keyon

eberhard@keyon.ch, V1.8

About Keyon AG

IT-Security - successfully implemented

Corporate PKI
Software Engineering
Digital Signature Services
Identity & Access Management
Information Rights Management
On-Prem, Cloud- & Mobile Security

keyon

Data classification

How to classify & protect sensitive data
on prem, in the cloud and on mobile devices
using Rights Management

Goals of this presentation

- Understand classification schemas and the impact to user behavior, data processing and data protection
- Understand how unstructured data can be classified and protected with Rights Management
- Understand the different DLP approaches “Rights Management” vs. “Boundary Scanning”

keyon

Data classification

Why is data classification important?

Why has data classification been neglected till now?

Neglected classification till now

- Does your organization have data classification policies? "Yes" is assumed
- What percentage of your data is being classified today?
  "A lower two digit percentage" is assumed
- Is your data appropriately protected and processed according to its classification level?
  "A lower two digit percentage" is assumed

Neglected classification till now

- The reality is

55%

of IT professionals say data classification is too complex to plan, manage and deploy

63%

of IT professionals are not certain that their company's classification scheme is aligned with how data is created, used and shared

88%

of IT professionals say they ignored or circumvented data classification policies

Based on a survey of 100 IT professionals conducted by Secure Islands, Nov. 2015

Why is data classification important?

Information security starts with classification

Classification =

Data
+ value determination
+ persistent labelling

Why is data classification important?

- Key questions
  - How valuable is the data to the organization?
  - How valuable is the data to 3rd parties, competitors or outside individuals?
  - What is the impact / risk to the organization if valuable has leaked?
  - Who should / should not have access to the data (need to know)?

Classify data based on its value and protect / process it accordingly

Approach

1. Determine the value of the information
2. Apply an appropriate classification level to the data based on the value
3. Implement an appropriate security solution for the different classification levels which prevents the intentional or unintentional leakage of data (DLP).
4. As part of data life-cycle manage classification levels and access to the classified data

Classification levels

- Classification levels and efforts / impacts

	Public	Internal	Confidential	Secret
Determination effort	Medium	Low (default)	High	Low
RMS Protection effort	None	Low / Medium	Medium	Medium
Usability impact based on the classification level / protection	None	Medium	High	Medium / Low
Identity management pre requisites	None	Medium	Medium	Medium

Without data classification all data are protected / processed the very same way

keyon

Rights Management

How to classify and protect data in a real world scenario?

Yes, we can. Automated classification and protection solutions have been successfully implemented in large enterprises.

About Rights Management

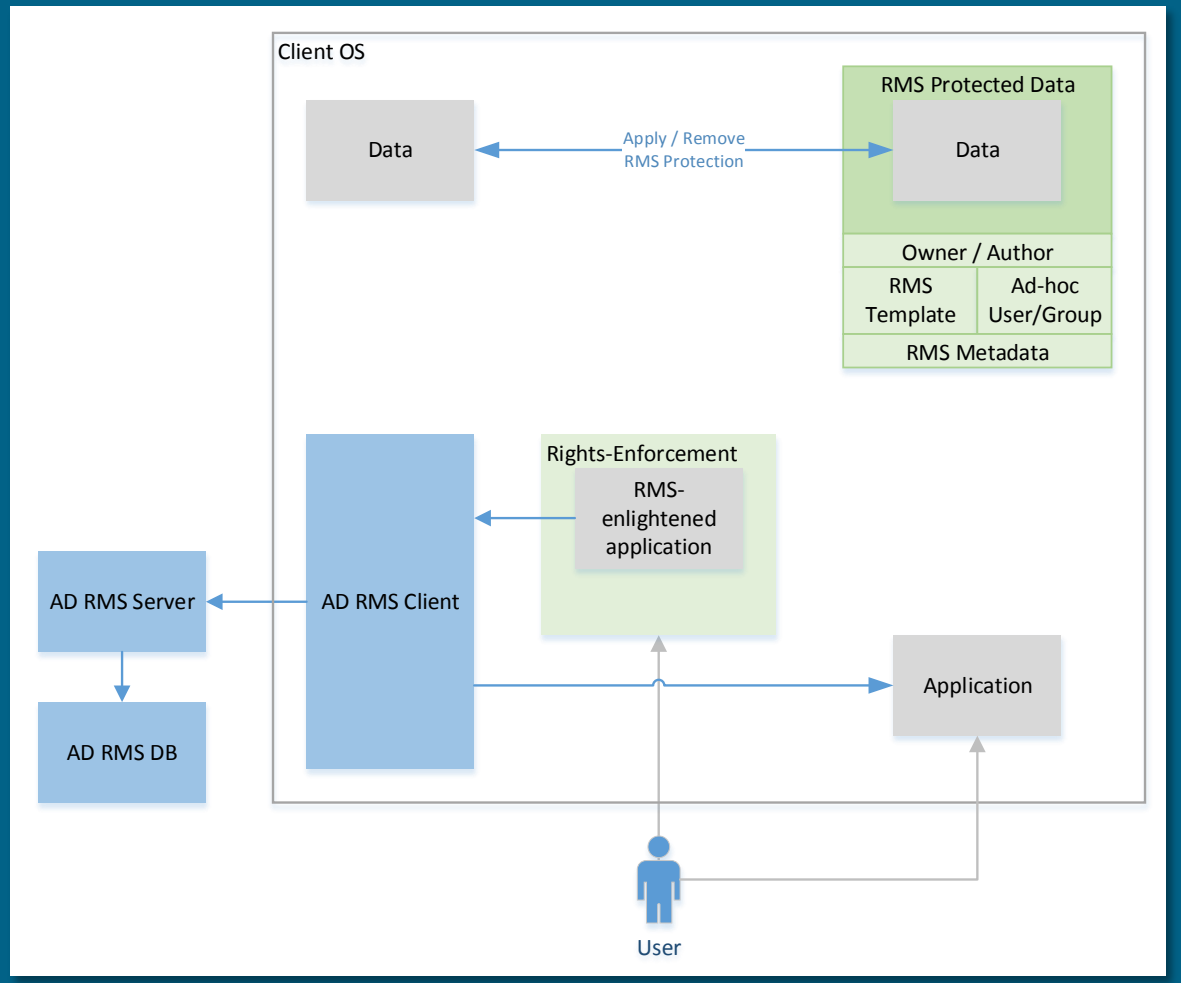
- Rights Management is a solution for organizations that want to classify and protect their data in today's challenging working environment (on-prem, in the cloud, on mobile devices)
- Comprehensive technology to protect confidential data across major platforms (Windows, iOS, Mac OS X, Android, Linux)
- Security is intrinsically tied to the data, independent of any technology used for data at rest or data in motion
- Flexible management of users and roles (joiners / movers / leavers / deputies / auditors / legal investigators)

