Drošība mākonī jeb kas būtu jāzina katram par datu drošību mākonī

Jānis Bērziņš, SQUALIO (DPA group) Senior Infrastructure Solutions Consultant

Is cloud secure or not?

What is information security?

Facts and numbers

Cloud security

What is information security?

Users	Processes	Data
Network	Infrastructure	Physical

TOP 3 barriers to adoption of Cloud Services

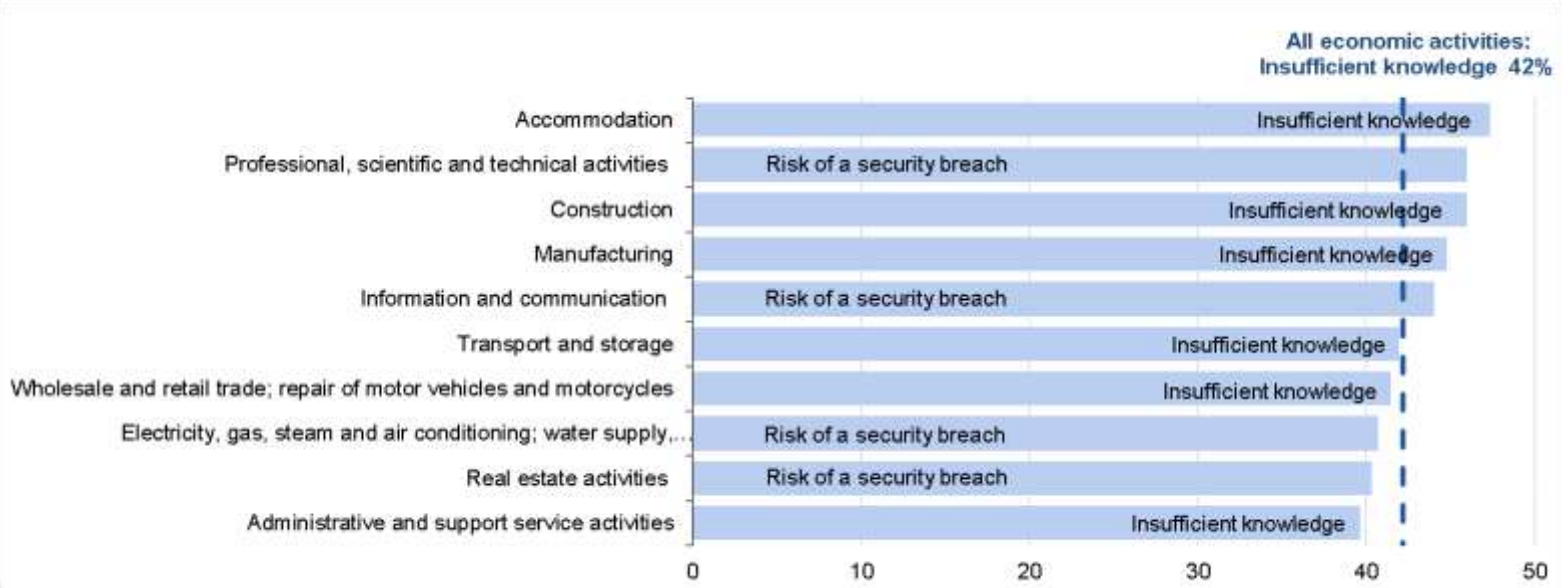
28% Data location, security and privacy risks

17% Integration with existing IT

16% Regulatory and compliance concerns

Data source: KPMG research- http://www.kpmg-institutes.com/institutes/shared-services-outsourcing-institute/articles/2015/03/spps-it-outsourcing-management-summary-2014-15.html

Factors preventing from using cloud computing services



Insufficient knowledge and risk of a security breach are the main factors

Data source: Eurostat - http://ec.europa.eu/eurostat/statistics-explained/mobile/index.php#Page?title=Cloud computing - statistics on the use by enterprises&lg=en

Factors limiting use of cloud Services

Large enterprises:

57% Risk of security breach

48% Location of data, legal jurisdiction

17% Insufficient knowledge and skills

Small and medium enterprises:

38% Risk of security breach

32% Insufficient knowledge and skills

32% High cost of cloud computing

Data source: Eurostat - http://ec.europa.eu/eurostat/statistics-explained/mobile/index.php#Page?title=Cloud computing - statistics on the use by enterprises&lg=en

