SEPTEMBER
2017

netskope

CLOUD REPORT

LITTLE CHANGE IN GDPR-READINESS LEVELS WITH MAY 2018 DEADLINE LOOMING

24.6% of cloud services rated high on GDPR-readiness

REPORT HIGHLIGHTS

- 24.6 percent of cloud services are GDPR-ready
- Enterprises have an average of 1,022 cloud services in use, cloud service usage hovers around the 1,000 mark
- Trends show increasing amount of Bitcoin-related malware, making up close to 1 percent of detections this quarter
- Webmail makes up 42.3 percent of DLP violations

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 April 1 through June 30, 2017.

This quarter, there was an average of 1,022 cloud services in use per enterprise, down slightly from last quarter's 1,053. We see a leveling off of average amount of cloud services, just above the 1,000 mark.

We found that only 24.6 percent of cloud services are rated 'high' in an assessment of GDPR-readiness, based on attributes like location of where data are stored, level of encryption, data processing agreement attributes, and more. Organizations should prepare to place additional security policies, access controls, and data protection for cloud services to ensure employees are handling sensitive personal data in a secure manner.

The Netskope Threat Research Labs found backdoors were detected the most with 27.4 percent of all detections, followed by ransomware with 8.6 percent, adware 8.1 percent, JavaScript 7.2 percent, Mac malware 7.1 percent, Microsoft Office macros 5.9 percent, and PDF exploits 2.7 percent. Bitcoin/cryptocurrency-related malware was .9 percent with mobile and generic detections closing out the numbers with .8 percent and 31.3 percent, respectively. We've noticed a trend this quarter in cryptocurrency-related malware both in terms of the kinds of malware (mining malware) and monetization strategy of attackers. In severity levels this quarter, high made up 86.9 percent and low severity was 13.1 percent. 23.8 percent of malware-infected files were shared with others, including internal or external users or publicly.

Send, login, create, edit, view, download, share, invite, logout, and delete were the top cloud activities this quarter, respectively. Ranked by cloud service categories, top activities remained similar. View was the top activity for the cloud storage and business intelligence categories, edit for the finance and collaboration categories, and download for HR services.

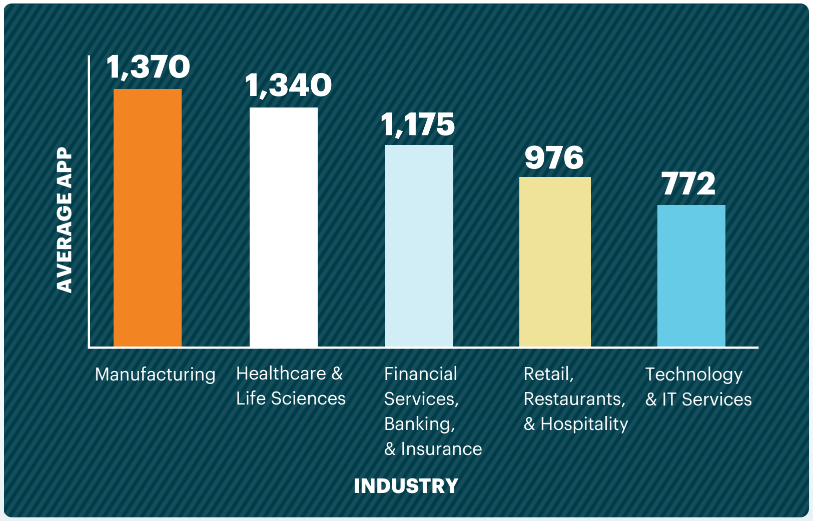
In DLP violations, webmail comprises 42.3 percent of violations, followed by cloud storage at 30 percent, collaboration services at 9.5 percent, and all others 18.2 percent. By activity type, upload took the top place with 53.6 percent of violations. Download took 28.0 percent while send and other were 16.6 percent and 1.8 percent of violations, respectively. By type, PII was the most prevalent with 27.8 percent, PHI had 19.8 percent, source code 25.4 percent, PCI 1.5 percent, and all others (including confidential and profanity) 25.5 percent.

ENTERPRISES USE AN AVERAGE OF 1,022 CLOUD SERVICES

This quarter, the average amount of cloud services per enterprise decreased 2.9 percent to 1,022 cloud services, compared to 1,053 last quarter. 92.1 percent of these services are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI). As discussed in last quarter's cloud report, the average amount of cloud services have leveled off, suggesting a saturation of usage in organizations. This quarter's report focuses on the GDPR and how ready cloud services are to comply with the regulation. Organizations should build their cloud security programs with the assumption that while some cloud services are more GDPR-ready than others to comply with the regulation, all of them should be covered with some security policies or access controls to prevent risky behaviors.

