WINTER 2018

CLOUD REPORT

HR'S LOVE OF CLOUD GROWS STRONGER DESPITE LOOMING GDPR DEADLINE

On average, 139 HR apps are used in organizations

REPORT HIGHLIGHTS

- Enterprises have an average of 1,181 cloud services in use with 92.7 percent not enterprise-ready.
- HR and marketing apps are the most highly used in organizations, with an average of 139 and 121, respectively.
- Detections of cryptocurrency- and Bitcoin-related malware as well as banking malware continue to trend in organizations.

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 October 1 through December 31, 2017.

This quarter, there was an average of 1,181 cloud services in use per enterprise, up from last quarter's 1,022. The average amount has hovered in the low thousands in the past couple quarters. In conducting cloud risk assessments and helping secure cloud usage for customers, we've found that the amount of cloud services can vary from a few hundred to over 3,000 at larger organizations but usually average in the 1000s.

We looked at the top HR cloud services used in organizations this quarter. HR apps in use include SuccessFactors, Ultimate Software, and Workday. There was an average of 139 HR apps in use across organizations, the highest average we've had yet for a category. Many of these apps are not necessarily sanctioned, IT-led services, leading to concern for sensitive data leakage and security. We recommend organizations find and evaluate which HR services are in use (especially shadow IT ones procured by lines of businesses or individuals) and place appropriate visibility and control measures, especially in light of regulations like the General Data Protection Regulation (GDPR).

Malware detections from the Netskope Threat Research Labs are as follows: generic types of malware (Flash exploits, worms, etc.) made up 41.6 percent, backdoors made up 33.6 percent, followed by Microsoft Office macros with 8.6 percent, adware 4.0 percent, PDF exploits 3.2 percent, ransomware 3.1 percent, Mac malware 2.3 percent, JavaScript malware 1.5 percent, mobile types 1.1 percent, PowerShell 0.5 percent, cryptocurrency/Bitcoin 0.4 percent, and banking 0.1 percent. Cryptocurrency and banking-related malware (malware that attempts to steal user credentials for banking sites) are called out specifically as there has been a rise in number of detections, even though they make up a smaller percentage of the total. Another type to note is PowerShell malware, which remains an issue for organizations as traditional endpoint AV solutions still have trouble scanning and remediating this type of malware.

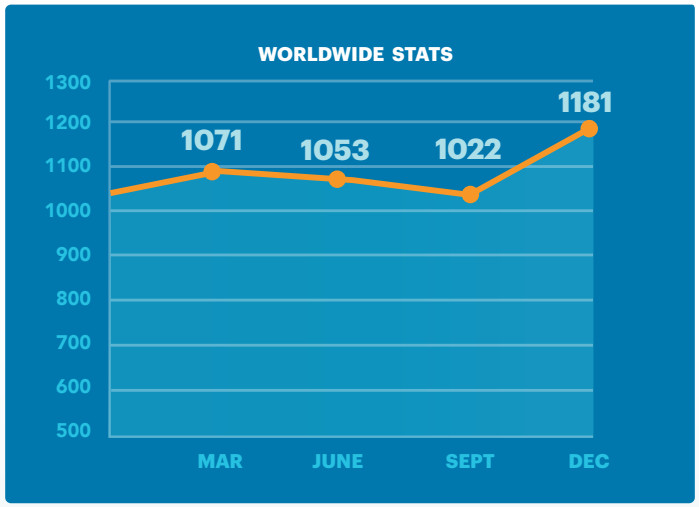
The top cloud activities this quarter were login, send, edit, create, view, share, download, upload, invite, and delete, respectively. Downloads and uploads are one of the most heavily restricted activities that have policies set against them in Netskope, a good reminder for organizations under compliance-related mandates to ensure proper controls are in place across not only managed, corporate devices, but also unmanaged ones accessing sensitive data in cloud services.

