JUNE
2017

WORLDWIDE
EDITION

netskope

CLOUD REPORT

HYBRID CLOUD AND WEB THREATS ON THE RISE IN ENTERPRISES

3.3% of enterprises see rapidly-rising hybrid cloud and web threats

REPORT HIGHLIGHTS

- 3.3 percent of enterprises seeing hybrid cloud and web threats in their environments.
- Enterprises have an average of 1,053 cloud services in use, a slight decrease from 1,071 last quarter.
- GDPR-readiness metrics show little change, 66.9 percent of cloud services do not specify customer owns data in terms of service.
- 9.8 percent of DLP violations from collaboration cloud services, with the rise of Slack, Microsoft Teams, and other similar services.

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 January 1 through March 31, 2017.

There was a slight decrease in average amount of cloud services in use at enterprises, going to 1,053 from 1,071. Microsoft again had 8 cloud services in the list of top 20 used cloud services, while Slack moves up the list to number 12.

The focus of this quarter's report is on hybrid threats, malware that use both cloud and web services to deliver malicious payloads to users. This type of threat has increased in occurrence across customers over time, appearing in 3.3 percent of tenants this quarter. Hybrid threats emphasize the need for security solutions that can detect threats across cloud and web services – and unify that information for security admins. Aside from this, we found that adware surged to first place with 31.7 percent of all detections. The rest of the detections were as follows: backdoors 16.9 percent, Mac malware 11.0 percent, mobile malware 15.3 percent, and generic detections 15.3 percent. The common ransomware delivery vehicles totaled 9.8 percent, consisting of Microsoft Office macros with 4.3 percent, JavaScript 2.4 percent, PDF exploits 1.3 percent, and Flash exploits 0.3 percent. We broke out the pure ransomware category at 1.5 percent, encompassing all other delivery methods other than phishing emails, which are the most popular delivery vehicle for initiating a ransomware attack.

We check in with the European Union General Data Protection Regulation (GDPR) as the deadline for compliance is less than a year away in May 2018. 66.9 percent of cloud services do not specify that the customer owns the data in their terms of service. 89.9 percent of cloud services do not support encryption of data at rest and 40.7 percent of cloud services replicate data in geographically dispersed data centers.

Send, create, login, edit, view, download, invite, upload, share, and delete, were the top cloud activities this quarter, respectively. By cloud service categories, the results were similar as last quarter with view being the top activity in cloud storage services, download for HR, share for business intelligence, and edit for the finance and collaboration categories.

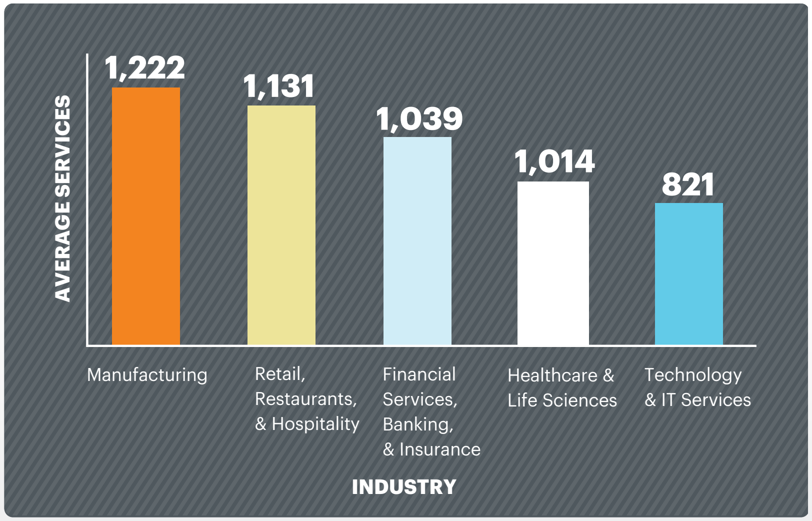
Finally, in DLP violations, webmail continues to lead for the second quarter in row with 43.3 percent of all DLP violations, followed by cloud storage at 30.6 percent. We call out collaboration category services this quarter as services like Slack are on the rise, contributing to 9.8 percent of DLP violations. Other rounded the categories out at 16.3 percent. Upload was still the top violation in activities with 65.0 percent. Send followed with 17.5 percent, download 16.2 percent, and other 1.3 percent.

