JANUARY
2017

WORLDWIDE
EDITION

CLOUD REPORT

Half of all users of a
sanctioned cloud storage service have a
personal instance of the same service

REPORT HIGHLIGHTS

- Unsanctioned versions of cloud services present problems for IT. Half of all users of a sanctioned cloud storage service have a personal instance of the same service.
- Enterprises have an average of 1,031 cloud services in use, up from 977 last quarter.
- Microsoft has the most services in the top 20 list while enterprise services like ServiceNow and Slack make gains. Netskope finds unexpected IaaS usage and an average of 4 IaaS services.
- 7.4 percent of cloud malware found this quarter was ransomware.
- With GDPR compliance deadlines on the horizon next year, only 33.7 percent of cloud services are rated GDPR-ready.

EXECUTIVE SUMMARY

In this Netskope Cloud Report™, we've compiled the most interesting trends on cloud service adoption and usage based on aggregated, anonymized data from the Netskope Active Platform™. Report findings are based on usage seen across millions of users in hundreds of accounts globally and represent usage trends from July 1 through September 30, 2016.

This quarter, our main finding is that on average, half of all users of a sanctioned cloud storage service have a personal instance of the same service. Essential in addressing this is using a cloud access security broker (CASB) that will differentiate between instances of the same cloud service so IT security admins can apply distinct policies across personal versus corporate instances.

The average number of cloud services in use per enterprise this quarter rose to 1,031, from 977 last quarter. Microsoft Office 365 remains a leader and took the top 2 spots on our top-used cloud services list, with Microsoft Office 365 OneDrive for Business and Office 365 Outlook.com taking the number 1 and 2 spots, respectively. Slack premiered on our list last quarter and increased to the 16th position this quarter. ServiceNow makes an appearance at number 20. This quarter, we did an analysis of IaaS usage and found that enterprises use an average of 4 IaaS services, including Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

View, share, and edit were the top activities in cloud storage services. In HR apps, download, create, and edit took the top spots. Edit and create were the top two activities for finance and collaboration apps. In finance, the third most common activity was delete. For collaboration, it was view. Finally, in the business intelligence category, share, view, and download were the top activities, respectively.

Similar to past quarters, the lion's share of DLP violations occurred in cloud storage services at 82.2 percent. This is followed by webmail at 14.2 percent and other with 3.6 percent. This quarter, upload was the activity that took the top spot for DLP violations with 65.8 percent, followed by send with 20.1 percent, download 12.6 percent, and other 1.5 percent. By type, PII and PHI were the most with 35 percent and 32.4 percent, respectively. PCI followed with 16.5 percent, source code at 9.4 percent, and other at 6.7 percent.

Continuing with our Netskope Threat Research Labs investigations, this is the first quarter that we report on cloud ransomware as a type of malware in our categorizations. This quarter, the category percentages are as follows: 43.2 percent of detections were backdoors, adware 9.8 percent, Javascript malware 8.1 percent, ransomware 7.4 percent, Mac 6.7 percent, Microsoft Office macros 5.3 percent, mobile 5.2 percent, and other types 14.3 percent. 26.5 percent of the malware was shared with others, including internal or external users, or publicly, a drop from last quarter's 55.9 percent. This may be attributable to the fact that Netskope customers are proactively taking steps to address cloud malware risks.

