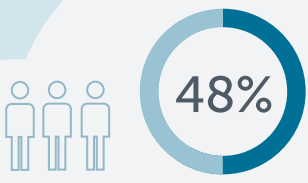
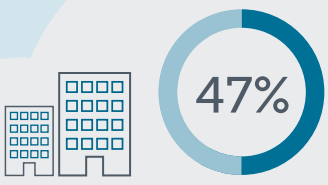
Take Action to Find & Protect Sensitive Data

How do you ensure that your organisation's confidential payroll and employee medical records, customer credit card details and intellectual property information are not stored on shadow IT cloud services?

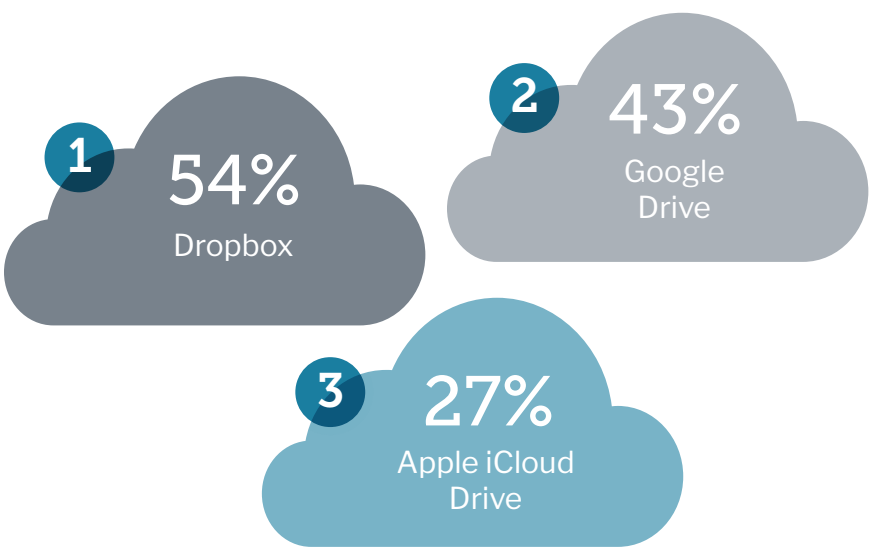


of employees use apps that were not distributed by their IT team



of corporate data stored in cloud services is not managed or controlled by IT departments

The three most popular unsanctioned cloud storage services



1.5+ Billion

Researchers discovered more than 1.5+ billion sensitive business files online

>50%

Most information security proffesionals say that >50% of their cloud data is sensitive business infomation

56%

It leaders at 56% of businessees say their organization isn't careful about sharing sensitive information in the cloud with third parties

4 steps to protecting your cloud data

Discover
all cloud services used by employees

Understand
where data is stored and whether it's sensitive

Determine
the impact of cloud app usage on your compliance requirements

Adopt
a strategy to protect data in the cloud

See how Forcepoint makes it easy to protect your organisation's cloud data.

Sources: Harvey Nash/KPMG, Blissfully, 451 Research/Thales, The SaaS Report, Harmon.ie, Spiceworks, Digital Shadows, Oracle/KPMG, Gemalto/Ponemon, Gartner, LogicMonitor, Wired, Computer Reseller News

FORCEPOINT