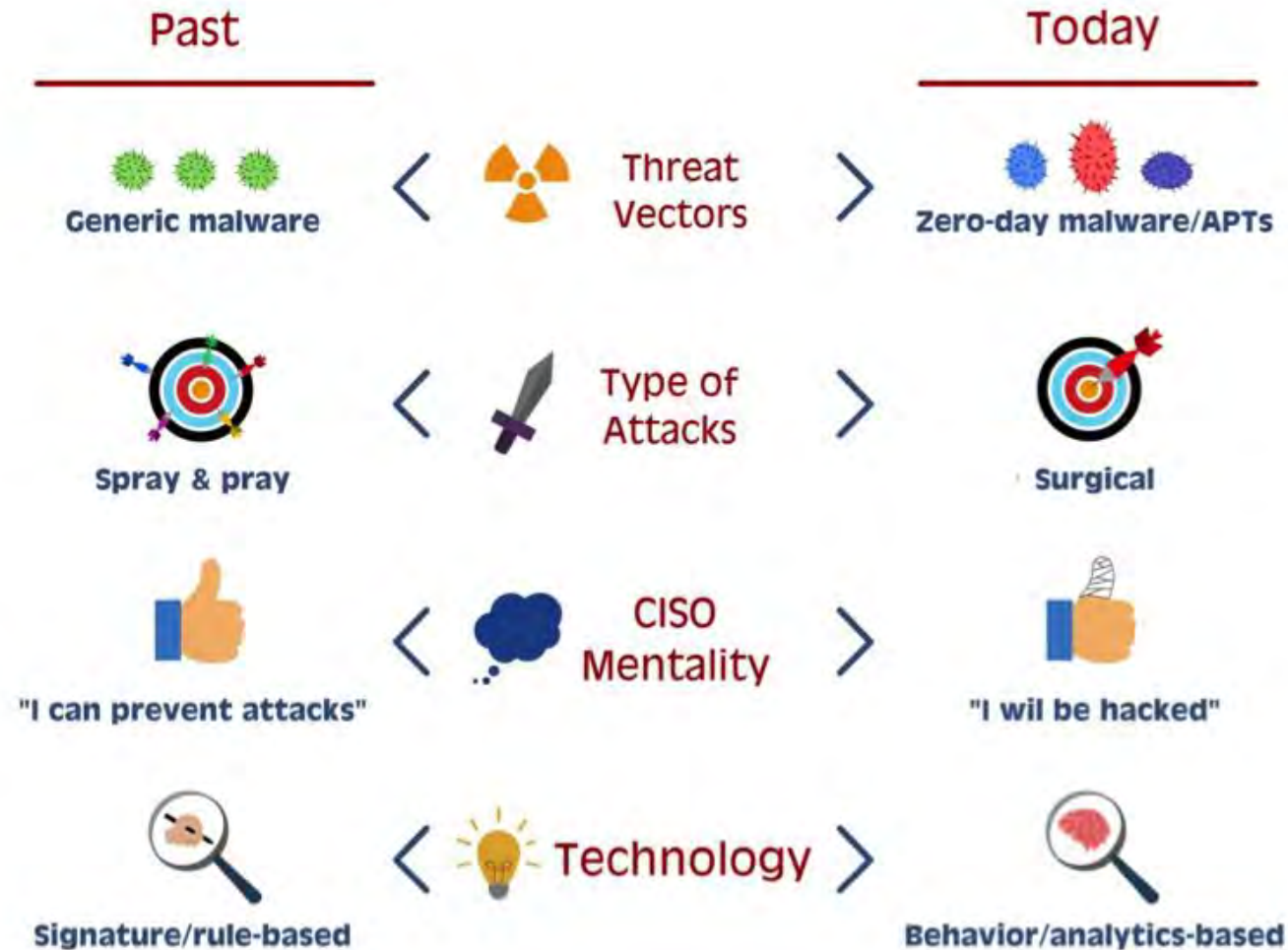
Problem: privacy and control of data shall be ensured and data center hosted outside Switzerland is a serious risk for such information, but also unauthorized access (because of leaked credential).

⚡ Malicious hackers can target physicians via spear-phishing attack to get credentials.



⚡ Login credentials are lost or stolen, resulting in unauthorized access to patient record.

Mentality must evolved



What is Data Governance

3

Data Management Program Drivers

- Need to share and integrate data with external partners
- Alignment with Business Strategy supporting innovation
 - Allow the business to identify opportunities being more agile
- Need to cope with different kinds of business built over time with specific priorities and different subsidiaries
 - Rather independent departments/subsidiaries with own processes
 - Part of the tools not shared or used differently
 - Tools continuously changing
- Control the risk
 - Responsibility of the company towards shareholders, customers and authorities (*)
 - Information lifecycle must be very well controlled
 - The company must be able to provide consistent and reliable information

*: Example: **General Data Protection Regulation (Regulation (EU) 2016/679)**, **FINMA Circular 2008/21 "Operational Risks – Banks"**,

EU Regulation 73-2010 Aeronautical Data and Information Quality, Solvency II Directive 2009/138/EC ,



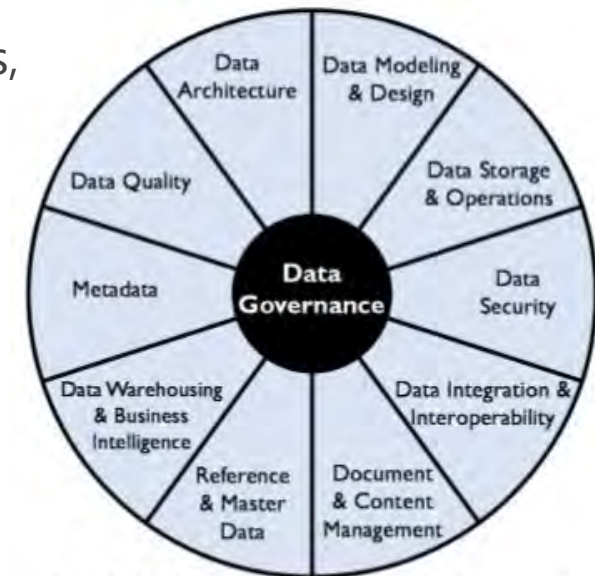
Data Governance

Data Governance: decision making and oversight process that prioritizes investments, allocates resources and measures results to insure that data being managed is leveraged to support business needs

■ Goals:

1. Enable an organisation to manage its data as an asset
2. To sponsor, track, and oversee the delivery of data management projects and services
3. Define, approve, communicate and implement principles, policies, procedures, metrics, tools, and responsibilities for data management
4. To manage and resolve data related issues

➤ Data Governance is more than Data Quality, Policies, Standards.
It is about aligning Data Management with **Corporate Needs** and **Strategy**, to **optimize its results** and to **control risks**