IT security statistics don't change

96%

SIMPLE ATTACKS

«TO DATE, THERE HAVE BEEN

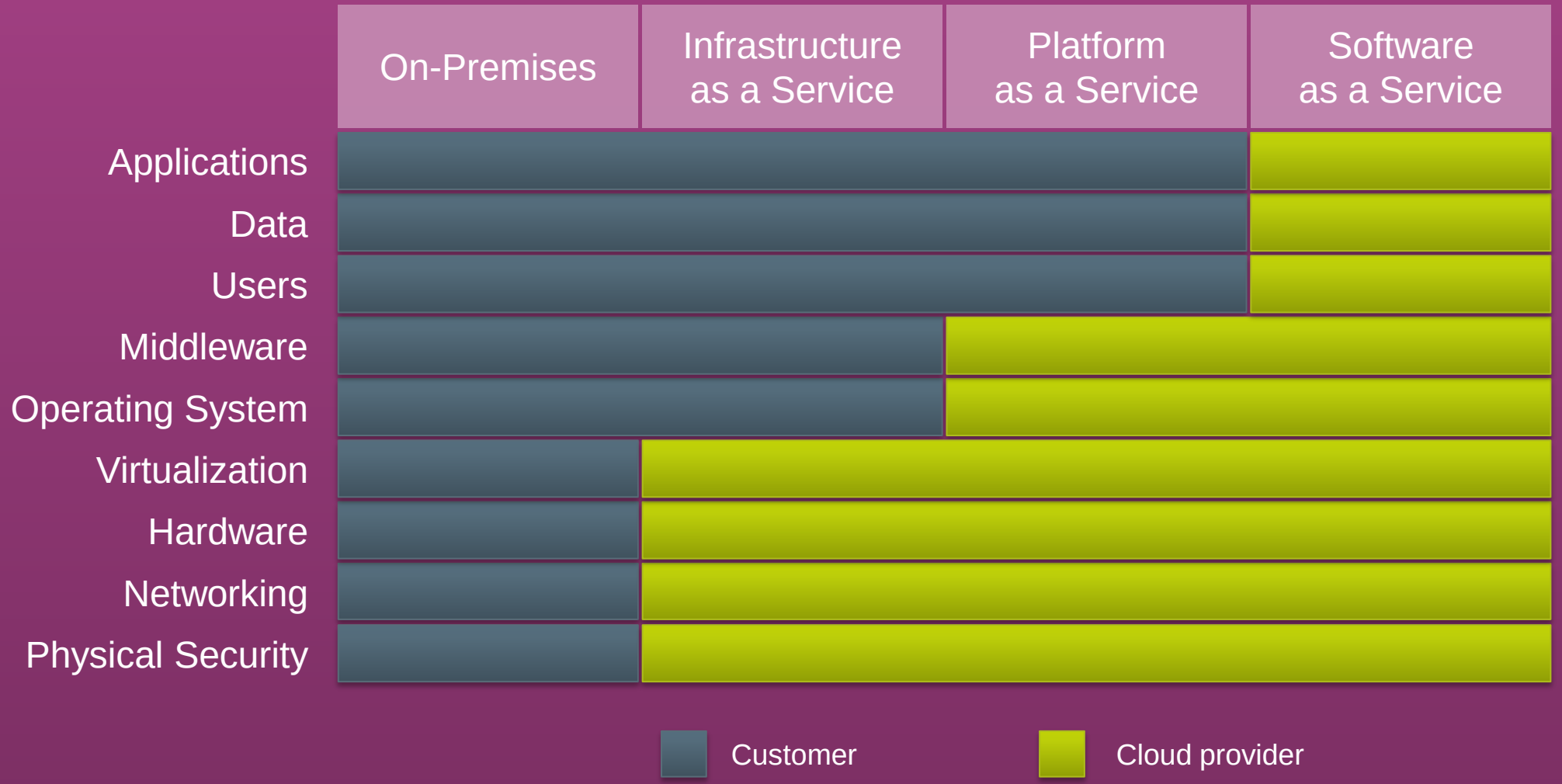
VERY FEW SECURITY BREACHES IN THE PUBLIC CLOUD

- MOST BREACHES CONTINUE TO INVOLVE ON-PREMISES DATA CENTER ENVIRONMENTS.»

Gartner Inc.

