

Securing Sensitive Data on Microsoft 365



As cloud service adoption increased, so did threats aim cloud services with a higher concentration on collaboration services like Microsoft 365. Most cloud computing security risks are related to cloud data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues circle back to the data placed in the cloud.

Growth of Cloud Services



Collaboration tools are integral to a hybrid workforce to integrate communications and messaging with project management functions.



94%

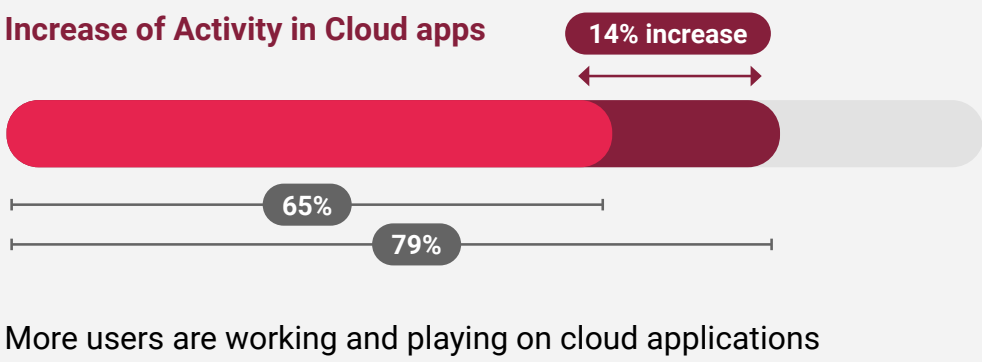
Companies need stronger protections for their Microsoft 365 and Google Workspace applications.