Why RMS?

- Gartner predicts that by 2019, 90% of EDRM deployments will incorporate Microsoft RMS components (G00292633, G00275948)
- Enterprise digital rights management (EDRM) is a mature technology for enterprise wide persistent protection of data (G00275948)
- A broader data-centric security strategy requires a combination of EDRM with other technologies such as classification, data loss prevention (DLP) and data centric audit and protection (DCAP). (G00275948)

How RMS works (simplified)

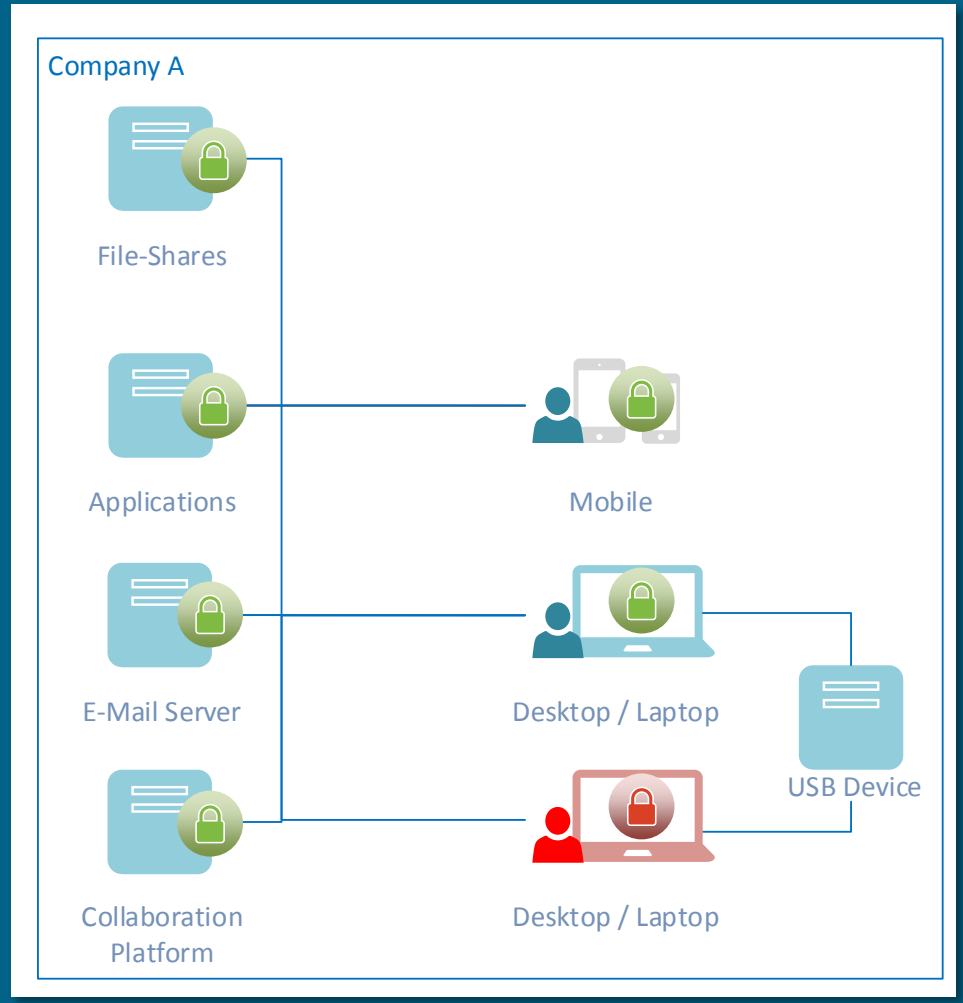
- Strong symmetric (AES) and asymmetric (RSA) cryptography
- User must be entitled to acquire an RMS use license to get access to RMS protected data.
- "Superuser" has unrestricted access to any RMS protected data