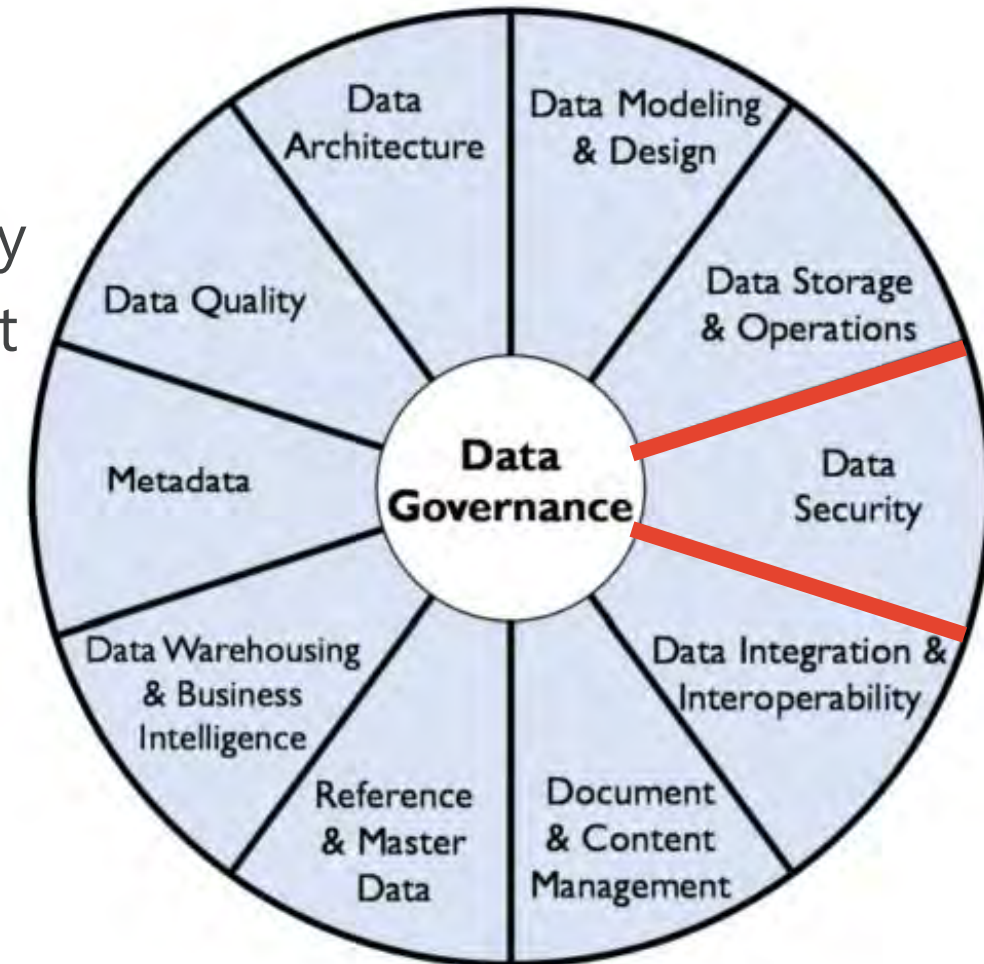


DAMA-DMBOK2 Data Management Framework

Copyright © 2017 by DAMA International

DMBOK Data Management Framework

- A **framework** for understanding comprehensively and see relationships between Data Management components
- The 11 **functions** (knowledge areas) depend on one another and need to be aligned
- Ideas and concepts will be **applied differently** based on organization industry, culture, maturity level, strategy, vision and challenges it is facing



The DAMA-DMBOK2 Data Management Framework (The DAMA Wheel)

How to comply with regulations

3

Applicable regulations : GDPR



Replaces and extends European Directive 95/46/EC from May 25th 2018

Applies to controllers or processors established in the Union

Applies to controllers or processors not established in the Union where the processing activities relate to the offering of goods or services to data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.

GDPR roles and entity

Data subject

The data subject is a natural person whose personal data processed by a processor or controller

Personal Data

Information that is an attribute or can directly/indirectly identify a data subject

Data Processor

The entity or individual that processes personal data on behalf of the data controller

Data Processing

Operation performed on data subject's personal data no matter if the data is processed automatically or not wholly automated

Profiling

The recording and analysis of data which is intended to evaluate Data Subject's behavior

Data Controller

The entity that determines the purpose of processing data subject's data

Personal Data Breach

refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, transmitted, stored, processed

DPO

The DPO is a person who will administer the organization's compliance with their data protection processing activities



Applicable regulations Swiss Federal Data Protection Act



Needs to be harmonised with EU standards. The Federal Council has adopted a DPA revision process in Sept. 2017 and released a draft version of the future DPA

Apply to controllers and processors established in Switzerland

The revised DPA is announced for the end of 2018

Data privacy framework by ELCA

Governance

- ▶ Data privacy policies
- ▶ Data privacy roles & responsibilities
- ▶ Data privacy training & awareness
- ▶ External criteria tracking

Operational processes

- ▶ Inventory of personal data & data transfers
- ▶ Respect of the data subjects' rights
- ▶ Protection of Personal data
- ▶ Data breach management
- ▶ Monitoring of new operational practices

Legal & compliance

- ▶ Data Privacy Risk Assessments
- ▶ Data privacy by design and by default
- ▶ Data privacy notices
- ▶ Contractual clauses
- ▶ Data privacy audits

FINMA controls

#1 Governance

#1 Client Identifying data
CID

#3 Location & Access to
Data

#4 Security standards for
IT & Tech

#5 Selection, monitoring
and training of employee
with access to CID

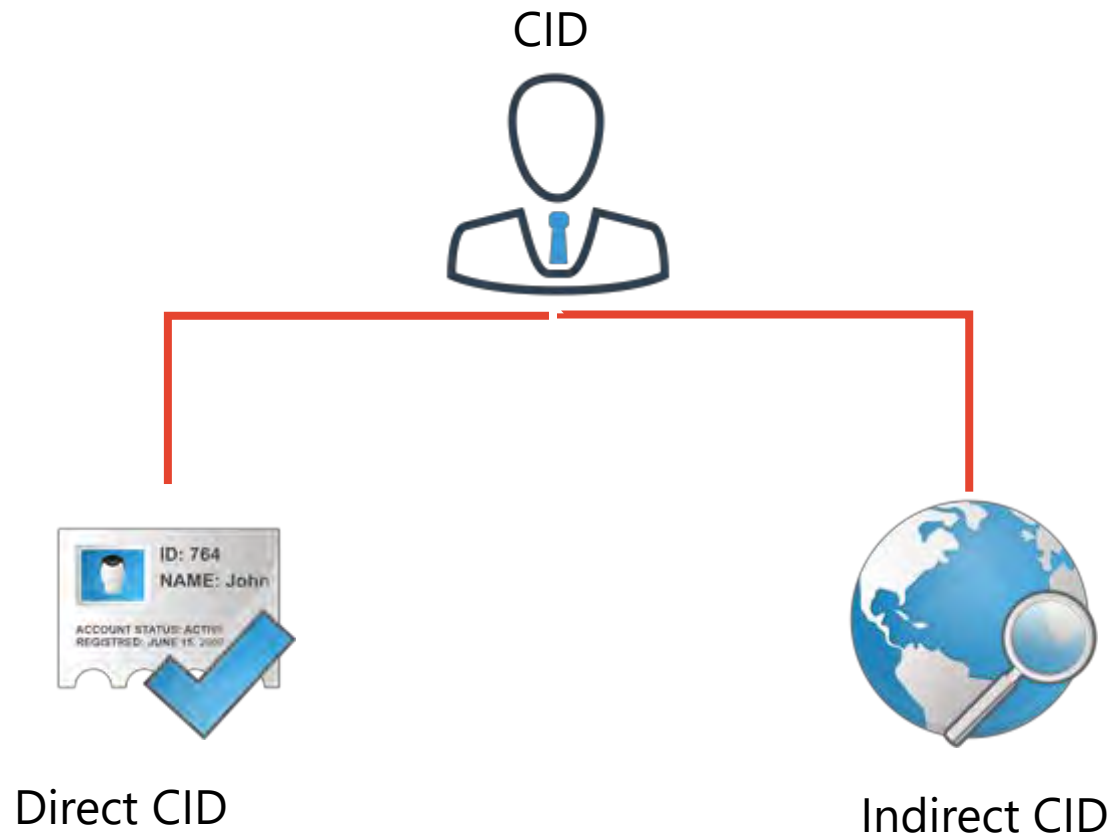
#5 Identifying and
controlling risks related to
the confidentiality of CID

#7 Confidentiality of CID :
risk mitigation

#8 Incident related to
the confidentiality of CID,
internal /external comm

#9 Outsourcing providers
and large projects in
regard to CID

Client Identification Data (CID)

