Event Public Sector

Protection de vos données dans Azure

Thomas Eklund – Microsoft
Thibaud Merlin - Kyos

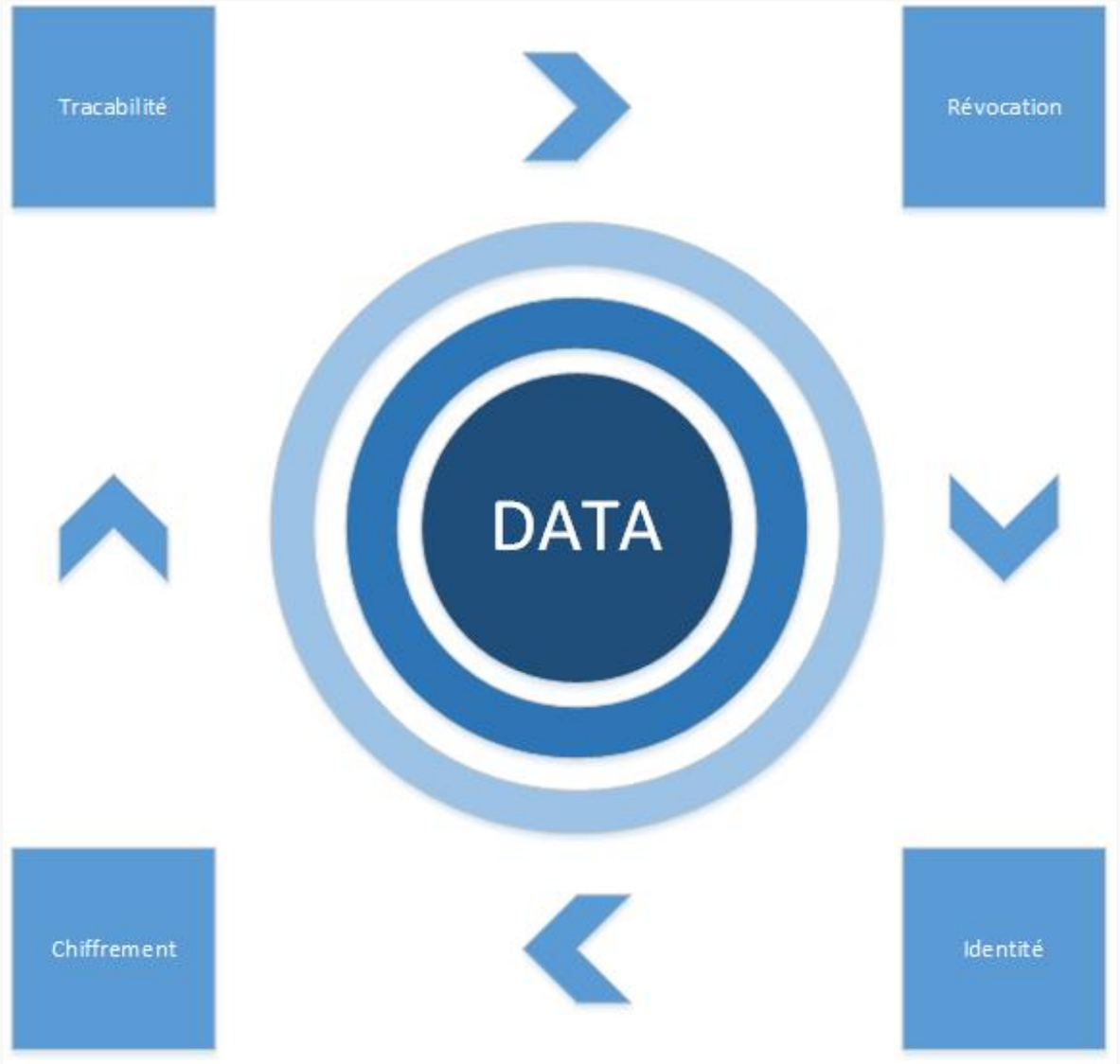
Microsoft

kyos embedded security

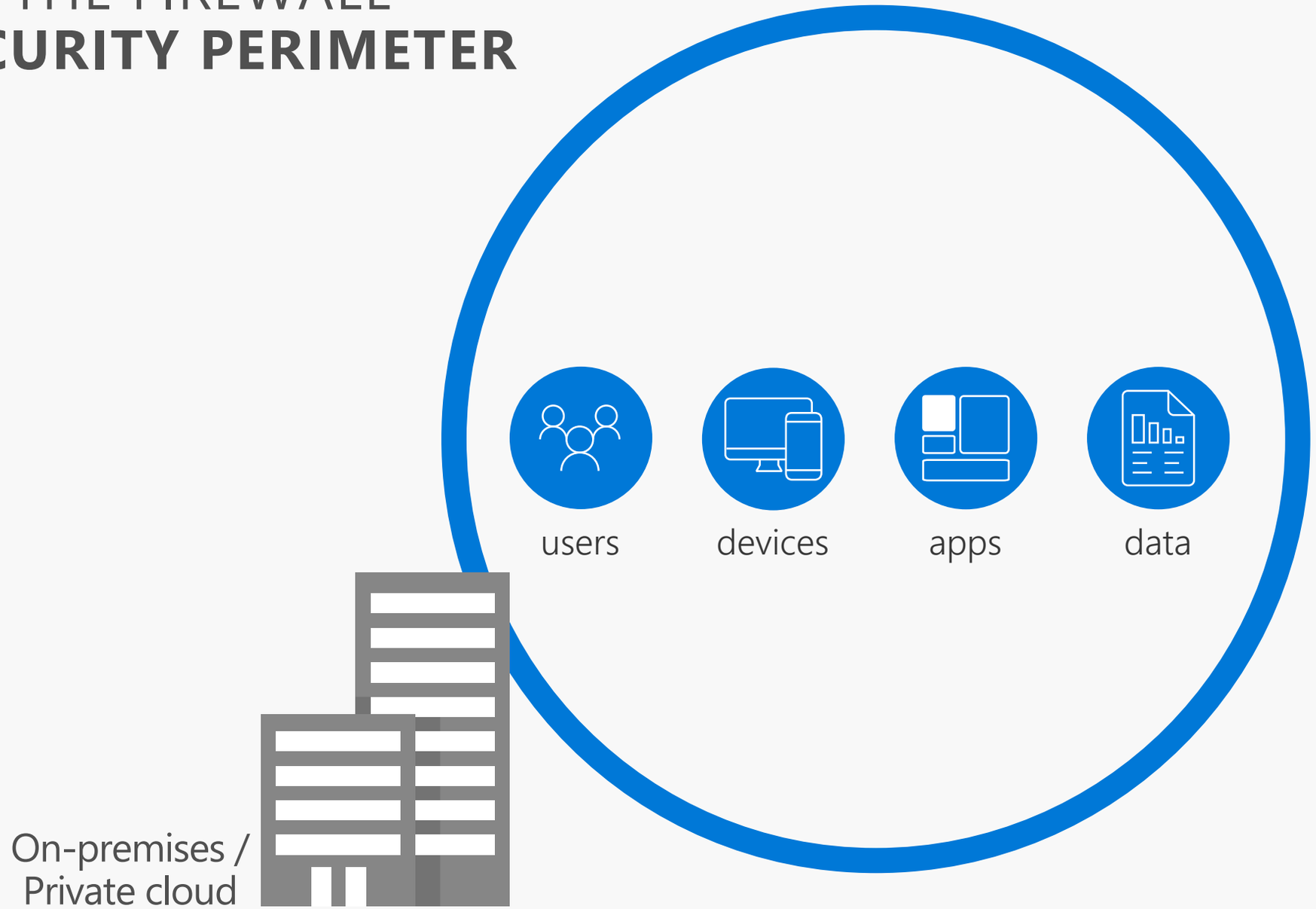
Agenda

Introduction
Etat du marché, notamment Romand
Overview des produits 'cloud' Microsoft
Overview des services Kyos
Solutions de Sécurités Microsoft
Overview AIP
Demo AIP
AD-RMS/BYOK/HYOK
Use case pratique
Implémentation AIP avec des services on-prem
AIP et conditionnal access et Azure AD
BYOK et Thales CCKM avec Azure Key Vault