RMS from a users point of view

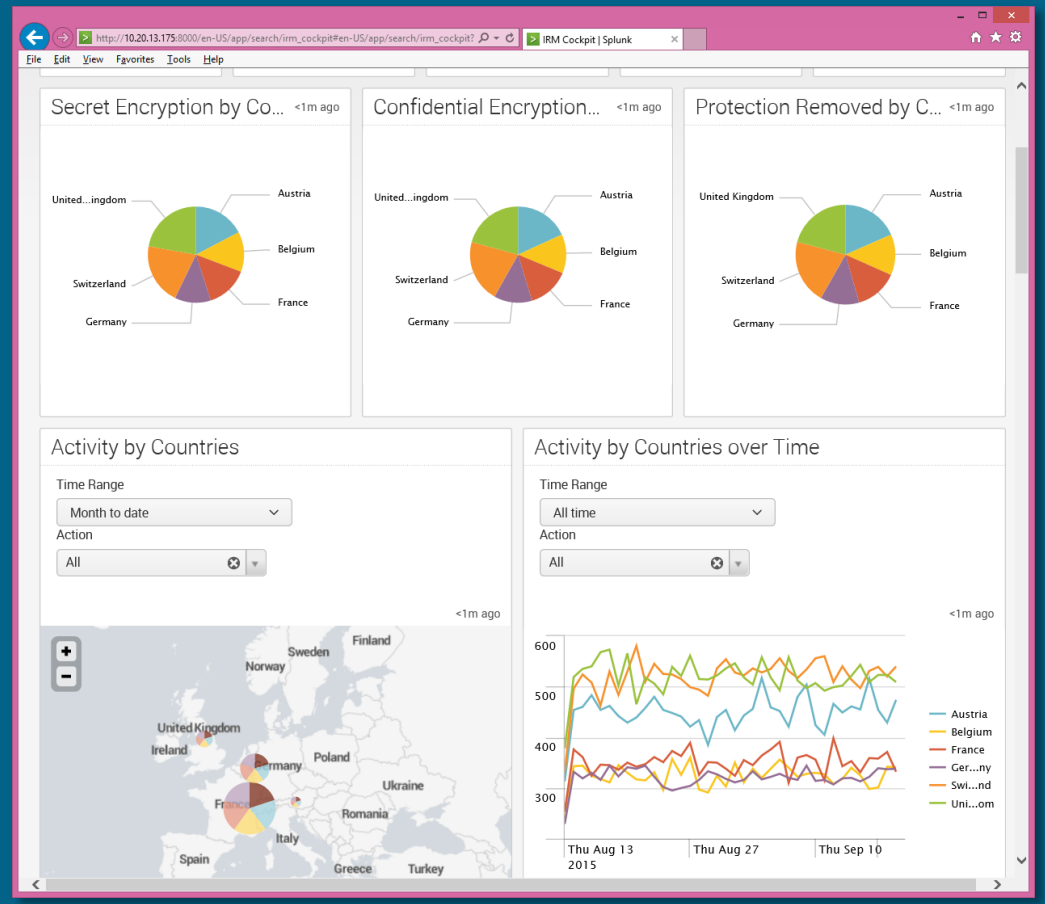
- Automated classification and protection
  - copied into / out of a folder
  - downloaded from / uploaded to a web application (including SharePoint)
  - content contains patterns, meta data
  - in folders / shares (bulk process)
  - SDK used by an application
  - In proxies or gateways

Application specific access rights (ACL) is leveraged to the data



RMS – Document Tracking

- Keyon - true-Xtended Reporting
  - Determine who tried to get access / re-classify / re-protect / a document by when and where
  - Track business related document usage (e.g. who got access to the internal specification of our latest artificial hip joint)
  - Collects log-files and events from many sources



keyon

Data Loss Prevention (DLP)