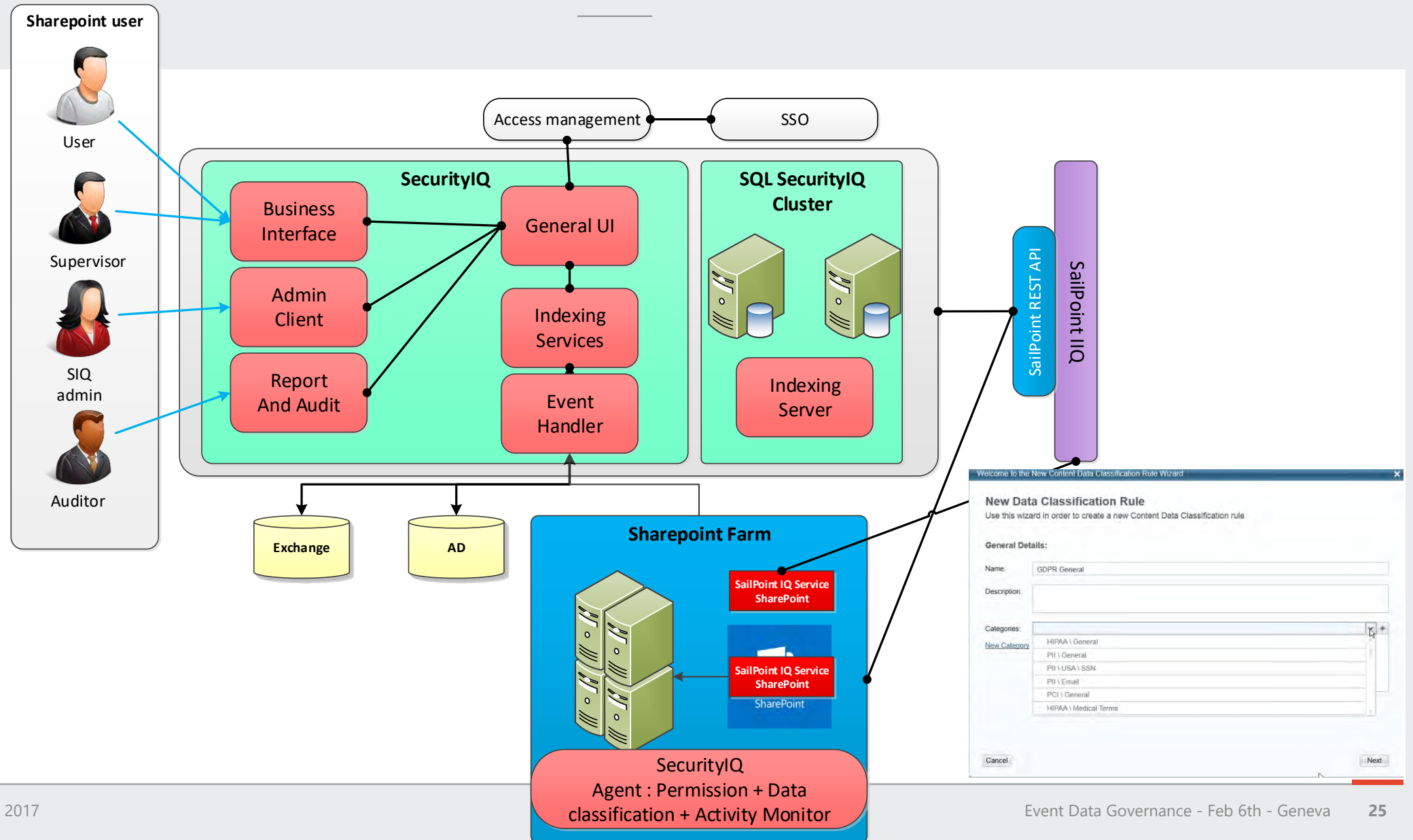


Direct : First name, last name, signature, e-mail address, social network IDs, private or business address, name of company

Indirect : Passport ID, ID Card, Social security number, Tax ID, Car number plates, customer number, IBAN/BIC, Account number, Safe deposit number, Contract numbers, User ID / Passwords, Card numbers (credit and debit cards), IP address (static, dynamic) / Career details

Inference : Day and month of birth, year of birth, nationality, age, gender, diplomatic status hobbies, memberships in professional, private or charity clubs, homeland, zip code, professional qualification, currency of account, credit rating, transaction data

Sharepoint compliant platform with SIQ



How manage CID data in a Sharepoint and being compliant

Need to know principle

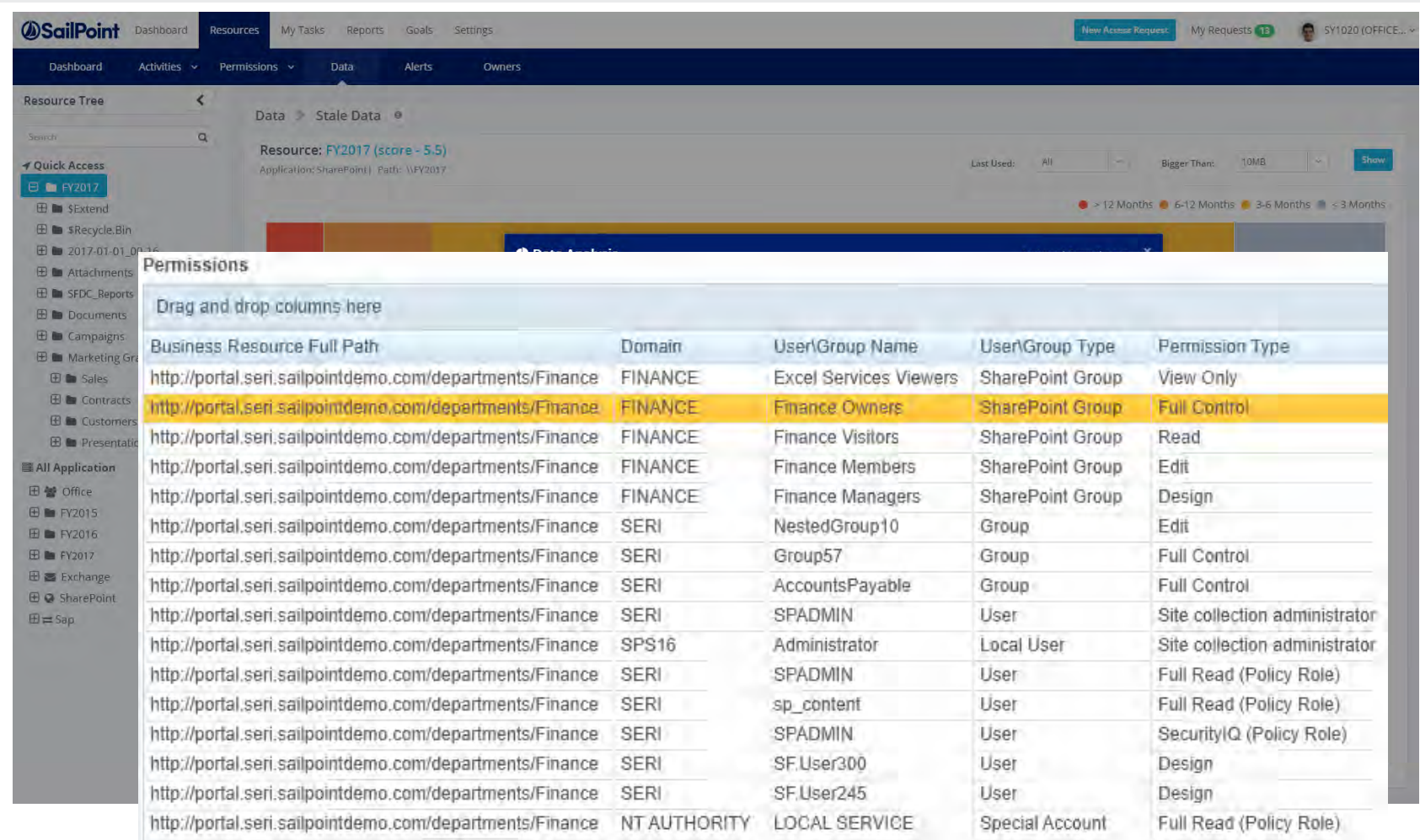
#5 Identifying and controlling risks related to the confidentiality of CID

CID Discovery and tagging

#1 Client Identifying data
CID

Who access what ?