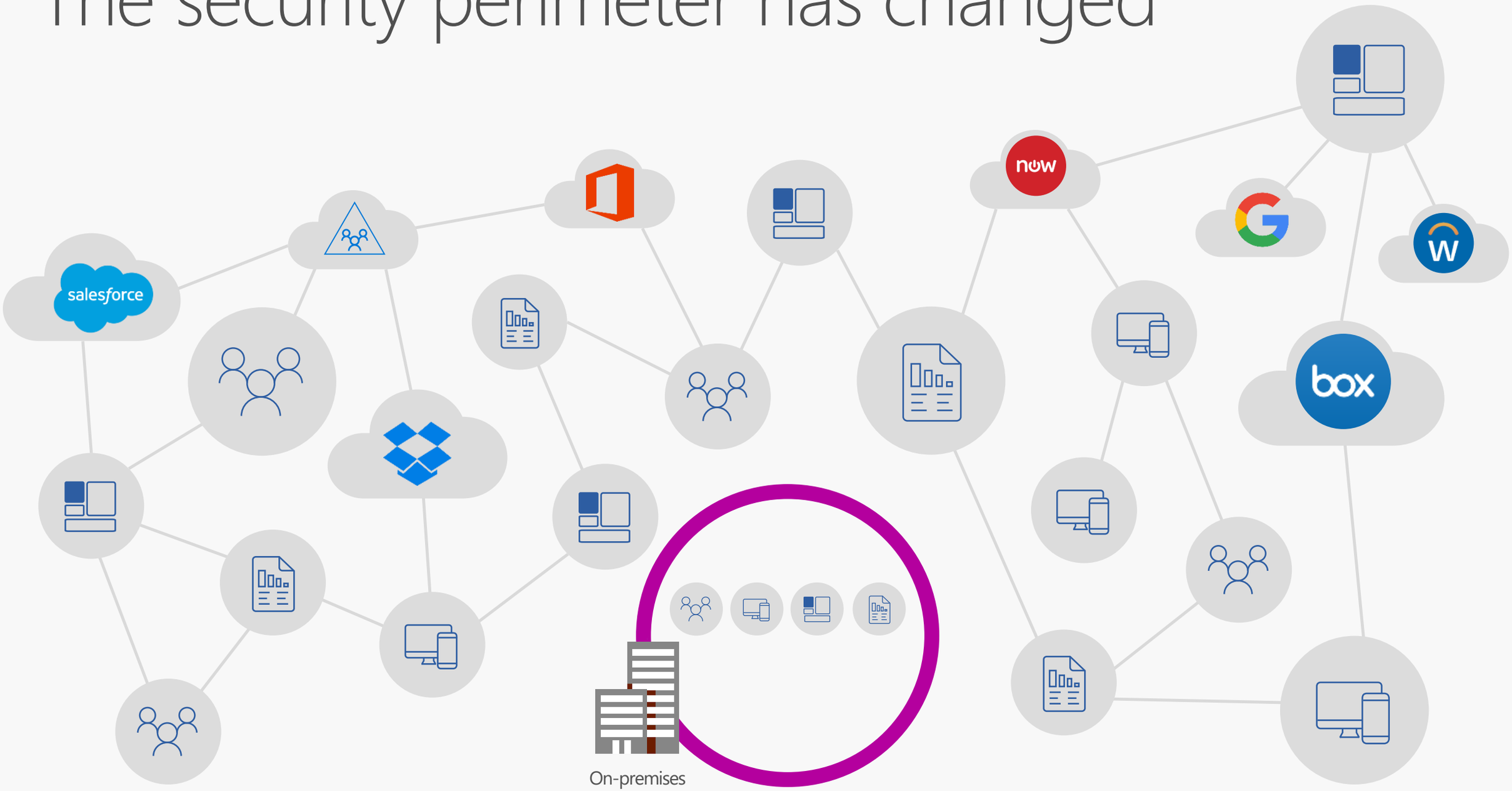
Classifier et protéger vos données : L'approche 'Data Centric'



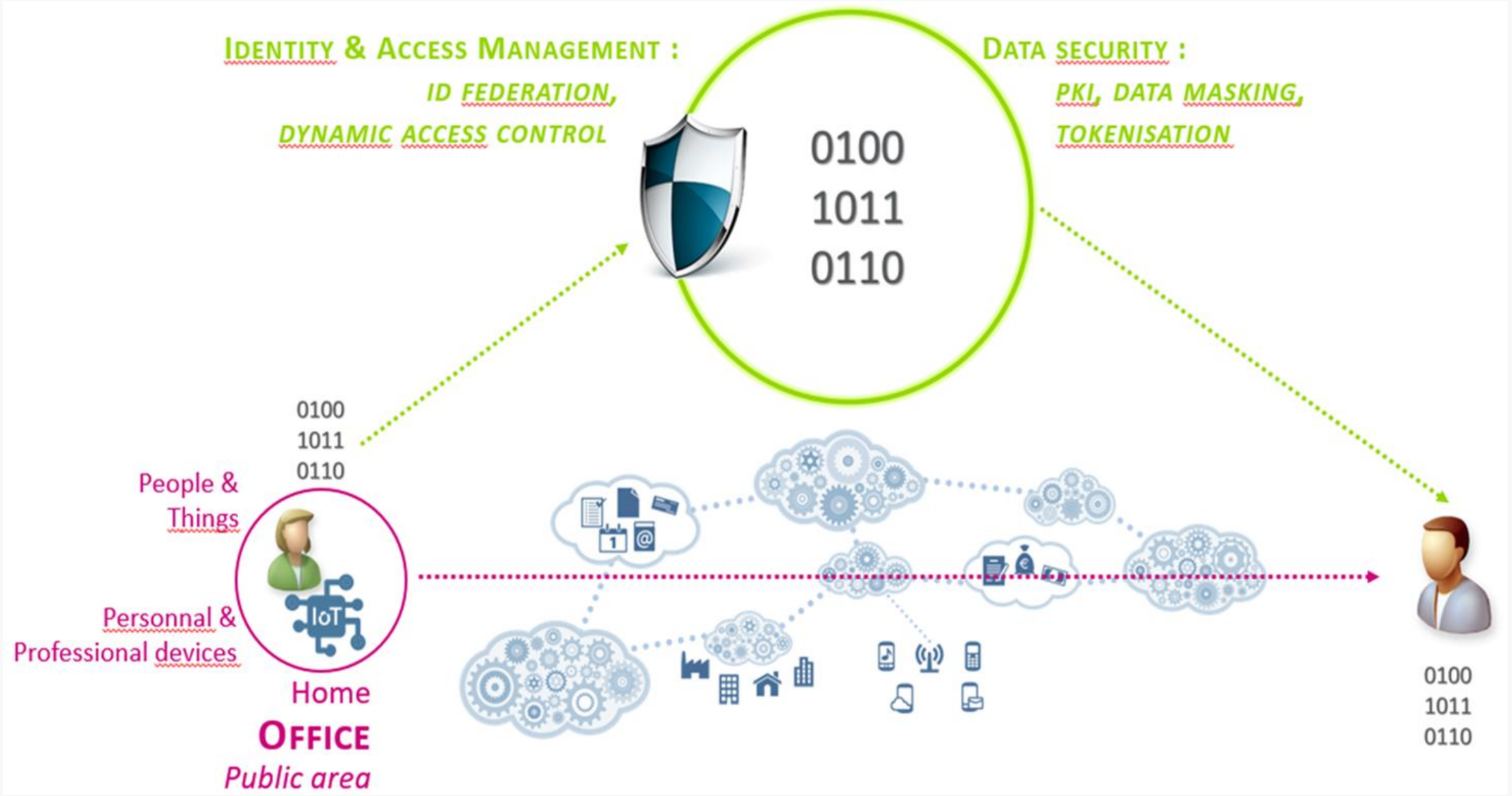
IN THE PAST, THE FIREWALL WAS THE **SECURITY PERIMETER**



The security perimeter has changed



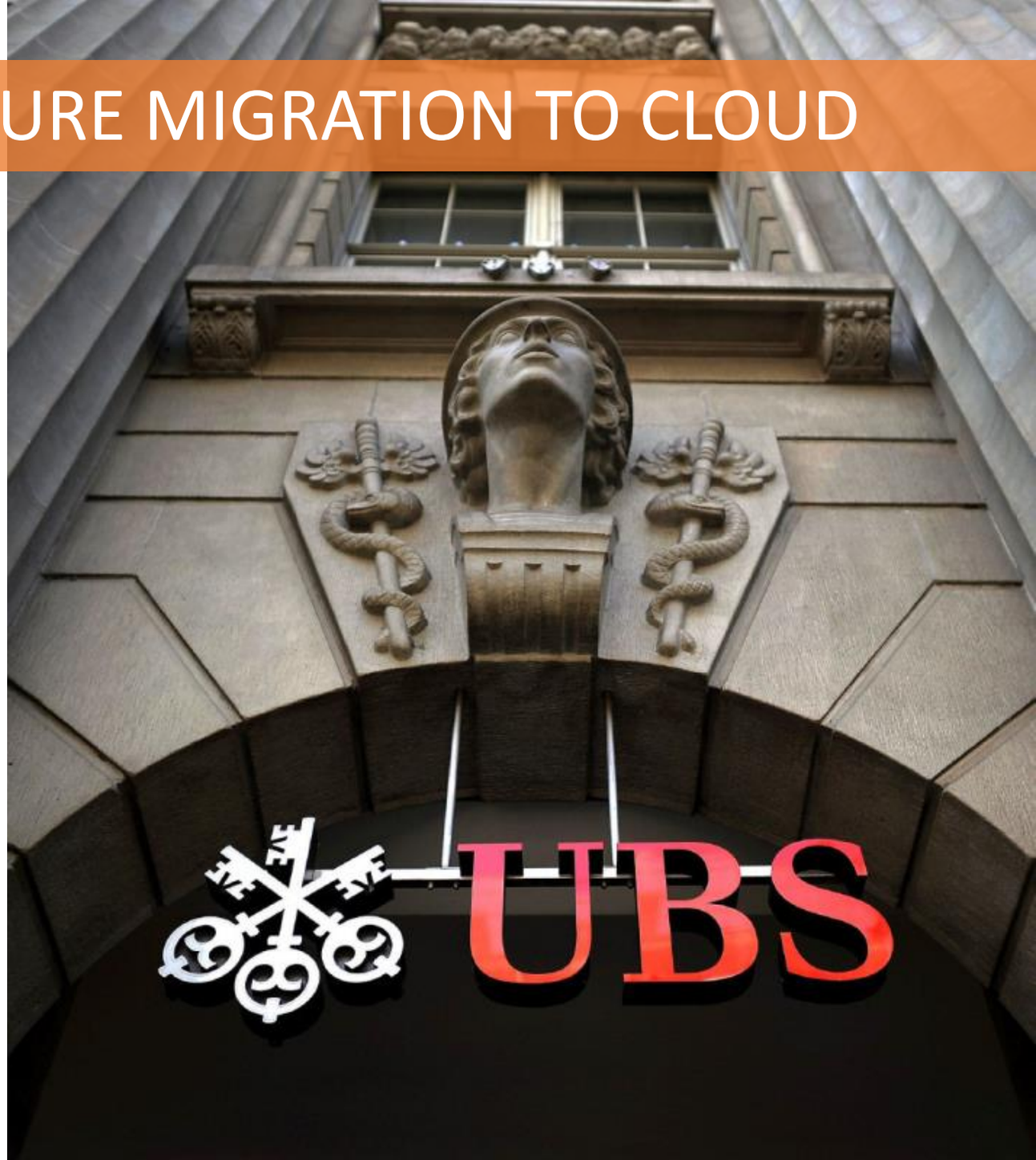
Notre Vision



Où en sommes-nous en Suisse dans les secteurs hautement régulés?

