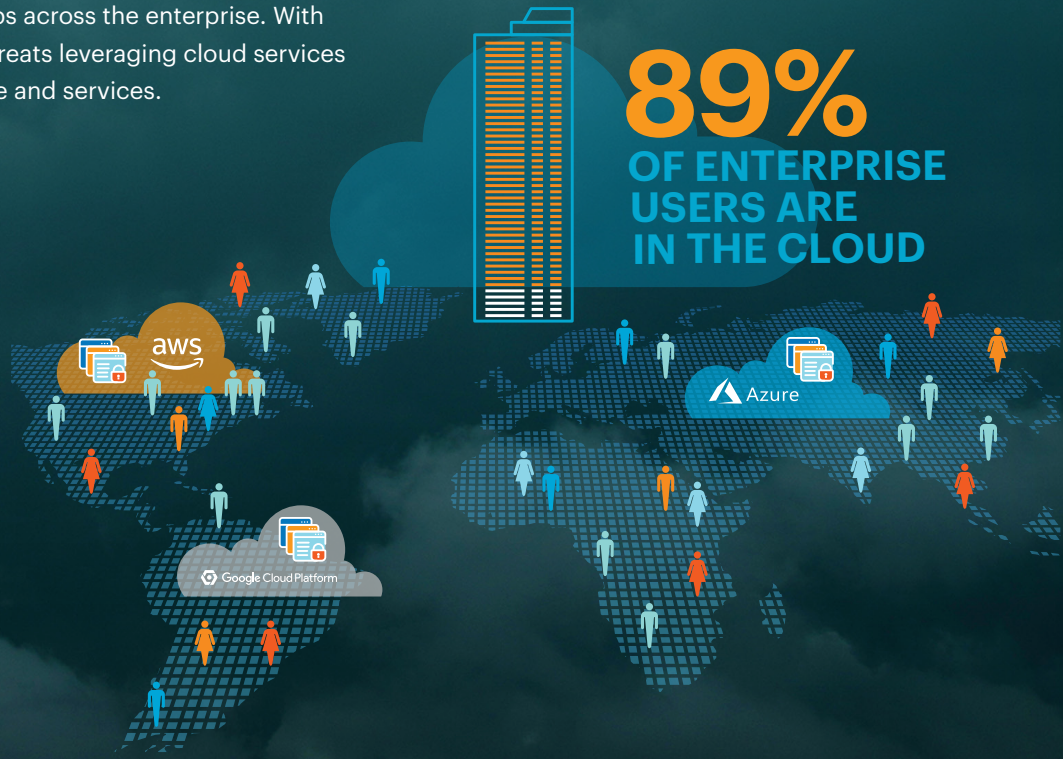

netskope
THE DARK SIDE OF THE CLOUD
CLOUD ENABLED THREATS ARE ON THE RISE
&
SENSITIVE DATA IS MOVING BETWEEN CLOUD APPS
BROUGHT TO YOU BY:
netskope
THREAT LABS

EXECUTIVE SUMMARY

Digital Transformation is accelerating the adoption of cloud services and apps across the enterprise. With this rise of cloud, we see the "Dark Side of the Cloud" emerging to enable threats leveraging cloud services for various kill chain stages and an increase for data risks using cloud storage and services.

This report offers insights into how cloud-enabled threats and the shifts of sensitive data into and across the cloud are occurring and complicating the security posture of organizations. Combined with the network inversion caused by increasingly mobile and remote users that are accessing public and private applications in the cloud, the risk to enterprises is elevated, necessitating new security architectures and approaches. Adding to the risk are legacy defenses that are unable to decode managed and unmanaged cloud services and app traffic, legacy appliances lacking performance to decrypt TLS encrypted cloud and web traffic, and the practice of whitelisting managed cloud services to bypass critical defenses providing a red carpet entry for cloud-enabled threats.