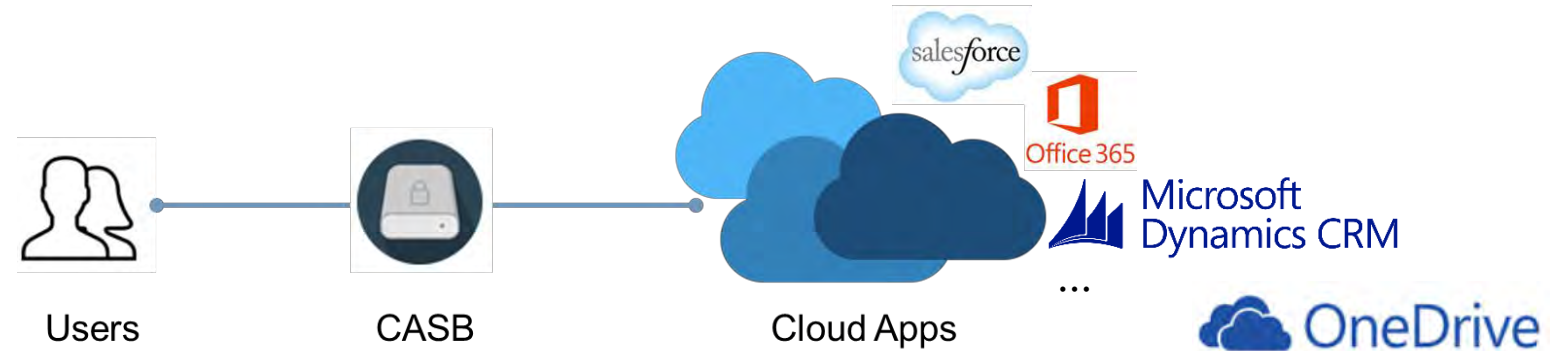
#3 Location & Access to
Data



The screenshot shows the SailPoint interface with the 'Data' tab selected. The 'Resource Tree' on the left lists various resources, including 'FY2017'. The main area displays 'Data > Stale Data' for the resource 'FY2017 (score - 5.5)'. Below this, a 'Permissions' table is shown, listing various permissions for the resource. The table has columns for Business Resource Full Path, Domain, User/Group Name, User/Group Type, and Permission Type. The permissions listed include View Only, Full Control, Read, Edit, Design, and Full Read (Policy Role) for various users and groups.

Business Resource Full Path	Domain	User/Group Name	User/Group Type	Permission Type
http://portal.seri.sailpointdemo.com/departments/Finance	FINANCE	Excel Services Viewers	SharePoint Group	View Only
http://portal.seri.sailpointdemo.com/departments/Finance	FINANCE	Finance Owners	SharePoint Group	Full Control
http://portal.seri.sailpointdemo.com/departments/Finance	FINANCE	Finance Visitors	SharePoint Group	Read
http://portal.seri.sailpointdemo.com/departments/Finance	FINANCE	Finance Members	SharePoint Group	Edit
http://portal.seri.sailpointdemo.com/departments/Finance	FINANCE	Finance Managers	SharePoint Group	Design
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	NestedGroup10	Group	Edit
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	Group57	Group	Full Control
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	AccountsPayable	Group	Full Control
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	SPADMIN	User	Site collection administrator
http://portal.seri.sailpointdemo.com/departments/Finance	SPS16	Administrator	Local User	Site collection administrator
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	SPADMIN	User	Full Read (Policy Role)
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	sp_content	User	Full Read (Policy Role)
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	SPADMIN	User	SecurityIQ (Policy Role)
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	SF.User300	User	Design
http://portal.seri.sailpointdemo.com/departments/Finance	SERI	SF.User245	User	Design
http://portal.seri.sailpointdemo.com/departments/Finance	NT AUTHORITY	LOCAL SERVICE	Special Account	Full Read (Policy Role)

What is a CASB ?



Visibility

who is using which app and
which data is stored where



Threat protection

detects malware stored in the cloud
and suspect behaviours



Data Loss Prevention

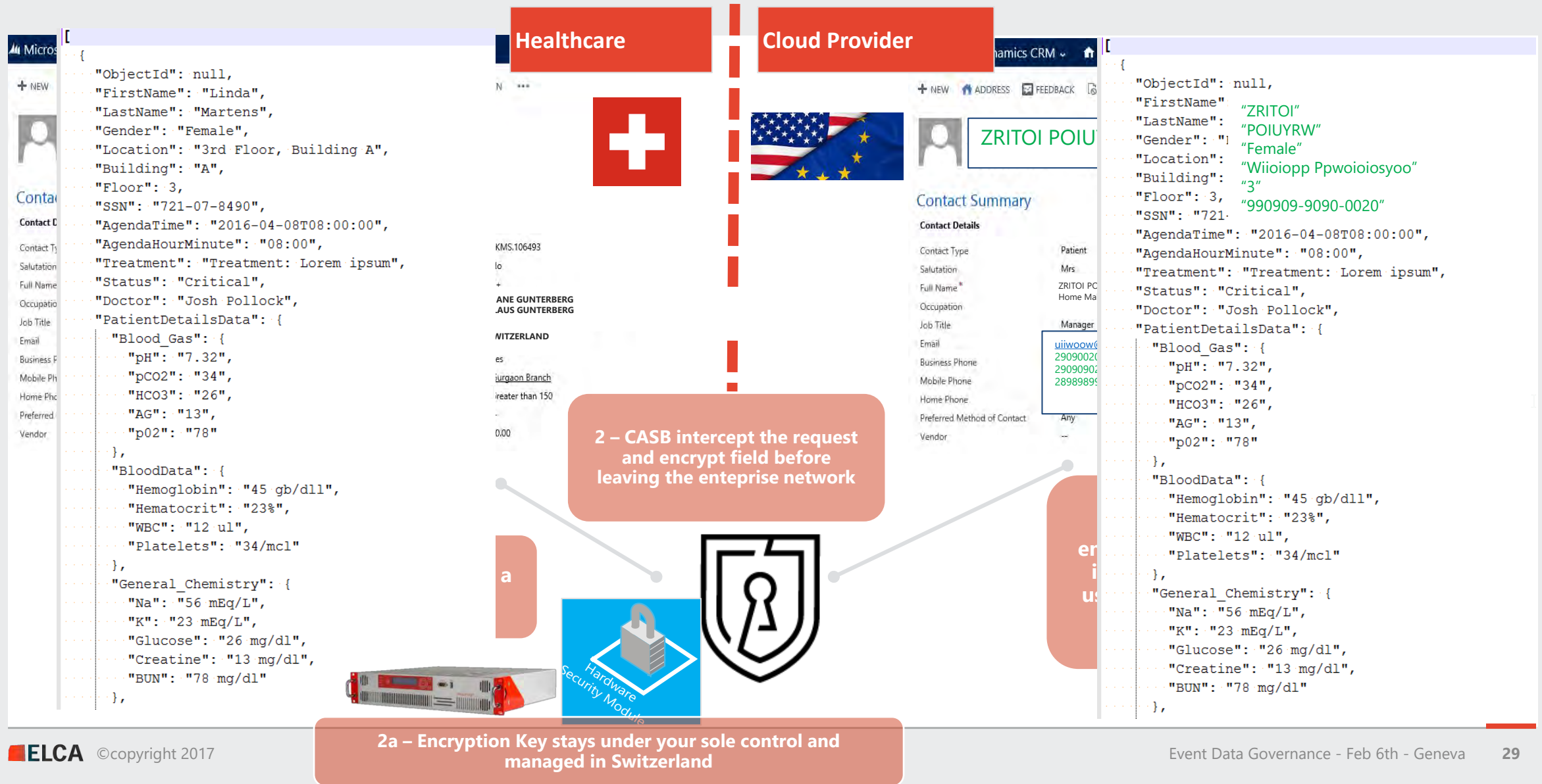
handle information according to
its specificities (ciphering,
tokenization)

