

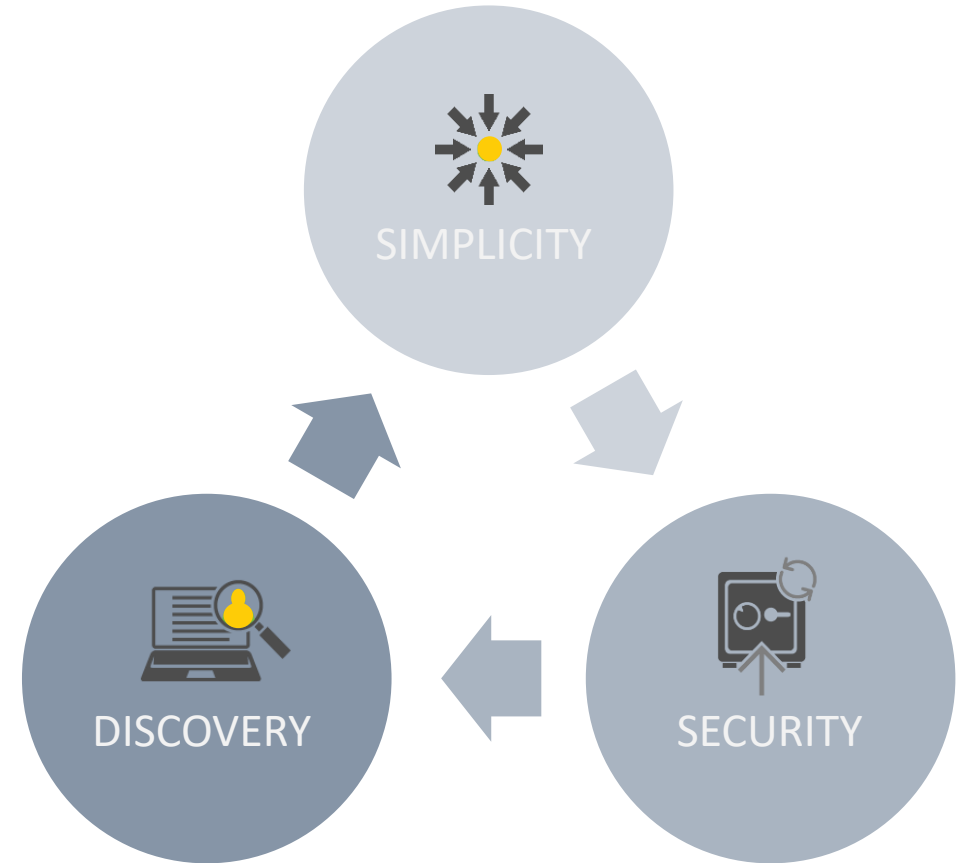


protection now.
safe lifetime.