This report is based on anonymized data collected from the Netskope Security Platform across millions of users from August 1 through December 31, 2019.



REPORT HIGHLIGHTS

- 89% of enterprise users are active in managed and unmanaged cloud services and apps
- 44% of threats leverage cloud services across various kill chain stages
- 20% of users move data laterally, including between managed and unmanaged cloud services, plus company and personal instances
- More than 50% of data policy violations come from cloud storage, collaboration, and webmail apps
- 33% of enterprise users work remotely on average

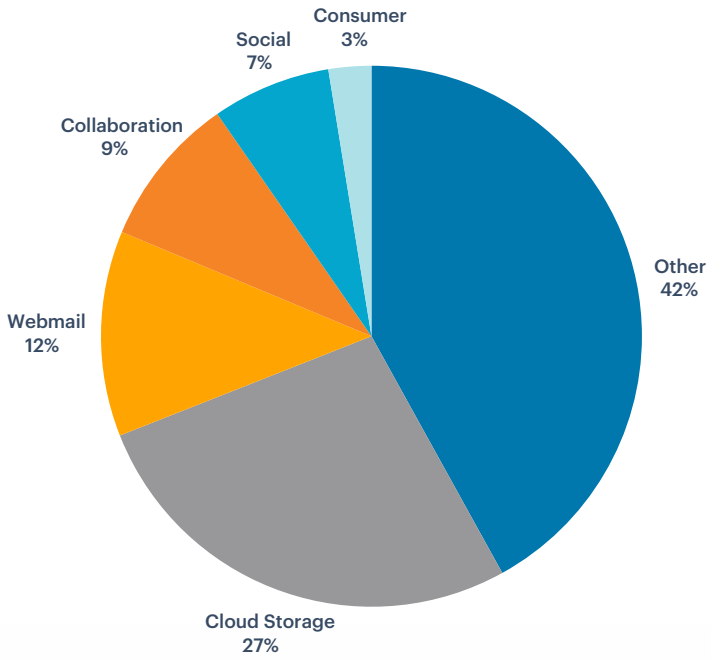
CLOUD-ENABLED THREATS ARE ON THE RISE

Cybercrime continues to be well-funded and organized in how to increase its success rate and evade detection. A common strategy has been to leverage “watering holes” of the Internet, where most valuable users can be found. This trend is reflected in the list of the top website categories for threats and sets the stage for its practice using cloud services and apps.

1. Content Servers
2. Online Ads
3. Personal Sites & Blogs

The top categories are not high-risk categories like bulletproof hosting providers and newly registered domains. Instead, attackers are blending into the mainstream, spreading threats through common website categories. One recent example is a wide-reaching adware campaign that spread through malicious Chrome extensions.

The chart to the right shows a breakdown in the categories of cloud apps being abused by attackers: the majority of the cloud threats are in the top 5 cloud service and app categories: Cloud Storage, Webmail, Collaboration, Social, and Consumer. The remaining 42% are spread among the other 24 categories.



Digital Transformation has accelerated cloud application usage in the enterprise where 89% of users are active, making cloud apps the new "watering hole." Attackers are moving to the cloud to blend in, increase success rates and evade detections. Attackers launch attacks through cloud services and apps using familiar techniques including scams, phishing, malware delivery, command and control, formjacking, chatbots, and data exfiltration. Of these, the two most popular cloud threat techniques are phishing and malware delivery.