UBS taps the cloud to power critical workloads

SECURE MIGRATION TO CLOUD



> With Microsoft Azure, we are building on the industry's leading cloud platform in terms of innovation, technology, security and regulatory compliance, which is very important as a Swiss financial institution."
>
> — **Paul McEwen**, Head of Technology Services, UBS

UBS

▷ Watch

UBS taps Microsoft Cloud to power business-critical tech

USE CASE: SECURE MIGRATION TO CLOUD

The results —

- speeding calculation time by 100 percent,
- saving 40 percent in infrastructure costs,
- gaining nearly infinite scale within minutes, securely

— means UBS can have more working capital on hand and employees can make quicker, more informed decisions for their clients on a secure platform

MIGRATION TO CLOUD

UBS head office in London, 2008

COMPANIES > MICROSOFT

UBS Said to Prepare Cloud Move to Secret Microsoft Data Centers

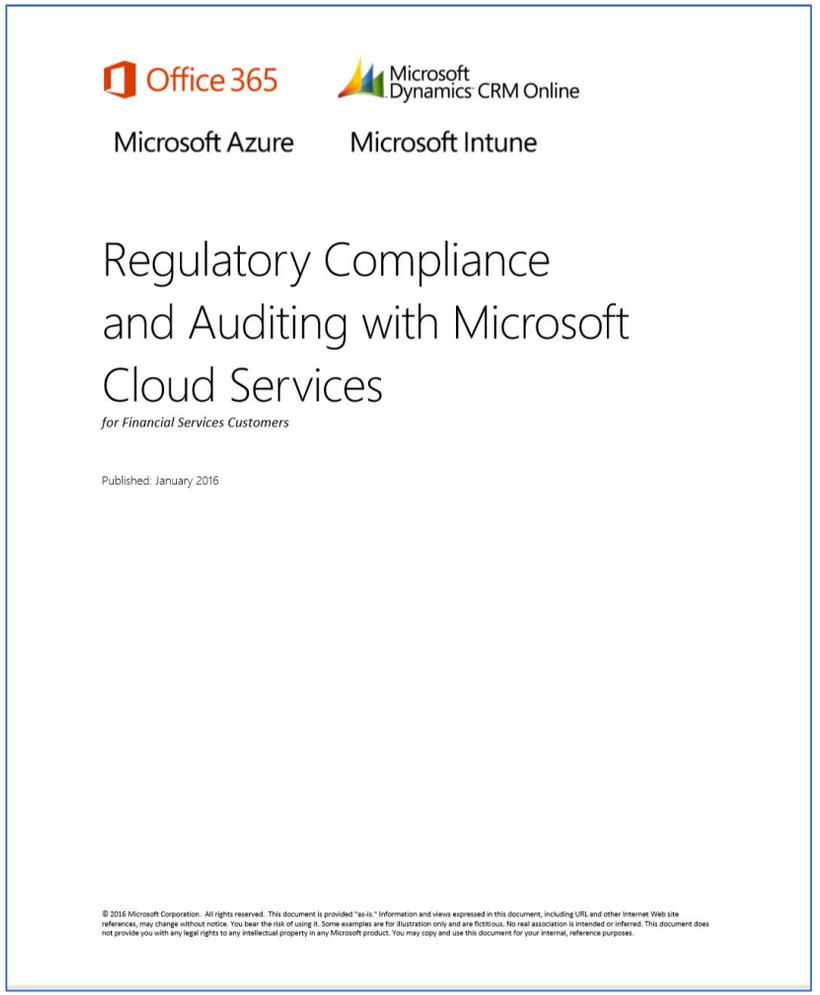
UBS Group will spend hundreds of millions of Swiss francs to use Microsoft's cloud services hosted in two Swiss data centers, anonymous sources told Bloomberg News • Switzerland's largest bank wants to scale back the number of its own data centers over the next four years • It currently has 25 of them

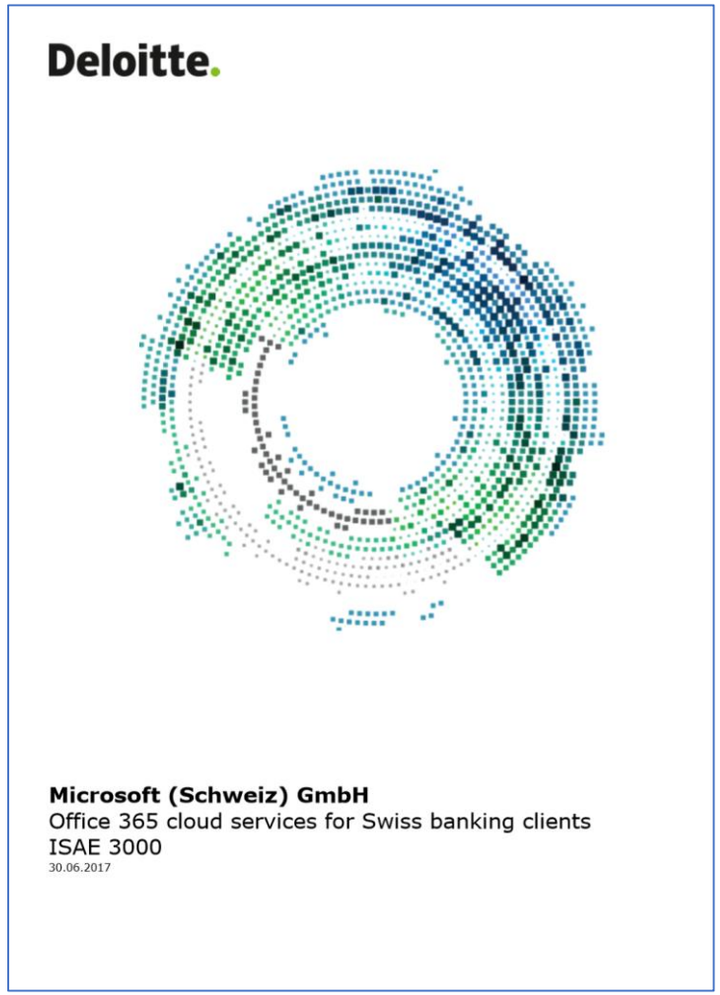
Bloomberg | Dec 12, 2018

UBS taps the cloud to power critical workloads

Banks in Switzerland, the world's largest center for offshore wealth, are under pressure to **cut costs** as low interest rates and the dismantling of the nation's banking secrecy **squeeze profits**. While using cloud services can eliminate the need to maintain costly data centers, Switzerland's financial regulator Finma enforces strict laws regarding what data can be moved outside of the country.

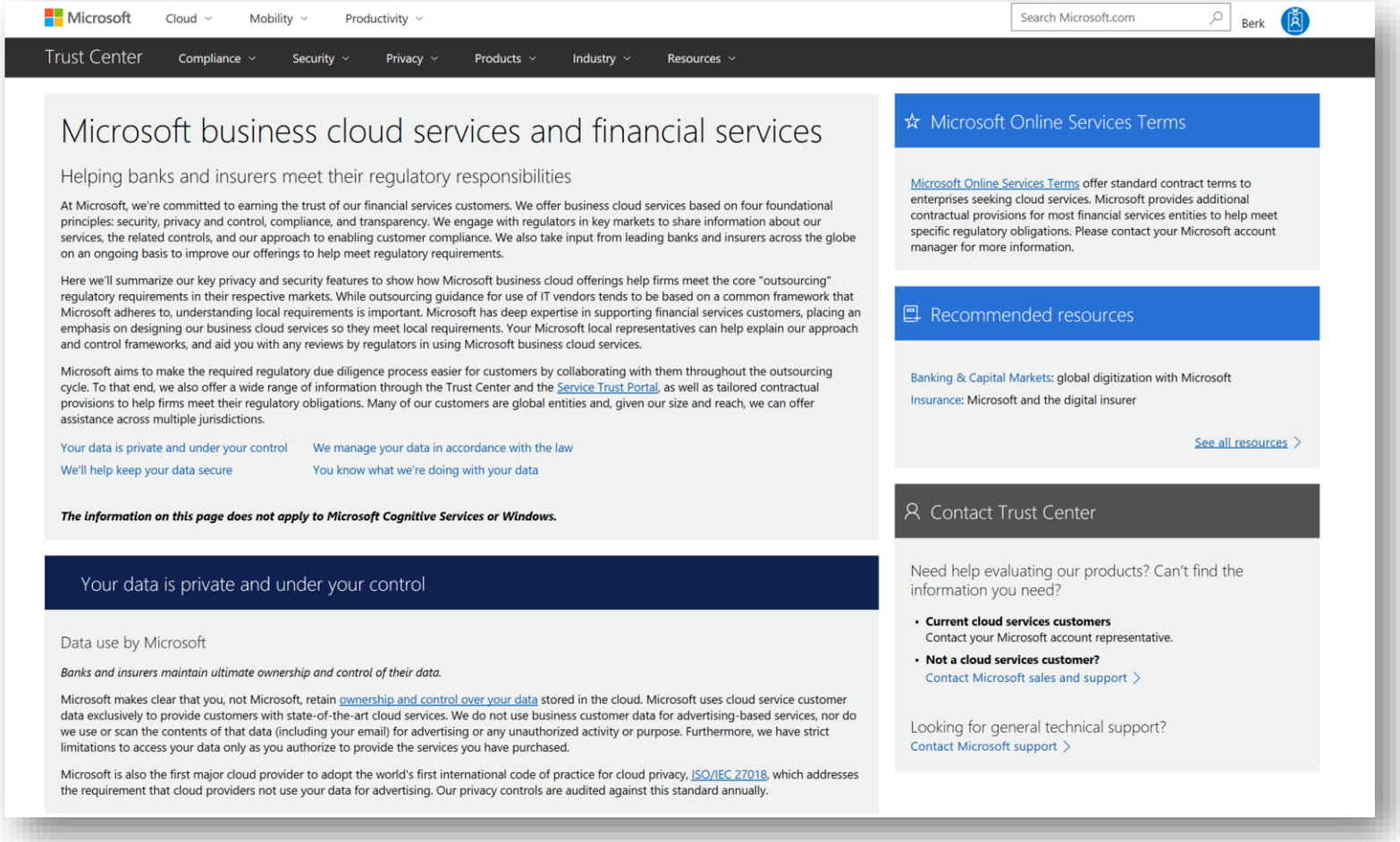
Regulatory Compliance and Auditing with Microsoft Cloud Services





Helping **banks and insurers** meet regulatory responsibilities

Microsoft Trust Center



Helping **banks and insurers** meet regulatory responsibilities

Regulatory Compliance and Auditing with Microsoft Cloud Services

Helping **banks and insurers** meet regulatory responsibilities

Et le secteur public?