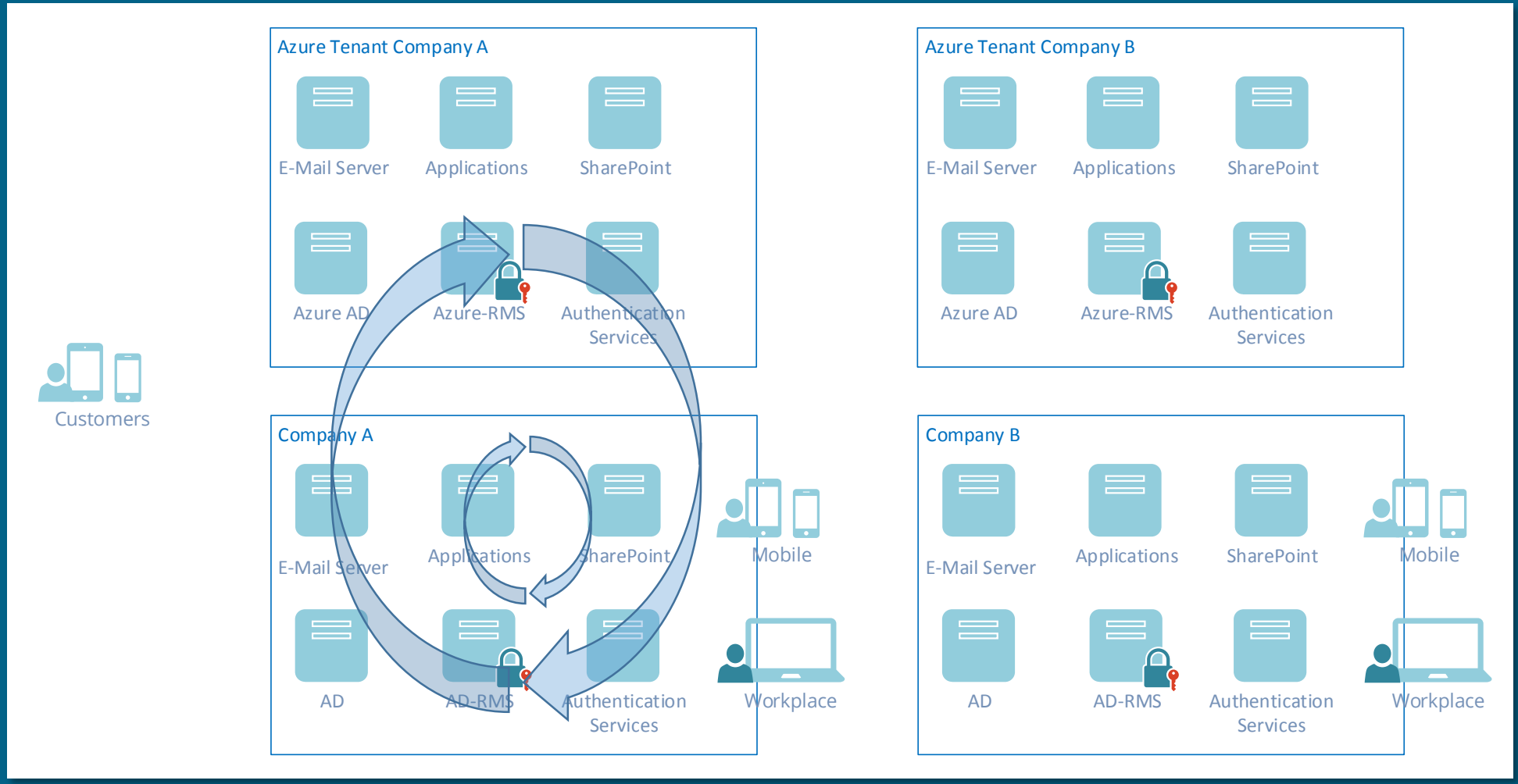
DLP Approaches: Rights Management
vs.
Scanning (boundary control)

DLP objectives

- Prevent intentional and unintentional loss of data
- Own and control data and the usage of the data
- Identify sensitive data and defend against unauthorized access
- Support users in their daily business to meet policies and regulatory provisions
- Ensure e-discovery
- Do not stop business – seamless and broad integration