During the last half of 2019, Netskope Threat Labs identified 44% of all of the malicious threats as cloud-enabled threats. Generally, attackers have targeted the most popular cloud services and apps, intending to abuse the implicit trust users and admins place in those cloud apps, where some are even whitelisted to bypass critical defenses making it easier for attacks. The following list highlights this trend—the top five apps in which Netskope detects threats are also among the most popular cloud services and apps in the enterprise:

1. Microsoft Office 365 OneDrive for Business
2. Box
3. Google Drive
4. Microsoft Azure
5. GitHub

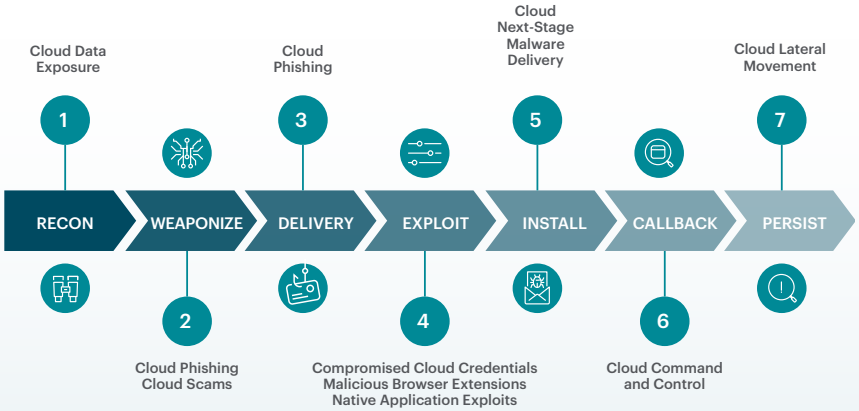
Cloud threats and their defenses can be modeled using the Cloud Kill Chain or the Mitre Cloud ATT&CK matrix. In total, Netskope Threat Labs has detected cloud threats across 1,609 different cloud services and apps, showing the extent to which cybercrime has extended its reach.

Security defenses for a handful of managed cloud services and apps will not address the problem. Only decoding managed and unmanaged cloud services and apps in the thousands for threat and data protection defenses fully addresses the challenge posed by attackers with the shift into the Cloud Kill Chain.

CLOUD ATT&CK MATRIX

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

CLOUD-ENABLED KILL CHAIN



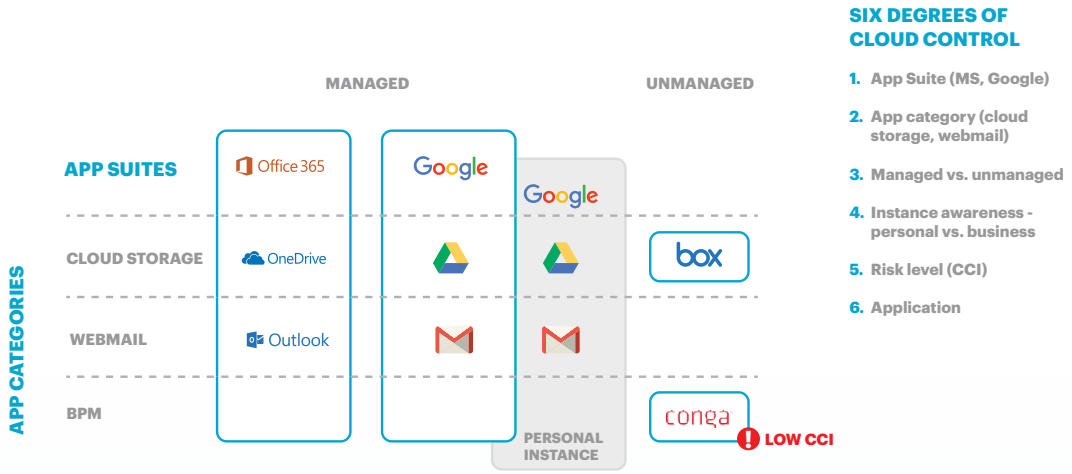
SENSITIVE DATA IS ON THE MOVE

Cloud-enabled organizations approve specific account instances of cloud applications to store their sensitive data. While this is a good strategy, Netskope research shows users are moving sensitive data across multiple dimensions among a wide variety of cloud services and apps including personal instances and unmanaged apps in violation of organization policies. The majority of data policy violations occur in cloud storage, collaboration, and webmail apps. Among these categories, the top 10 most common cloud services and apps are:

1. Microsoft Office 365 Outlook.com
2. Microsoft Office 365 OneDrive for Business
3. Microsoft Office 365 Sharepoint Sites
4. Box
5. Google Gmail
6. Google Drive
7. Salesforce.com
8. Egnyte
9. Microsoft OneDrive
10. Amazon S3

The types of data being detected by these data policy violations are primarily DLP rules and policies related to privacy, healthcare, and finance, including:

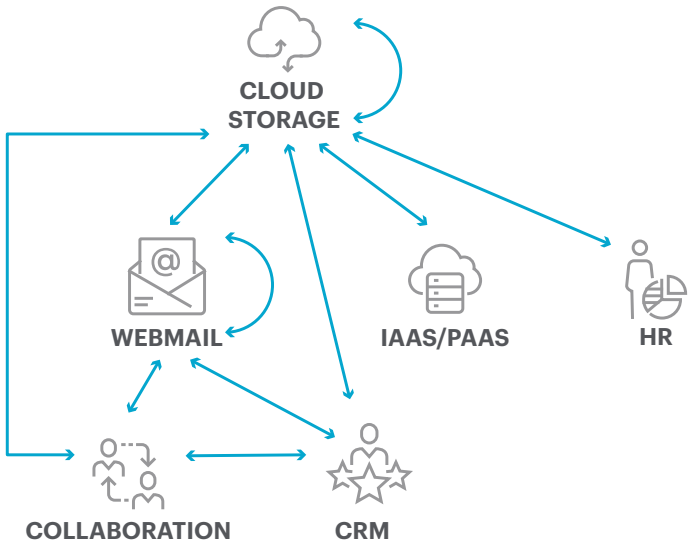
- Personally Identifiable Information (PII)
- General Data Protection Regulation (GDPR)
- Protected Health Information (PHI)
- Payment Card Information (PCI)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- Source Code
- Passwords, Credentials, and Keys



Even more significantly, sensitive data movement between cloud services and apps is also increasingly common, including managed and unmanaged cloud apps and services, plus company and personal instances. At least 20% of enterprise users move data laterally between cloud applications. More importantly, the data crosses many boundaries: moving between cloud app suites, between managed and unmanaged apps, between app categories, and between app risk levels (Netskope Cloud Confidence Index Levels). Moreover, 37% of the data that users move across cloud apps is sensitive. In total, Netskope has tracked lateral data movement among 2,481 different cloud services and apps, indicating the scale and the variety of cloud use across which sensitive information is being dispersed.

Certain types of cross-app data movement are more common than others. The following is a list of the pairs of app categories with the most cross-app data movement. The most common data movement occurs among different Cloud Storage apps or between Cloud Storage apps and apps in another category. Movement between different webmail apps also made the top 10 list, indicating that individuals are using more than one webmail app to share files in the enterprise and beyond: cloud apps and services are also often a source of data leakage because they make it very easy to share data.

1 Cloud Storage ⟷ Cloud Storage
2 Cloud Storage ⟷ Collaboration
3 Cloud Storage ⟷ Webmail
4 Cloud Storage ⟷ Customer Relationship Management
5 Webmail ⟷ Customer Relationship Management
6 Webmail ⟷ Collaboration
7 Collaboration ⟷ Customer Relationship Management
8 Cloud Storage ⟷ IaaS/PaaS
9 Cloud Storage ⟷ HR
10 Webmail ⟷ Webmail



The widespread movement of data to the cloud necessitates better monitoring, controls, and governance. Legacy defenses unable to decode cloud services and apps for visibility and control over these cloud data movement, including managed and unmanaged cloud services and apps, and across company and personal instances leave an organization vulnerable to potential data exposure and theft. Moreover, unprotected data within cloud storage continues to make headlines where a best practice of continuous security assessments with rules and automated remediation can effectively remove the risk.