Personal Apps: Sensitive Data at Risk

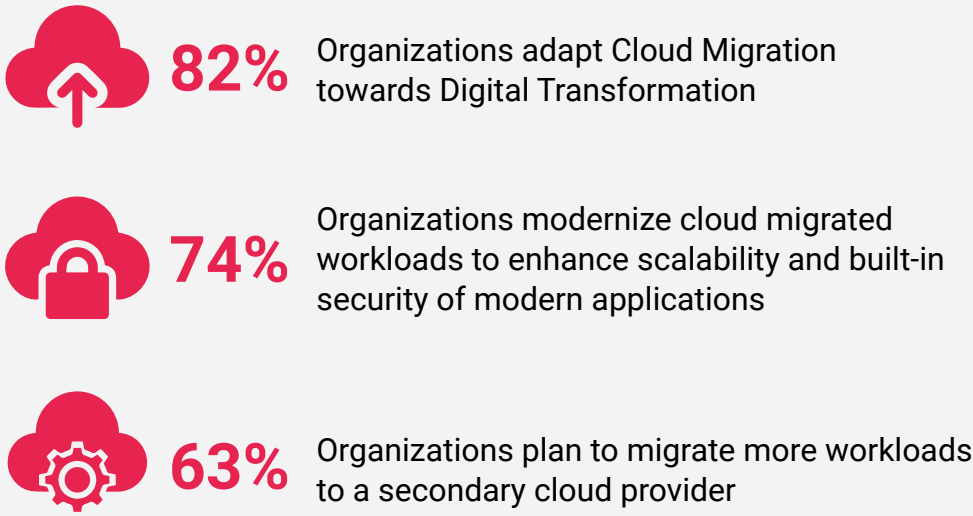


Source: Cloudwards

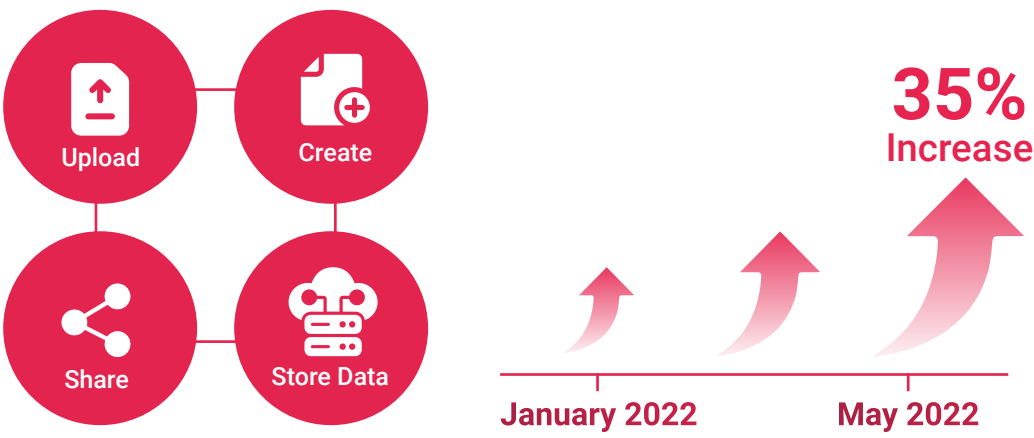
Data Activity By First Half of 2022



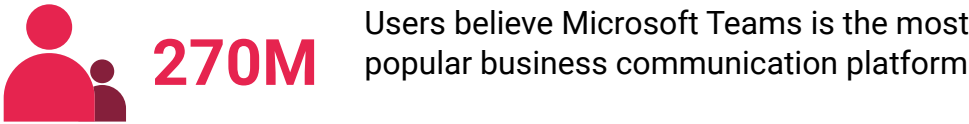
Three Key Cloud Adoption Trends



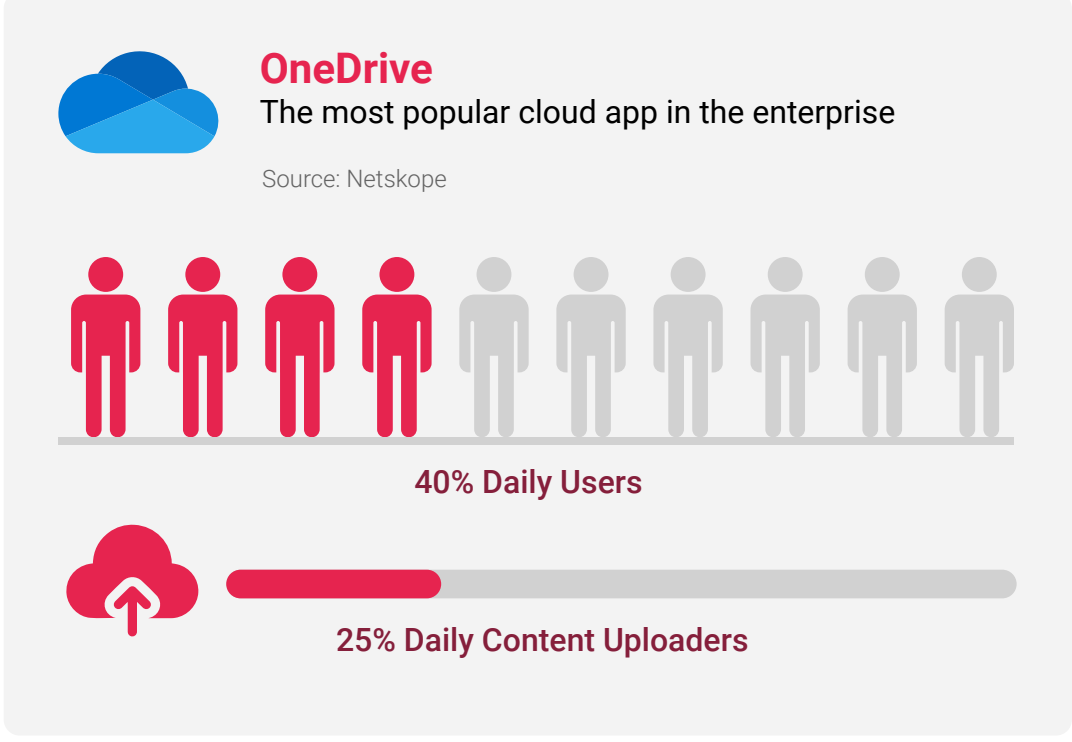
Source: Microsoft



Microsoft 365: Driving Collaboration