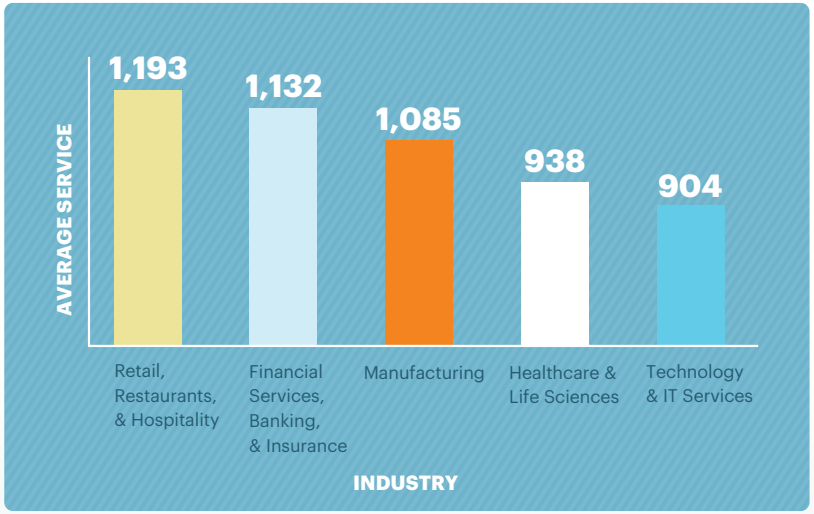
We conclude this quarter's report with an update of our European Union General Data Protection Regulation (GDPR) stats. We find that 66.3 percent of all cloud services are not ready for the GDPR, meaning they lack proper security and privacy controls and industry certifications to be considered ready to comply with the requirements of GDPR. We also found that 66.4 percent of cloud services do not specify that their customers own the data in the terms of service and 42.0 percent don't allow admins to enforce password controls, among other stats.

1,031 CLOUD SERVICES PER ENTERPRISE

This quarter, the average amount of services per enterprise has crossed into the thousands, at 1,031, compared to 977 last quarter. 94.8 percent of these apps are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI).

The retail industry took the lead with highest average number of cloud services used at 1,193. There were increases across the board of the average number of cloud services, with financial services, banking, and insurance coming in second this quarter.

In terms of category, marketing has the highest amount used per enterprise with 105. This quarter, HR is in second place with 77, followed by collaboration at 73. Most of these categories have greater than 90 percent of services not being enterprise-ready, with cloud storage having the least amount of not enterprise-ready at 76 percent.