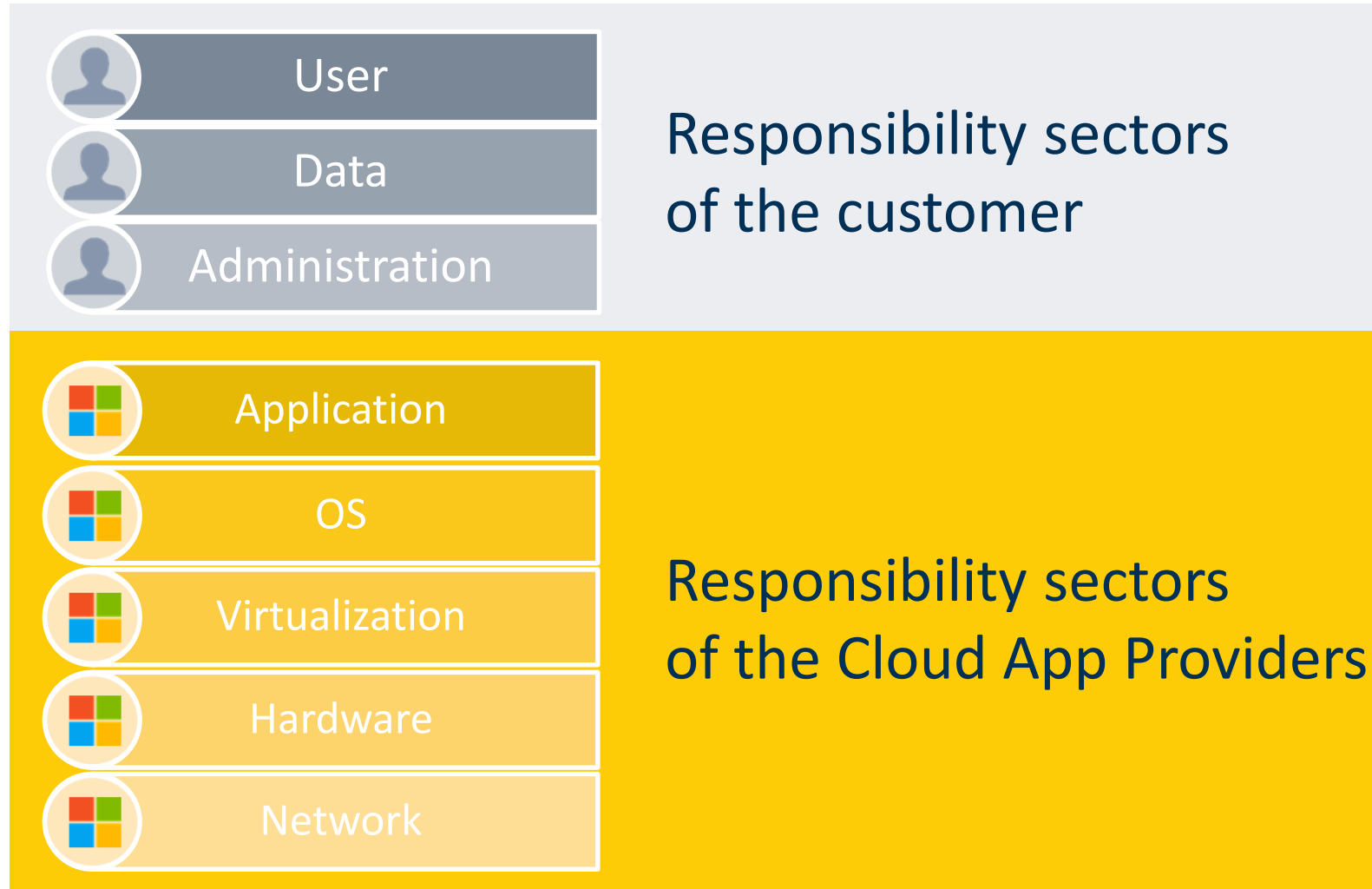


SEP Cloud Application Protection Service:

SECURITY FOR OFFICE 365, G SUITE & SALESFORCE



RESPONSIBILITY FOR DATA IN CLOUD APPS







THREATS TO OFFICE 365 DATA

Responsibility sectors of the customer

-  Human Errors
-  Programming Errors
-  Malicious Deletes
-  External Hackers
-  Viruses/Malware

Responsibility sectors of the Cloud App Providers

-  Hardware Failure
-  Software Failure
-  Natural Catastrophe
-  Power Failure

SEP CLOUD APP PROTECTION SERVICE



- Cloud 2 cloud backup and restore of Office 365, Salesforce, G Suite
- Backup Software-as-a-Service

Responsibility

The responsibility for protecting data in the cloud is no different from the responsibility for protecting on-premise data.

- No one doubts that a secure backup of on-premise data is needed!
- It is the responsibility of cloud users to secure data and ensure easy recovery!