Manufacturing led the way with the highest average amount of cloud services used with 1,370, followed by healthcare and life sciences with 1,340. Financial services, banking, and insurance came in third with 1,175 and retail, restaurants, and hospitality fourth with 976. Technology and IT services dropped to 772 this quarter.

In the cloud service category cut, HR remains the category with the highest average number of cloud services used at 109, follow closely by marketing at 102. Across the categories we report over, HR would probably have the most personal data as defined by the GDPR. Organizations should audit the HR services in use, sign appropriate data processing agreements with sanctioned ones, and place appropriate security policies and controls to ensure that personal data are being secured and used appropriately.



CATEGORY	# PER ENTERPRISE	% NOT ENTERPRISE-READY
HR	109	95%
Marketing	102	98%
Collaboration	85	84%
Finance/Accounting	59	94%
CRM/SFA	50	93%
Software Development	33	75%
Productivity	32	75%
Social	24	89%
Cloud Storage	24	67%
IT Service/Application Management	22	96%

TOP 20 CLOUD SERVICES LIST COMPRISED MAINLY OF CLOUD STORAGE AND COLLABORATION

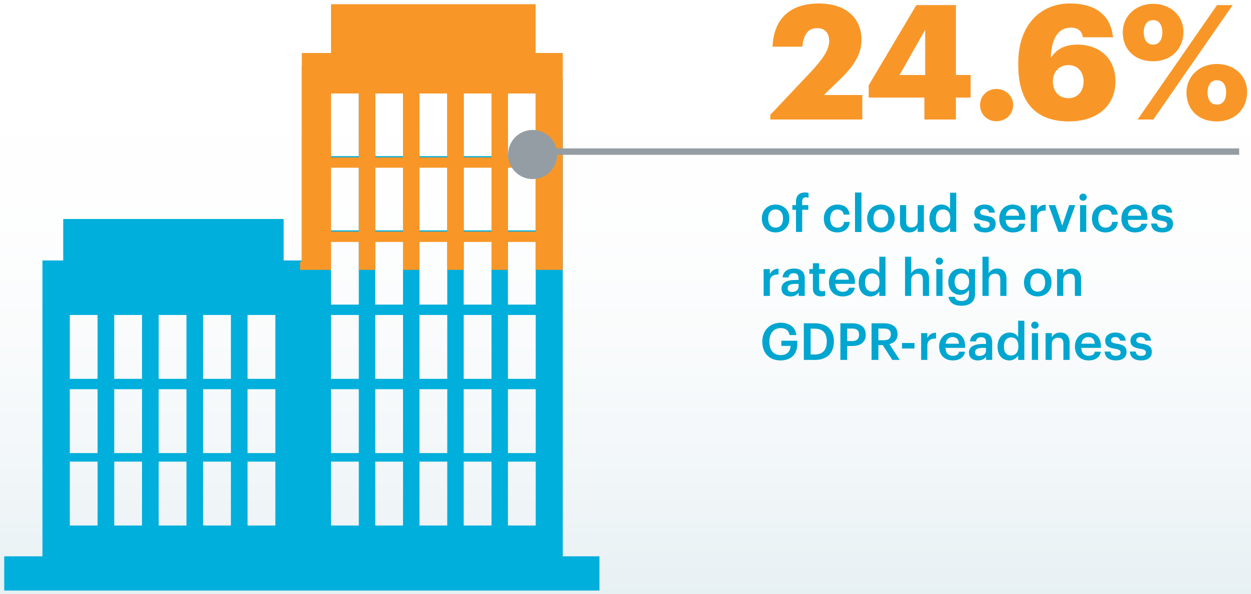
Microsoft Office 365 OneDrive for Business is at the top of the list, again. With half of the top 20 list consisting of cloud storage or collaboration services, we recommend that organizations take a look at the data flowing in and out of these services. We've discussed placing controls on ecosystem services – these collaboration and cloud storage services all hook into suites like Microsoft Office 365 or G Suite – so a comprehensive cloud security program should take into account what controls to place in cloud service-to-cloud service communications and processing.

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

GDPR-READINESS METRICS FOR CLOUD SERVICES

This quarter we focus the report on the GDPR-readiness of cloud services, finding that only 24.6 percent of services rated highly on our scale. We measure this rating by taking into account multiple parameters like the data ownership terms of the cloud service, encryption used (if at all), whether the data is processed in various geographies, and more. This percentage shows little progress has been made since we reported on this number in our June 2016 Cloud Report.