“Est-ce que des clients ont déjà franchi le cap???

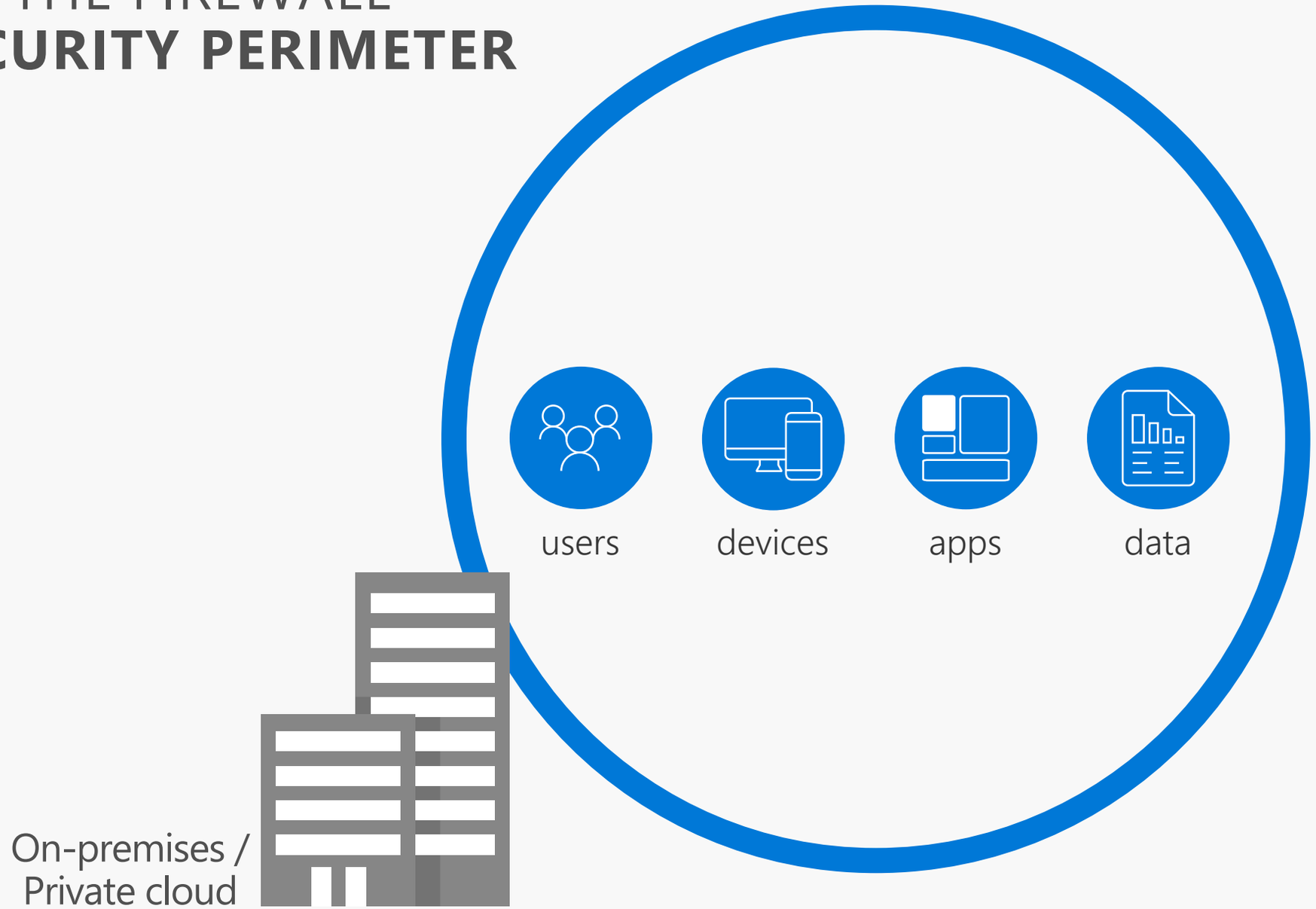
Et en Suisse romande?

“Est-ce que des clients ont déjà franchi le cap???