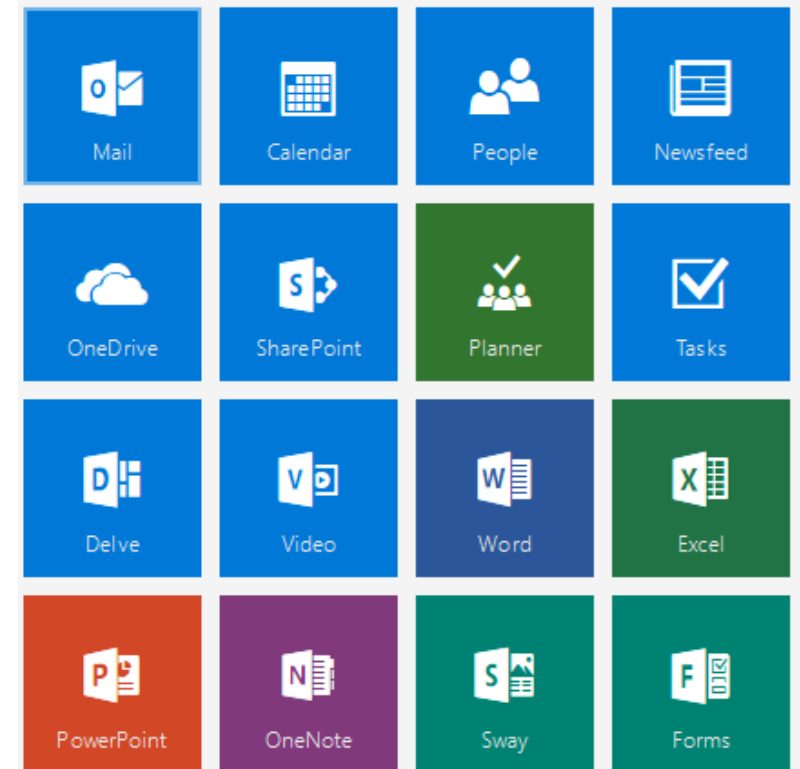
SEP CLOUD APP PROTECTION SERVICE



What is backed up at Office 365?

SEP Cloud APS automatically backs up all data on the Office 365 platform at least once a day:

- E-mails and shared e-mails (public folders)
- in-place Archives
- Calendar, Tasks, Contacts
- SharePoint Sites
- OneDrive
- Groups (conversations, plans, files, websites, calendars)
- Teams



SEP CLOUD APP PROTECTION SERVICE



What is secured at G Suite?

SEP Cloud APS automatically backs up all G Suite Apps data at least once a day:

- Gmail
- Google Drive
- Google Team Drive
- Calendar
- Google Sites
- Tasks



SEP CLOUD APP PROTECTION SERVICE



What is secured with Salesforce?

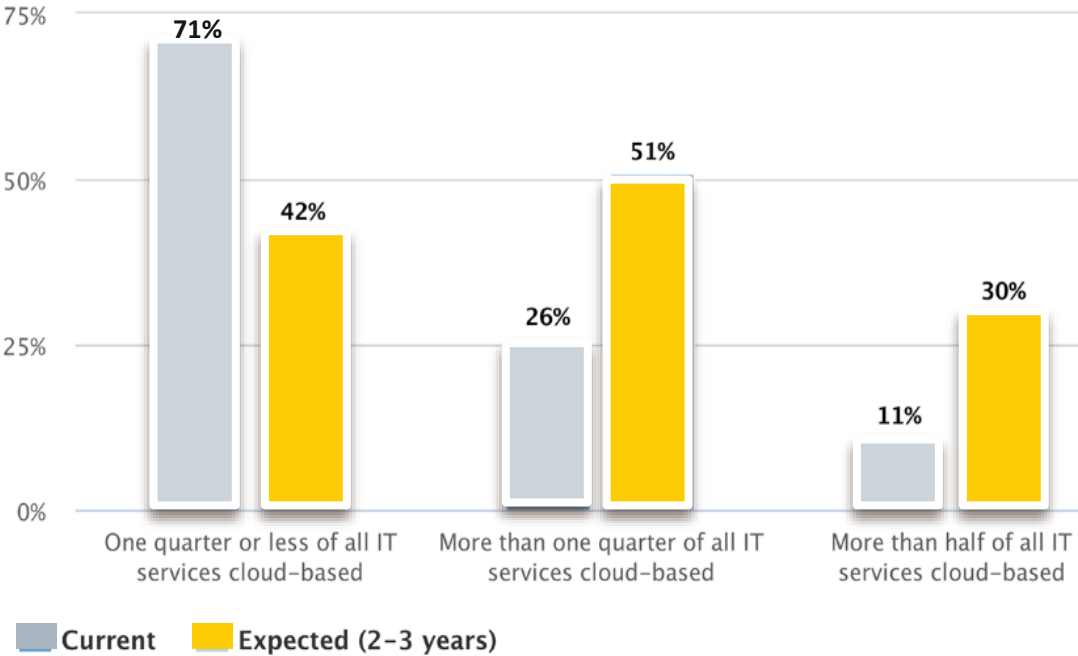
SEP Cloud APS automatically backs up all Salesforce objects at least once a day, detects new objects, and adds new objects to the backup set. User-defined fields can also be backed up.