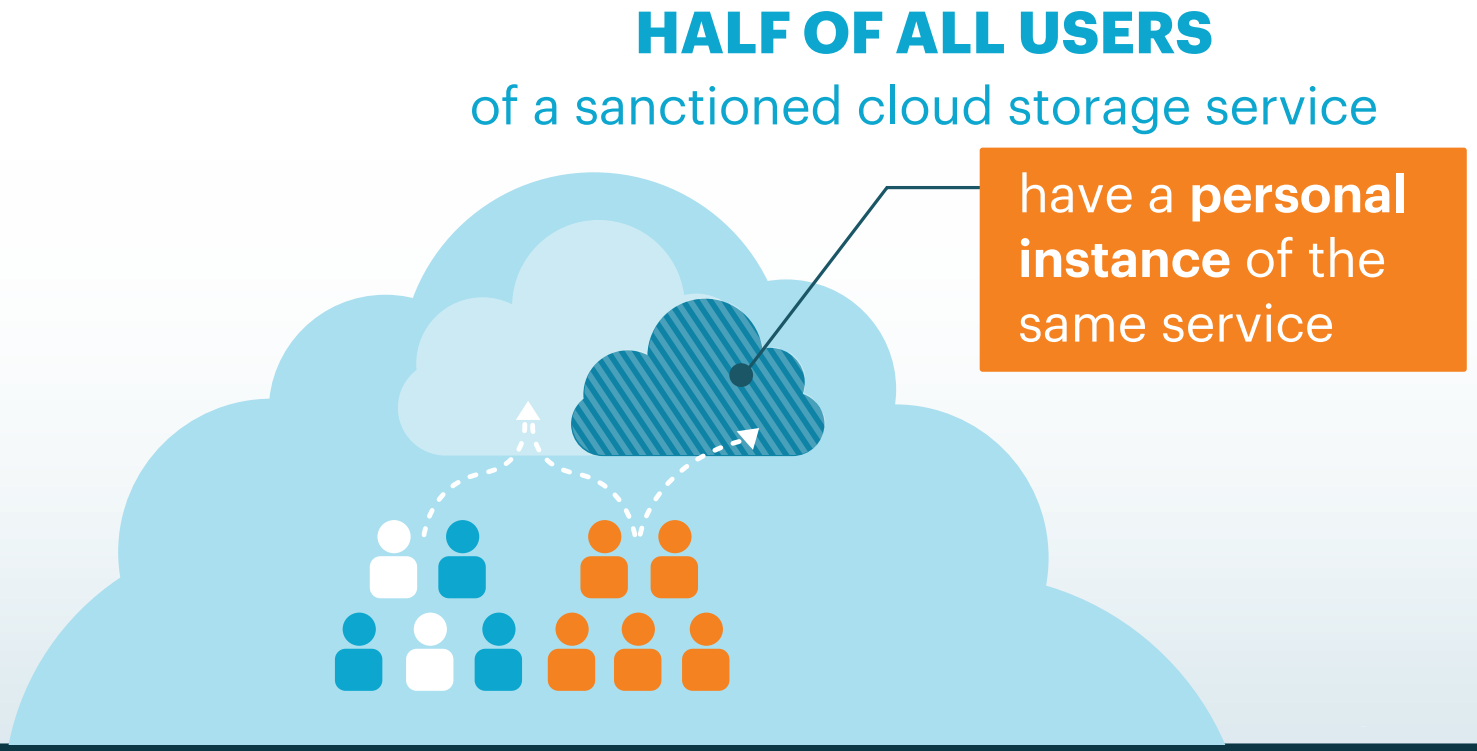


CATEGORY	# PER ENTERPRISE	% NOT ENTERPRISE-READY
Marketing	105	98%
HR	77	97%
Collaboration	73	91%
Finance/Accounting	63	96%
Productivity	61	98%
Software Development	40	96%
Social	32	90%
CRM / SFA	30	93%
Cloud Storage	29	76%
IT/Application Management	23	98%

SERVICE USAGE TRENDS

When Netskope customers set security policies for their cloud services, we always recommend differing the policies place on sanctioned versions of cloud services versus unsanctioned, personal instances. An example of this is encrypting PII data being uploaded to a sanctioned cloud storage service like Box while restricting and blocking upload of that same corporate data to personal instances of Box. This way, the organization can ensure data security and compliance without impeding an employee's productivity. Looking across our customers, we've found that on average, half of all users of a sanctioned cloud storage service have a personal instance of the same service. This means that if you have 1000 users on your corporate Box instance, you actually have 501 instances of Box being used in your environment (the original sanctioned service instance plus 500 individuals' private versions). This indicates the importance of differentiating between specific instances of cloud services to ensure you're correctly governing corporate data and resources while maintaining employee productivity. Placing a blanket, universal policy across a cloud service lacks the granularity needed for your business.

More than 90 percent of Netskope customers use IaaS services like Amazon Web Services, Microsoft Azure, and Google Cloud Platform. The use of these services has increased throughout this year and we've found that enterprises use on average 4 IaaS platforms within their organizations. Such use includes both sanctioned and unsanctioned, across services (besides the big three) like, CloudShare, Apache CloudStack, Digital Ocean, Linode, Rackspace Managed Cloud, and Openstack. Use cases range from development and testing to demos, POCs, education/training, and perform big data anaylsis. We recommend governing this usage with access and DLP policies as well as auditing of activities in each platform to ensure compliant usage and proper data protection.



BUSINESS-RELATED SERVICES OVERSHADOW CONSUMER

Microsoft takes the top two places in our top 20 cloud services list this quarter. Microsoft has a total of 7 services on the list this quarter, which is showing a trend of consumer ones like Pandora being pushed down the rankings by work/business services. Slack first appeared in the rankings last quarter and remains on the list this quarter at 16. Although there are less consumer services like Pandora, services such as ServiceNow are rising in popularity, which are in the scope of CASBs for additional visibility and control.