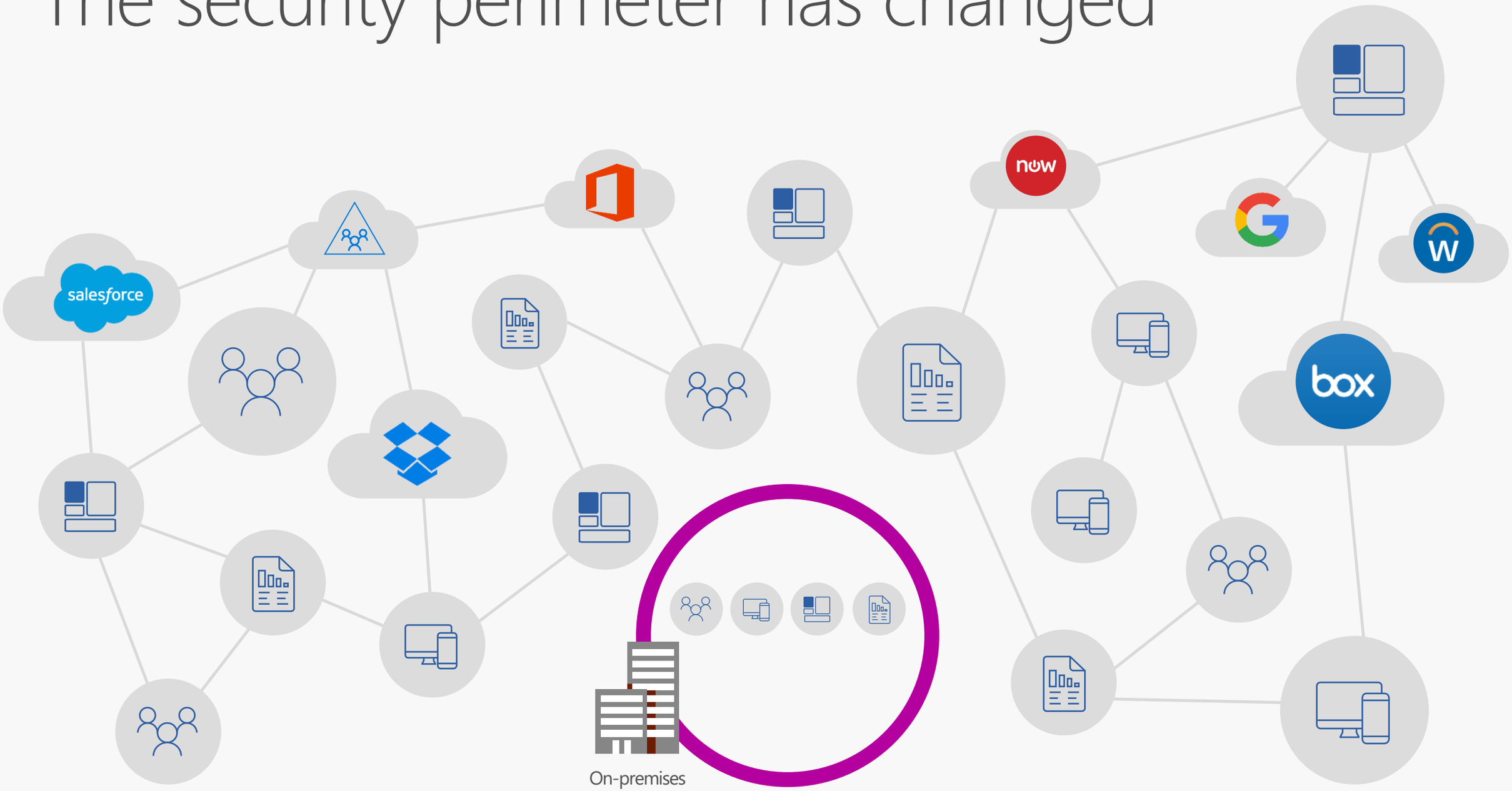
AIP/DLP

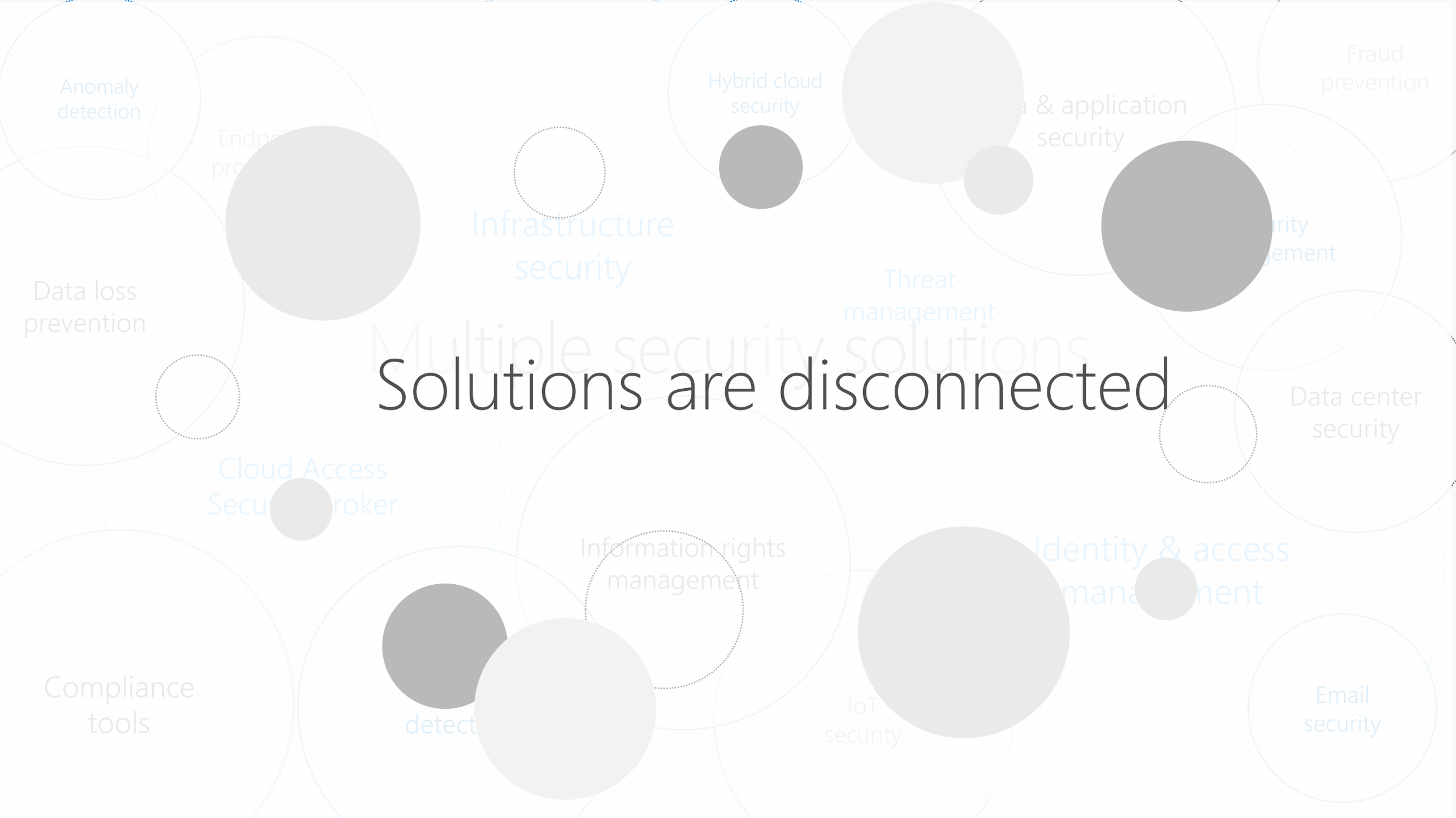
Thomas Eklund
Technology Solutions Professional

IN THE PAST, THE FIREWALL WAS THE **SECURITY PERIMETER**



The security perimeter has changed





Solutions are disconnected

Focusing security efforts in a complex landscape

Adopt identity-based protection

Enable Seamless and secure identity and access for employees, partners and customers

Apply persistent data protection

Protect sensitive data – wherever it lives or travels.

Protect against sophisticated hackers

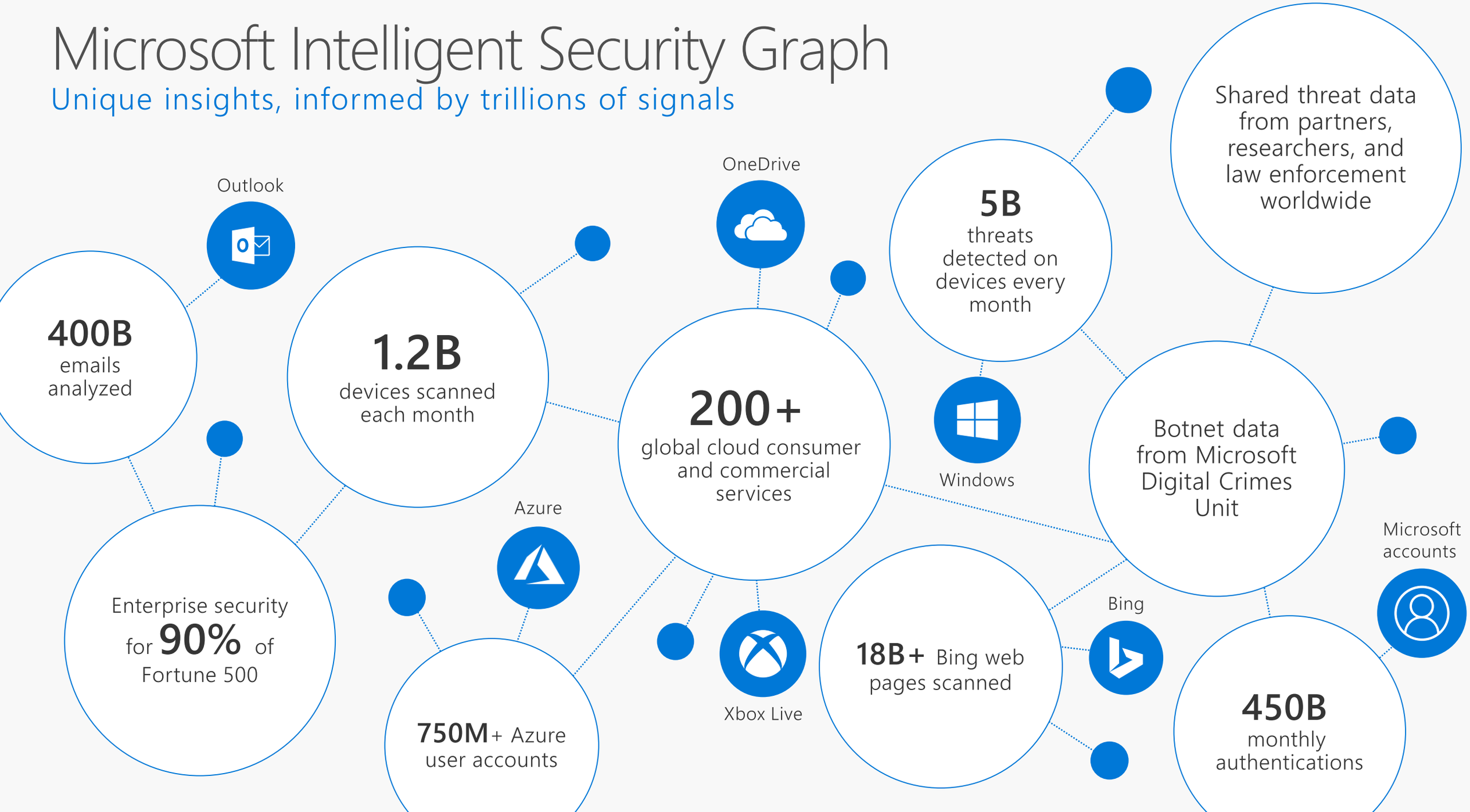
Protect, detect and remediate against threats across the modern workplace.

Simplify security management

Streamline management with built-in intelligence and recommendations.