- Accounts
- Contacts
- Leads
- Opportunity
- Activities
- Notes
- Tickets
- User-defined fields for objects

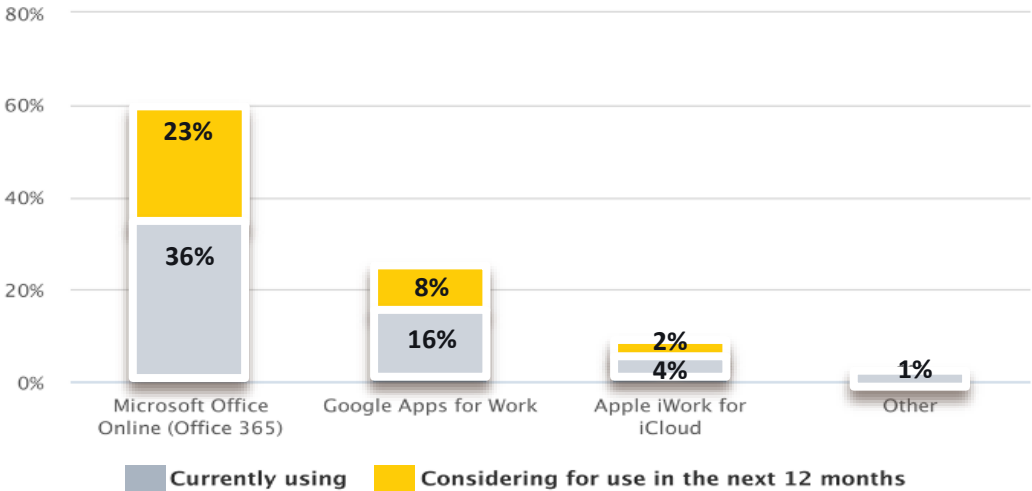


GROWING CLOUD

Percent of Organizations' Cloud-Based IT Services (Data based on all IT pros surveyed)



Usage of Cloud-Based Productivity Suites (Data based on all IT pros surveyed)



SECURITY



**There are only two types
of companies:**

**Those that have been hacked,
and those that will be.**

Robert Mueller, FBI-Director, 2012



RANSOMWARE CONSIDERATIONS



65%

More worried about Cyber threat than 12 months ago

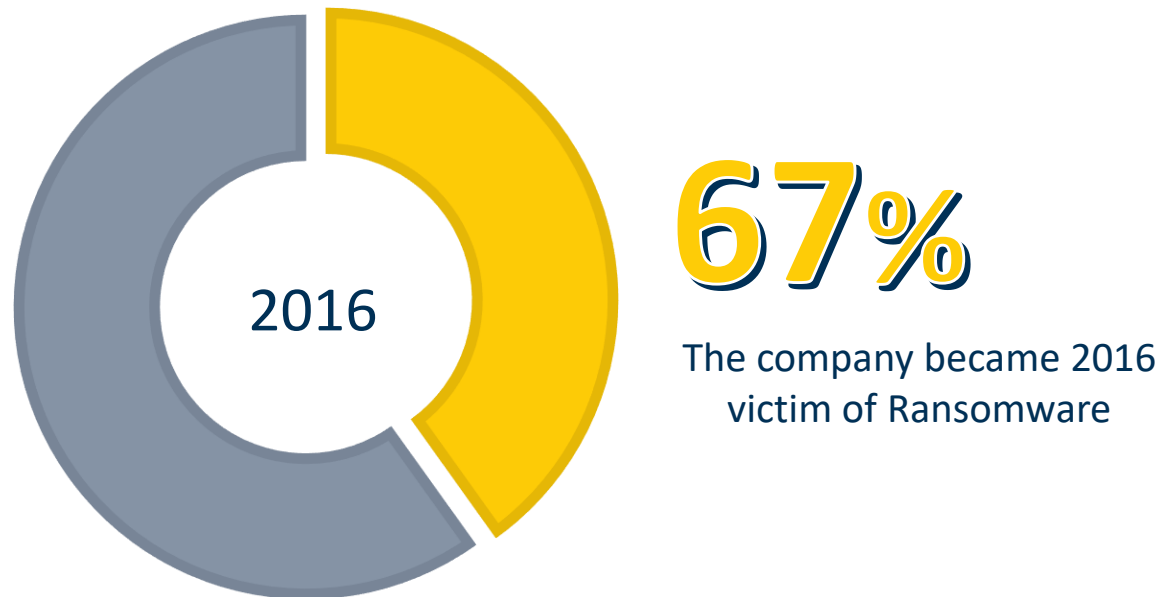
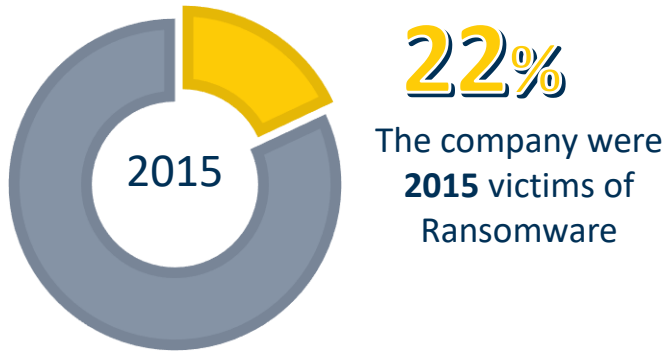
*PWC rapport