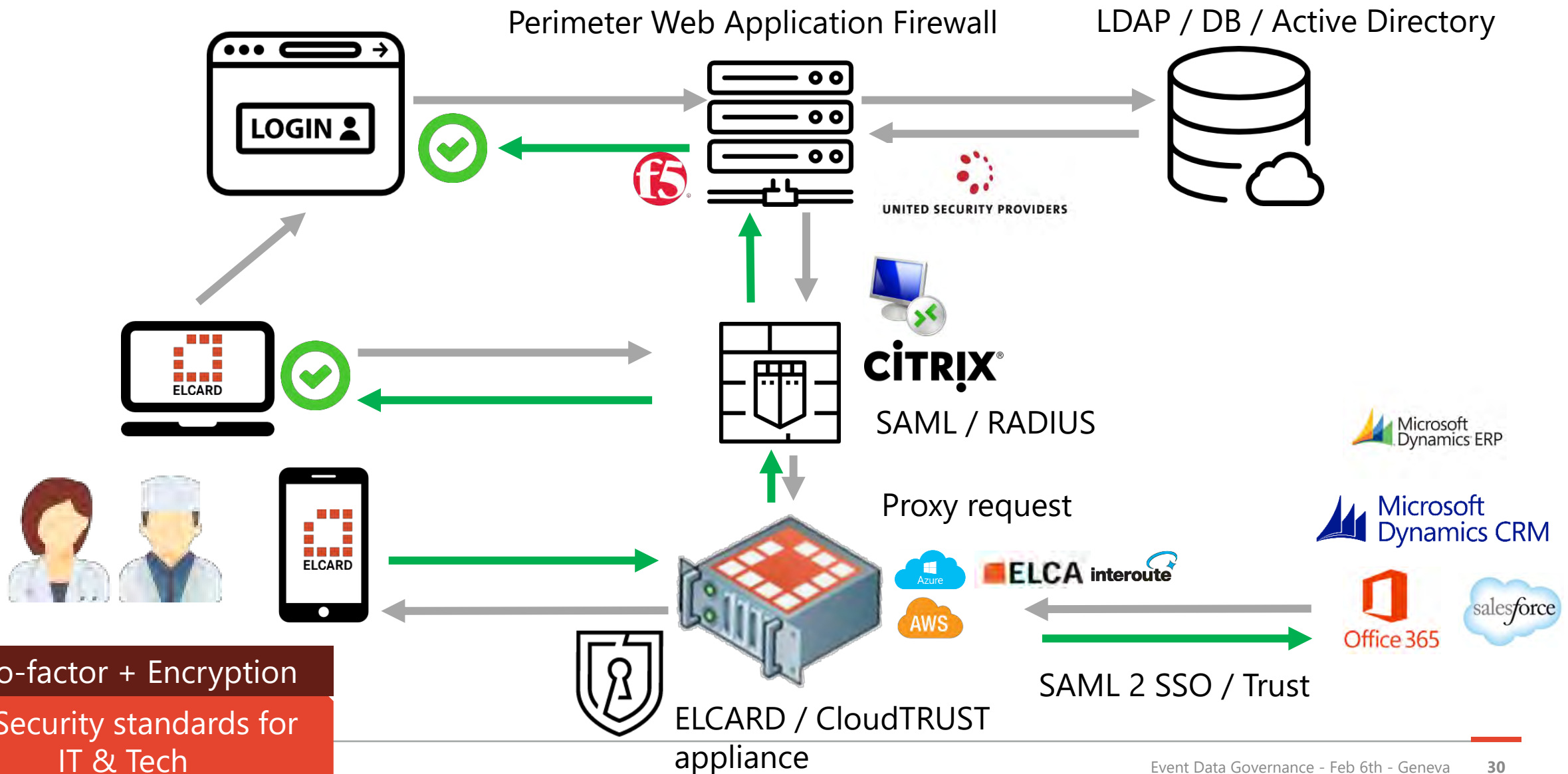


Compliance

ensure compliance with specific
industry regulations

Example : Protect patient data in CRM Online





360° Data Security Approach

360° approach



— **Identify** sensitive, valuable or regulated data (CID). Provide a mean to authenticate user based on claims.

— **Segregate** data to avoid spills

— **Authorize** access based on data classification and user or device via claims

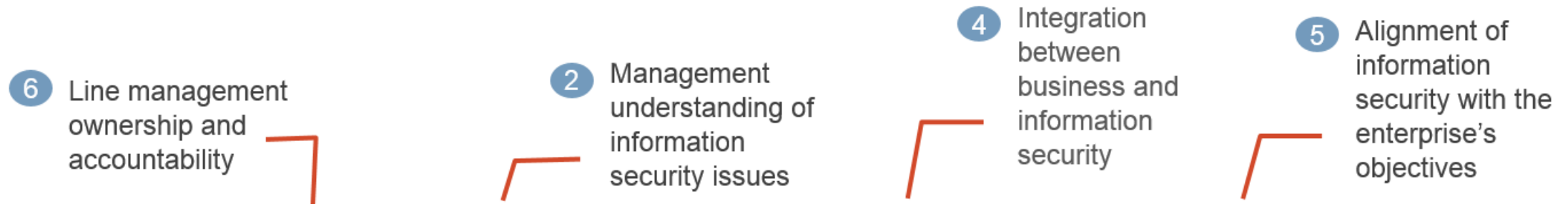
— **Protect** critical data automatically with right management and powerful access control model (like ABAC)