Shared responsibility

REDUCES SECURITY COSTS + MAINTAINS FLEXIBILITY, ACCESS, & CONTROL



Physical security

- Cameras
- 24X7 security staff
- Barriers
- Fencing
- Alarms
- Two-factor access control: Biometric readers & card readers
- Security operations center
- Seismic bracing
- Days of backup power

Perimeter

Building

Computer room

Infrastructure security

Physical & logical security

Systems management & monitoring

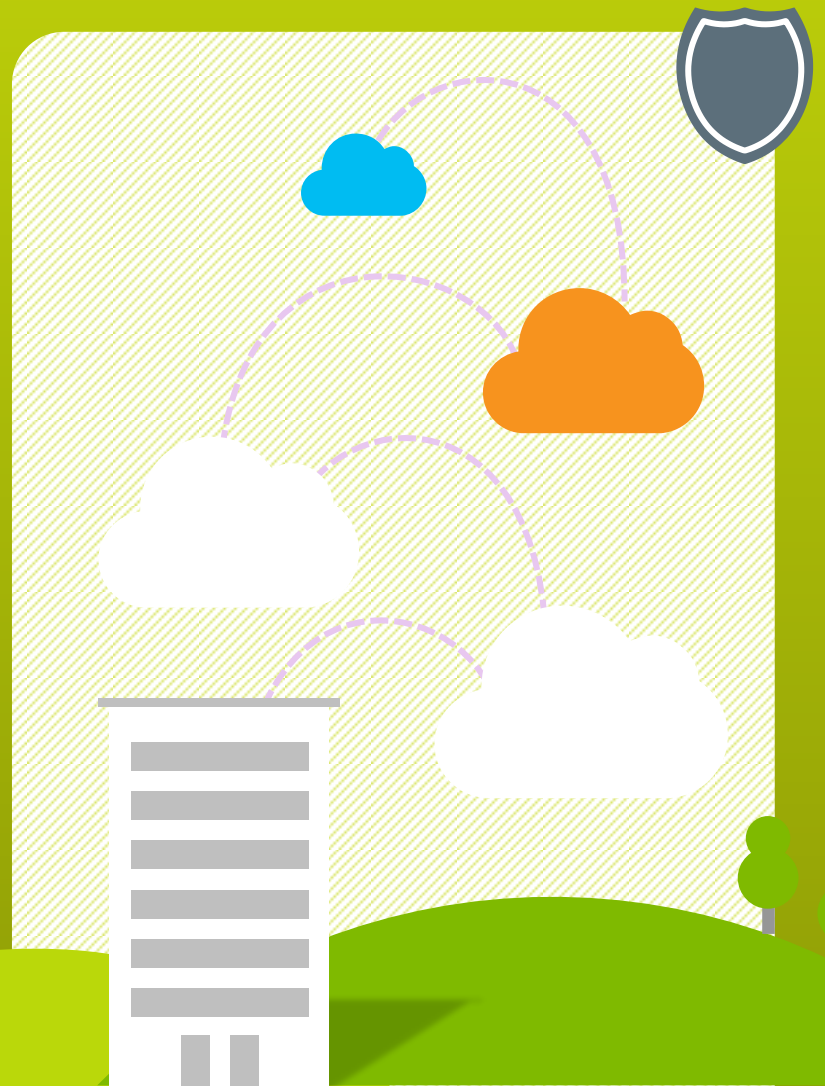
Threat defense

Network protection

Virtual Networks

Network Security Groups

Cloud to on-premises connections