How concerned are you about Office 365 and/or the migration to Office 365 or other cloud service?

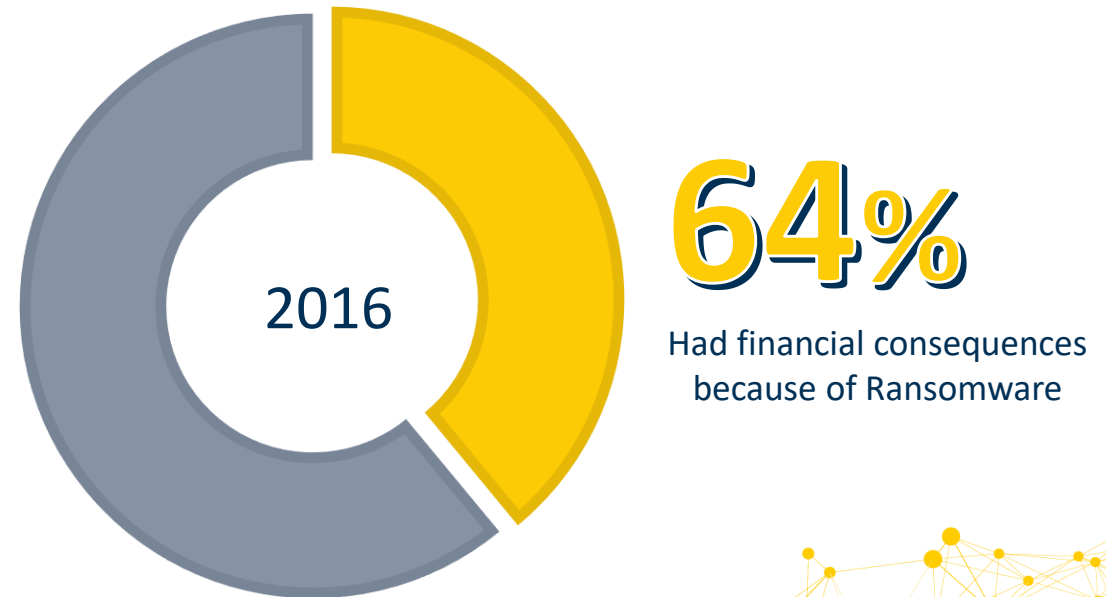
	Very/extremely	Not concerned
Loss of data while migrating	27%	17%
Trusting one vendor with all of our data	35%	8%
Lack of oversight	25%	7%
Unsure where our company data is stored	24%	10%
Not having our data in-house	33%	8%
Data is more vulnerable to loss when in the cloud	35%	10%



CONSEQUENCES



300% increase since 2015



For more than 1/3 the cost exceeded 150.000€*.