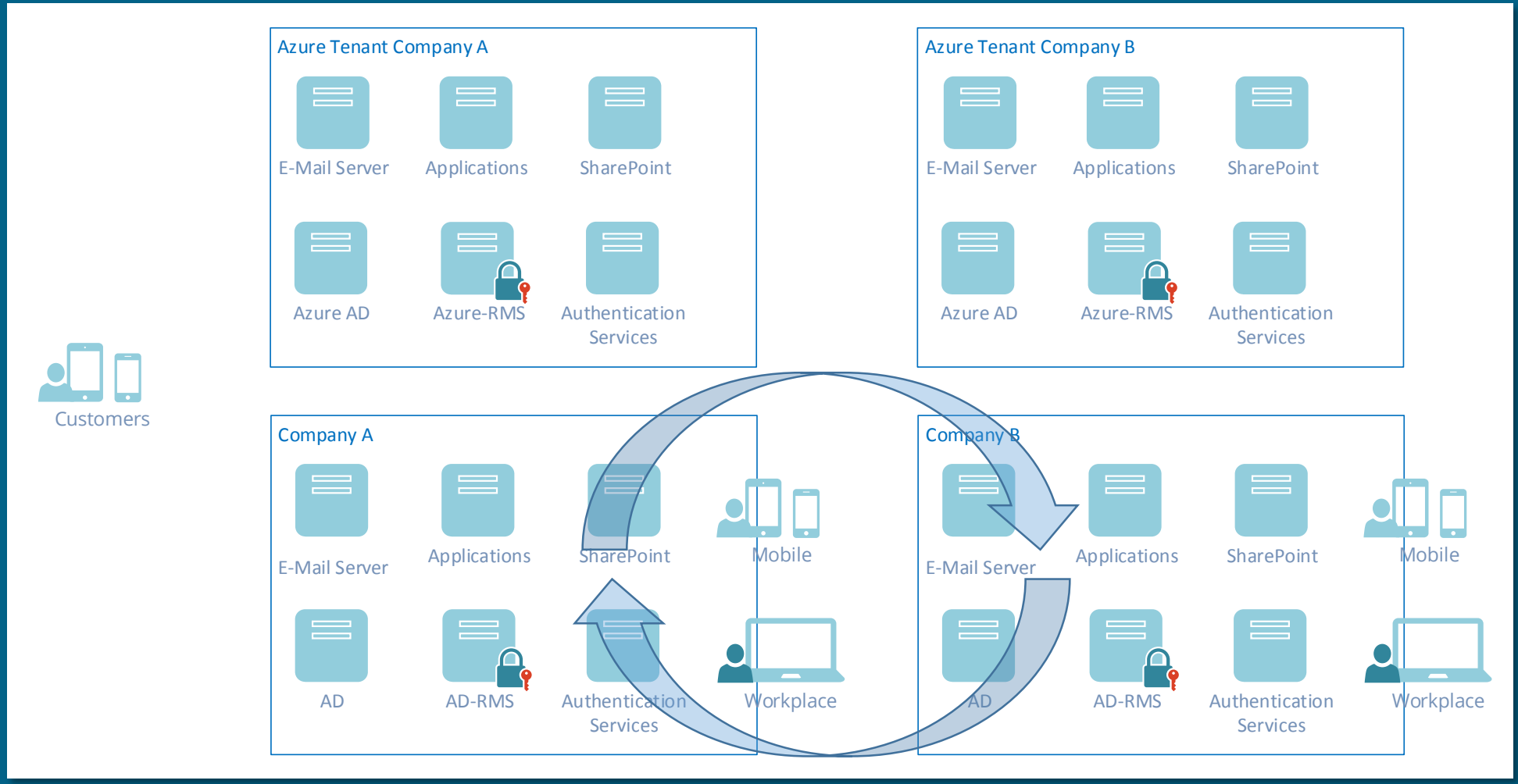
Where is data being used?

- Inside the company (many collaboration channels)



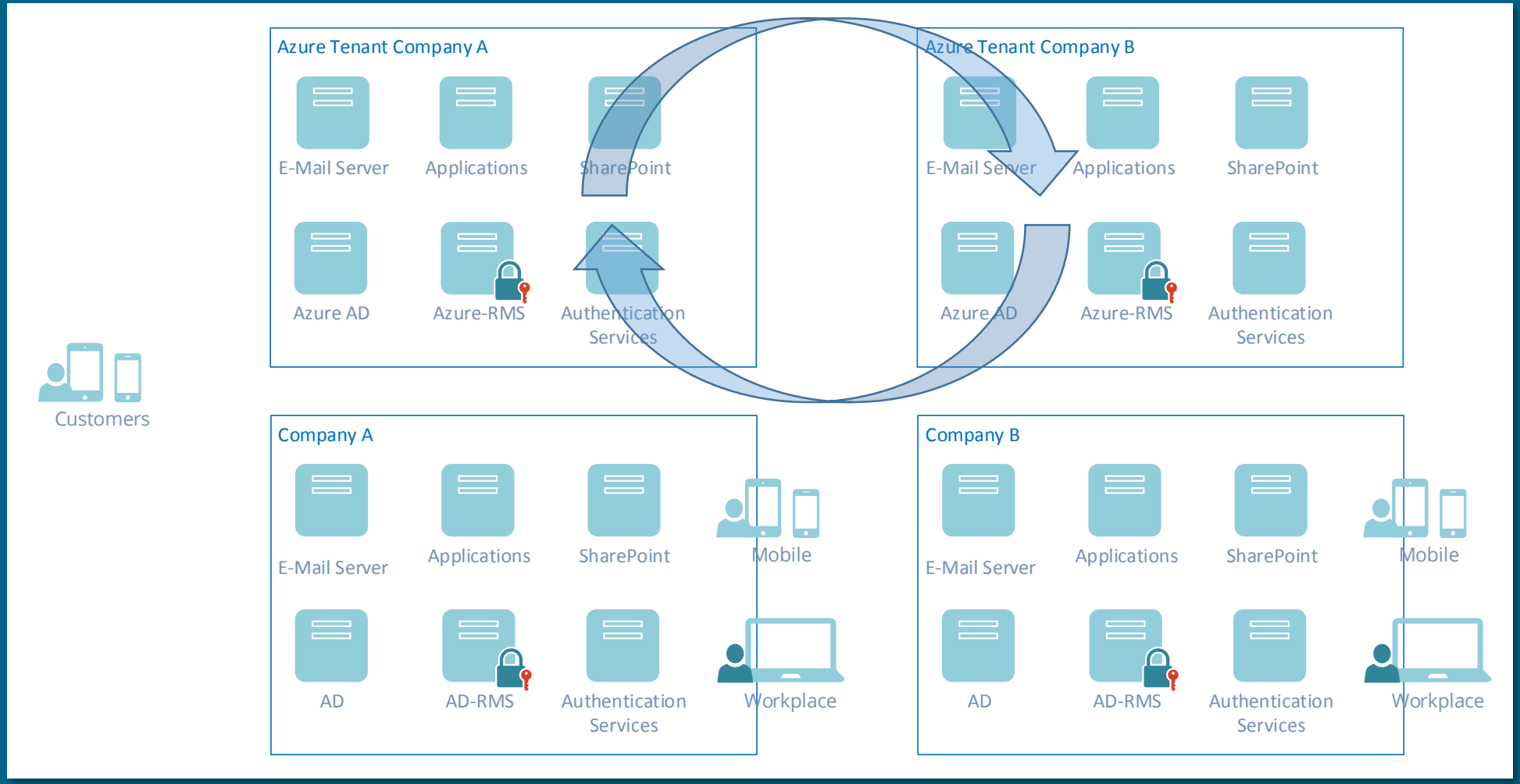
Where is data being used?