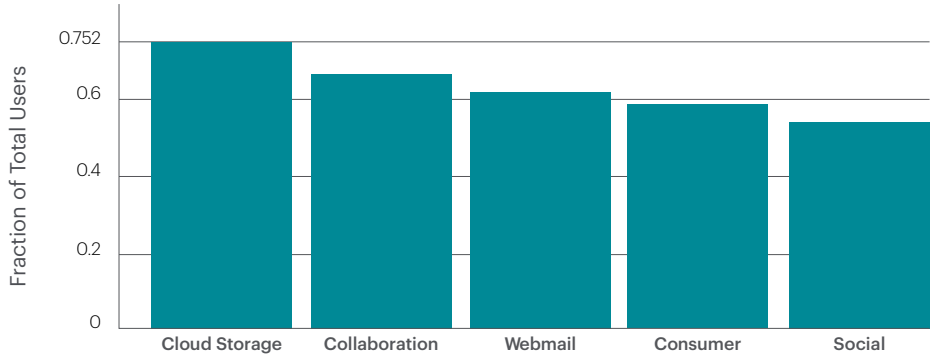
THE NETWORK IS INVERTED: USERS, DATA, AND APPS ARE OUTSIDE

Cloud-enabled organizations exhibit three trends that invert the traditional network:

- Increasing use of public cloud services and apps
- Increasing remote work even partially for main office employees
- Migration of private apps and data to the cloud

On average, a single organization uses 285 distinct cloud services and apps in the top three categories: Cloud Storage, Collaboration, and Webmail. In total, the average enterprises uses 2,415 distinct cloud services and apps. The top 10 apps overall are:

1. Google Drive
2. Youtube
3. Microsoft Office 365 OneDrive for Business
4. Facebook
5. Google Gmail
6. Microsoft Office 365 Sharepoint Sites
7. Microsoft Office 365 Outlook.com
8. Twitter
9. Amazon S3
10. Linkedin



Increasing remote work

On average, 33% of users in an enterprise work remotely on any given day. The top 10% of organizations for remote work see more than 80% of their workforce working remotely. Users are also mobile: On average, each user works from 8 different locations, with the top 10% of remote users working from at least 18 locations. This trend shows increasing demand on legacy VPNs and questions the availability of defenses to protect remote workers. The evolution of Zero Trust Network Access and highly available cloud native defenses provides a more secure and lower risk alternative.

Migration of private apps to the cloud

Organizations are also moving internally developed apps and data to public cloud providers like AWS, Azure, and GCP. Netskope research shows that organizations using AWS, Azure, and GCP for private apps have deployed on average more than 300 private compute instances in 3 different regions. The top 10% deploy private instances in multiple cloud providers and at least 7 different regions. Running your own apps in the cloud, whether private or public, means you need to also ensure that they meet regulatory standards and don't open up new security vulnerabilities.

A network transformation is occurring, with users more mobile and apps and services in the cloud. With it, enterprise security is transforming as well—focusing on securing data wherever it lives and updating the Zero Trust networking model for the cloud era.

CLOUD SECURITY BEST PRACTICES AND RECOMMENDATIONS

1. Inspect and decode all web and cloud traffic for malicious threats, such as cloud phishing and malware delivery. Ensure inspection of the content, instance, and activity to detect and block threats regardless of origin.

2. Implement cloud DLP capabilities to secure your data that is moving to the cloud and moving laterally between cloud services and apps. Establish DLP policies and rules with granular activity-level controls, application instance-awareness, and adaptive behavioral analytics, alongside known regulatory compliance DLP policies.

3. Empower your workforce to work from anywhere through a flexible, scalable private access solution and protect them no matter what device they are using through a combination of cloud-native inline and API-based security defenses.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to: https://www.netskope.com/resources/netskope-threat-research-labs.

For more information on tools to help you mitigate cloud-based threats,

WWW.NETSKOPE.COM/PRODUCTS/NEXT-GEN-SWG