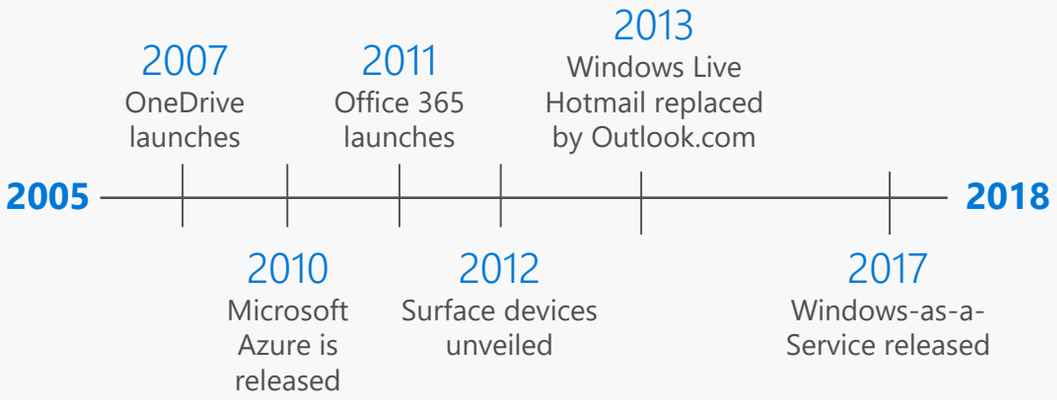
Microsoft Intelligent Security Graph

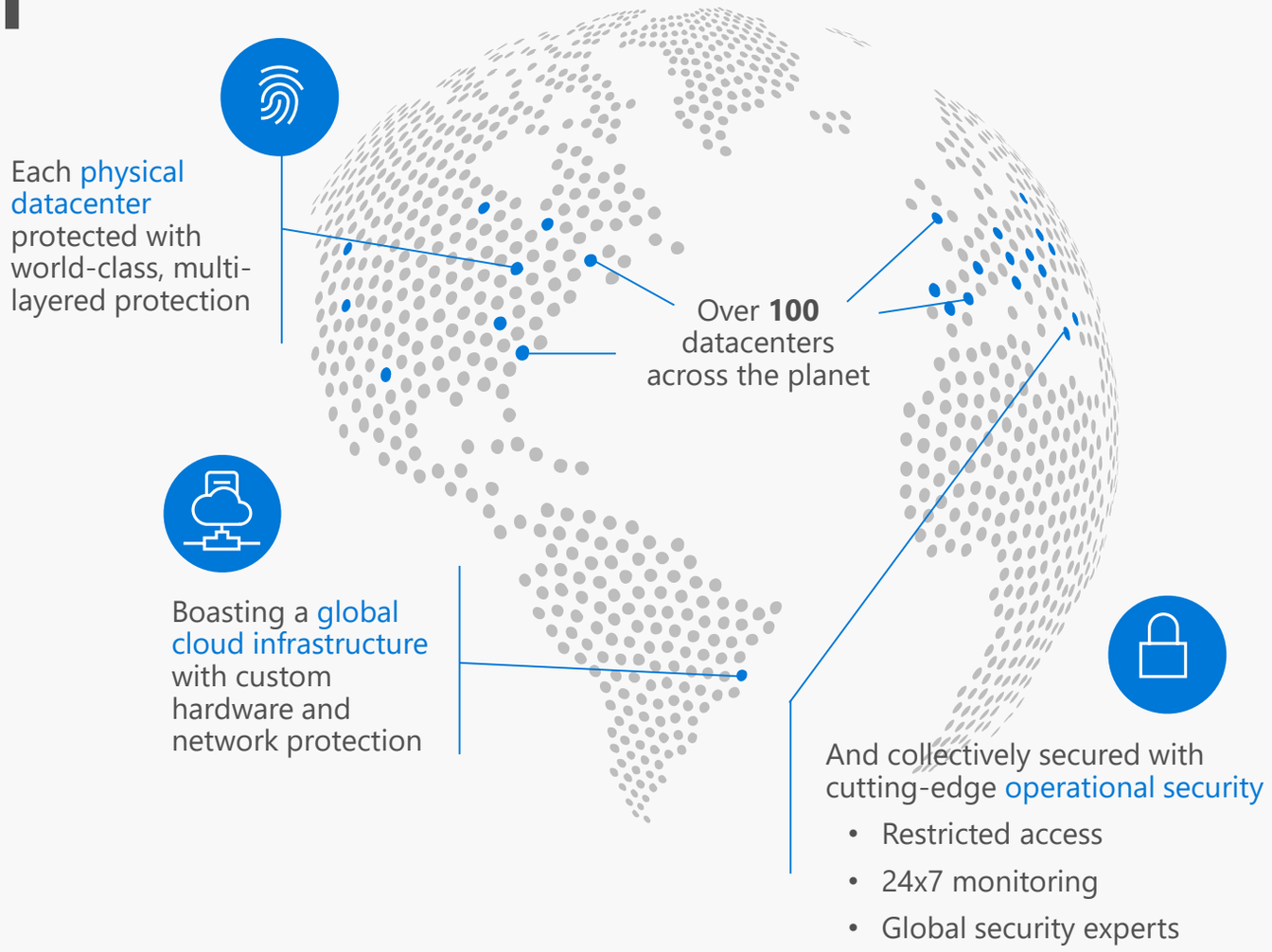
Unique insights, informed by trillions of signals