- B2B on prem (mainly using e-mail)



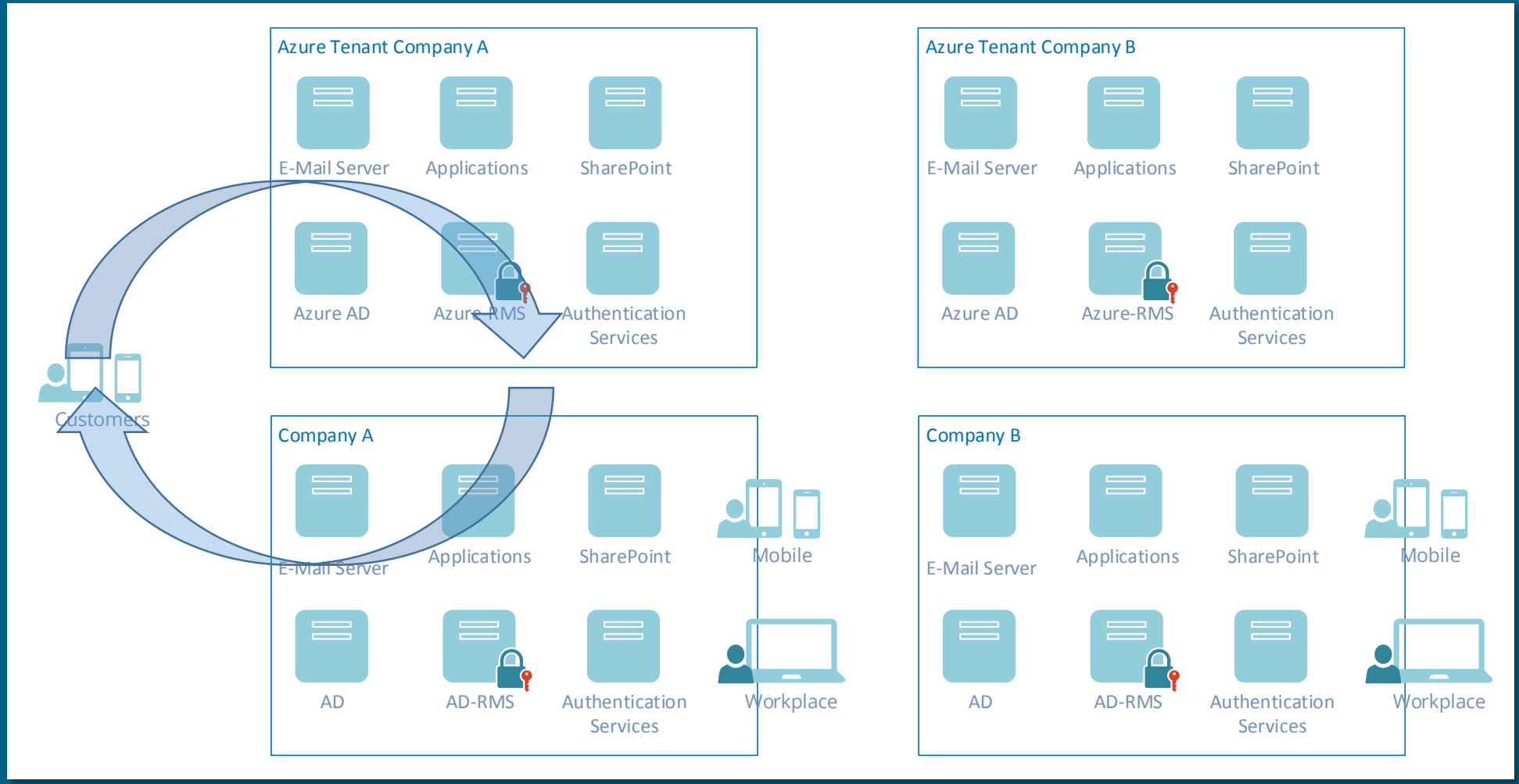
Where is data being used?