Finally, in DLP violations this quarter, cloud storage took the lead with 54.7 percent of all violations. Webmail followed with 42.5 percent, collaboration with 2.2 percent, and other with 0.6 percent. By activity, download and upload were even at 40.4 percent and 40.3 percent, respectively. Send made up 17.1 percent of violations and other 2.2 percent. In terms of types of data, PII led the way with 61.7 percent of violations while other (mostly confidential documents) followed with 20.5 percent, source code 8.6 percent, PHI 7.4 percent, and PCI 1.8 percent.

ENTERPRISES USE AN AVERAGE OF 1,181 CLOUD SERVICES

This quarter, the average amount of cloud services per enterprise increased 1.6 percent to 1,181 cloud services, compared to 1,022 last quarter. 92.7 percent of these services are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI).

HR and marketing apps remain the highest types of cloud services in use in terms of average number, followed by collaboration. When creating policies and access controls to secure data, security teams should start with these categories first, especially HR and collaboration as those apps have the greatest potential to contain sensitive data being shared. Many of the top HR apps in use like SuccessFactors and Workday contain personal data, necessitating DLP and access controls to ensure compliant usage of that data. And with marketing apps, many are user-led, shadow IT apps that contain customer or prospect data which are also covered by regulations like GDPR.



CATEGORY	# PER ENTERPRISE	NOT ENTERPRISE-READY
HR	**139**	**95%**
Marketing	121	97%
Collaboration	95	81%
Finance/Accounting	63	94%
CRM	62	94%
Social	24	89%
Cloud Storage	24	66%
IT Service/Application Management	22	97%

TOP 20 CLOUD SERVICES LIST

Microsoft Office 365 apps Outlook.com and OneDrive for Business take the top two spots, respectively. We continue to see that cloud storage and collaboration apps make up the majority of the list. Security policies should start with the apps in the previous categories but security teams should remember that social media services like Facebook and Twitter are popular as well and may need activity-level policies for compliance reasons. As an example, we've seen organizations restrict specific words in Twitter posts, combined with ticker symbols for public companies, in order to meet financial regulatory standards.

1	Microsoft Office 365 Outlook.com	Webmail	11	Linkedin	Social
2	Microsoft Office 365 OneDrive for Business	Cloud Storage	12	Box	Collaboration/ Cloud Storage
3	Google Gmail	Webmail	13	Salesforce	CRM
4	Facebook	Social	14	Microsoft Live OneDrive	Cloud Storage
5	Skype	Collaboration	15	Microsoft Teams	Collaboration
6	Google Drive	Cloud Storage	16	ServiceNow	Infrastructure
7	Microsoft Office 365 SharePoint	Collaboration	17	Microsoft Live Outlook	Webmail
8	Microsoft Power BI	Business Intelligence	18	Slack	Collaboration
9	iCloud	Cloud Storage	19	Dropbox	Collaboration/ Cloud Storage
10	Twitter	Social	20	Microsoft Skype for Business	Collaboration

GDPR-READINESS METRICS FOR CLOUD SERVICES

Across the cloud services used across Netskope customers, 67.9 percent of them did not specify that the customer owns the data, 80.7 percent of the services did not support encryption at rest, and 40.5 percent replicated data in geographically dispersed data centers. These levels have changed little from last quarter. With the May 2018 deadline for GDPR compliance coming up, we remind organizations to take steps to find all personal data across their cloud services first to inform their security policies around that data. Many ecosystem apps connected to enterprise cloud services make it hard to track data.