Across the cloud services used across Netskope customers, 67.1 percent of them did not specify that the customer owns the data, 80.4 percent of the services did not support encryption at rest, and 41.9 percent replicated data in geographically dispersed data centers. We took a look at the 24.6 percent of services rated as 'high' in GDPR-readiness as well. The first two stats were lower but the percentage of services that replicated data across geos was almost double in cloud services that were highly rated in GDPR-readiness. This higher percentage could be explained by the fact that more enterprise-ready services fulfill data availability and backup requirements better. By replicating data across various locations, the service remains highly available and offers a better SLA even if this makes complying with the GDPR more difficult for organizations trying to understand and control where personal data flows. This also emphasizes the need for organizations to place controls across all cloud services, not just the ones that are rated highly in GDPR-readiness as there may be gaps that need to be addressed.



DATA OWNERSHIP TERMS

67.1% of cloud services do not specify that the customer owns the data in their terms of service

DATA ENCRYPTION AT REST

80.4% of cloud services do not support encryption of data at rest

DATA BACKUP IN OTHER GEOS

41.9% 41.9% of cloud services replicate data in geographically dispersed data centers

AMONG THE CLOUD SERVICES RATED AS HIGH FOR GDPR-READINESS:

DATA OWNERSHIP TERMS

38.3% of cloud services do not specify that the customer owns the data in their terms of service

DATA ENCRYPTION AT REST

57.1% of cloud services do not support encryption of data at rest

DATA BACKUP IN OTHER GEOS

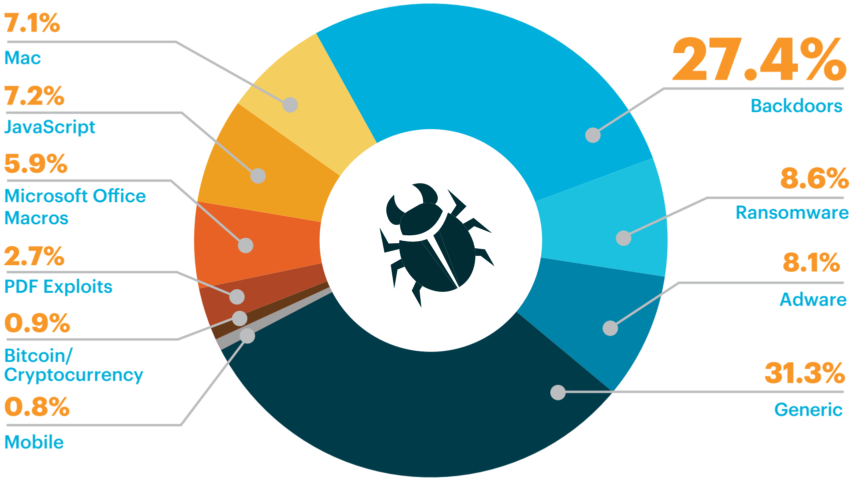
80.3% of cloud services replicate data in geographically dispersed data centers

MALWARE TYPES TREND TOWARDS BITCOIN AND CRYPTOCURRENCY-RELATED INFECTIONS

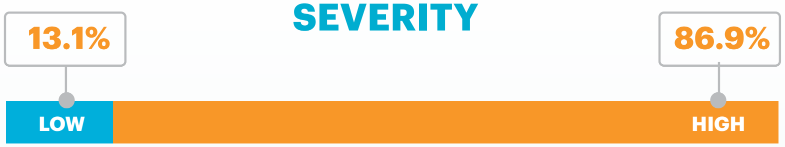
The Netskope Threat Research Labs found backdoors were detected the most with 27.4 percent of all detections, followed by ransomware with 8.6 percent, adware 8.1 percent, JavaScript 7.2 percent, Mac malware 7.1 percent, Microsoft Office macros 5.9 percent, and PDF exploits 2.7 percent. Bitcoin/cryptocurrency-related malware was .9 percent with mobile and generic detections closing out the numbers with .8 percent and 31.3 percent, respectively. The labs team has noticed variability across types of detections across quarters and adjusts malware categories accordingly to show current trends. As we've written about on the Netskope blog, this quarter has had a rise in cryptocurrency-related malware (both in terms of monetization for attackers and as a malware like crypto miners installed maliciously on resources owned by unsuspecting organizations) and our detection engines have detected more of this type of malware across customers. We call out the category this quarter and advise customers to enact best-practice policies like enabling versioning for critical content in cloud storage services, creating firewall rules to block bitcoin pools, and scanning uploads and downloads across cloud services. Many of the crypto-related malware are hosted in IaaS environments like Amazon Web Services, placing an importance in scanning downloads from unsanctioned, user-led instances of these services. This will help to prevent unsuspecting users from infecting corporate servers and devices with crypto mining software.

In severity levels this quarter, high made up 86.9 percent and low severity was 13.1 percent. 23.8 percent of malware-infected files were shared with others, including internal or external users or publicly.