ENTERPRISES USE AN AVERAGE OF 1,053 CLOUD SERVICES

This quarter, the average amount of cloud services per enterprise decreased 1.7 percent to 1,053 cloud services, compared to 1,071 last quarter. 93.6 percent of these services are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI). We attribute the leveling off of average amount of cloud services in use to a saturation of usage across organizations. As we onboard customers, we're noticing a threshold of usage of cloud services that hovers around the low thousands. Note, even if cloud services are enterprise-ready and have high CCI scores, they are still susceptible to "cross-app instance grant attacks." One example of this is when attackers use Google Drive or Microsoft OneDrive to host malicious files and share those files with users. Users accept the invitation and are redirected to an app that uses Google or Microsoft permissions. They are then asked to grant the appropriate permissions. Once the attacker has full permissions to the user's email account, they can further propagate the attack. See the Netskope blog post on "Cloudphishing" for more information on this.

The manufacturing industry had the highest average amount of cloud services used this quarter at 1,222. Retail, restaurants, and hospitality fell to second place with 1,131. Financial services, banking, and insurance followed at 1,039, with healthcare and life sciences and technology and IT services coming in at 1,014 and 821, respectively.

This quarter, the HR category took the lead with an average of 98 average cloud services used, followed by marketing with 87. HR would not typically be thought of as the most cloud-forward in an organization, but this category has been in the upper rankings for a while now. As organizations move employee data to the cloud and use HR cloud services as their systems of record, this is a good reminder to place the proper security controls over all HR services to prevent sensitive data loss and comply with regulations like GDPR.



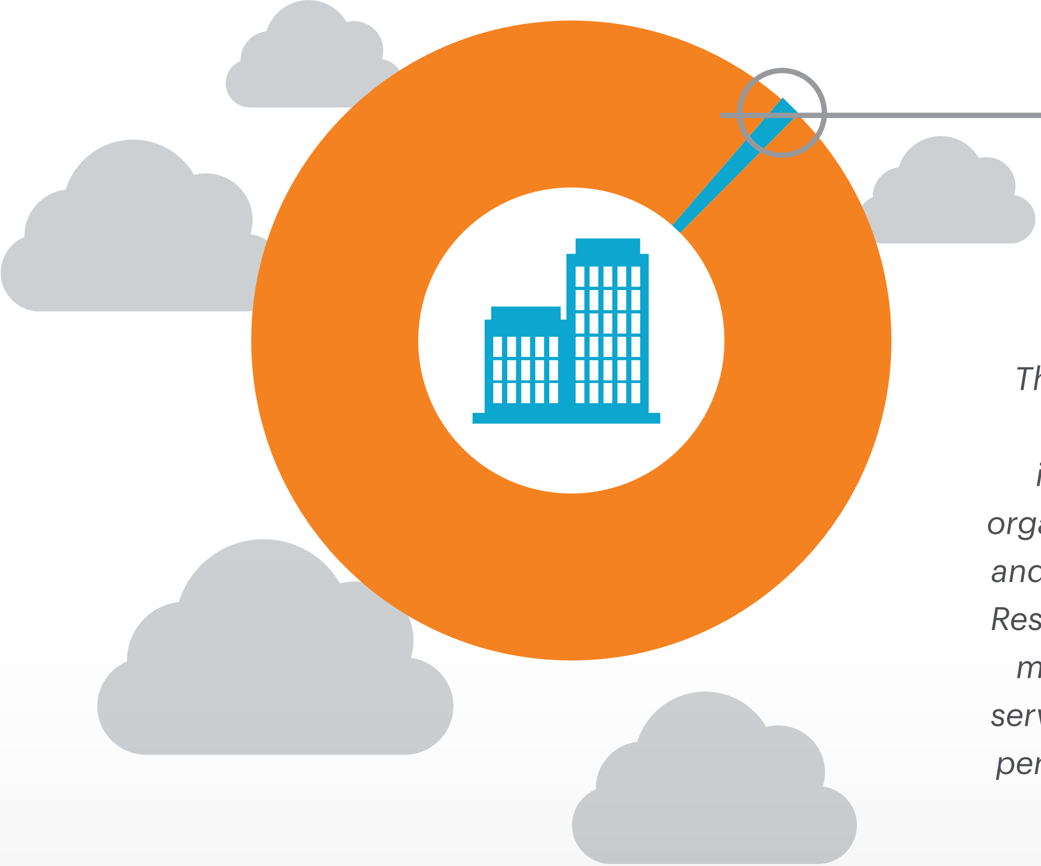
CATEGORY	# PER ENTERPRISE	ENTERPRISE-READY
HR	98	96%
Marketing	87	97%
Collaboration	71	87%
Finance/Accounting	63	96%
CRM	43	94%
Software Development	40	96%
Productivity	38	95%
Social	29	91%
Cloud Storage	26	73%
IT Service/Application Management	25	98%

