netskope

REMOTE WORK @ RISK

161% RISE IN USE OF HIGH RISK APPS AND WEBSITES, WITH 64% OF WORKERS NOW REMOTE

BROUGHT TO YOU BY:

netskope

THREAT LABS

EXECUTIVE SUMMARY

We are in new territory with the pandemic: working remote, meeting online, and facing new challenges on a daily basis. The number of people working remotely has more than doubled and changes in user behavior have been dramatic in the first half of 2020 as work and life have mixed together. An alarming trend for security teams: The use of risky apps and websites, including adult content, from managed devices has nearly doubled.

Device sharing at home is validated by the traffic to websites and apps categorized as *Education* and *Kids*, where managed devices are used for remote education efforts within families. Even with an increase in personal use of managed devices and high risk websites, the most popular apps remain the leading delivery method of cloud-enabled threats and malware. And finally, as expected, the use of collaboration apps increased greatly as remote teams aim to stay connected.

For this report we broke out the average number of apps used by company size, from the hundreds of apps for smaller organizations to over 7,000 apps and cloud services for the largest enterprises. Providing 'data context' for cloud use is key for leading customer use cases including unintentional and unapproved data movement, protecting data from internal and external threats, and safely enabling cloud use with conditional and contextual access.

USE OF RISKY APPS AND WEBSITES

↑ 161%

GAMBLING | DRUGS | ADULT CONTENT - PORNOGRAPHY | PIRACY & COPYRIGHT THEFT | ADULT CONTENT - OTHER | SHAREWARE / FREEWARE

This report is based on anonymized data collected from the Netskope Security Cloud platform across millions of users from January 1, 2020 through June 30, 2020.

REPORT HIGHLIGHTS

- 64% workers are now remote, a 148% increase with the pandemic
- 161% increase in visits to high-risk apps and sites
- 600% increase in visits to adult content
- 97% increase for personal use of managed devices
- 80% increase in the use of collaboration apps
- Cloud-based malware delivery (vs web) increased to 63%

KEY POINTS

Network Inversion

The COVID-19 pandemic accelerated network inversion by more than doubling the number of people working remotely. Along with this increase in remote work came an **80% increase in the use of collaboration apps** as remote workers sought to remain connected with their colleagues, and a 2% increase in the total number of cloud apps being used in the average enterprise.

Personal Use of Managed Devices

When working remotely, the lines have blurred between business and personal use as employees are much more likely to use their devices for personal reasons and engage in risky activities. Personal use of devices increased by 97% and **use of risky apps and websites increased by 161%.**

Cloud Threats

Attacker cloud adoption continues to grow, with the two most common techniques being cloud phishing and cloud malware delivery. Cloud malware delivery increased its lead over web malware delivery by 4 points, to 63%. **The most popular cloud apps continue to be the apps most abused by attackers.**

Insider Threats

7% of all users uploaded sensitive corporate data to personal instances of cloud apps. This put sensitive data at risk of inappropriate use and theft.