A **secure foundation** at global scale

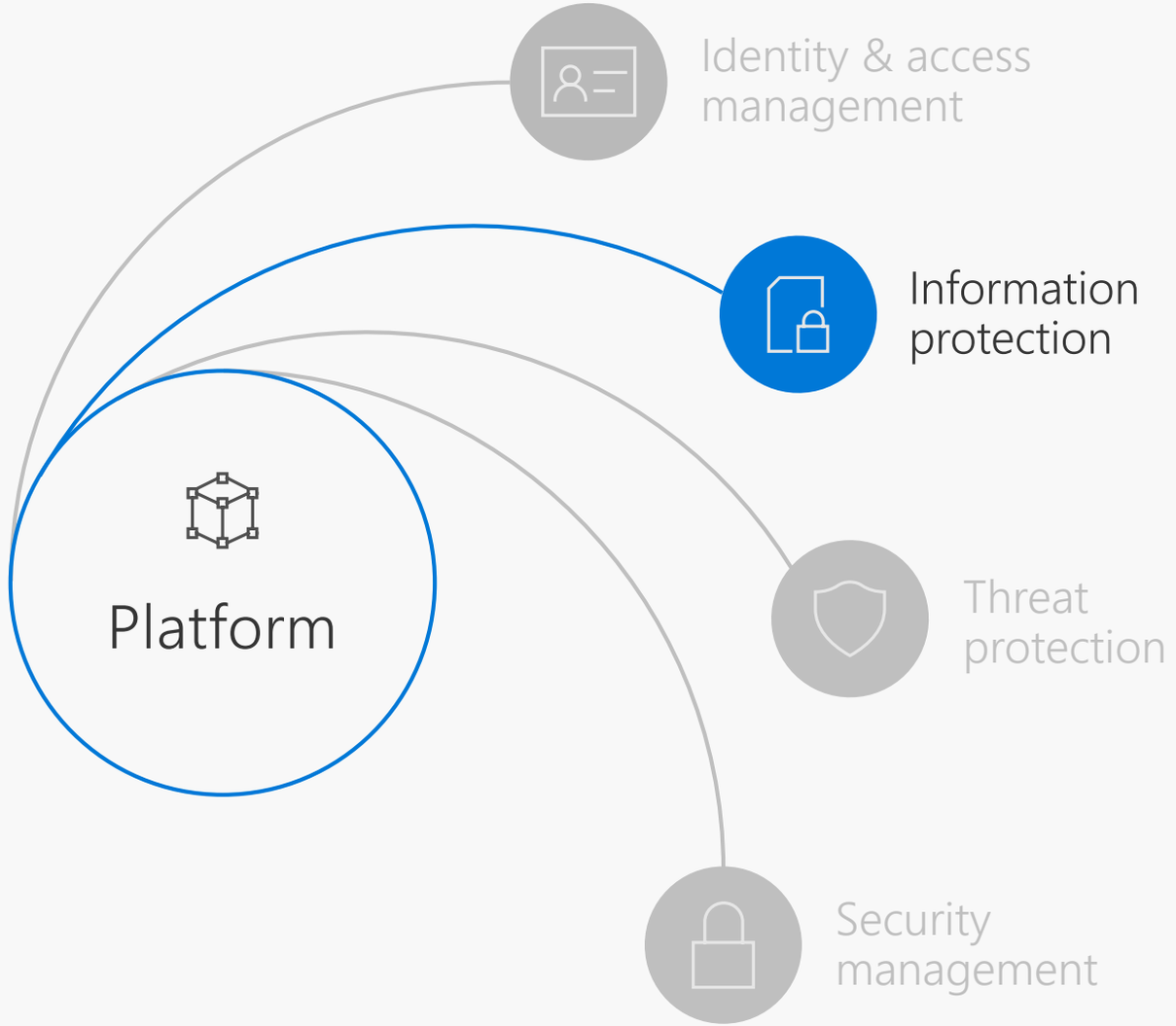
Experience and history in the cloud



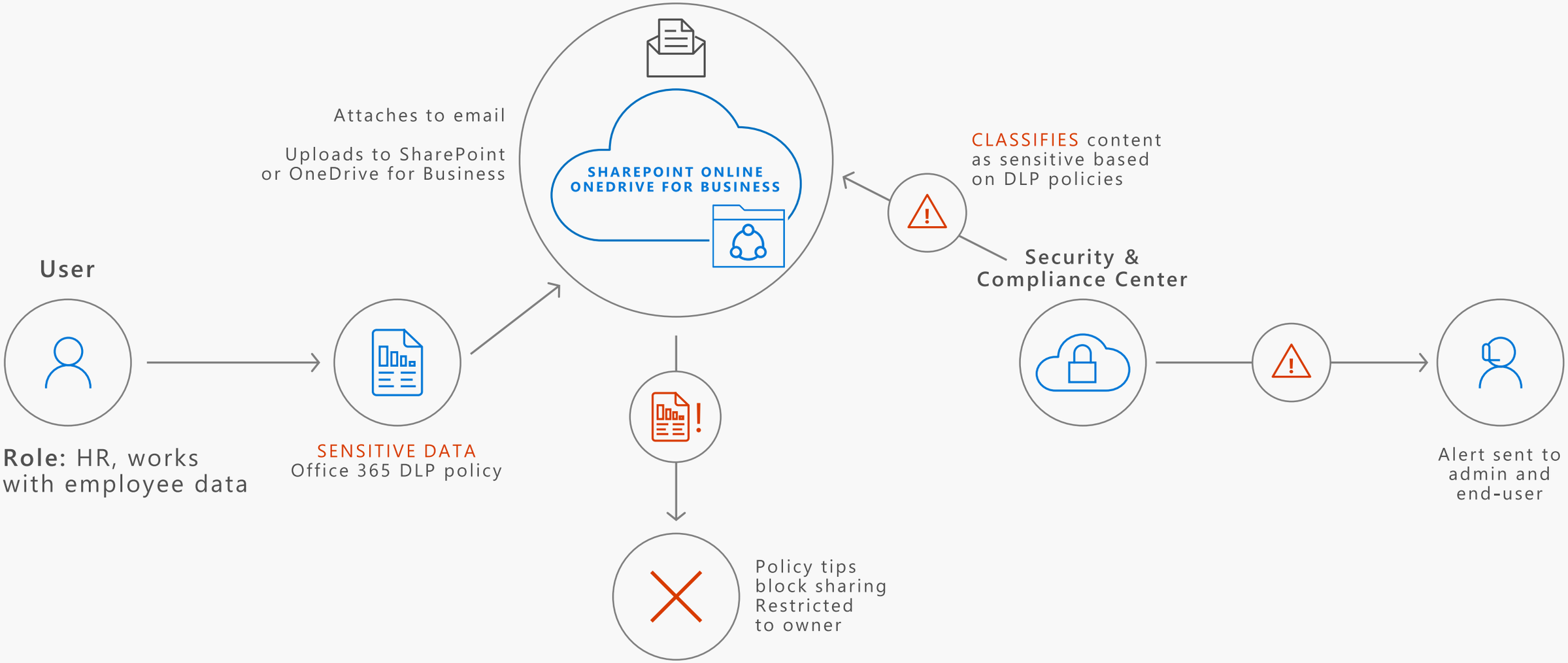


Mobile + PCs + Cloud + Datacenters

Built in security



Prevent data loss in Office 365



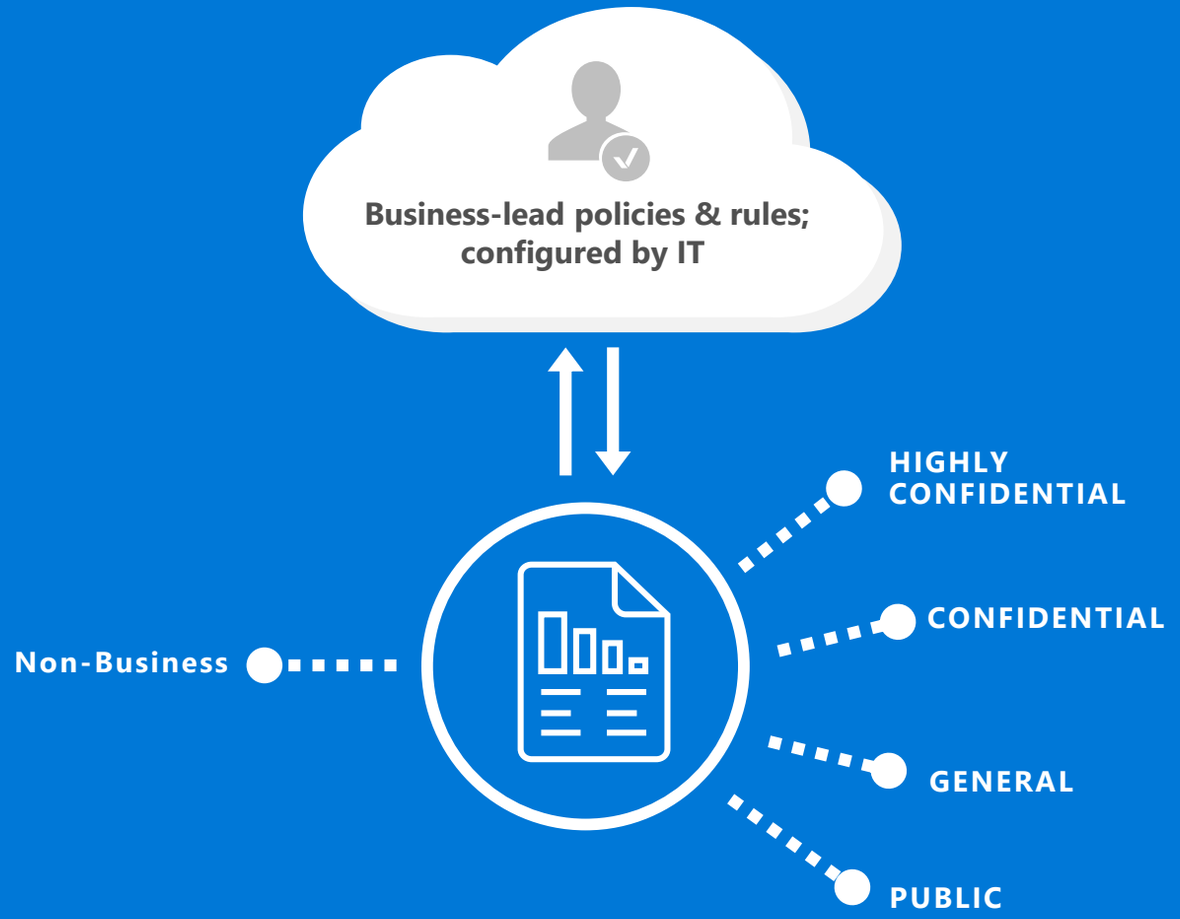
Flexible classification options

Automatic classification
Policies can be set by IT Admins for automatically applying classification and protection to data

Recommended classification
Based on the content you're working on, you can be prompted with suggested classification

Manual reclassification
Users can override a classification and optionally be required to provide a justification

User-driven classification
Users can choose to apply a sensitivity label to the email or file they are working on with a single click



Apply sensitivity labels that persist with the document

Document labeling – what is it?
Metadata written into document files

Travels with the document as it moves

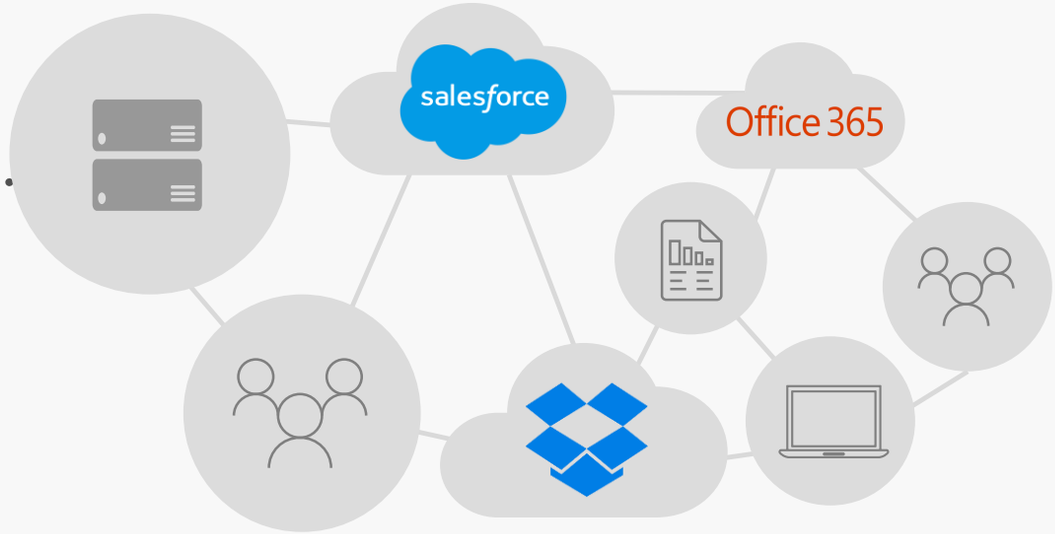
Readable so that other systems such as DLP engines can understand and take action

Used for the purpose of apply a protection action or data governance action – determined by policy

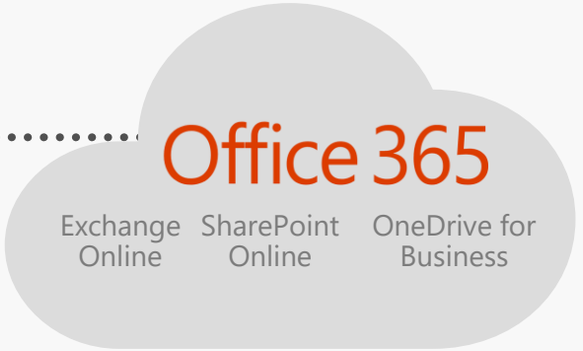
Can be customized per the organization's needs

Classification & labeling enables policy-driven actions

Protection actions across locations
Classification and labeling is used to apply protection policies – encryption, permissions, DLP actions, end-user notifications and IT alerts



Data governance actions for Office 365 files
Classification and labeling is used to apply data governance policies in Office 365, including data retention, expiration and deletion