— **Audit** data activity for full visibility



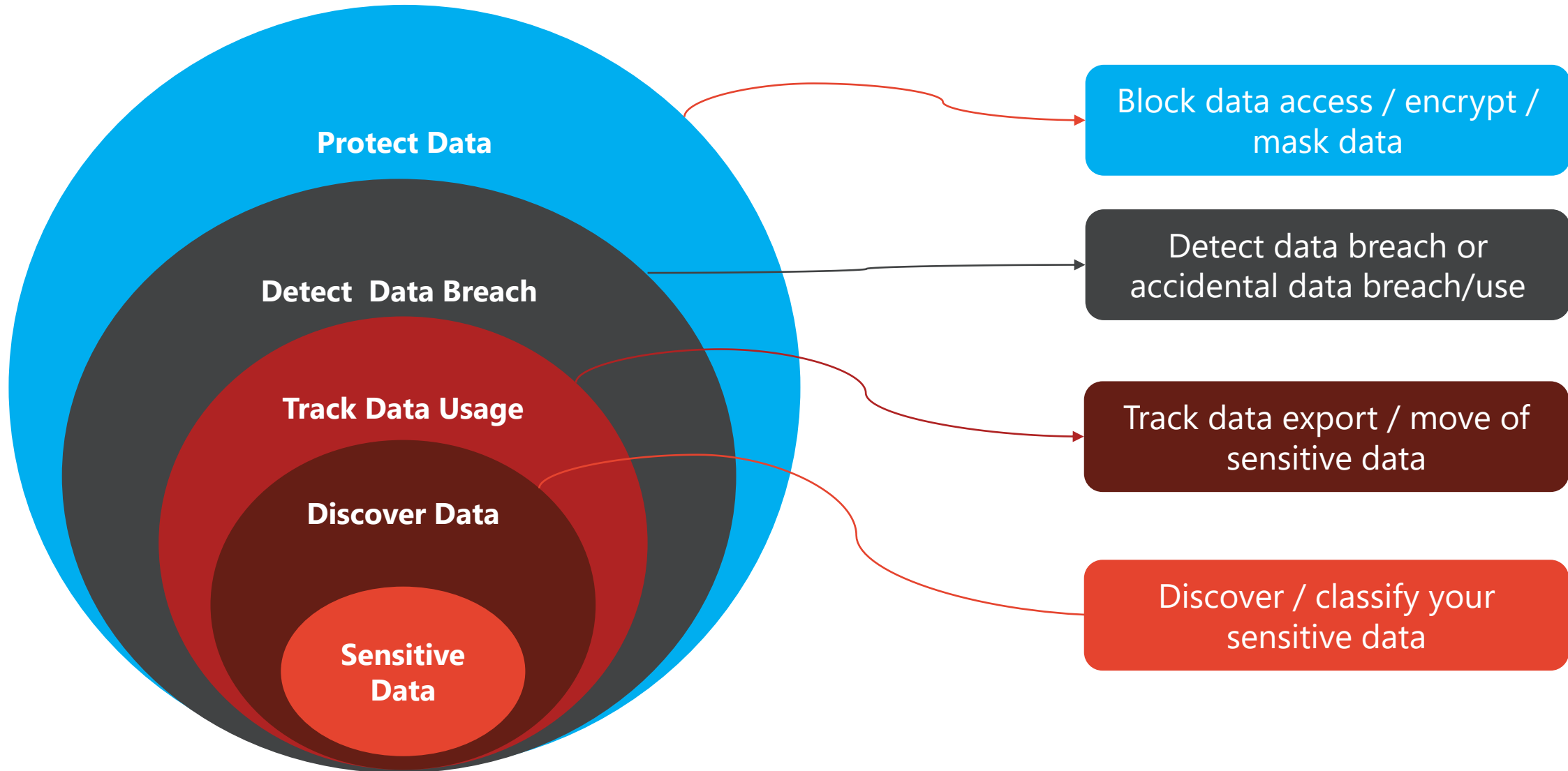
Discover your sensitive Data

Data classification



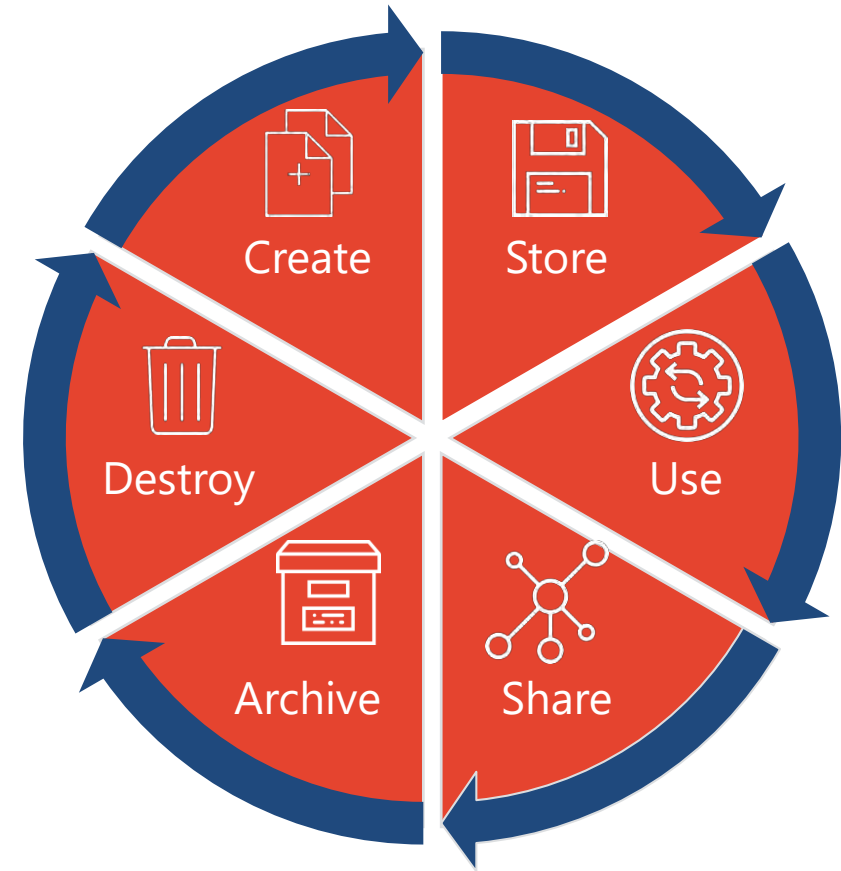
Data type	Owner	Description	Security requirements			Rationales	Impact area
			C	I	A		
Procurement data	Head of procurement	Procurement data include information involved in purchasing, contracting, and negotiating activities within CompanyX.	Medium	Basic	'	Procurement data have medium confidentiality requirements. Conditions granted to a supplier could be coveted by its competitors. Integrity of suppliers' list and associated bills is also important to avoid financial loss due to internal fraud.	Finance, Legal/compliance
Staff/job applicants personal data	Head of HR	This category includes all personal information related to CompanyX's workforce and job applicants	Medium	'	'	Staff/job applicants data have medium security requirements in terms of confidentiality (with regards to the Swiss data protection law and given the sensitivity of remuneration levels).	Reputation, Legal/compliance
			Medium	Medium	'	Payroll data have specific integrity requirements as they are involved in the tax calculation process. The employer endorses penal liability if taxes are not duly paid to the State.	
Financial data	CFO	Financial data comprise all elements necessary to manage CompanyX's performance in terms of profits, revenues, operating income, etc. and to issue its financial statements	Basic	High	Basic	These data have basic confidentiality requirements. The integrity criterion is high, as manipulation of data could lead to fraud and alteration could result in a biased perception of the company's financial health as well as to possible refinancing issues. Given the high transactions volume, unavailability of financial data may leads to bottlenecks in the corresponding workflows.	Operations, Finance, Reputation, Legal/compliance
...

Onion approach for data security



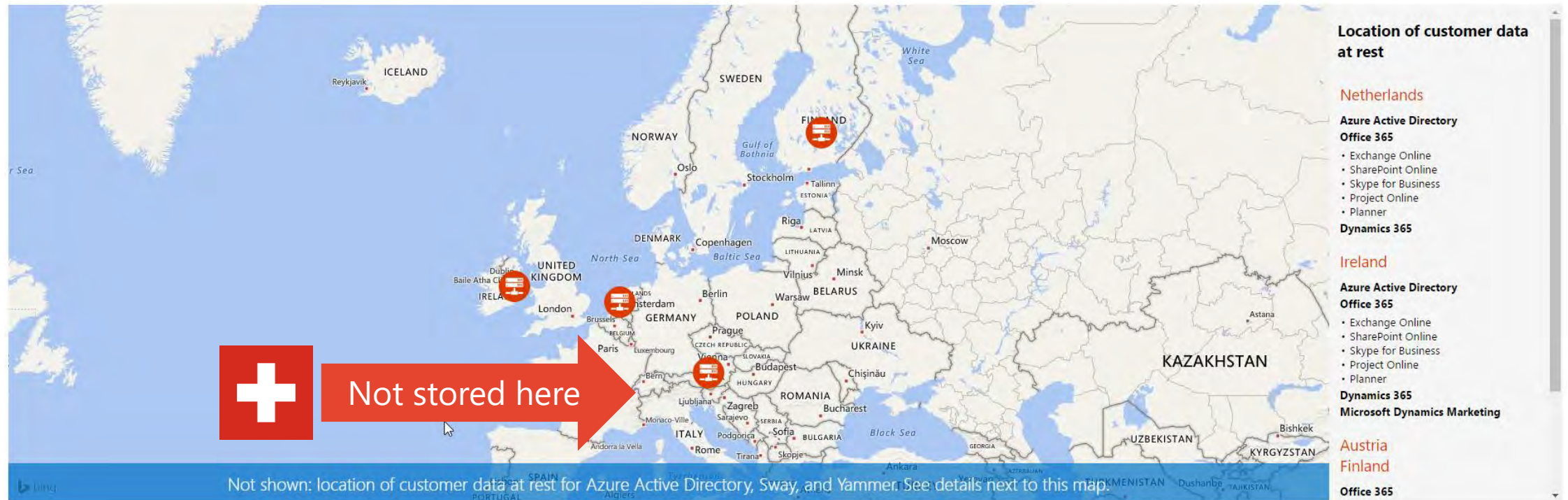
Data lifecycle and cloud challenge

- Generation : trust data ?
- Collection : Which data ?
- Storage : where ?
- Usage : who use it ?
- Sharing : Is it allowed
- Archive : How long ?
- Removal : Definitive ?



Where is my data ?

