
netskope
HEY, YOU, GET OUT OF MY CLOUD
CLOUD AND THREAT REPORT:
JULY 2021 EDITION
BROUGHT TO YOU BY:
netskope
THREAT LABS

EXECUTIVE SUMMARY

This report makes our fifth edition focusing on cloud data risks and threats, and the trends are becoming more apparent. Digital transformation continues with enterprise cloud app adoption up 22% during the first half of this year, compared to a 12% increase during the first half of 2020. 97% of cloud apps used in the enterprise are shadow IT, unmanaged and often freely adopted by business units and users. Personal app usage continues to present a data security challenge, as departing users upload sensitive data to personal app instances ahead of their departure. At the same time, third-party app plugins present a hidden data risk for managed cloud apps, and exposed cloud workloads provide attackers possible infiltration vectors. Attacker cloud adoption also continues, with attackers increasingly hosting malware payloads in cloud apps and using malicious Office documents to gain initial footholds.

If one topic stands out in our fifth edition, it is that a Pandora's box of personal app instances is a target destination for data movement and exfiltration. While the findings are concerning, the ability to decode and analyze apps and cloud services inline, including company and personal instances of popular Software-as-a-Service (Saas) apps, shadow IT, and public cloud services is the building block to these findings.

Netskope Threat Labs research is built upon this broad visibility and rich metadata. Your security stack should have the same visibility and control to reduce these data risks and threats.

REPORT HIGHLIGHTS

- **Departing employees upload 3x more data to personal apps** in the last 30 days of employment where personal Google Drive and Microsoft OneDrive instances are the most popular targets.
- **97% of Google Workspace users have authorized at least one third-party app** to have access to their corporate Google account, potentially exposing data to third parties due to scopes like "View and manage the files in your Google Drive."
- **More than 35% of all workloads are exposed to the public internet** within AWS, Azure, and GCP, with RDP servers—a popular infiltration vector for attackers—exposed in 8.3% of workloads.
- **Cloud-delivered malware has increased to an all-time high of 68%** with cloud storage apps accounting for 66.4% of cloud malware delivery and malicious Office docs now accounting for 43% of all malware downloads, up from 20% at the start of 2020.
- **Cloud app adoption increased 22% during the first six months of 2021** where the average company with 500–2,000 users now uses **805 distinct apps and cloud services**. Concerningly, 97% of those apps are shadow IT—unmanaged and often freely adopted by business units and users.
- **70% of users continue to work remotely as of the end of June 2021**, a trend that started in March 2020 with the pandemic, and signaling a widespread return to the office has not started.

EXITING EMPLOYEES USING CLOUD APPS TO TAKE DATA

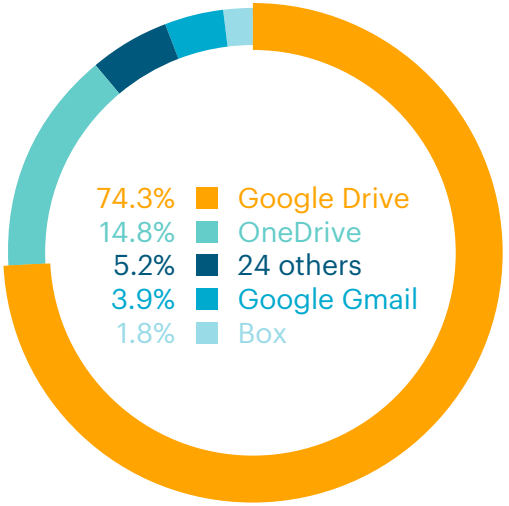
Employees leaving an organization pose a data security threat when they take data with them. One of the popular ways in which users take data with them is by uploading data to personal app instances. In their last 30 days of employment, **one-third** of the users leaving an organization create a spike in uploads to personal instances that is **three times** higher than their baseline behavior. Google Drive and Microsoft OneDrive are the two most popular personal apps among exiting users.