SLACK RISES IN TOP 20 CLOUD SERVICES

Microsoft has a total of eight services on the list this quarter, again. Office 365 OneDrive for Business has solidified its lead as the top cloud service as it's in the first position again. Collaboration service Slack has moved steadily up in the rankings as well though, coming in at number 12. We emphasized the importance of securing not only the major Microsoft Office 365 suite of services but also ecosystem services last quarter and guidance remains the same. And with the increasing use of collaboration services, robust DLP controls will remain critical in securing sensitive data.

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

HYBRID CLOUD AND WEB THREATS INCREASINGLY A CONCERN IN ORGANIZATIONS



3.3%

of enterprises see rapidly-rising hybrid cloud and web threats

This quarter, we introduce the concept of hybrid cloud and web threats, increasingly relevant threats faced by organizations as the lines between cloud and web converge. The Netskope Threat Research Labs defines a hybrid threat as malware that uses both cloud and web services to deliver malicious payloads or perform an attack on a system or a user.

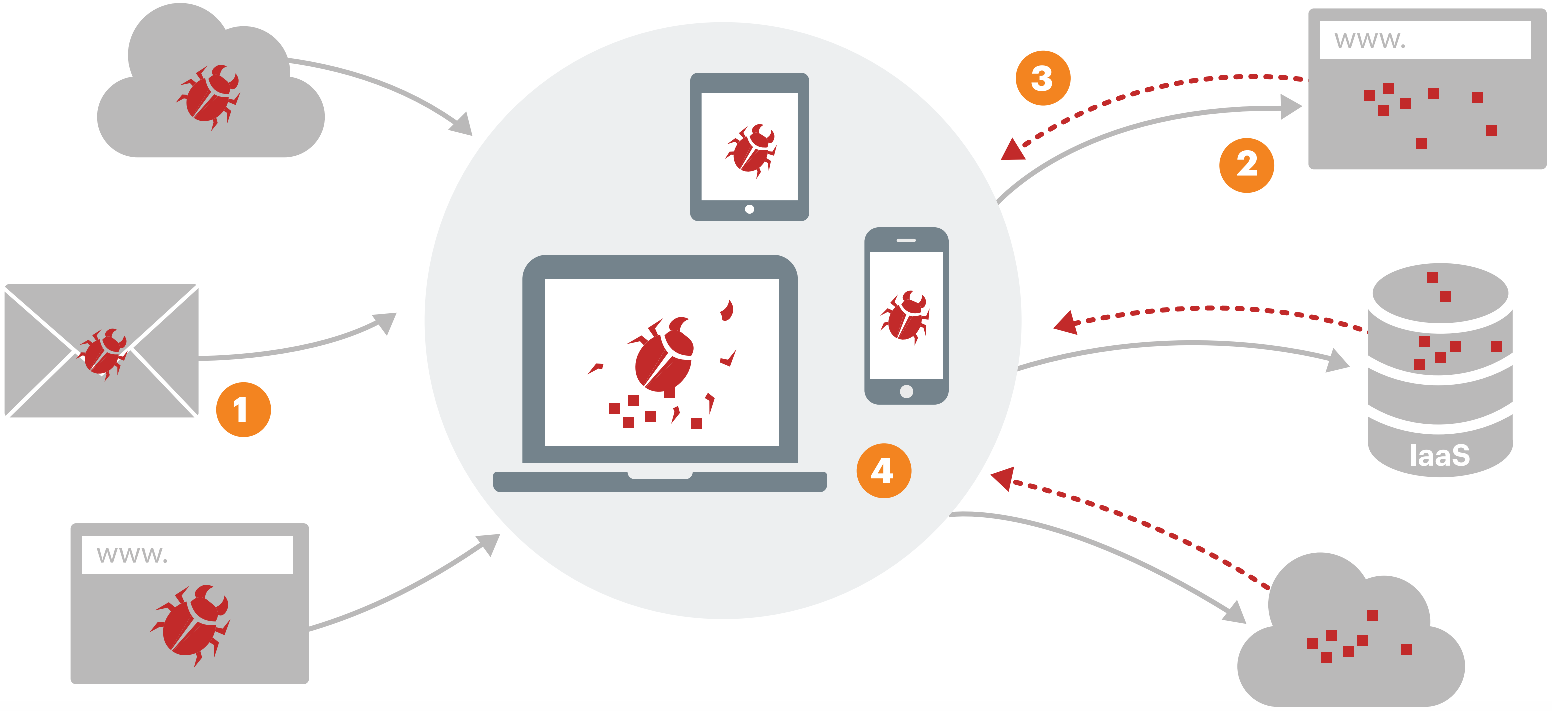
This quarter, we introduce the concept of a hybrid cloud and web threat, an increasingly relevant kind of threat faced by organizations as the lines between web and cloud services converge. The Netskope Threat Research Labs defines a hybrid threat as malware that uses a hybrid of both cloud and web services to deliver malicious payloads or perform an attack on a system or a user. These threats may be delivered in a variety of ways, from phishing emails to compromised websites, with command and control servers hosted in places like IaaS, cloud storage services, and websites. This quarter, the Netskope Threat Research Labs found and remediated hybrid cloud and web threats in 3.3 percent of customer tenants.