- B2B in the cloud (collaboration platform)



Where is data being used?

- B2C on-prem and in the cloud (collaboration platform)



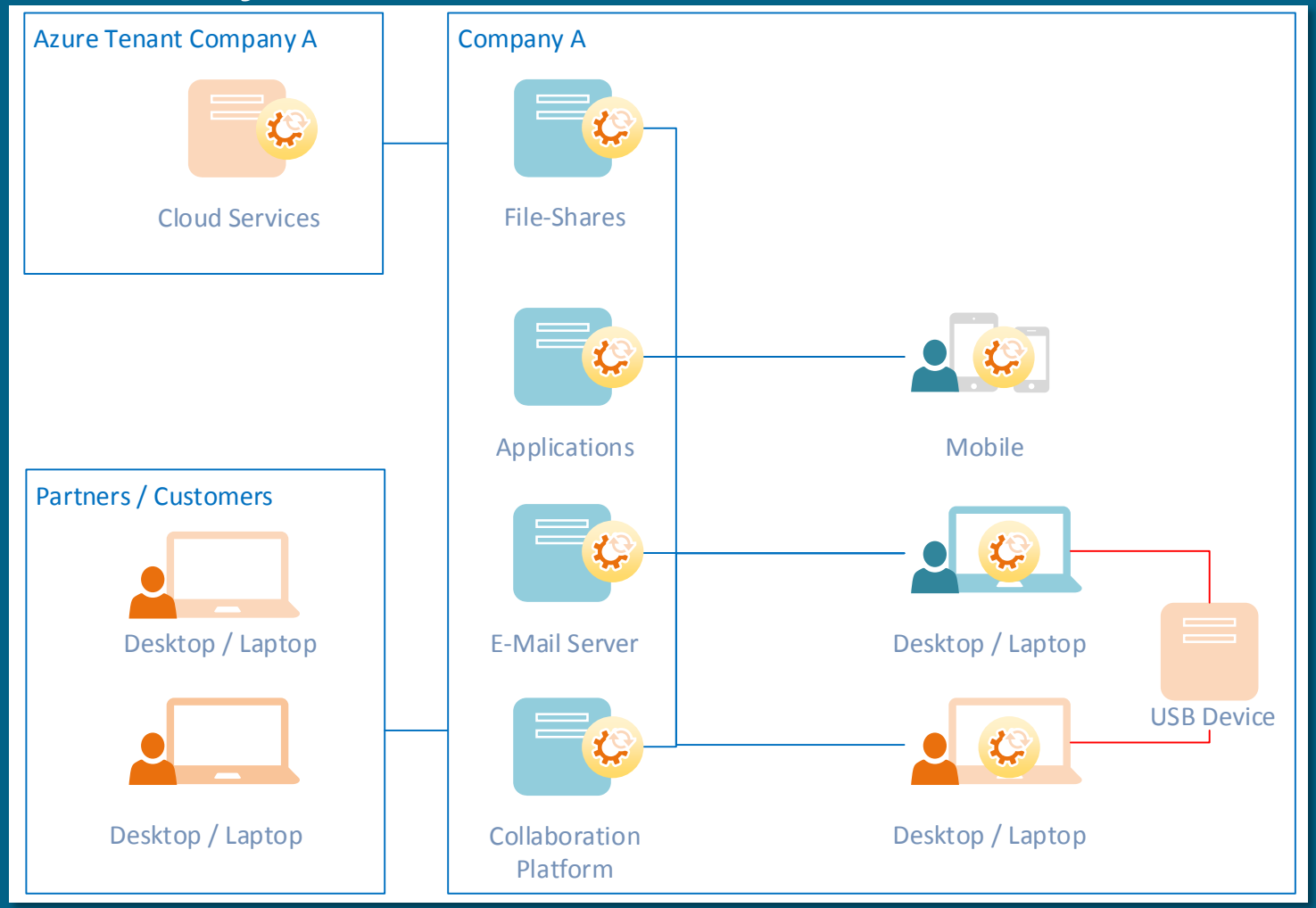
DLP Approach – elevator pitch

keyon

Scanning (boundary control)	Rights Management
Block / reject transmission of sensitive data based on pattern matching or exact data matching	Identity-bound data protection, access control to sensitive date based user- and device policies
• Data remains untouched • Implement scanning, pattern matching / exact data matching technologies for DAR, DIM, DIU • Disable features (e.g. USB port, drop box, etc.) • Monitor vs. Prevent approach	Security is intrinsically tied to the data, independent of any other technology or security measure. Security is ideally applied at origin.