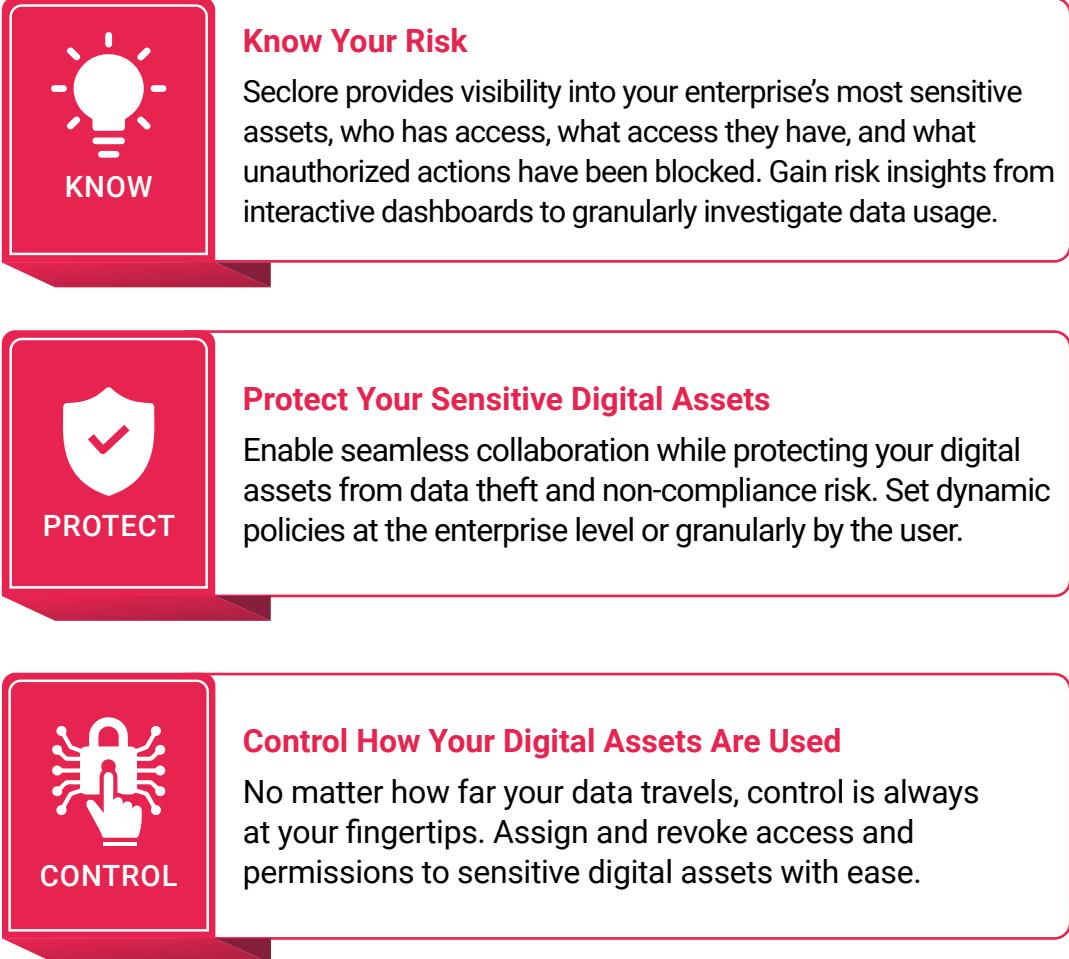


Source: Microsoft Teams Statistics

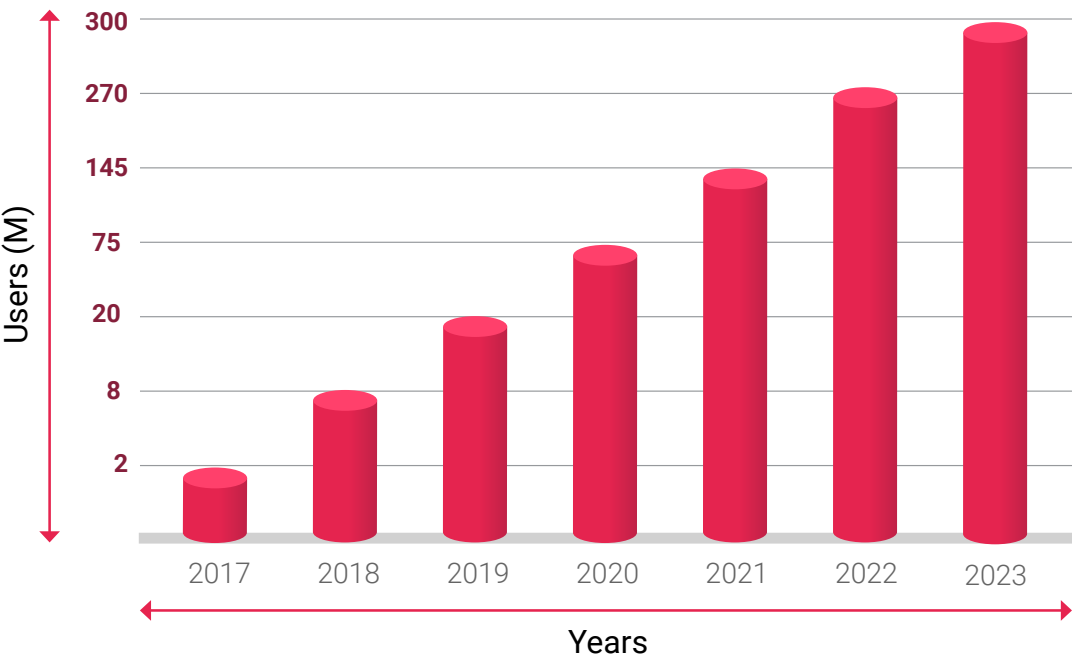


Source: Netskope – Cloud Sprawl Report

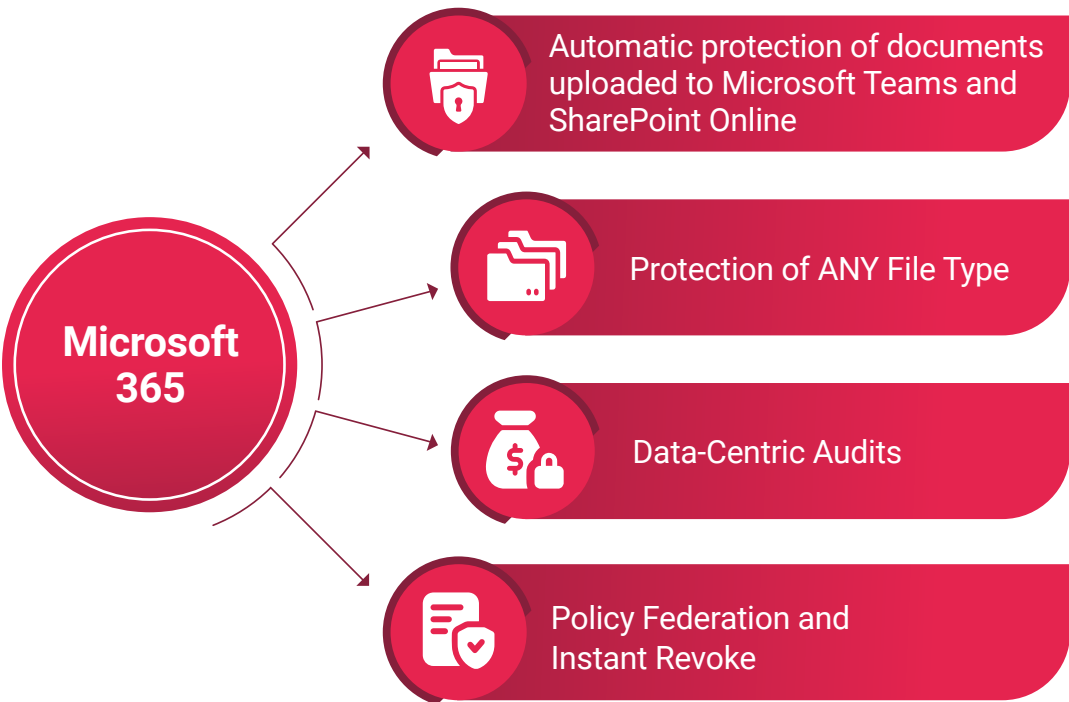
The Seclore Approach



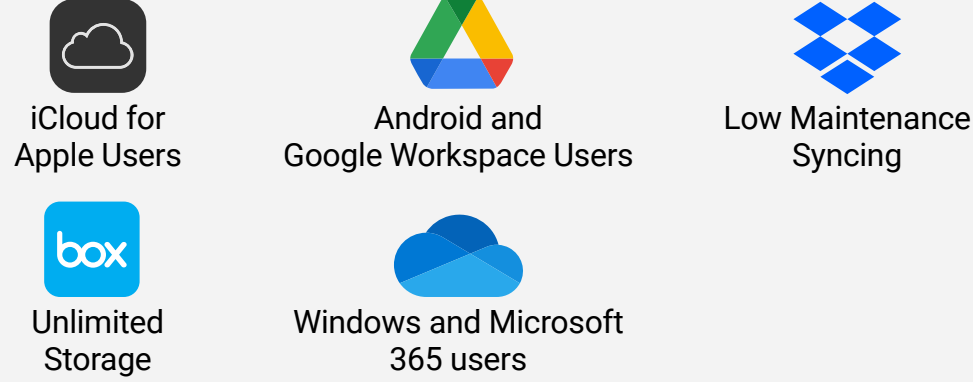
Usage of Cloud Apps Over the Years



Secure Microsoft 365 with Rights Management



The Top Best Cloud Storage Apps



The most popular apps include personal instances of typically managed apps, particularly Google Drive, OneDrive, Gmail, and Outlook.

Download this whitepaper to learn about the data security gaps with using Microsoft 365 and how Seclore helps fill the gaps.

Download Whitepaper