DATA LOSS IN THE CLOUD

REASONS FOR DATA LOSS:

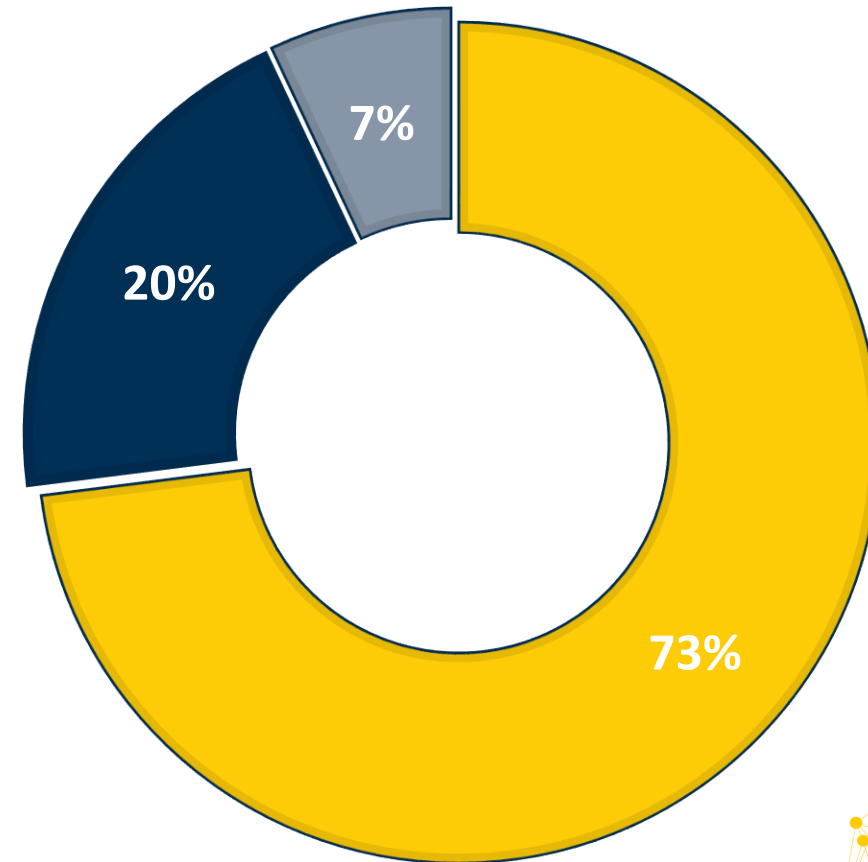
■ Human Error 73 %

- Accidental deletion & overwrites 63 %
- Closed accounts 10%

■ Hacking & Insider Threats 20 %

- Hackers 13 %
- Malicious deletes 7 %

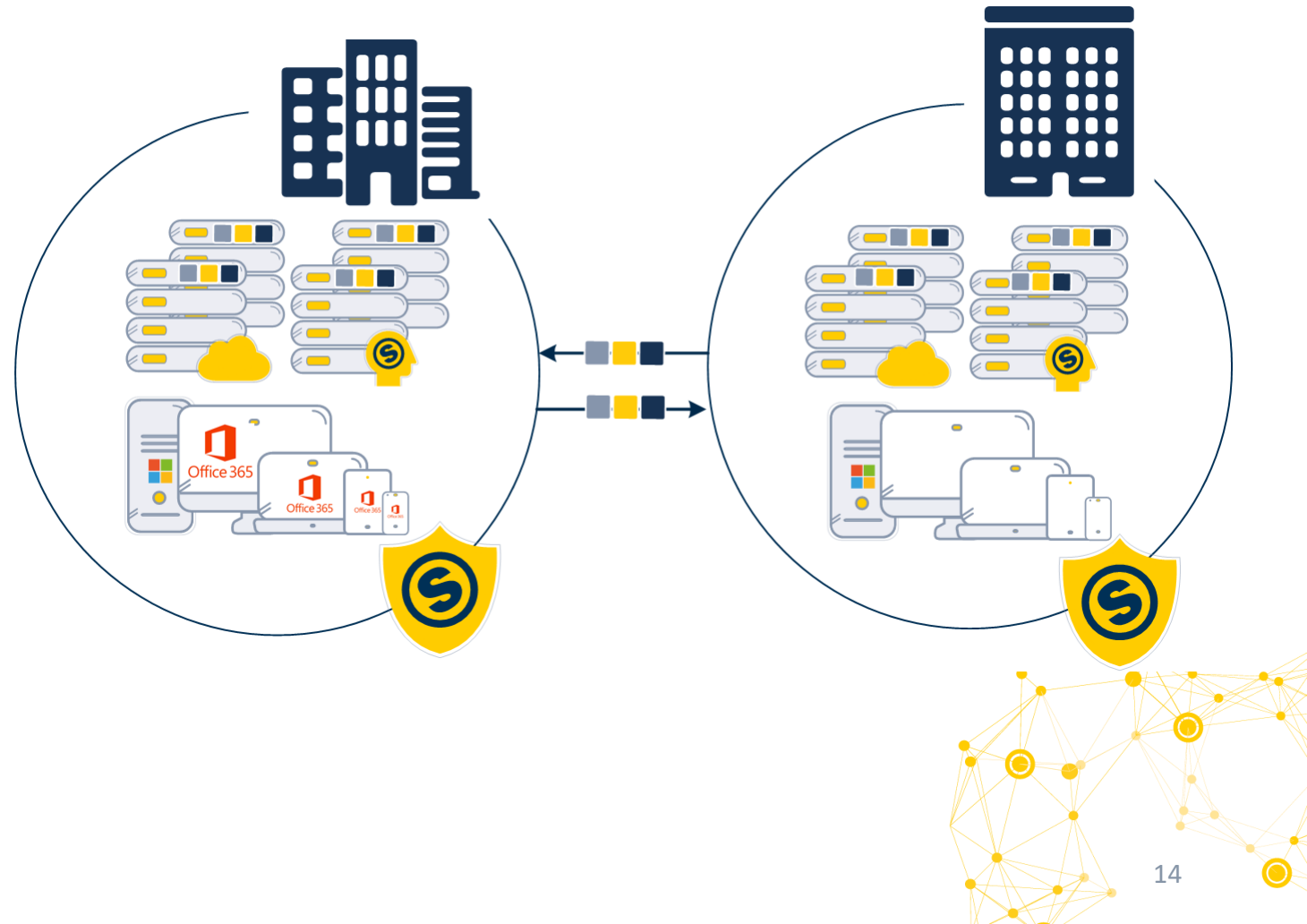
■ 3rd Party Software 7 %



Source: Aberdeen Group