DATA OWNERSHIP TERMS

67.9% of cloud services do not specify that the customer owns the data in their terms of service

DATA ENCRYPTION AT REST

80.7% of cloud services do not support encryption of data at rest

DATA BACKUP IN OTHER GEOS

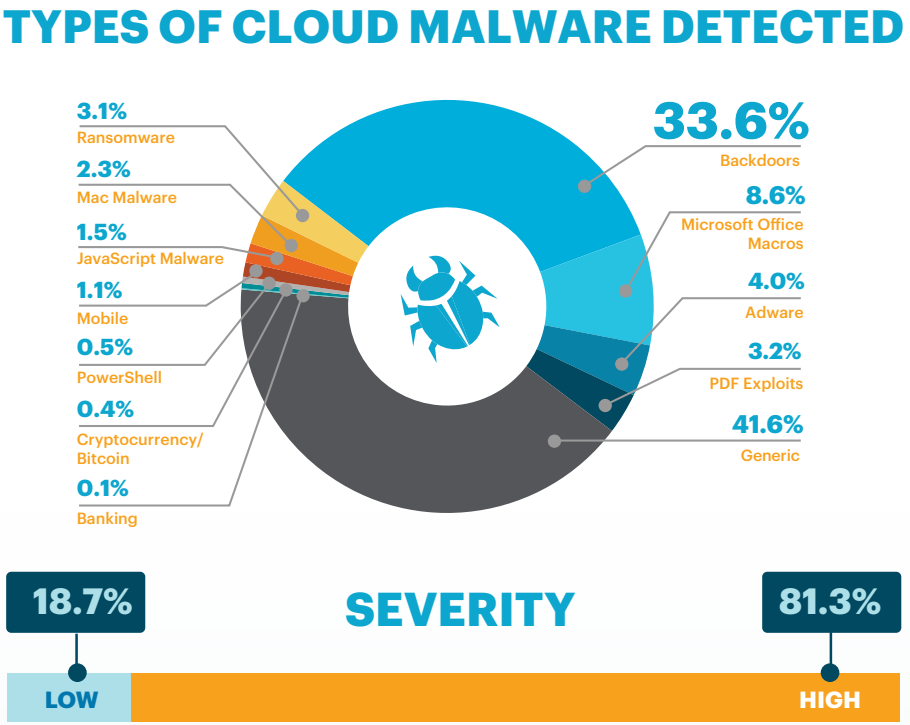
40.5% of cloud services replicate data in geographically dispersed data centers

BANKING AND CRYPTOCURRENCY- AND BITCOIN-RELATED MALWARE STILL TOP-OF-MIND

This quarter, the Netskope Threat Research Labs found that generic types of malware (Flash exploits, worms, etc.) made up the majority of detections with 41.6 percent. Backdoors made up 33.6 percent, followed by Microsoft Office macros with 8.6 percent, adware 4.0 percent, PDF exploits 3.2 percent, ransomware 3.1 percent, Mac malware 2.3 percent, JavaScript malware 1.5 percent, mobile types 1.1 percent, PowerShell 0.5 percent, cryptocurrency/Bitcoin 0.4 percent, and banking 0.1 percent. We still see variability across malware types but point out new categories of note as we see them. This quarter, cryptocurrency- and Bitcoin-related malware still trend as we called out last report, with a rise in banking-related malware, which steal online banking user credentials, as well. We continue to see a decent amount of PowerShell malware, which remains an issue for organizations as endpoint AV solutions still have trouble scanning and remediating this type of malware.

Note the variety of malware types detected and remediated by Netskope across various sanctioned, IT-led cloud storage services. Besides varying levels of AV/malware scanning and remediation capabilities across cloud storage services, with the amount of new malware being produced, much of the malware is missed by these services. Netskope recommends putting in place multiple layers of threat protection so your organization's security stack has various checkpoints to stop malware and other threats. Applying policies on uploads and downloads of data to scan for malware also helps with this.

In severity levels this quarter, high made up 81.3 percent and low severity was 18.7 percent.



TOP CLOUD ACTIVITIES

The top cloud activities this quarter were login, send, edit, create, view, share, download, upload, invite, 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 a cloud service. Examining cloud service activities in the context of the category, we call out

Top Activities in Cloud Storage

1. Share
2. View
3. Edit

Top Activities in Finance

1. Edit
2. Create
3. View

Top Activities in HR

1. Create
2. Download
3. Edit

Top Activities in Collaboration

1. View
2. Edit
3. Create

Top Activities in Business Intelligence

1. View
2. Share
3. Download

the top three activities besides login for each of five important categories, cloud storage, HR, business intelligence, finance, and collaboration.