As hybrid threats involve both cloud and web, security solutions have a difficult time detecting them. A given security solution needs to scan the entirety of a file before coming to conclusions about it. Some may detect the web component while others only the cloud part -- but without full context across the kill chain, it's difficult to identify and remediate this kind of threat. Oftentimes, when a security solution detects only one portion of these fragmented threats and attacks, the actions are recognized as being innocuous (there's no reason to identify a call to an AWS server as malicious) when it's actually the setup to compromising a user. The example here is if a user has malware on his or her device that calls for downloads from Dropbox, URL 1, URL 2, an Amazon AWS server, and so on, the attack would not be detected. Only when the pieces are downloaded onto the device, decrypted, and compiled, will a malicious payload start executing.

The Netskope Threat Research Labs has found that the initial malware infection can be accomplished by a variety of methods. Users can get malicious phishing emails or download directly from a cloud storage service link shared by others. The latter is a prime example of the "fan-out" effect that we described in prior reports where synced folders can propagate malware-infected files to all users that the file is shared with. Another way a user can get the initial malware that initiates the fragmented attack is by visiting compromised websites. These websites may be legitimate websites that have been compromised by malicious ads or iframes. As the cloud and web blend together, we expect to see more of this – websites are increasingly dynamic and look more like cloud services as they use APIs to pull together content from various other sites and cloud services to deliver ads and content.