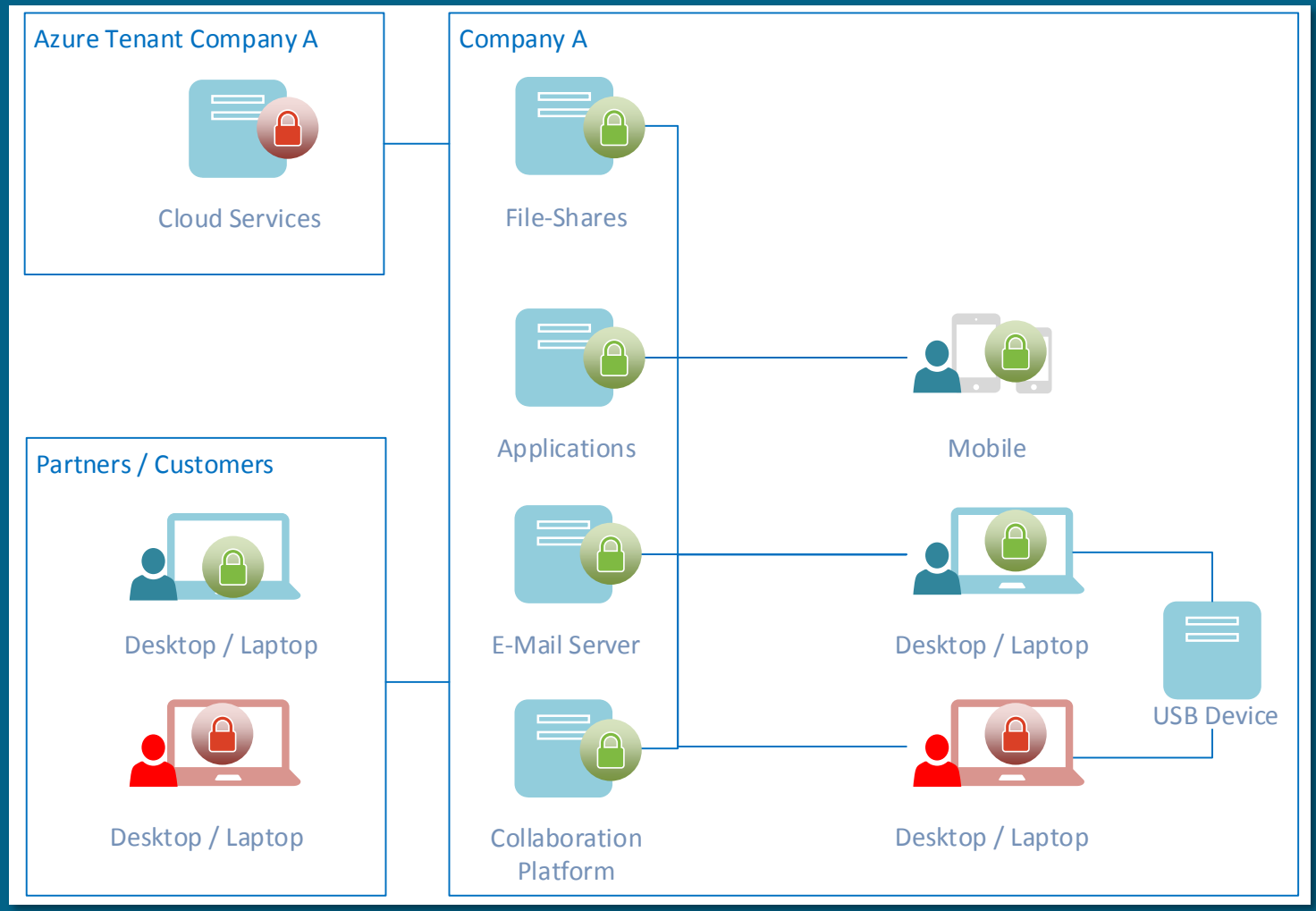
DLP with Scanning approach

- Pattern based / EDM at every interface / channel



DLP with Rights Management

- Classification and protection



Implementation guidelines

- Automation is key
- Focus on the most important data and processes
- Define appropriate leakage boundaries
  - Small boundaries for projects, teams or OEs in case of file shares and web applications (incl. SharePoint with projects- or team rooms)
  - Large boundaries otherwise (Global, R&D, HR in case or manual classification)
- Define appropriate rights enforcement
  - Full control, View and Edit, View only, Copy and Print

Implementation guidelines

- Consider journaling, archiving, malware scanning and legal investigation
- Control the usage of the data (dashboard, doc tracking)
- Train users and support
  - In case of automated processes and if a user is entitled to get access to data he won't really recognize the security measures are in place

keyon

Questions & Answers

Thank you for your attention