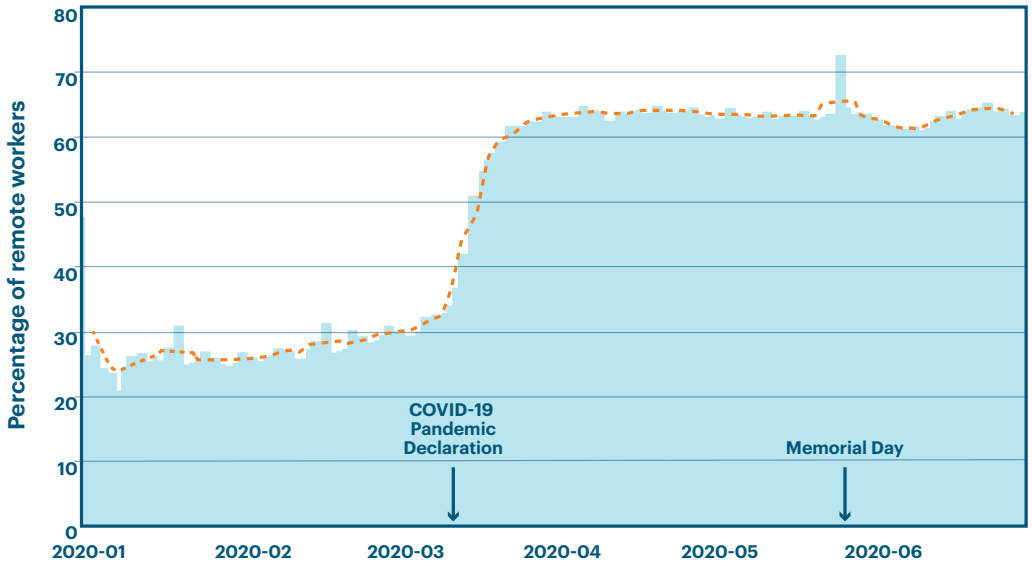
NETWORK INVERSION

The COVID-19 pandemic accelerated network inversion — the number of individuals working remotely increased by 148% during the week following the WHO's COVID-19 pandemic declaration. **Nearly two-thirds of the workforce has been working remotely** since and are projected to continue in the near future. As a result, organizations have moved to adopt more formal remote working policies and are considering reducing office space.

With the movement to remote work came an increase in use of collaboration apps in the enterprise. The number of users leveraging collaboration apps daily increased 20% while the amount of activity happening within collaboration apps increased by 80%, indicating that existing users have significantly increased their use.

Among the collaboration apps seeing the greatest increase in use are chat applications, like Slack and Google Chat, video conferencing apps like Zoom, GoToMeeting, and Teams, and specialty apps like Miro, which provides an online whiteboard for collaboration.

The total number of cloud apps in use in the enterprise increased on average by 2%, with the largest enterprises now using more than 7,000 apps.



	SIZE (USERS)	AVERAGE NUMBER OF APPS
SMALL	0-500	562
MEDIUM	500-2000	863
LARGE	2000-4000	1148
X-LARGE	4000+	2949

PERSONAL DEVICE USE

Along with the shift to remote work came an increase in **personal use of enterprise devices: personal app and web traffic increased by 97% after the start of the COVID-19 pandemic**. This personal use appears as an increase in traffic to many different categories of cloud apps and websites, including:

- Alcohol
- Consumer
- Education
- Entertainment
- Fashion
- Financial News
- Forums
- Games
- Kids
- News & Media
- Personal Sites and Blogs
- Pets
- Streaming & Downloadable Video

The increase in certain categories — like *Education* and *Kids* — indicates that enterprise devices are being shared with other members of the household and perhaps being used to help homeschool children. Use of devices by non-employees increases the risks to the security of those devices. There was also a dramatic 161% increase in traffic to high risk websites and cloud apps, including:

- Adult Content - Other
- Adult Content - Pornography
- Drugs
- Gambling
- Piracy & Copyright Theft
- Shareware / Freeware

In certain categories, like *Adult Content*, the number of users visiting such websites increased by 240% and the total amount of traffic increased by 600%.

PERSONAL USE
OF MANAGED DEVICES

↑ 97%

VISITS TO
ADULT CONTENT

↑ 600%

CLOUD THREATS

The two most common types of cloud threats in the first half of 2020 were cloud malware delivery and cloud phishing as continuing threat tactics noted in the Netskope Cloud and Threat Report - February 2020. The total amount of both cloud and web-delivered malware increased by 7%. Of that malware, 63% was delivered over cloud applications — a 4 point increase from the end of 2019 — indicating that the cloud continues to grow in popularity as a malware delivery platform. The top cloud apps and services from which Netskope blocked malware downloads were:

1. Microsoft Office 365 OneDrive for Business
2. Sharepoint
3. Box
4. Google Drive
5. Amazon S3

The percentage of phishing attempts being delivered through cloud applications held steady at 15% with a variety of apps being used to deliver the bait, including cloud storage, webmail, web hosting, and social media apps. This statistic, combined with those reported by the Anti-Phishing Working Group, indicates that phishers are both using the cloud to phish and phishing for cloud credentials. *Cloud Storage*, *Webmail*, and *Social* apps were among the most popular apps used for phishing, with the top 5 apps being:

1. Microsoft Office 365 OneDrive for Business
2. Microsoft Live Outlook
3. Blogger
4. AOL Mail
5. Facebook

↑ 7%

INCREASE IN TOTAL AMOUNT OF BOTH CLOUD AND WEB-DELIVERED MALWARE.

OF THAT MALWARE

63%

WAS DELIVERED OVER CLOUD APPLICATIONS

SENSITIVE DATA

In the Netskope Cloud and Threat Report - February 2020, we reported that 33% of users transfer data between apps. In this report, we focus on a specific type of data movement, the transfer of sensitive data to personal app instances. In total, 7% of all users uploaded regulated data, source code, company confidential data, and other sensitive data to personal instances, exposing the data to potential misuse and theft. **Cloud Storage and Webmail apps are the two most popular types of personal instances used to upload sensitive data**, with the 5 most popular apps being:

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

The top 5 most common types of sensitive data being uploaded to personal instances are:

1. Protected Health Information (PHI)
2. Personally Identifiable Information (PII)
3. General Data Protection Regulation (GDPR)
4. Source Code
5. Company Confidential Information

Across the Netskope Security Cloud platform, 14% of file uploads are images which may contain sensitive data. Netskope uses machine-learning based image and document classifiers to detect desktop screen captures, passports, licenses, tax forms, patents, resumes, and source code inline and via API inspection.

7% OF ALL USERS **INTENTIONALLY** UPLOADED **SENSITIVE DATA** TO PERSONAL INSTANCES OF CLOUD APPLICATIONS

14% OF FILE UPLOADS ARE IMAGES WHICH MAY CONTAIN SENSITIVE DATA

SUMMARY

The abrupt network inversion of 2020 is unprecedented on many levels. What we are learning from the data and our customers is that cloud adoption continues to grow and is a significant part of an organization's cyber terrain. The significant trends in remote working are major forces shifting security control planes towards identity, app, and data. Remote working only adds more risks as personal use of managed devices increases in a blend of work/life online activity at home.

Cybercrime continues to abuse the most trusted and popular cloud apps, including for cloud phishing and cloud malware delivery. Leveraging trusted domains, valid certificates, and the practice of allow-listing popular apps to bypass inline defenses only reduces friction for attack success.

Allow/deny no longer works as you need to safely enable cloud and web access as there are many boundary crossings for data movement, plus the delivery of threats that increasingly seek credentials for access to cloud data.

CLOUD SECURITY TEN BEST PRACTICES TO PROTECT YOUR DATA AND USERS INCLUDE:

1. Strong authentication and access controls (SSO, MFA, *etc.*)
2. Adaptive access controls based on the user, app, device, location, data, and destination to selectively grant access to specific activities
3. Zero-trust network access 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
5. Cloud inline analysis of managed and unmanaged cloud apps for data context to enable data and threat protection defenses
6. Selective and safe enablement of cloud applications based on a 3rd party risk assessment of applications with the ability to recommend safer alternatives
7. Granular policy controls for data movement to and from apps, instances, users, websites, devices, and locations
8. Cloud data protection (DLP) for sensitive data from internal and external threats
9. Behavior analysis for anomalies, plus confidence index scores for users with event correlation timelines to visualize changes in behavior
10. Real-time coaching to users on activity and data movement with justification collection, proceed/cancel, or warning alerts to change user behavior

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 tools to help you mitigate risks, please visit
NETSKOPE.COM/SOLUTIONS/SECURING-REMOTE-WORKERS