INFRASTRUCTURE FOR SEP CLOUD PROTECTION

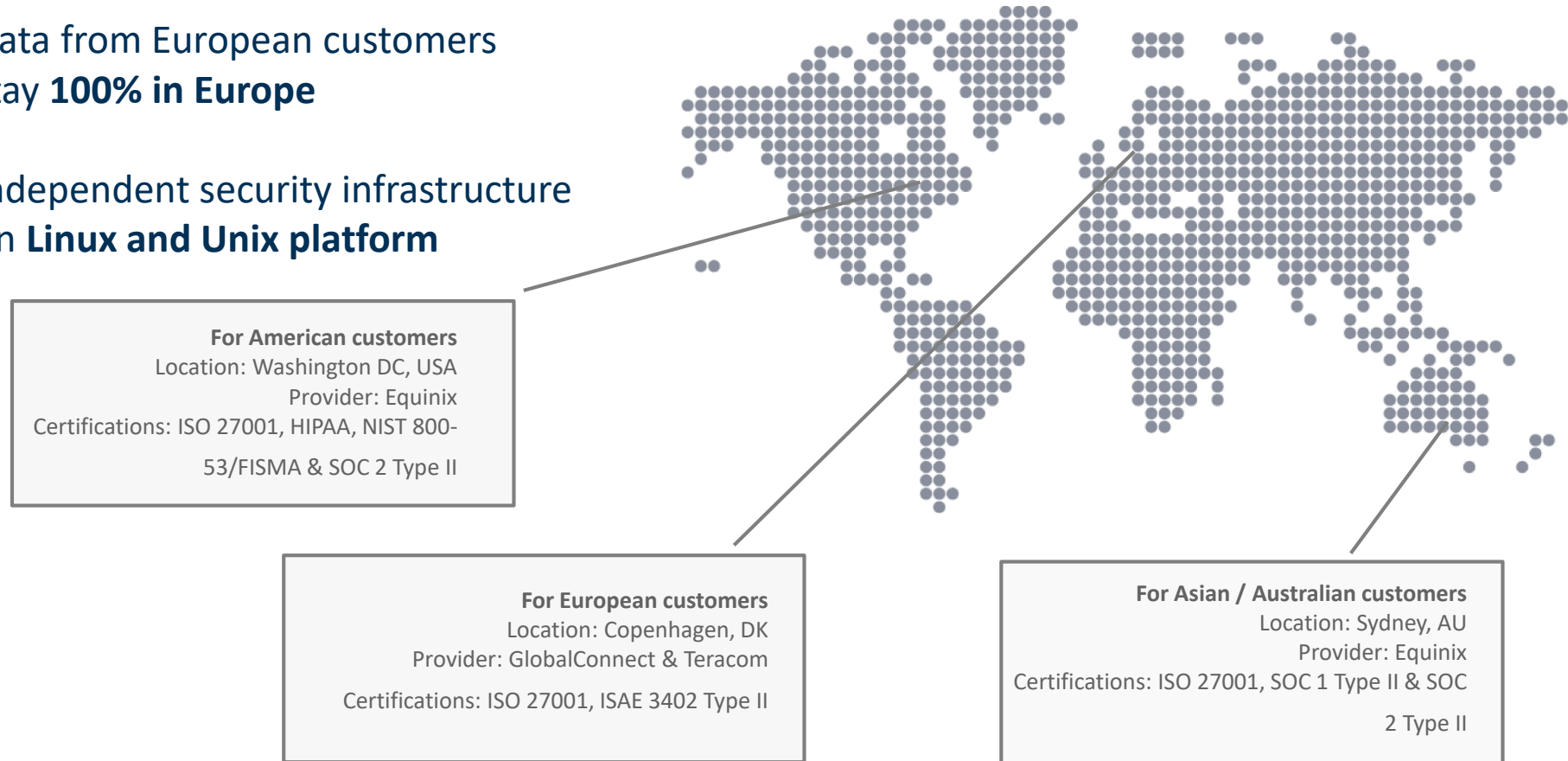
- High Security HA Cluster
- Based on Linux/Solaris infrastructure
- Highly available Replication Technology
- Flexible scaling Options
- System can be completely set up, administered and controlled via API
- Intelligent Snapshot Queue