Of the exiting users uploading to personal app instances, 15% either upload files that were copied directly from managed app instances or that violate a corporate data policy. Files that were copied directly from managed instances came primarily from managed instances of OneDrive and Box and were uploaded to personal Google Drive instances. Files that violated corporate data policies included:

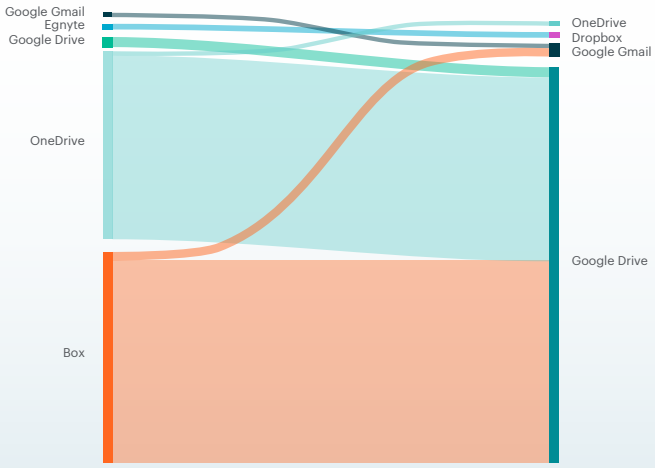
- Personally identifiable information
- Protected healthcare information
- Intellectual property
- Source code

If the Great Resignation is happening, it is creating some big potential security risks as exiting users leverage personal cloud apps to take data with them when they leave.

Most Popular Personal App Destinations



Company to Personal App Instances



THIRD-PARTY APP PLUGINS POSE DATA RISK

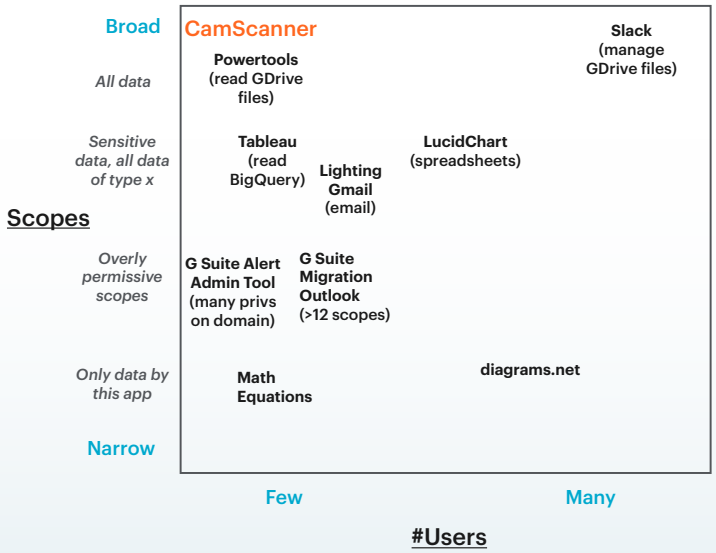
Third-party app plugins pose a data security threat when they provide third-party apps access to sensitive data. For example, 97% of Google Workspace users have authorized at least one third-party app access to their corporate Google account. Each third-party app requests a scope, which varies from "Basic account info," which provides access only to publicly accessible information from a Google profile, to "View and manage the files in your Google Drive," which provides access to all of your data in Google Drive. Third-party apps that request scopes like "View and manage the files in your Google Drive" pose a data security threat because they can expose sensitive data to third parties. For example, the CamScanner app requests the "View and manage the files in your Google Drive" scope and was found by Kaspersky in August 2019 to contain malware and was banned by the Indian government over security concerns in June 2020.

Top 5 most popular Google Plugins

1	Google Chrome	Chrome browser	463,286	91.0%
2	iOS Account Manager	iOS application	183,730	36.1%
3	Zoom	Video calls	135,361	26.6%
4	Android device	Operating-system level, mobile	117,927	23.2%
5	Slack	Messaging	95,848	18.8%

In addition to potentially exposing data to third parties, attackers actively build malicious app plugins to gain access to victims' environments in a style of attack known as an illicit consent grant. One way to identify third-party app plugins is to look for apps that request broad scopes and are used by relatively few users.

