
netskope
Cloud and Threat Report:
Cloud Data Sprawl
BROUGHT TO YOU BY
netskope
THREAT LABS

EXECUTIVE SUMMARY

In this edition of the Cloud Threat Report, we focus our attention on data sprawl by examining how organizations use cloud apps to create, upload, share, and store data. The number of cloud apps that an organization uses continues to increase steadily, up 35% in the first five months of 2022. Depending on the size of the organization, 138 to 326 different apps are used to create, upload, share, or store data. The apps include managed app instances, unmanaged apps and app instances freely adopted by business units, and personal apps and app instances.

While most users create, upload, and store data in managed app instances, 22% of users regularly do so with personal apps and instances. Furthermore, 20% of users upload an unusually high amount of data to personal apps and instances immediately before they leave an organization. Using personal apps and instances enables users to retain access to data even after they leave.

Organizations can implement policies to limit the use of personal instances, reducing the risk they pose to data security. Organizations in the Financial Services sector on average have the strictest policies and, as a result, see less than half as much data uploaded to personal instances than other sectors.

REPORT HIGHLIGHTS

- **79% of users** regularly upload, create, share, or store data in cloud apps, an **increase of 22%** in the first five months of 2022.
- Organizations with 500–2,000 users upload, create, share, or store data in 138 different apps, an **increase of 35%** in the first five months of 2022.
- **22% of users** upload, create, share, or store data in personal apps and instances.
- Personal app and instance use is lowest among organizations in the **Financial Services sector**.
- 20% of users upload data to personal apps and instances before they leave an organization, an **increase of 33%** since last year.

ABOUT THIS REPORT

Netskope provides threat and data protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization. Stats in this report are based on the five month period from January 1, 2022 through May 31, 2022. Popularity is measured in terms of the number of distinct users uploading, creating, sharing, or storing data in popular cloud apps, not considering the content or sensitivity of the data.

Netskope Threat Labs

Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DefCon, BlackHat, and RSA.

79% of users upload, create, share, or store data in cloud apps

From January 2022 to May 2022, the number of apps where users upload, create, share, or store data increased by 35%. An organization with 500-2,000 users uses an average of 1,558 distinct cloud apps each month. Of those apps, 138 (9%) are used to upload, create, share, or store data. As organization size increases, the number of apps increases accordingly. Organizations with 2,000-4,000 users average 204 apps, while organizations with more than 4,000 users average 326 apps. The percentage of users who upload, create, share, or store data in cloud apps is also increasing, up from 65% to 79% in the first five months of 2022.

The top three categories of apps in which organizations upload, create, share, or store data are Cloud Storage, Collaboration, and Webmail apps. The top apps in each of those categories include managed app instances, unmanaged app instances freely adopted by business units, and personal apps and instances. Some apps can have both managed and unmanaged instances. For example, Microsoft OneDrive typically includes both managed and personal instances, Microsoft Teams typically includes only managed instances, and WeTransfer is typically a personal app.

In the top three categories, there were seven apps that saw their popularity more than double in the first five months of 2022, including three Cloud Storage apps and five Collaboration apps. Collaboration apps include a wide variety of point-solutions, leading organizations to adopt a growing number of different apps within that category, as we will explore more in the next section.

» Most Popular Cloud Storage Apps

1. Microsoft OneDrive
2. Google Drive
3. Amazon S3
4. Box
5. WeTransfer

» Most Popular Collaboration Apps

1. Microsoft Teams
2. Microsoft Sharepoint
3. Google Chat
4. Slack
5. Smartsheet

» Most Popular Webmail Apps

1. Google Gmail
2. Outlook.com
3. Yahoo Mail
4. AOL Mail
5. GMX

» Fastest Growing Cloud Storage Apps

1. Amazon Workdocs
2. Baidu Object Storage
3. Google Cloud Storage

» Fastest Growing Collaboration Apps

1. HelloSign
2. Figma
3. Evernote
4. Wrike
5. Prezi

Organizations use many apps with overlapping functionality

Of the 138 apps for which an organization with 500–2,000 users uploads, creates, shares, or stores data, there are on average 4 Webmail apps, 7 Cloud Storage apps, and 17 Collaboration apps. Other categories with multiple apps include HR apps (7) and File Converters (9). Outside of those five categories, there is a long tail of many different apps in many different categories that make up the remaining 94 of the total 138 apps.

The reasons an organization uses multiple apps in the same category vary, some organizations have divisional or regional preferences, some organizations adopt a new app without retiring its predecessor, and some simply add new apps as they grow through mergers and acquisitions. A common contributor to the proliferation of multiple apps with overlapping functionality is individual choice. For example, the average nine different File Converters an organization uses are typically all personal apps. The growth in overlapping apps can lead to security issues, such as misconfigurations, policy drift, and inconsistent access policies. Personal apps and instances—to which 22% of users upload, create, share, or store data—present an especially challenging problem because users maintain access to data stored in those instances even after they leave.

