



Take Action to Find & Protect Sensitive Data

Is your organisation one of the many whose confidential payroll and medical records, customer credit card details and intellectual property information can be found on unsecured cloud storage services?



48%

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



47%

Of corporate data stored in the cloud is not managed or controlled by IT departments

The three most popular unsanctioned cloud storage services

1

54%

Dropbox

2

43%

Google Drive

3

27%

Apple iCloud Drive



1.5+ Billion

Researchers discovered more than 1.5+ billion sensitive business files online

>50%



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

56%



IT leaders at 56% of businesses 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