Europe, Middle East, Africa ▼

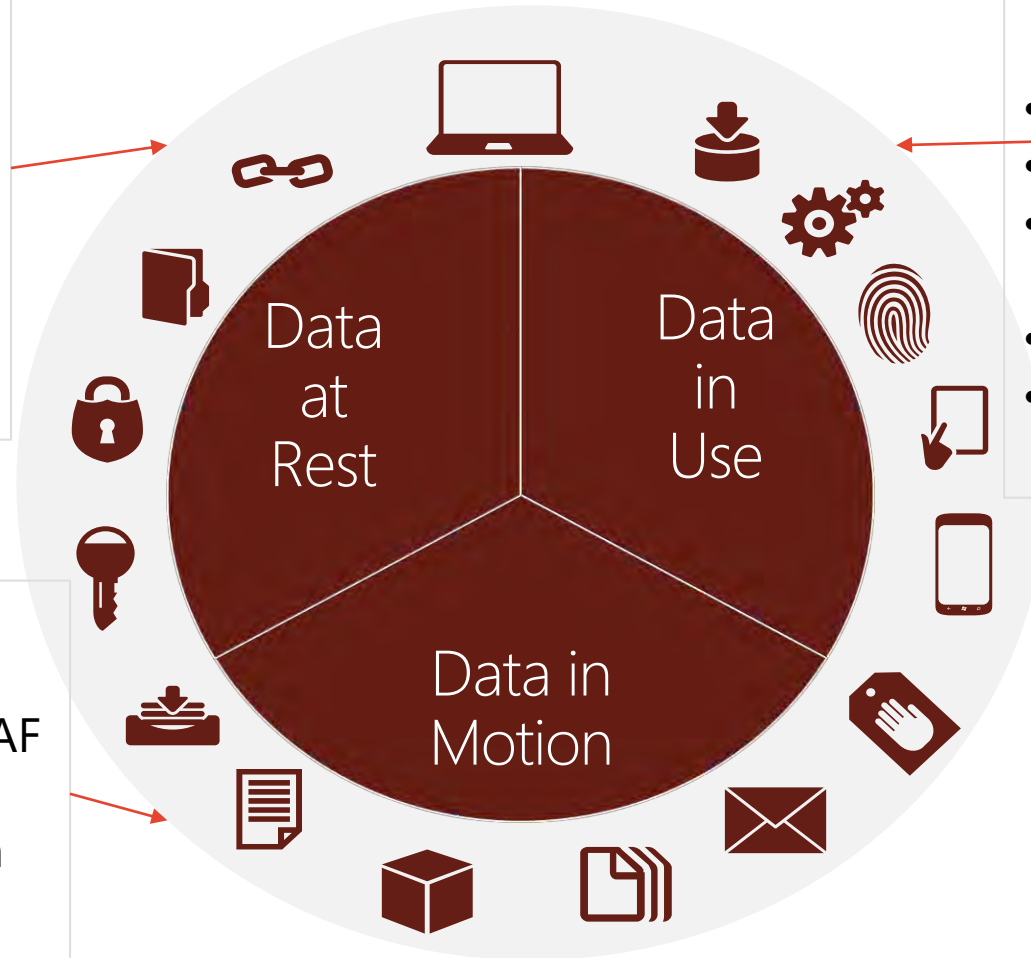


Always Protected

- Database Encryption
- Credential Encryption
- **HSM Key Vaulting**
- Anonymization / Tokenization / Obfuscation
- Network / Server control
- Physical Media Control
- Archive / Destruction

- Privileged Access Management
- **Privileged Account Monitoring**
- Workstation Hardening
- Application Access Control
- Data classification/labelling/tagging
- Removal/media control
- Export control

- Perimeter Security – **WAF**
- Network traffic monitoring/blocking L3-L 7 – WAF
- Web application Firewall – L7
- Data collection and classification
- Remote Access



Source : Microsoft

Classification with SailPoint SecurityIQ

The screenshot displays the SailPoint SecurityIQ web interface. The top navigation bar includes tabs for Activities, Compliance, Permissions, Policies (highlighted in orange), and System. On the left, a sidebar shows a navigation menu with 'Data Classification Policy' selected. Below the menu is a search bar and a tree view showing the hierarchy: Active Directory > Windows File Servers > SERI - Windows File Server > Data. The main content area is titled 'Data Classification Policy' and shows a breadcrumb path '\\ad-resource\Data'. It features a 'Sub-Resources Policies (0)' section with a toolbar containing buttons for New, Associate, Revert, Save, Inherit Rules (set to True), Policy Status (set to Enable), and Configuration. Below the toolbar is a list of policies, each with a red bar on the left and a dropdown menu on the right. The policies are: Finance Folders (ThresholdClassification, Active, Categories Applied: [icon], Inherited from: SERI - Windows File Server, description: The following behavior must match at least 70% of the activities over the last week), Animals (DataClassification, Active, Categories Applied: [icon], Inherited from: SERI - Windows File Server), PCI Terms (DataClassification, Active, Categories Applied: [icon], Inherited from: SERI - Windows File Server), PCI - Visa (DataClassification, Active, Categories Applied: [icon], Inherited from: SERI - Windows File Server), and PII - DoB (DataClassification, Active, Categories Applied: [icon], Inherited from: SERI - Windows File Server).

SecurityIQ

Activities Compliance Permissions Policies System

< Navigation

Access Policy

Data Classification Policy

Data Remediation Policy

Advanced Forensics Control

Search: [input]

- Active Directory
- Windows File Servers
- SERI - Windows File Server
 - Data

Data Classification Policy

\\ad-resource\Data

Sub-Resources Policies (0)

New Associate Revert Save Inherit Rules: True Policy Status: Enable Configuration

Finance Folders | ThresholdClassification | Active | Categories Applied: [icon] | Inherited from: SERI - Windows File Server | The following behavior must match at least 70% of the activities over the last week

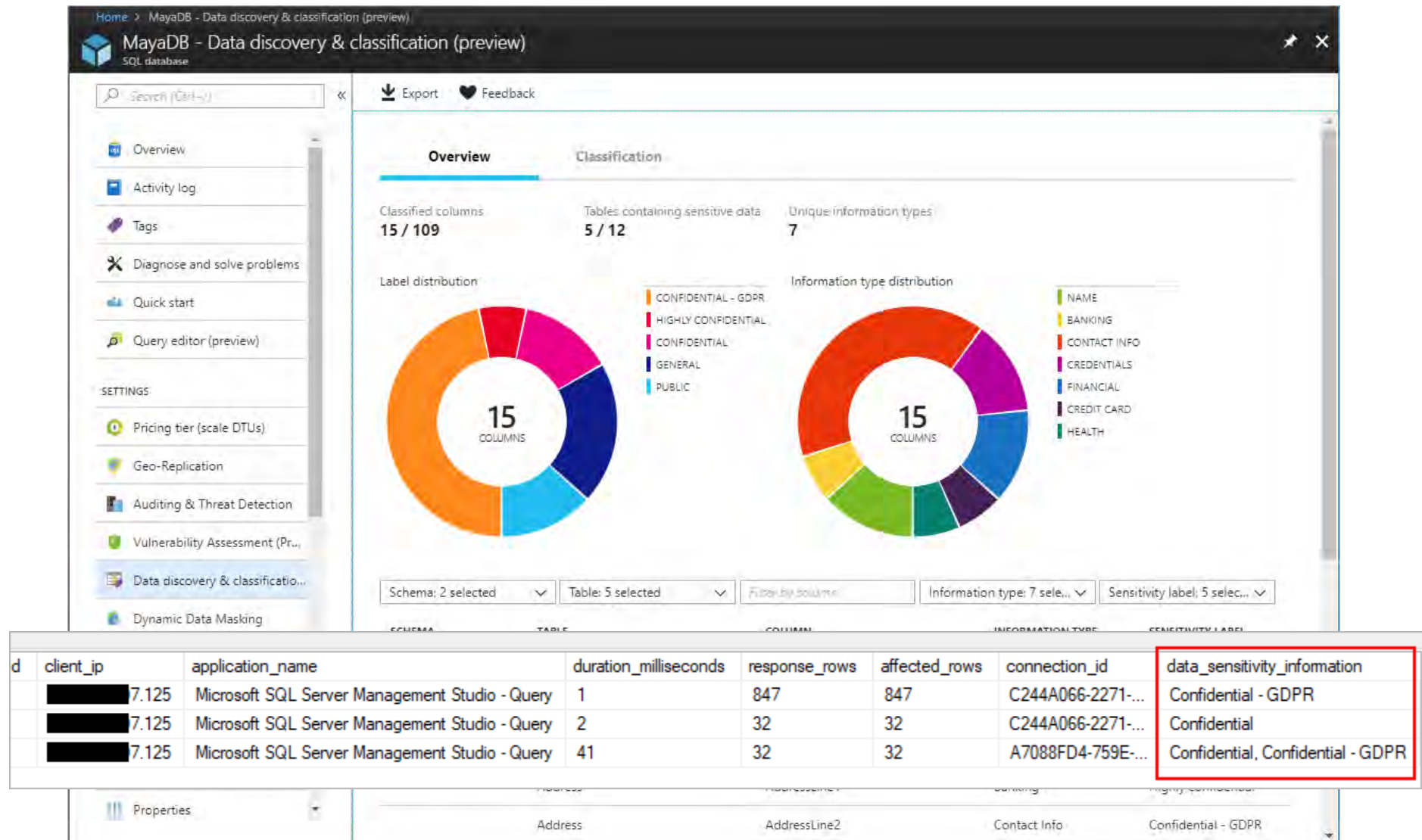
Animals | DataClassification | Active | Categories Applied: [icon] | Inherited from: SERI - Windows File Server

PCI Terms | DataClassification | Active | Categories Applied: [icon] | Inherited from: SERI - Windows File Server

PCI - Visa | DataClassification | Active | Categories Applied: [icon] | Inherited from: SERI - Windows File Server

PII - DoB | DataClassification | Active | Categories Applied: [icon] | Inherited from: SERI - Windows File Server