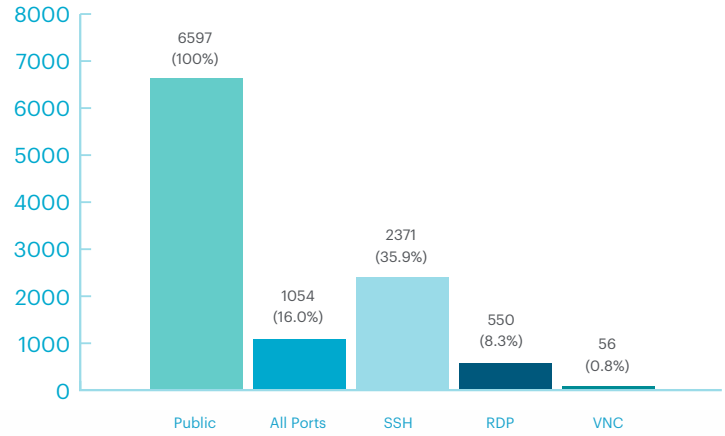
App Plugin Data Scopes



PUBLIC ACCESS TO CLOUD ENVIRONMENTS CREATES OPPORTUNITIES FOR ATTACKERS

Exposing a workload to the public internet creates a possible infiltration vector for attackers. In AWS, Azure, and GCP, more than 35% of enterprise workloads are exposed to the public internet. This means that they have a public IP address and are reachable from anywhere on the internet. Of those publicly exposed workloads, 8.3% expose the Remote Desktop Protocol (RDP), a popular infiltration vector for attackers. Sophos reports that 30% of cyberattacks begin with an exposed RDP server; one recently publicized example was the Equinix breach in September 2020, in which 74 RDP servers were exposed to the internet. Other popular remote access protocols exposed to the public internet include SSH and VNC. In most cases, the risk of infiltration through a publicly exposed cloud workload can be mitigated by using a virtual private network (VPN) or Zero Trust Network Access (ZTNA) solution.

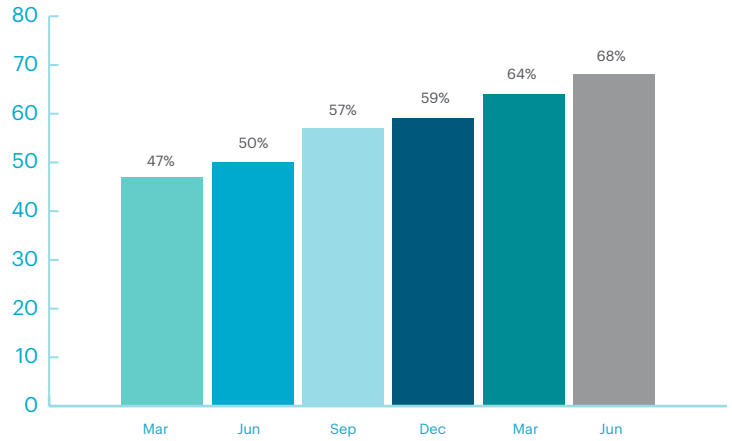
AWS Public Compute Instances: Remote Access



ATTACKERS ABUSE CLOUD APPS TO EVADE DETECTION

Attackers increasingly abuse popular cloud apps to deliver malware and avoid blocklists. In the second quarter of 2021, 68% of all malware downloads were delivered from cloud apps. Of the cloud-delivered malware, 66.4% was delivered using cloud storage apps. Collaboration apps and development tools account for the next largest percentage, as attackers abuse popular chat apps and code repositories to deliver malware. In total, Netskope detected and blocked malware downloads originating from 290 distinct cloud apps in the first half of 2021.