» Most Popular HR Apps

1. Workday
2. SuccessFactors
3. Oracle Human Capital Management
4. Lever
5. Achievers

» Most Popular File Converter Apps

1. I Love PDF
2. Sejada PDF
3. Convert.io
4. PDFSimpli
5. PDFfiller

» Most Popular Apps in Other Categories

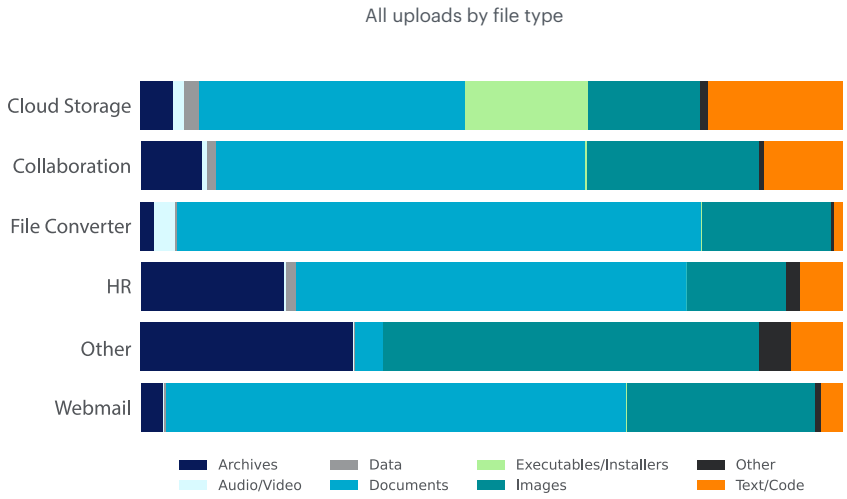
1. Microsoft Forms **Survey Solutions**
2. LinkedIn **Professional Networking**
3. WhatsApp **Chat, IM & other communication**
4. SurveyMonkey **Survey Solutions**
5. SalesForce **Customer Relationship Management**
6. Facebook **Social**
7. Jira **Development Tools**
8. Youtube **Streaming and Downloadable Video**
9. Twitter **Social**
10. GitHub **Survey Solutions**

15% of users upload data to personal apps and instances

In the first five months of 2022, the percentage of users uploading files to cloud apps increased from 54% to 65%. Documents accounted for 30% of all uploads and Images accounted for 29% of all uploads.

While the distribution of file types varies for each app category, Images and Documents together always account for the majority of uploads. The file type with the most pronounced differences is Executables/Installers, which account for 17% of uploads to Cloud Storage apps. Text/Code uploads are most common in Cloud Storage apps while Archive uploads are most common in other app categories.

In the first five months of 2022, the percentage of users uploading files to personal apps and instances remained constant at 15%, with Images and Documents dominating the uploads. The most popular apps include personal instances of typically managed apps, particularly Google Drive, OneDrive, Gmail, and Outlook. The other apps listed in the top ten are personal apps that are typically not managed by the organization. In the next section we explore how uploads to personal apps and instances differ by industry.



» **Top Personal Apps and Instances**

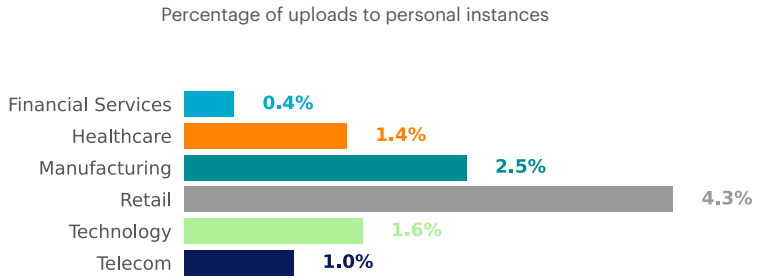
1. Gmail
2. WhatsApp
3. Google Drive
4. iLovePDF
5. Outlook.com
6. Facebook
7. Yahoo Mail
8. OneDrive
9. WeTransfer
10. LinkedIn

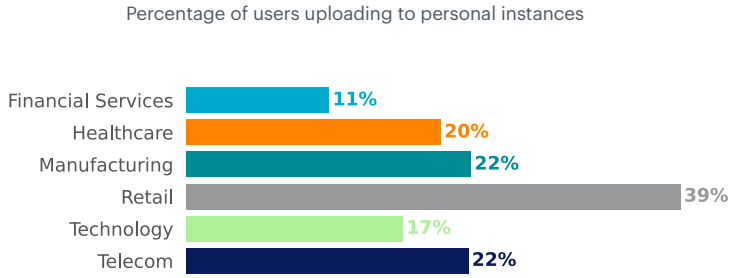
Personal app and instance usage is lowest in Financial Services sector

To reduce the risks of personal apps and instances—particularly the risk that users might use them to maintain access to sensitive data after they leave—many organizations adopt policies that limit how personal apps and instances can be used.