1	Microsoft Office 365 OneDrive for Business	Cloud Storage	11	Dropbox	Cloud Storage
2	Microsoft Office 365 Outlook.com	Webmail	12	LinkedIn	Social
3	Facebook	Social	13	Salesforce	CRM / SFA
4	Twitter	Social	14	Box	Cloud Storage/ Collaboration
5	iCloud	Cloud Storage	15	Microsoft Live OneDrive	Cloud Storage
6	Google Drive	Cloud Storage	16	Slack	Collaboration
7	Cisco WebEx	Collaboration	17	Microsoft 0365 SharePoint	Collaboration
8	Skype	Collaboration	18	Yahoo! Mail	Webmail
9	Gmail	Webmail	19	Microsoft Live Outlook	Webmail
10	YouTube	Consumer	20	ServiceNow	Infrastructure

TOP CLOUD ACTIVITIES

The top cloud activities this quarter were send, edit, create, login, view, download, invite, share, upload, and delete, respectively. Netskope normalizes more than 50 possible cloud activities across cloud services within categories and even across categories, so whether a user shares a file from a cloud storage service or a report from a business intelligence one, each of those are recognized as a share activity. This is useful in understanding risk, auditing user activity, and being able to say deterministically whether a data policy violation has occurred. It is also useful in isolating policy enforcement to a risky activity like share, rather than only being able to allow or block an app. Examining cloud service activities in the context of the service category, we call out the top three activities besides login for each of five important business service categories, cloud storage, HR, business intelligence, finance, and collaboration.

Top Activities in Cloud Storage Services

1. View
2. Share
3. Edit

Top Activities in Finance Services

1. Edit
2. Create
3. Delete

Top Activities in HR Services

1. Download
2. Create
3. Edit

Top Activities in Collaboration Services

1. Download
2. Create
3. View

Top Activities in Business Intelligence Services

1. Share
2. View
3. Download

TOP POLICY VIOLATIONS IN THE NETSKOPE ACTIVE PLATFORM

Beyond measuring usage and activity, we also look at policy violations within cloud services. Policies can be enforced based on a number of factors, including user, group, location, device, browser, service, instance, category, enterprise-readiness score, DLP profile, activity, and more. Through data abstraction and normalization of those factors, we're able to discern the services, categories, and activities surrounding a violation. Policies observed include blocking the download of PII from an HR app to a mobile device, alerting when users share documents in cloud storage services with someone outside of the company, and blocking unauthorized users from modifying financial fields in finance services.

Here are the top activities globally that constituted a policy violation per cloud service category, with DLP violations noted where they apply. Just as activities can vary between services, policy violations involving those activities can vary. For example, a policy violation involving downloading from a cloud storage app can be the improper downloading of a non-public press release, whereas in a CRM/SFA app could signal theft of customer data by a departing employee.

APP CATEGORY	Delete	Download	Edit	Log In Successful	Post	Send	Share	Upload	View
Cloud Storage	4	1!	2!	7	8	–	6	3!	5
Collaboration	6	1!	4	7	2!	9	8	5!	3
CRM/SFA	8	2!	3!	4	7	9	6	5!	1
Finance/ Accounting	5	4	3	6	–	–	7	2	1
HR	2	4	6	3	–	–	7	5	1
Productivity	3	2	1	5	–	–	7	6!	4
Social	6	7!	4!	3	2!	–	8	5!	1
Software Development	6	2	3	5	8	–	7	4!	1
Webmail	2	1!	4	6	7	5!	9	8!	3

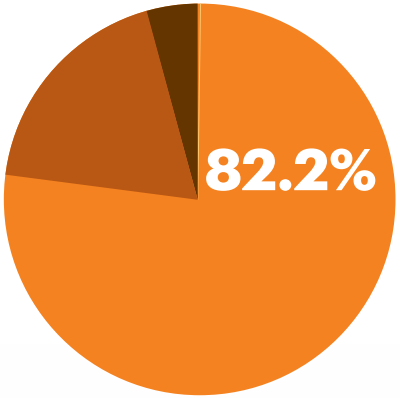
! Policy violation included in data loss prevention profile

1 Indicates highest occurrence of policy-violating activity for the category

CLOUD DLP POLICY VIOLATIONS

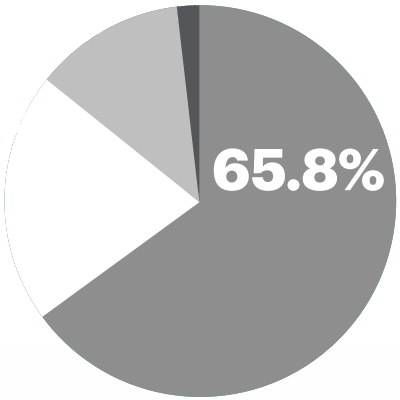
Cloud storage and webmail lead as the top two categories for DLP violations at 82.2 percent and 14.2 percent, respectively. Other categories combine to make up 3.6 percent.