This quarter, the Netskope Threat Research Labs found that adware surged to first place with 31.7 percent of all detections. Backdoors dropped to second in detections with 16.9 percent, followed by Mac malware at 11.0 percent, mobile malware 15.3 percent, and generic detections 15.0 percent. The common ransomware delivery vehicles totaled 9.8 percent, consisting of Microsoft Office macros with 4.3 percent, Javascript 2.4 percent, PDF exploits 1.3 percent, and Flash exploits 0.3 percent. We broke out the pure ransomware category at 1.5 percent, encompassing all other delivery methods other than phishing emails, which are the most popular delivery vehicle for initiating a ransomware attack. Hybrid threats were not called out as they are cross-category threats, oftentimes encompassing multiple types of malware. High severity consisted of 69.2 percent of the detections while low was 30.8 percent. 27.8 percent of the malware-infected files were shared with others, including internal or external users or publicly.

Hybrid Cloud and Web Threats



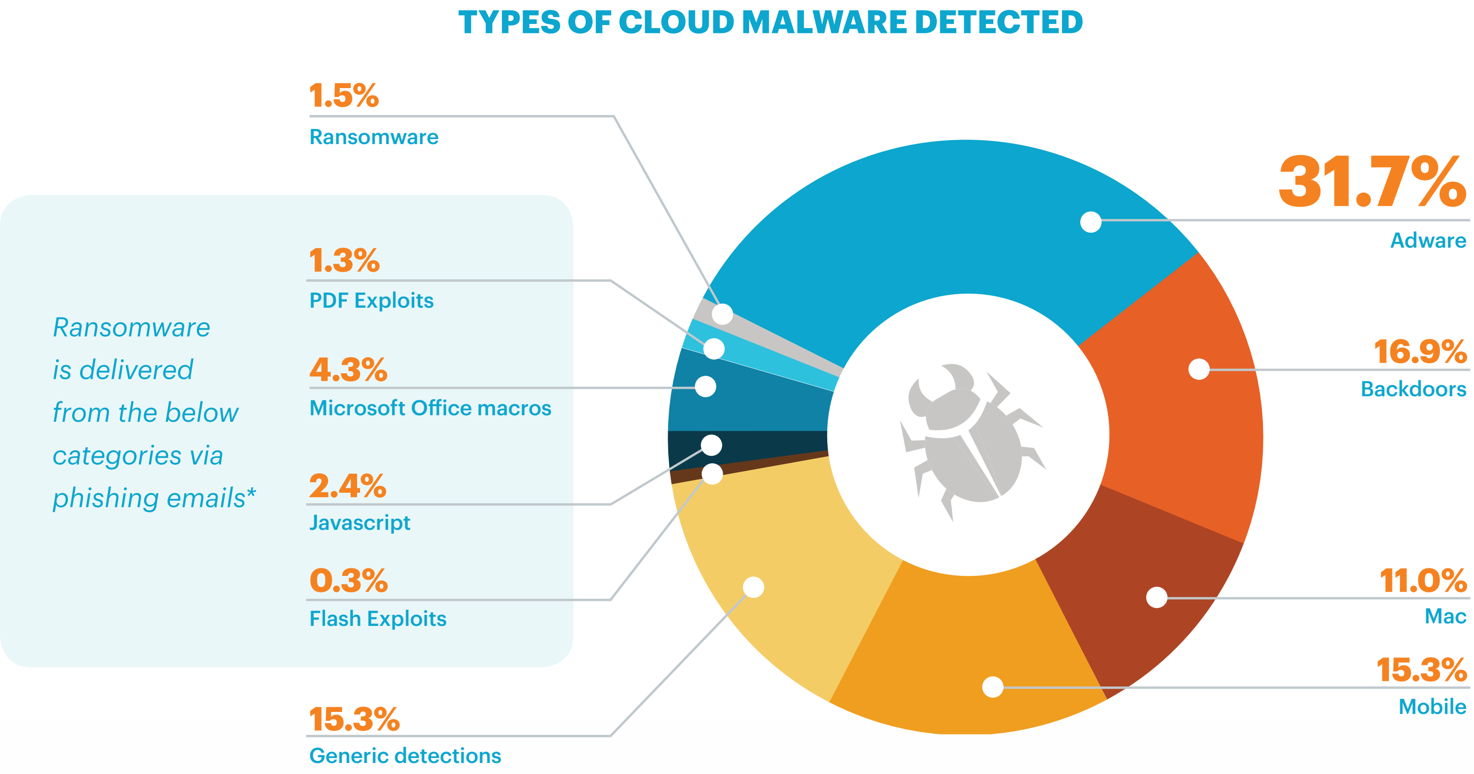
1 Malware infects user device via phishing email, compromised website, cloud service with infected file, etc.