On average, industries in the Financial Services sector have had the most success in limiting the flow of data into personal apps and instances. The Financial Services sector has 40% as many uploads to personal apps and instances as the next closest sector, Healthcare, and 10% as many as the farthest sector, Retail. The financial services sector also has fewer users on average uploading data to personal apps and instances, 64% as many as the next closest sector, Technology, and 28% as many in the farthest sector, Retail.

In the next section, we explore how users' interactions with personal apps and instances change when they are about to leave an organization.



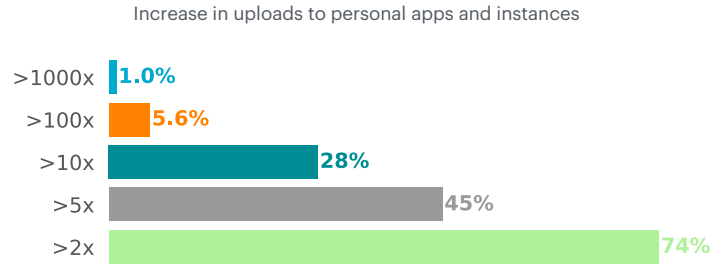


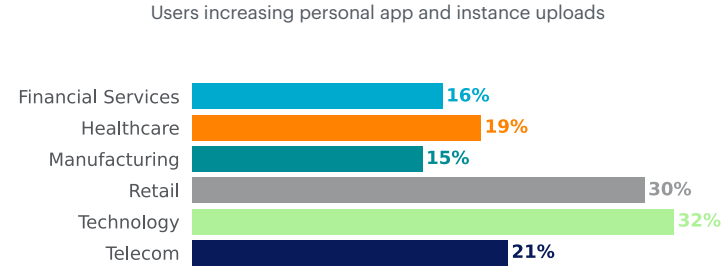
20% of users upload more data to personal apps and instances before they leave

Uploading data to unmanaged personal apps and personal instances of managed apps allows users to maintain access to the data even after they leave the organization. In the first five months of 2022, 20% of users leaving an organization uploaded more data than usual to personal apps and instances during their last 30 days at the organization. This represents a five-point increase from 15% in 2021. Of the users with an increase in uploads to personal apps and instances, 74.3% uploaded more than twice as much data as usual and 1.0% uploaded more than 1,000x as much data as usual, comparable to the ratios observed in 2021.

By industry, the percentage of users uploading more data to personal apps and instances before they leave varies from 15.6% to 32.7%. It is most common in the Retail and Technology Sectors, and least common in the Financial Services and Manufacturing sectors. As described in the previous section, the Financial Services sector also boasts the least usage of personal apps and instances overall.

The top two apps to which users upload data before they leave, Google Drive and Microsoft OneDrive, remained unchanged from 2021, with WeTransfer and Dropbox moving up in the rankings in 2022.





» **Top Apps**

1. Google Drive
2. Microsoft OneDrive
3. WeTransfer
4. Google Gmail
5. Dropbox

RECOMMENDATIONS

To control data sprawl and protect sensitive data, Netskope recommends taking the following precautions:

1. Deploy a security service edge (SSE) cloud platform with context for users, apps, instances, and data sensitivity in real-time with adaptive access controls and data loss prevention (DLP).
2. Enable multi-factor authentication (MFA) and single sign-on (SSO) for managed apps to maintain centralized access control over access to sensitive data. Extend MFA to unmanaged apps via your identity service provider or SSE platform.
3. Use Cloud and SaaS Security Posture Management (CSPM and SSPM) to ensure that all cloud apps that process or store sensitive data are appropriately locked down to protect such data from accidental or unauthorized exposure.
4. Enforce granular policy controls to limit data flow, including flow to and from apps, between company and personal instances, among users, to and from the web, adapting the policies based on device, location, and risk.
5. Deploy cloud data protection to limit the movement of sensitive data, including preventing its movement to unauthorized devices, apps, and instances.
6. Invoke real-time coaching to users to use safer app alternatives to protect data, justify unusual data activity, and provide step-up authentication for risky conditions within business transactions.
7. Use behavioral analytics to detect insider threats, including users that attempt to move data to unauthorized locations.
8. Enable zero trust principles for least privilege access to data with continuous monitoring from rich contextual analytics and reporting.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on how to mitigate risk, contact us today:
WWW.NETSKOPE.COM/REQUEST-DEMO

BROUGHT TO YOU BY

netskope
THREAT LABS