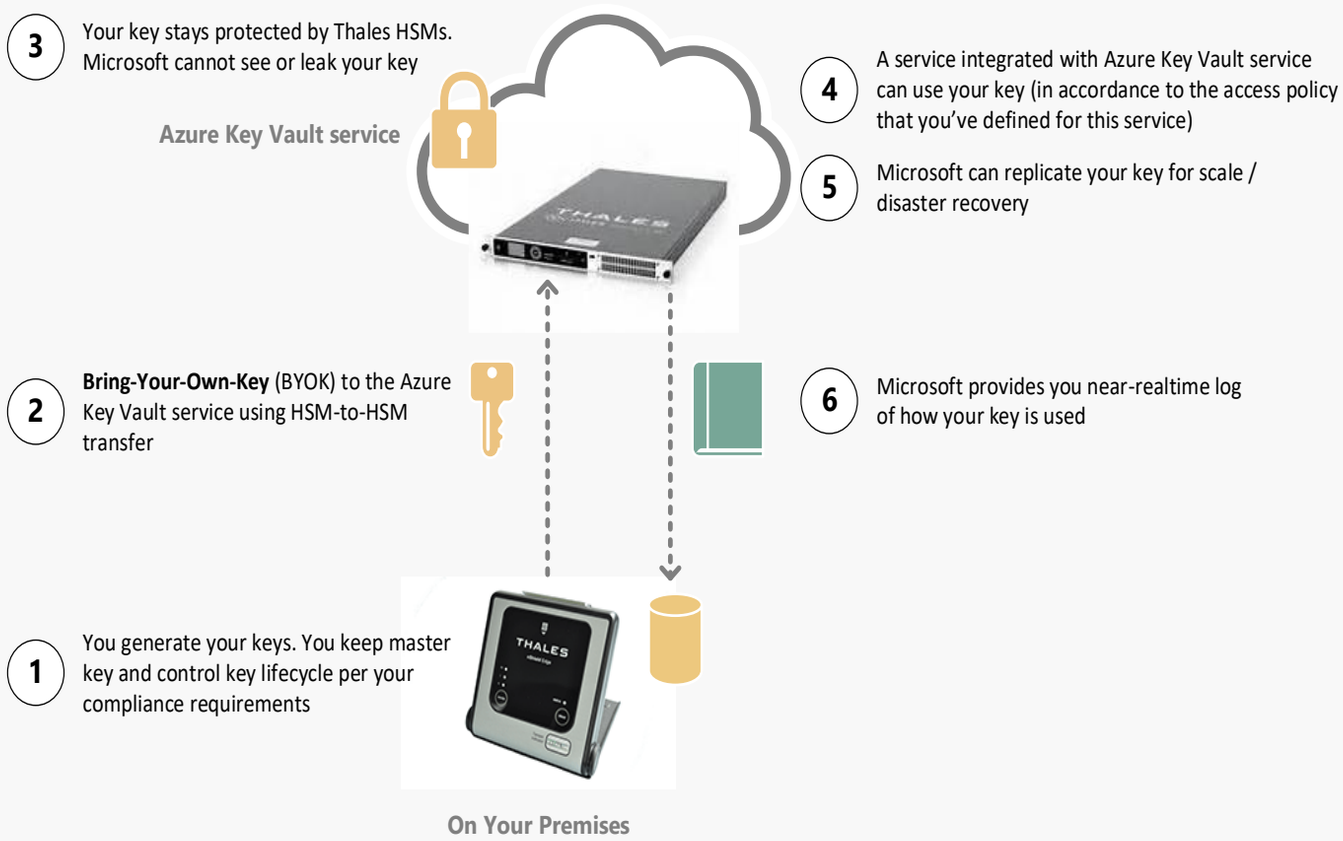


Time for a demo

Some context
Contoso corporation is planning a merger with a firm (Geneva Racing). How can they collaborate securely and avoid data leakage ?

Data encryption

Le terme Bring-Your-Own-Key défini un mode ou c'est vous-même qui utilisez votre HSM pour générer une clé. Il faut cependant noté que dans le cas Azure/Office365, vous devez répliquer cette clé dans les HSM de Microsoft pour pouvoir utiliser les services Online

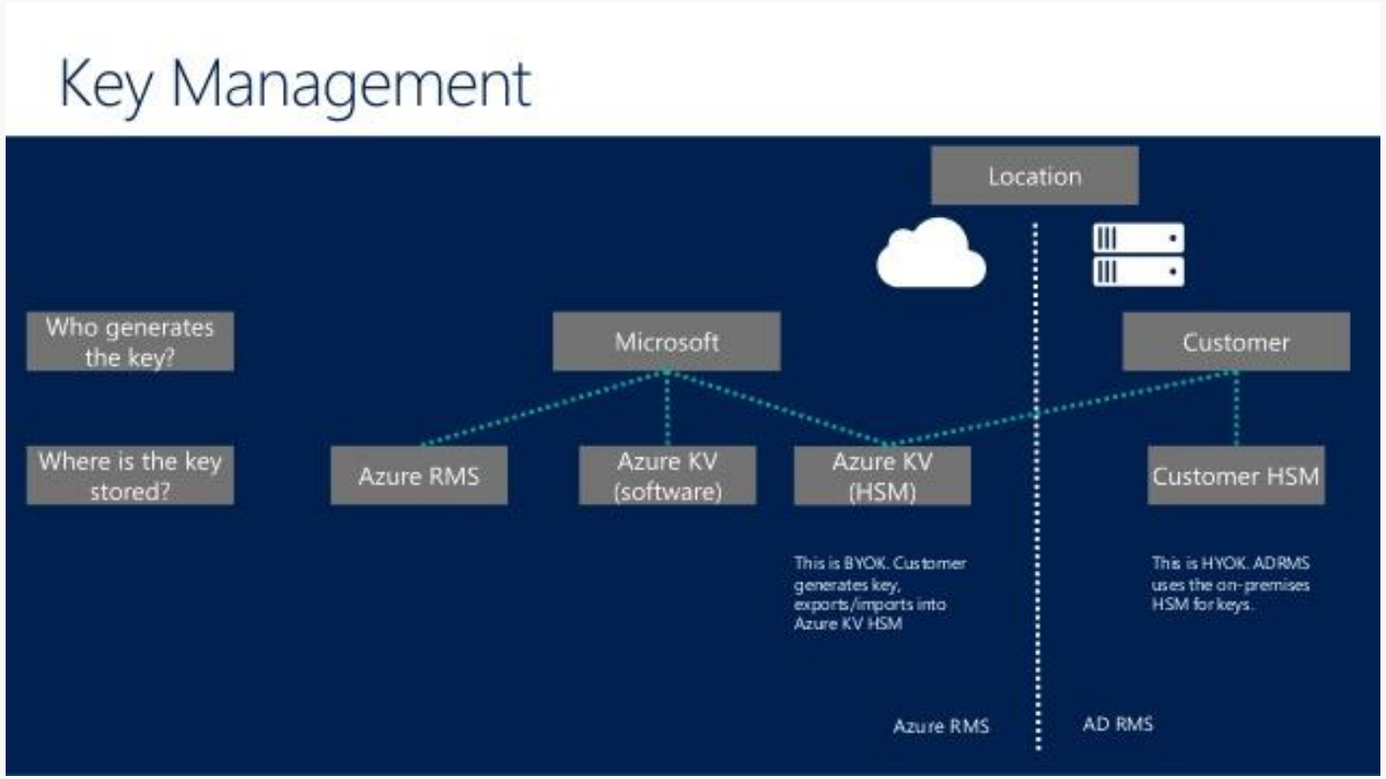
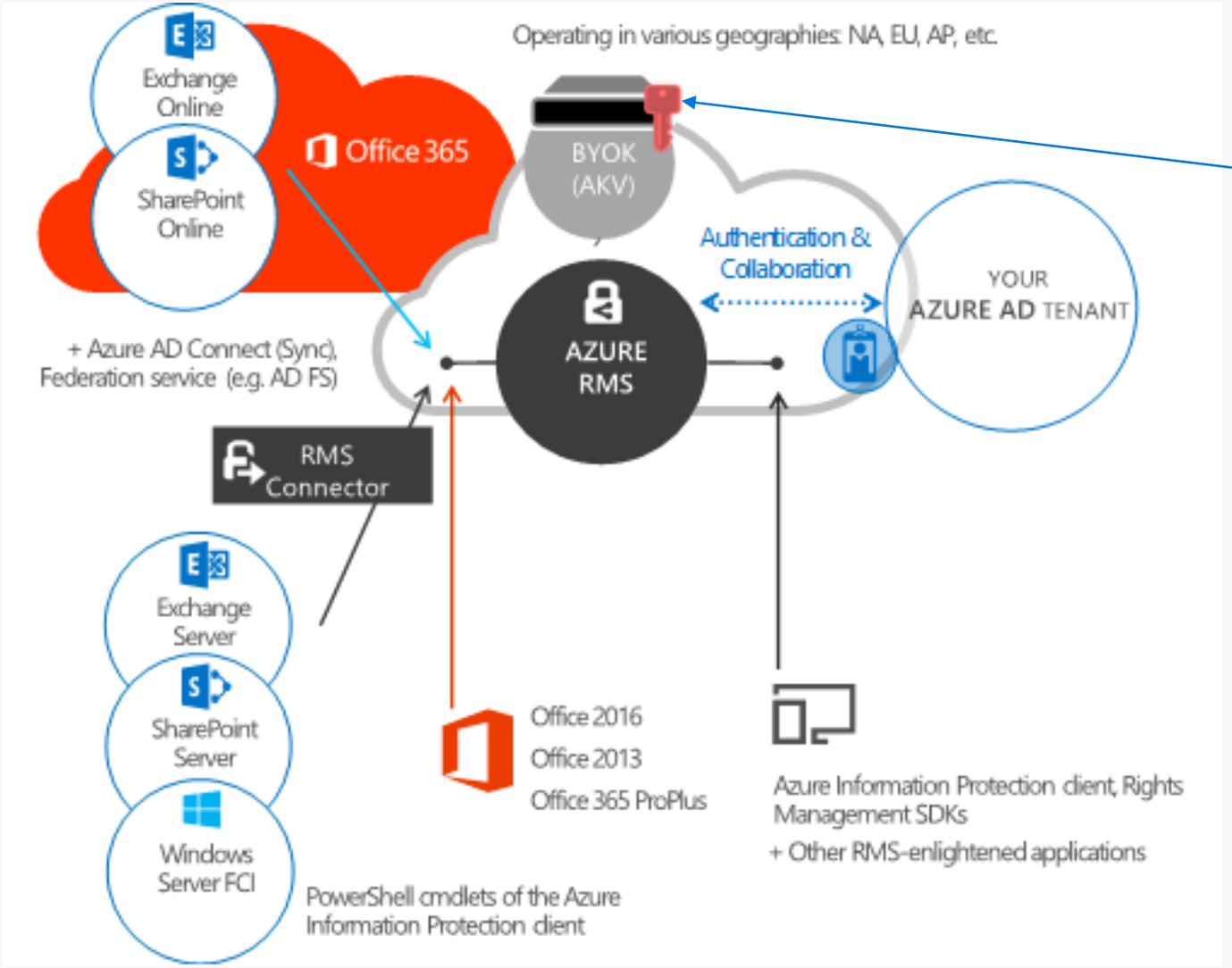


Data encryption

L'utilisation de clé pour chiffrer des emails/documents dans Office365 se dénomme BYOK with AIP :
- Protéger des fichier et emails avec AIP et Azure RMS, services : Sharepoint Online, Exchange Online, OneDrive for Business

L'utilisation de clé pour chiffrer les données au repos dans Office 365 se dénomme Customer Key :
- Chiffrer les données au repos sur les services Sharepoint Online, OneDrive for Business, Exchange Online et Skype for Business Online

L'utilisation de clé directement générées sur les HSM de Microsoft s'appelle Microsoft Managed



Bring Your Own Key (BYOK)