TYPES OF CLOUD MALWARE DETECTED



SEVERITY



23.8 percent of malware-infected files were shared with others, including internal or external users or publicly

TOP CLOUD ACTIVITIES

The top cloud activities this quarter were send, login, create, edit, view, download, share, invite, logout, 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 the top three activities besides login for each of five important categories, cloud storage, HR, business intelligence, finance, and collaboration.

Top Activities in Cloud Storage

1. View
2. Share
3. Download

Top Activities in HR

1. Download
2. Create
3. Edit

Top Activities in Business Intelligence

1. View
2. Share
3. Download

Top Activities in Finance

1. Edit
2. Create
3. Upload

Top Activities in Collaboration

1. Edit
2. View
3. Create

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 !	3	8	–	2	6 !	1
Collaboration	4	5 !	1	3	6 !	9	7	8 !	2
Customer Relationship Management	8	5 !	4	1	6	9	2	7 !	3
Finance/ Accounting	4	6	2	1	–	–	7	5	3
HR	4	2	5	1	–	–	7	6	3
Social	5	7 !	6	2	3 !	–	8	4 !	1
Webmail	6	4 !	2	7	–	1 !	8	5 !	3

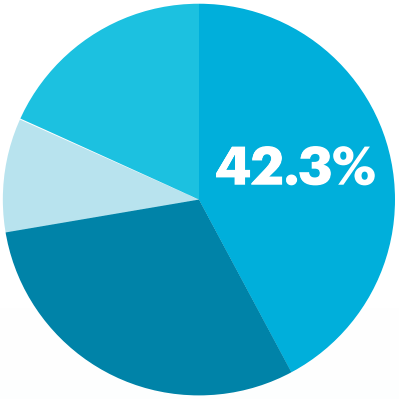
! Policy violation included in data loss prevention profile

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

CLOUD DLP POLICY VIOLATIONS

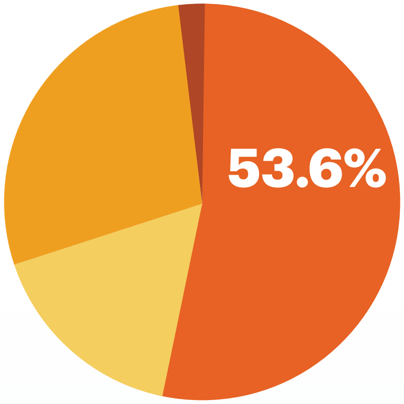
For cloud service category DLP violations, webmail still leads with 42.3 percent of the violations, no change from last quarter's 42.3 percent. Cloud storage is second with 30.0 percent. Collaboration services made up 9.5 percent of the violations. All other cloud service categories combined to make up 18.2 percent.

DLP violations by activity had uploads in the lead with 53.6 percent, a decrease from last quarter. Send violations were at 16.6 percent, followed by download at 28.0 percent and other at 1.8 percent. By type, we found that PII had 27.8 percent of all violations. PHI and source code followed with 19.8 percent and 25.4 percent, respectively. PCI and other (including confidential and profanity) rounded out the categories with 1.5 percent and 25.5 percent, respectively. With the large percentage of violations in the other category, mostly composed of confidential data, organizations should ensure proper controls and policies are placed for files that contain trade secrets, internal documents and plans, and the like to prevent data leakage to external parties.



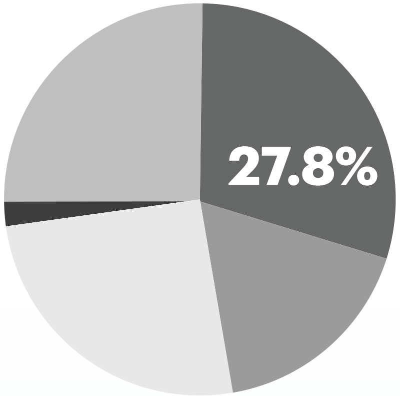
CATEGORY

- Webmail **42.3%**
- Cloud storage **30.0%**
- Collaboration **9.5%**
- Other **18.2%**



ACTIVITY

- Upload **53.6%**
- Send **16.6%**
- Download **28.0%**
- Other (including View) **1.8%**



TYPE

- PII **27.8%**
- PHI **19.8%**
- Source Code **25.4%**
- PCI **1.5%**
- Other (including Confidential and Profanity) **25.5%**

THREE QUICK WINS FOR ENTERPRISE IT

1 Assess GDPR-readiness of cloud services in environment to develop proper security policies and controls.

2 Scan for malware from IaaS platforms to protect from cloud threats.

3 Protect from sensitive data leakage via webmail by scanning for and remediating DLP violations.