

## Organizations are failing to protect sensitive data in the cloud

### 2019 Cloud Security Study

Results from the 2019 Thales Cloud Security Study, a survey of more than 3300 executives in 8 countries who are familiar with and involved in their companies' use of both public and private cloud resources. Survey, reporting and analysis conducted by the Ponemon Institute, commissioned by Thales

## Businesses are taking advantage of the cloud, but not applying adequate security



48%

of all corporate data is stored in the cloud compared to 35% three years ago



49%

of organizations are encrypting sensitive data in the cloud

## Businesses remain responsible for security of their data in the cloud regardless the provider



53%

of businesses are controlling the encryption keys when data is encrypted in the cloud,

despite 78%

saying it's important to retain ownership of the encryption keys

## Some businesses push responsibility for data security to cloud providers, but do not consider security a big factor when choosing them

48%

of organizations have a multi-cloud strategy, with AWS, Microsoft Azure and IBM being the top three cited cloud providers



30%

of organizations have a unified system for secure access to both cloud and on-premise applications



32%

don't employ a security-first approach to storing data in the cloud

## Businesses use 29 cloud applications on average, compared to 27 two years ago



over 10%

have more than 50 and the average US business has 41

## Businesses struggle to reduce complexity of managing privacy and data protection regulations in the cloud environment



46%

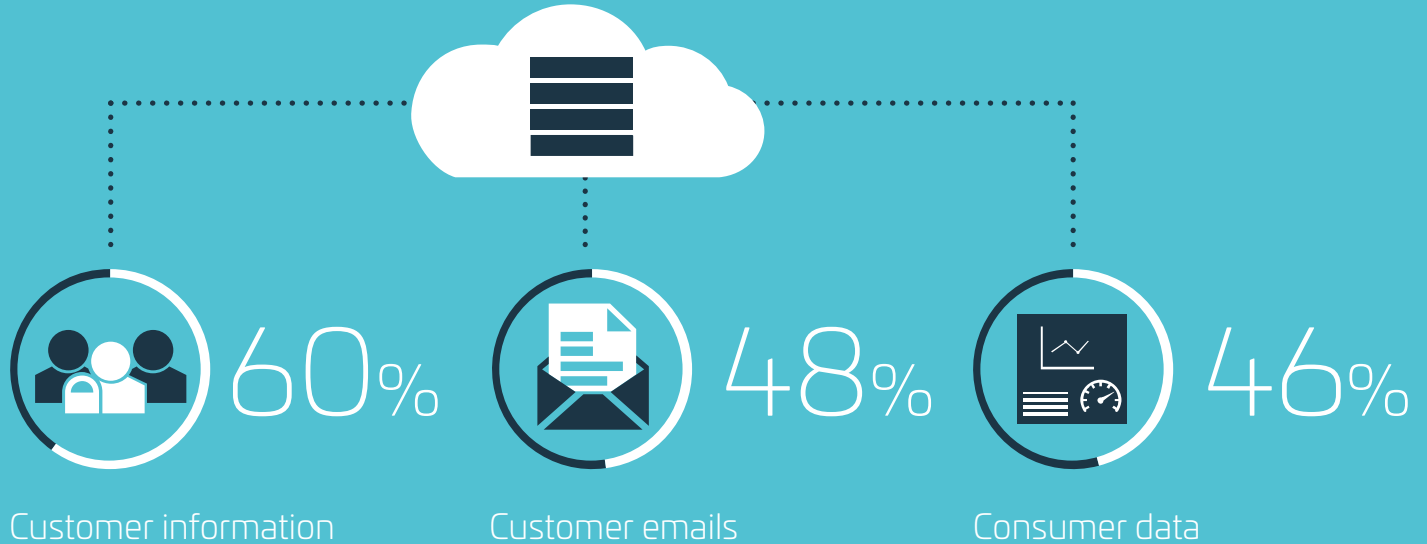
revealed that storing customer data in the cloud makes them more of a security risk and a compliance risk (56%)



44%

of organizations are careful about sharing sensitive information with third parties

## The biggest amount of data stored:



Follow us on:



#CloudSecurity



**Decisive technology**  
for decisive moments