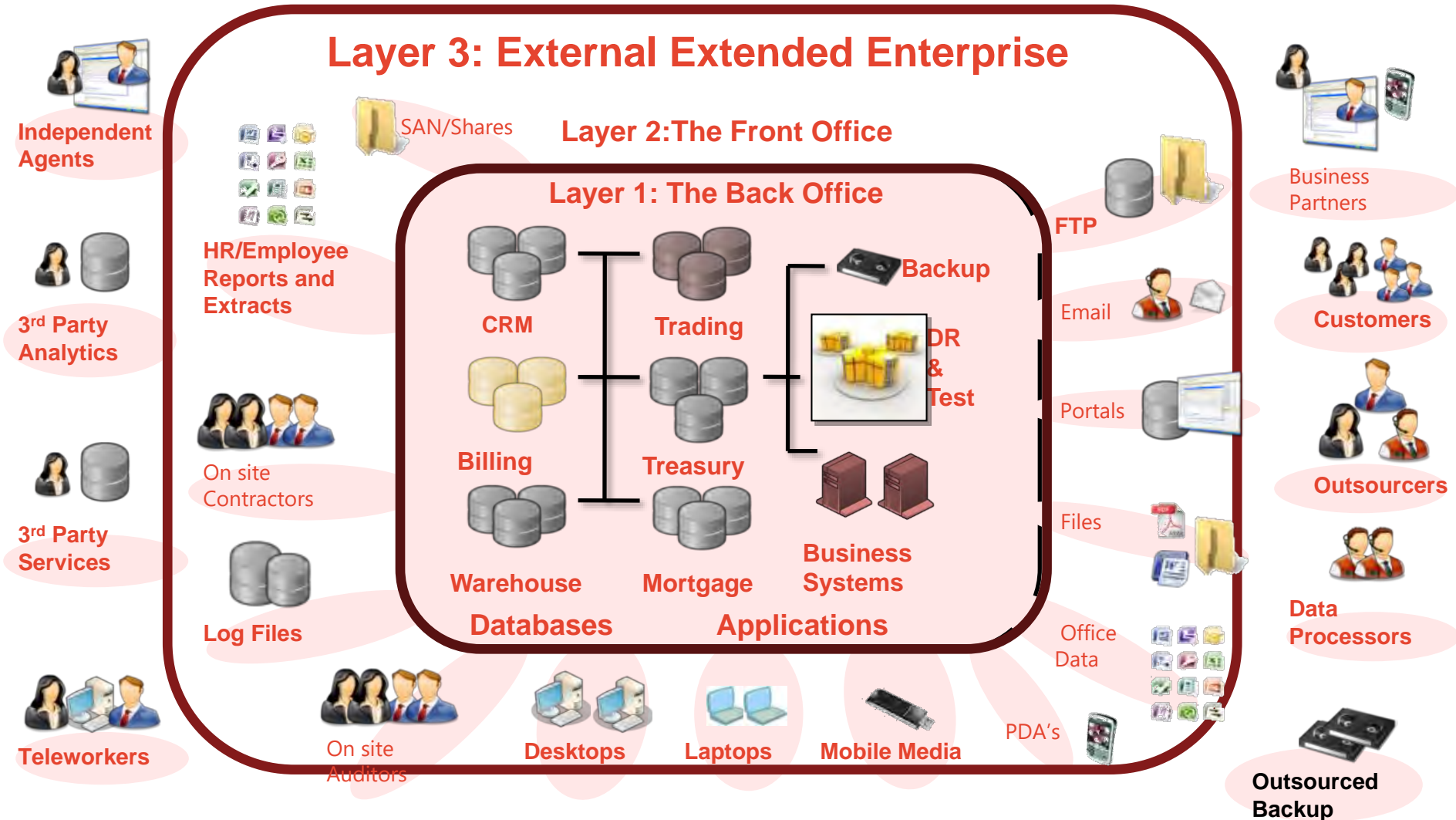
Example with Azure SQL Data classification





Protect your sensitive Data

Securing data is challenging



Tokenization



Mr John Doe
01/02/78

Original Data

Tokenization



Xe JPOwui Oisiypz
24/02/99

Token

Personally identifiable information	Token Management Data	Token
Mr	ID IV Timestamp Index etc	Xe
John Doe	ID IV Timestamp Index etc	JPOwui Oisiypz
01/02/78	ID IV Timestamp Index etc	24/02/99

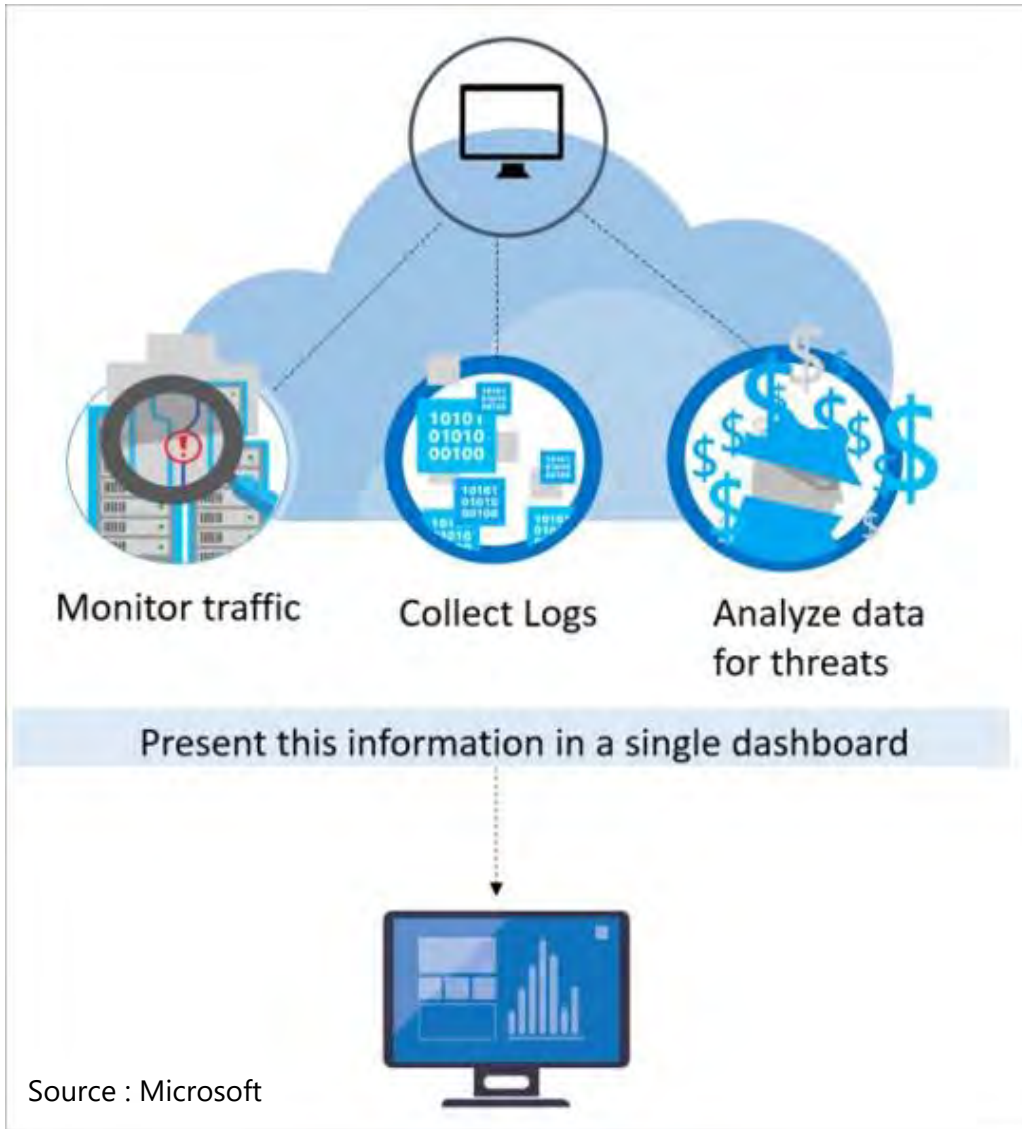


- ▶ Tokenization Replace live data *after* capture, *after* a database lookup
- ▶ Encryption still needed for initial data capture & to live data in “Vault”
- ▶ Encryption and Tokenization can be used together
- ▶ Performance of Token Lookup needs to be considered



Audit access to your sensitive Data

All consolidated Logs



Detect Security Breaches by identifying anormal user behavior and usage patterns.

Collect near-real time user and devices information by applying geo-patterns

Present dashboard with Risk and alert with policy violation to enable pattern detection

Don't ask your CISO to protect against data breach but rather ask him to prepare to react to a data breach⁶