Looking at activities, upload, send, and download make up the majority of violations with 65.8 percent, 20.1 percent, and 12.6 percent, respectively. In terms of data types, PII and PHI were again the majority of violations, followed by PCI. This is normal as these types of data are specifically regulated by various compliance regimens like HIPAA, Sarbanes-Oxley (SOX), or other international regulations like the GDPR. We advise that organizations take a two-pronged approach to securing activity and data. Secure risky activities like upload of PHI while at the same time placing policies on sensitive content stored in sanctioned services like restricting public links that have been shared for a set amount of time or encrypting that data.



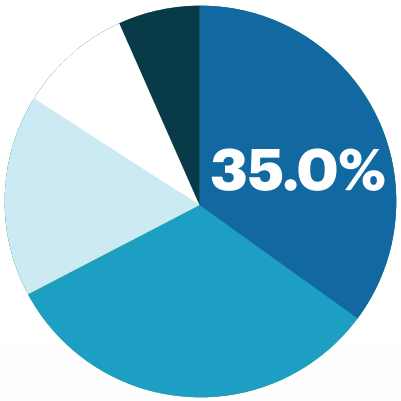
CATEGORY

- Cloud Storage **82.2%**
- Webmail **14.2%**
- Other (e.g., CRM/SFA, Social, and Collaboration) **3.6%**



ACTIVITY

- Upload **65.8%**
- Send **20.1%**
- Download **12.6%**
- Other (including View) **1.5%**



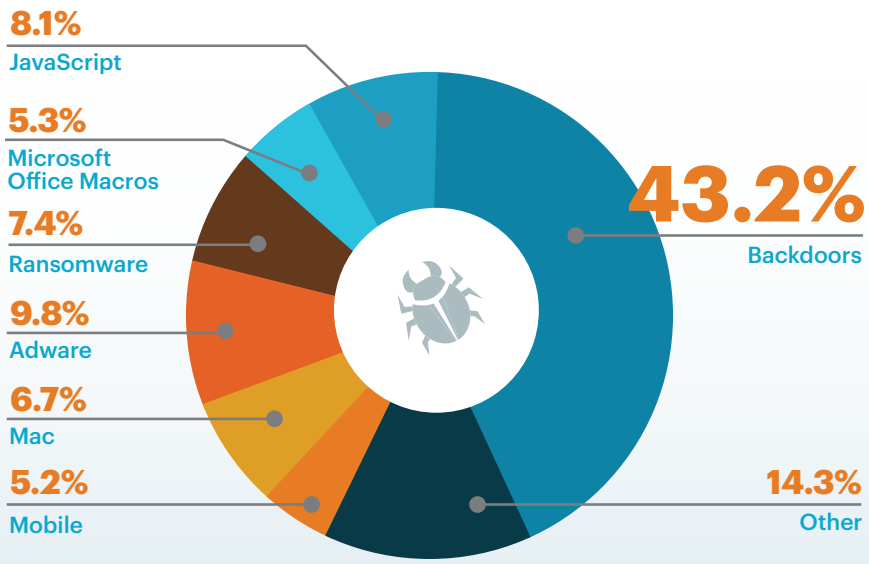
TYPE

- PII **35.0%**
- PHI **32.4%**
- PCI **16.5%**
- Source Code **9.4%**
- Other (including Confidential and Profanity) **6.7%**