ISOLATED DATA CENTRE LOCATIONS

Data from European customers stay **100% in Europe**

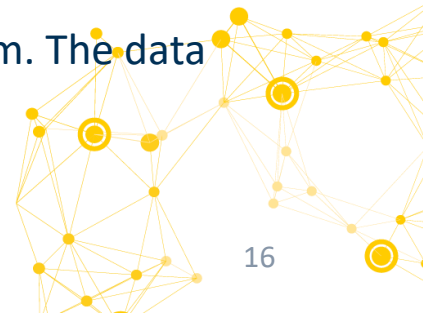
Independent security infrastructure on **Linux and Unix platform**





GDPR

- SEP CAPS is a data processor, which works exclusively on instruction of the data responsible person. This distinction is important because SEP does not collect or store data that is not expressly designated by the data controller. There will be no actions without the instruction of the data controller.
- Article 32 of the EU Block Exemption Regulation stipulates that systems "shall have the capability to restore rapidly the availability of and access to personal data in the event of a physical or technical incident". SEP ensures that we can quickly find, verify and recover user data. Usually in less than 2 minutes.
- **Dealing with personal data::**
 - › SEP acts solely on the instruction of the data controller and does not grant anyone else access to or control over data.
 - › All data is protected with appropriate technical and organizational security.
 - › SEP undertakes to permanently delete the data if or when they are needed.
 - › SEP is not and will not attempt to use personal data.
- SEP restricts access to user data through role-based access control and a role-based access control system. The data controller can grant or restrict appropriate access.



SEP UNIQUENESS



PROTECTION

*Restore & Migrate
Compliance*

- Manage and unify entire backup sets of cloud apps and devices with one click.
- Maximum protection of cloud application data.
- Transparent overview of all SaaS workloads & data.
- Very versatile service options (delegation via self-service options)
- Data recovery with just a few clicks



SIMPLICITY

*Holistic
User centric*

- The tamper-proof storage engine protects against overwriting existing elements.
- Transparent security policies
- Restore options (selectable restore target, new version, overwrite, release as link to external)
- User-defined retention periods
- Cross-user migration of content



DISCOVERY

*Search & Insights
Time Travel*

- Immediate access to all data after complete recovery
- Advanced search functions through a powerful search engine
- Preview mode of the most common formats for easier content identification





SEED & SECURITY

- 3-6 snapshots per day
- Intelligent backup algorithm ensures maximum data throughput
- Encryption of the data stream and the storage system





NEXT RELEASE

- Microsoft Dynamics 365 will be available as the 4th cloud application in **the 4th quarter of 2019**.