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, cloud 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 service 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 cloud 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 service can be the improper downloading of a non-public press release, whereas in a CRM service could signal theft of customer data by a departing employee.

Cloud service category	Delete	Download	Edit	Log In	Post	Send	Share	Upload	View
Cloud storage	7	5!	4!	1	8	–	3	6!	2
Collaboration	7	5!	3!	1	8!	9	4	6!	2
Customer Relationship Management	8	4!	5	1	6!	9	3	7!	2
Finance/ Accounting	5	4	2	1	–	–	7	6	3
HR	5	2	3	1	–	–	7	6	4
Social	6	7!	5	2	3!	–	–	4!	1
Webmail	6	3!	2	7	–	1!	8	5!	4

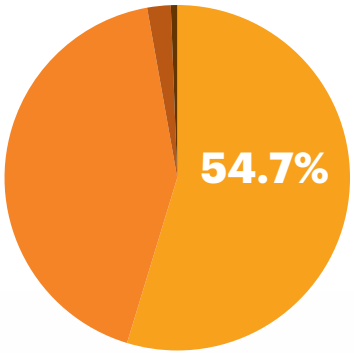
! Policy violation included in data loss prevention profile

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

CLOUD DLP POLICY VIOLATIONS

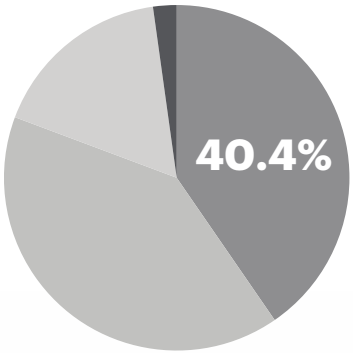
In cloud service DLP violations by category, cloud storage leads with 54.7 percent of violations. Webmail followed with 42.5 percent, while collaboration services and other rounded things out with 2.2 percent and 0.6 percent, respectively.

For DLP violations by activity, download had 40.4 percent, upload 40.3 percent, send 17.1 percent, and other (including View) 2.2 percent. With regulations like GDPR, we recommend placing restrictions or encrypting the data on upload activities to control sensitive data going into cloud services. With activity-level policies in place, organizations can protect sensitive data as it's being sent to the cloud, regardless of whether that cloud service is sanctioned by IT or not. Finally, DLP violations by type had mostly PII at 61.7 percent. Source code had 8.6 percent, PHI 7.4 percent, and PCI had 1.8 percent. The other category, which includes confidential documents and profanity policies, had 20.5 percent, with sensitive, confidential documents making up the majority.



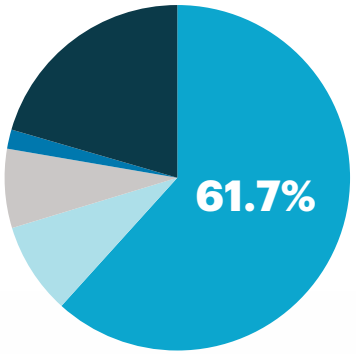
CATEGORY

- Cloud Storage **54.7%**
- Web Mail **42.5%**
- Collaboration **2.2%**
- Other **0.6%**



ACTIVITY

- Download **40.4%**
- Upload **40.3%**
- Send **17.1%**
- Other (including View) **2.2%**



TYPE

- PII **61.7%**
- Source Code **8.6%**
- PHI **7.4%**
- PCI **1.8%**
- Other (including Confidential and Profanity) **20.5%**

THREE QUICK WINS FOR ENTERPRISE IT

1. Ensure compliant usage of sensitive data with contextual, activity-level policies like restricting download of PII from unmanaged devices.

2. Educate employees on phishing scams and rising prevalence of banking malware.

3. Coach employees from risky actions like uploads of sensitive data across thousands of IT-led and business-led cloud services.