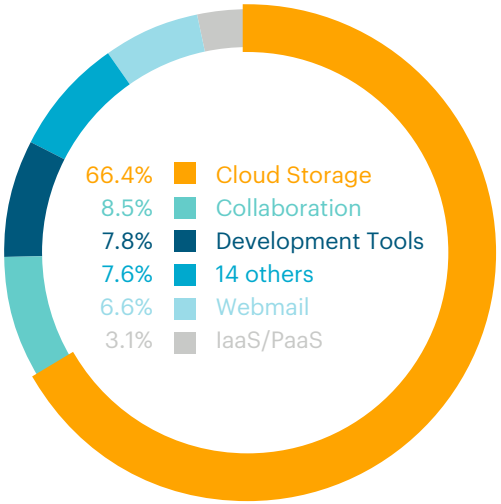
Increasing Cloud-delivered Malware



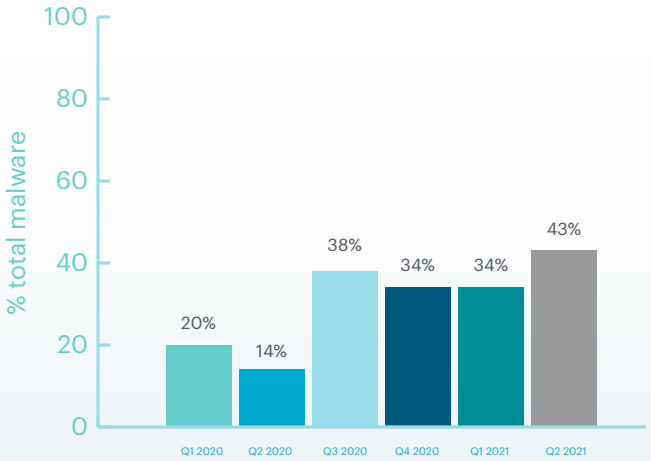
The primary reason attackers use cloud apps for malware delivery is to bypass blocklists and take advantage of any app-specific allow lists. Although attacks launched from the cloud are typically short-lived—the cloud service provider removes the malicious content when it is reported—attackers have illustrated that they can capitalize on the attack within the short time window that they have.

At the same time, malicious office documents continue to grow in popularity as malware authors have found new and creative ways to evade detection. In Q2 2021, 43% of all malware downloads were malicious Office docs, compared to just 20% at the beginning of 2020. This increase comes even after the Emotet takedown, indicating that other groups observed the success of the Emotet crew and have adopted similar techniques.