RANSOMWARE ON THE RISE IN CLOUD THREATS AND MALWARE

The Netskope Threat Research Labs continues its study of cloud malware. This quarter, backdoors comprised the majority of detections at 43.2 percent, followed by adware at 9.8 percent, and Javascript malware at 8.1 percent. Ransomware made up 7.4 percent of detections, as we have now started to specifically track ransomware. We saw less of the common carriers of ransomware this quarter (Javascript malware, Microsoft Office macros, and PDF exploits) but have seen a rise in actual ransomware infections throughout the quarter, hence the breakout of the category. Mac malware, Microsoft Office macros, mobile, and others made up the rest of the detections at 6.7 percent, 5.3 percent, 5.2 percent, and 14.3 percent, respectively. We've altered the categorizations from last quarter because backdoors had a big jump in detections this quarter while other categories decreased as part of the percentage due to this. The other categories all increased in actual numbers, but the most dramatic increase came from the backdoor category. Adware increased as well and so we made it a separate category callout. The variability in detections quarter over quarter seem to be typical, matching with patterns of frequent releases of new types of malware. We do see trends like increased ransomware in the data though, showing it as a formidable threat to organizations. Security professionals should take note to address ransomware being delivered from the cloud, with such actions as ensuring regular data backups and investing in ransomware detection and remediation solutions.

This quarter saw decreases in average pieces of cloud malware in enterprises at 23 (from 26 last quarter) and 26.5 percent of malware-infected files shared with others, including internal or external users or publicly. Anecdotally, these lower numbers may be due to organizations using Netskope Threat Protection to take action and remediate cloud threats and malware. We think the numbers will stabilize in future quarters as malware coming into organizations is detected and remediated and companies take proactive steps in securing the cloud.



23
average pieces of malware in enterprises

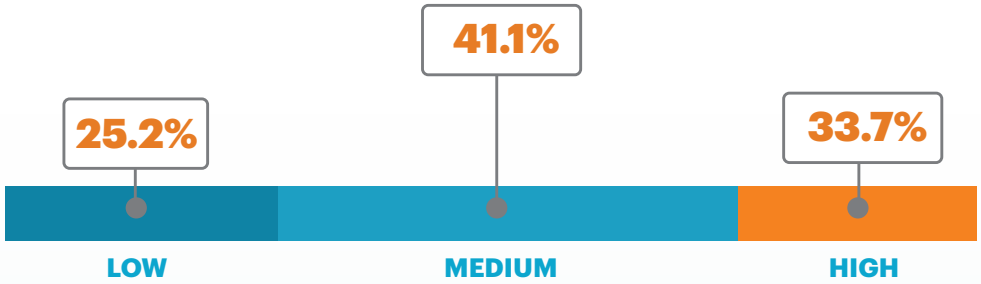
26.5%
of malware-infected files shared with others, including internal or external users or publicly

GDPR-READINESS STILL A CONCERN AS ENFORCEMENT DEADLINE DRAWS NEAR

As we start the new year, we're updating our GDPR numbers since organizations have been gearing up for GDPR compliance. This quarter, GDPR-readiness levels rose compared to when we first reported them in the June 2016 Cloud Report, with 33.7 percent of cloud services falling into the "high" GDPR-readiness group, 41.1 percent into the "medium" group, and 25.2 percent into the "low" group.

It's worth noting that even a "high" GDPR-readiness level may not mean a service is fully compliant, as the GDPR has a strict set of standards for dealing with privacy data and even the presence of capabilities doesn't mean the cloud services are being used in a compliant manner. Remember, there is a shared responsibility between cloud service vendors and their customers in which the vendors are responsible for inherent security and enterprise-readiness, and the customer organizations are responsible for how their employees make use of the cloud services. For example, a cloud storage service may have all of the right features to support privacy, but if a user uploads a file full of PII and the organization doesn't enforce the proper protections over that content, the service cannot protect against that compliance violation.

GDPR cloud-readiness levels



66.4
percent of cloud services do not specify that the customer owns the data in their terms of service

53.8
percent of cloud services keep data for longer than one week upon termination of service.

42.0
percent of cloud services do not allow administrators to enforce password controls.

82.4
percent of services **do not** encrypt data at rest.

40.4
percent back data up to a secondary location. Some of these locations may not conform to the GDPR's data residency requirements.

THREE QUICK WINS FOR ENTERPRISE IT

1. Use layered policies to enforce different controls for sanctioned versus personal instances of cloud services to maintain compliance and protect employee privacy.

2. Evaluate your current security programs to address ransomware, which is increasingly delivered via cloud.

3. Address GDPR requirements by enforcing security controls like protecting regulated data and ensuring data residency.