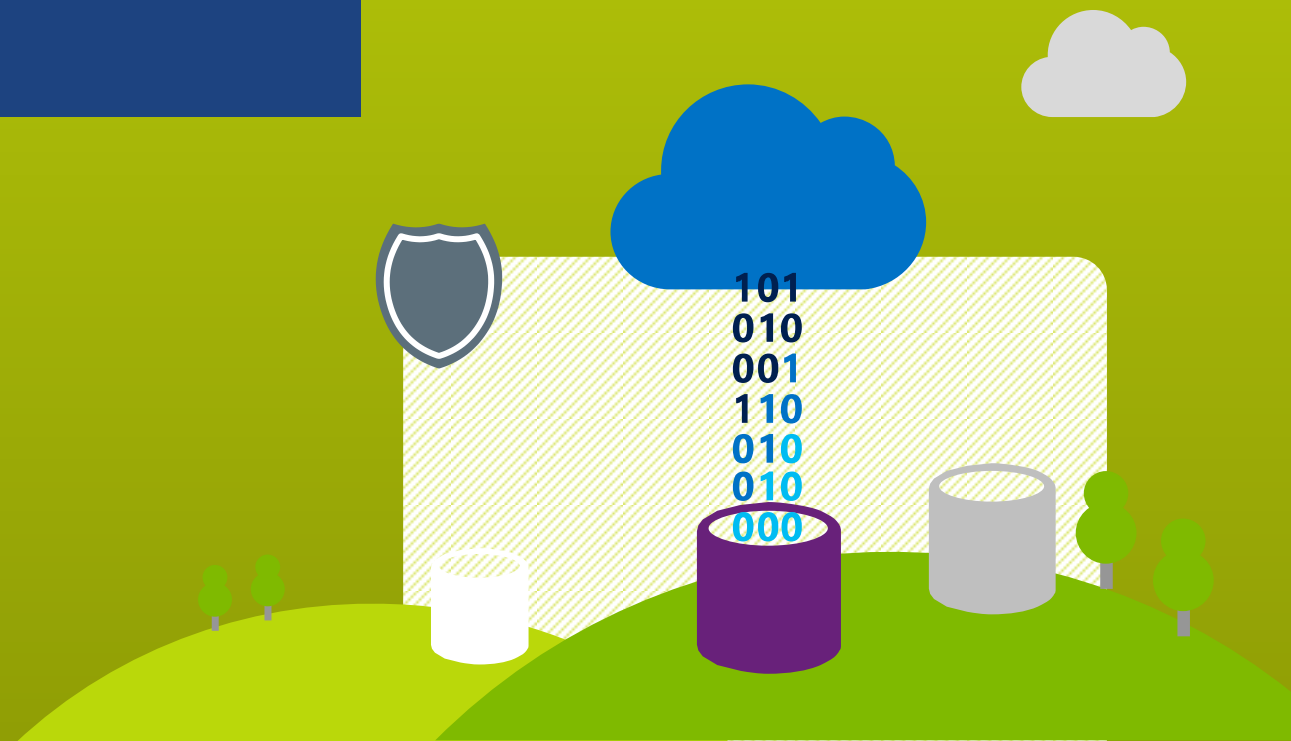


Data security

Encryption for data in transit

Securing data at rest

Data segregation



Expanded ecosystem of partner solutions

Security partners

cloudlink
TREND MICRO
Symantec
ALERTLOGIC Security. Compliance. Cloud.
Checkpoint
KASPERSKY lab
McAfee
Barracuda
CloudPassage

Where my data is located?

Where my data is located?

AZURE:

- Creates three copies of data in each datacenter
- Offers geo-replication in a datacenter hundreds of miles away
- Does not transfer Customer Data outside of a geo (ex: from US to Europe or from Asia to US)