Top App Categories for Malware Downloads



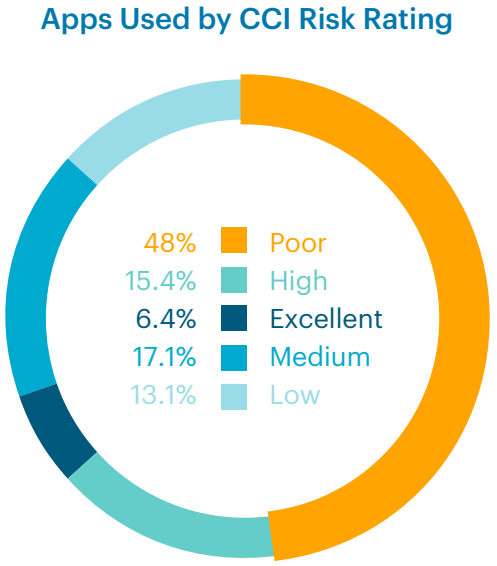
% Malicious Office Docs

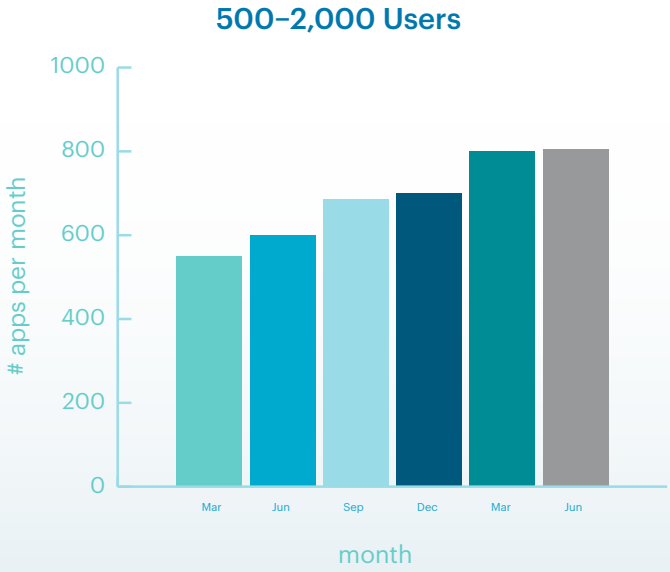


CLOUD COMPLEXITY INCREASES DATA AND THREAT RISKS

The number of cloud apps in use in the enterprise continues to rise, increasing 22% during the first half of 2021, compared to an increase of 12% during the first half of 2020. Organizations with 500–2,000 employees now use on average **805** distinct cloud apps per month, 97% of which are shadow IT apps that are freely adopted by business units and users, and 48% of which have a Poor CCI (Cloud Confidence Index™) risk rating, indicating enterprises should avoid using those apps and take steps to migrate to safer app alternatives.

The two app categories primarily responsible for the 22% growth were consumer apps and collaboration apps. This trend began in early 2020 with the COVID-19 pandemic as remote users sought out collaboration apps to stay connected to their teams. They started using more consumer apps as the lines between home and work continued to blur, and that use further accelerated toward the end of 2020 heading into 2021.

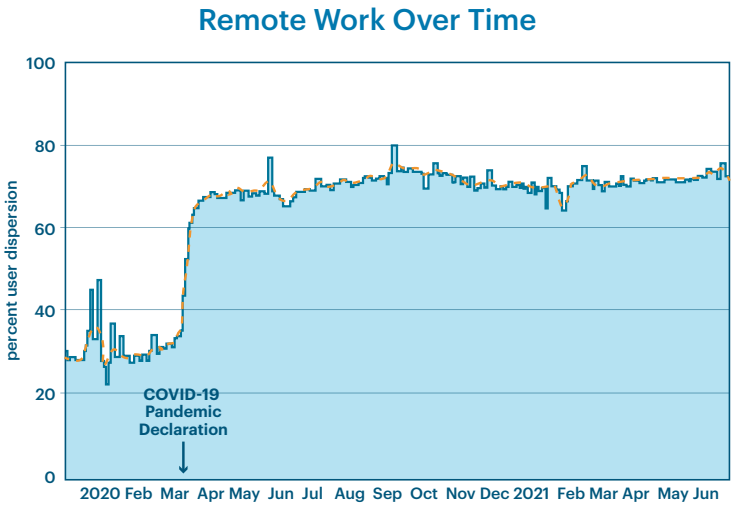


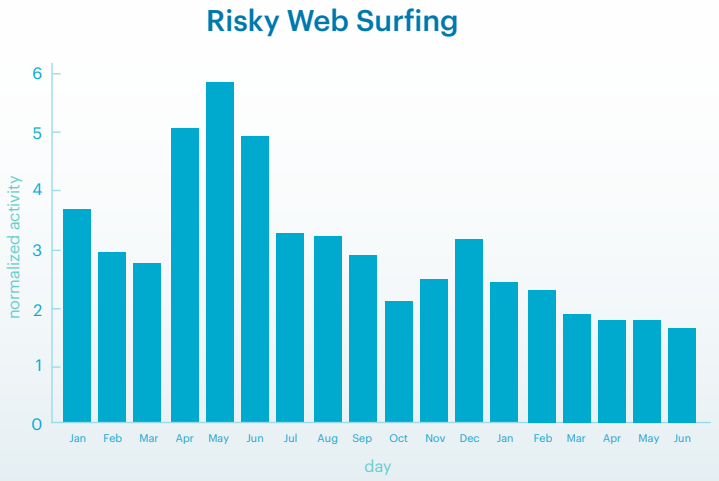


IF THERE'S A RETURN TO THE OFFICE, IT HASN'T YET STARTED

At the beginning of the COVID-19 pandemic in March 2020, we saw a sudden and dramatic shift to remote work, from 30% of users working remotely before the pandemic to 70% working remotely almost as soon as the pandemic took hold. As of the end of the first half of 2021, the percentage of users working remotely remains at 70% and has not yet started to return to pre-pandemic levels.

At the beginning of the pandemic when users began working from home, we saw a spike in users visiting risky websites, including adult content, file sharing, and piracy websites. Over time, this risky web surfing subsided as users presumably became more accustomed to working from home and IT teams were able to coach users on acceptable use policies.





10 CLOUD SECURITY BEST PRACTICES TO PROTECT YOUR APPS, DATA, AND USERS

1. Strong authentication and identity access controls (SSO, MFA, etc.) federated to managed and unmanaged apps and cloud services
2. Adaptive access controls based on the user, app, app risk, instance, device, location, data sensitivity, and destination to selectively grant access to specific activities or request step-up authentication before the activity
3. ZTNA to private apps in data centers and public cloud services to reduce exposure of apps and limit network lateral movement
4. Continuous security assessment of public cloud services to detect misconfigurations and publicly exposed data, plus storage scans for data at rest for data and threat protection
5. Cloud inline analysis of managed and unmanaged cloud apps for data context, plus web traffic within a single-pass secure access service edge (SASE) architecture to enable data and threat protection defenses with a fast user experience
6. Selective and safe enablement of cloud apps based on a comprehensive app risk assessment with the ability to recommend safer app alternatives via real-time coaching and proceed/cancel alerts
7. Granular policy controls for data protection including data movement to and from apps, between company and personal instances, shadow IT, users, websites, devices, and locations
8. Cloud data protection (DLP) for sensitive data from internal and external threats across web, email, SaaS, shadow IT, and public cloud services
9. Behavior analysis to detect anomalies of data activity, failed logins, and rare events, plus confidence index scores for users with event correlation timelines to visualize changes in behavior
10. Advanced analytics to visualize and uncover app and data activity risks, threat activity, data protection violations, key security metrics, and investigative details

CLOSING THOUGHTS

Over the past year, organizations have been tested to find new ways to run their businesses. The external forces that changed the business environment led to rapid adoption of new apps and business practices. In response, security teams have developed a better understanding of how to protect users, apps, and data that lies outside of the corporate network. We have seen tremendous interest in how organizations are now asking about how to apply security principles to protect information and minimize risk when traditional network perimeter controls are no longer relevant.

This year's findings provide reasons to be optimistic, such as the year-over-year reduction in risky web browsing, even with work-from-home policies extending to the present day. However, there is still significant work to be done, given that the access to managed cloud apps requires corresponding work to mitigate risk to Poor CCI apps and enforce boundaries for data movement.

The threat frontier continues to evolve, and this year's findings continue to reinforce the growing danger of malicious Office documents. This is no surprise, given that Office document malware evades many types of endpoint signature scans, eludes detection in sandboxes for portable executables, and exploits the user's trust in the apparent sender of the document to enable execution.

The configuration of the cloud (such as the findings for misconfigured remote access and the potential backdoors for data sharing in third-party app ecosystems) remains a thorny problem, because many organizations are still working through basic app visibility. Even with knowledge of the app's presence in the organization, the security team must further scrutinize how it operates to check for misconfigurations and the potential for downstream data sharing.

Although we do not yet see a significant return to the office, we expect that the lessons learned to implement better controls over user behaviors and interactions with the cloud and web will be directly applicable no matter what work situation—office, hybrid, or remote-first—organizations favor. The past year has taught all teams that they cannot depend on network boundaries alone as enforcement points to implement user-to-app access policies. This has always been true, but now it's readily apparent that the security model cannot rely on any physical part of the network topology itself. The path forward will be a security overlay based on Zero Trust principles that can protect sensitive data on the web and in the cloud.

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