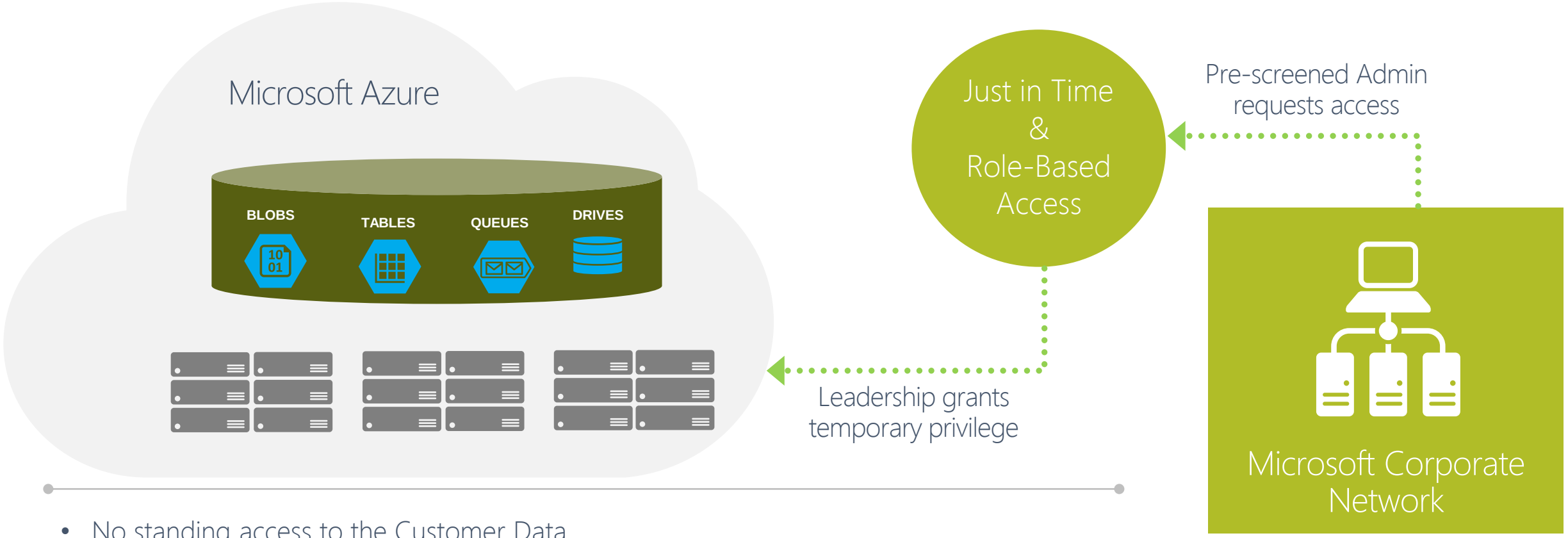
CUSTOMER:

- Chooses where data resides
- Configures data replication options

Note: Microsoft Azure data centers, Australia – Q2 FY15

Does cloud provider access my data?

Does cloud provider access my data?

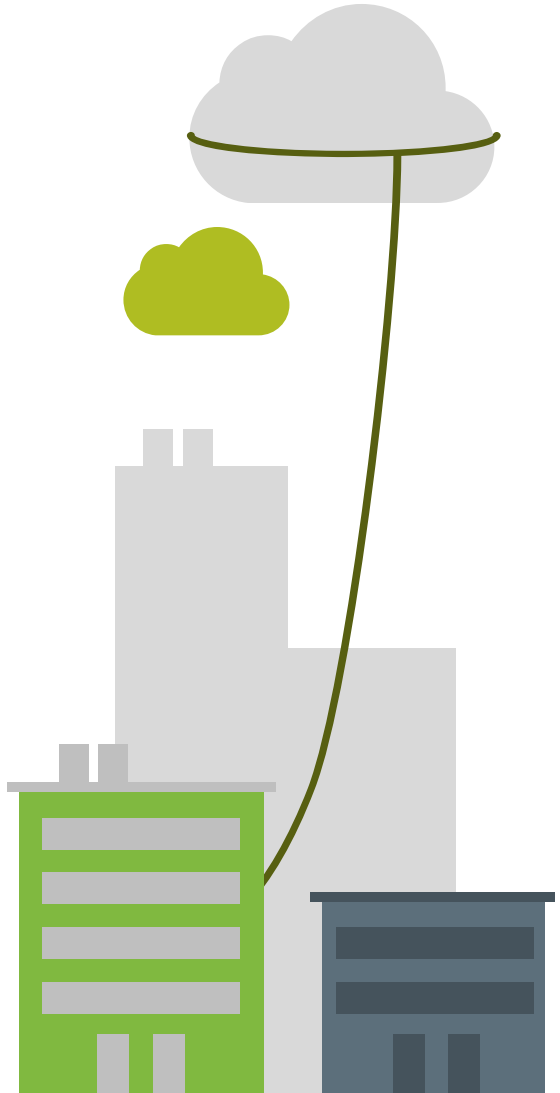


- No standing access to the Customer Data
- Grants least privilege required to complete task
- Multi-factor authentication required for all administration
- Access requests are audited, logged, and reviewed

I have heard that cloud is not secure. Is it?

Is the cloud secure or not?

Information security standards	Government certifications	Industry certifications
ISO 27001 ISO 27018 SOC 1 Type 2 SOC 2 Type 2	US FedRAMP/FISMA US CJIS UK G-Cloud Australia IRAP Singapore MCTS EU Data Privacy Approval	PCI DSS Level 1 HIPAA/HITECH Life Sciences GxP



CONCLUSION

Cloud security

Assess risks

At least the same as on-premises

Delegates responsibility

Thank you!

squalio

DPA group