2 Once malware is downloaded, it calls to various services like websites, cloud storage services, or even IaaS servers to download fragments of malicious code.

3 Malicious fragments are downloaded onto device with security solutions seeing these downloads as innocuous as they haven't been pieced together yet.

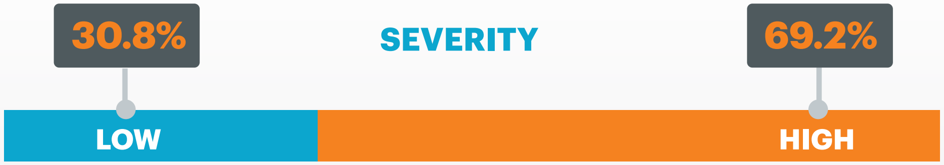
4 Initial malware decrypts and compiles the downloaded fragments to start an attack or whatever functions the malicious code is supposed to perform.

THREATS CONT.



*Ransomware is delivered from the below categories via phishing emails**

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



**We've added a category for pure ransomware as well, delivered through all other methods.*

GDPR-READINESS METRICS FOR CLOUD SERVICES

The deadline to comply with the EU GDPR is less than a year away. If they haven't already, organizations will need to understand the data flow of all PII in the cloud and secure that data. There has been little change in the GDPR-readiness metrics that the Netskope CCI tracks. The onus of compliance will fall heavily on organizations themselves in terms of finding the PII they process and touch and then implementing security and controls to comply with GDPR. Organizations that process EU citizens' data will need to ensure they are placing the appropriate security policies and processes to avoid fines that total 20 million euros or up to 4 percent of the organization's turnover, whichever is higher.

DATA OWNERSHIP TERMS

66.9% of cloud services do not specify that the customer owns the data in their terms of service

DATA ENCRYPTION AT REST

89.9% of cloud services do not support encryption of data at rest

DATA BACKUP IN OTHER GEOS

40.7% of cloud services replicate data in geographically dispersed data centers.

TOP CLOUD ACTIVITIES

The top cloud activities this quarter were send, create, login, edit, view, download, invite, upload, share, 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 app 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. Edit
3. Download

Top Activities in HR

1. Download
2. Create
3. Edit

Top Activities in Business Intelligence

1. Share
2. View
3. Download

Top Activities in Finance

1. Edit
2. Create
3. Download

Top Activities in Collaboration

1. Edit
2. Create
3. View

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

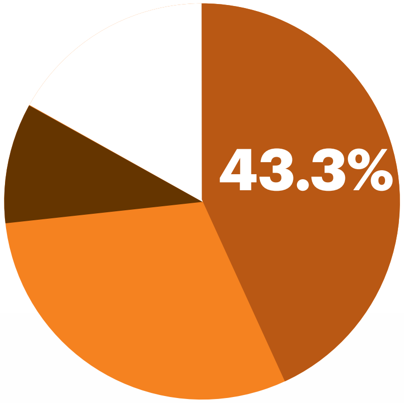
! Policy violation included in data loss prevention profile

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

CLOUD DLP POLICY VIOLATIONS

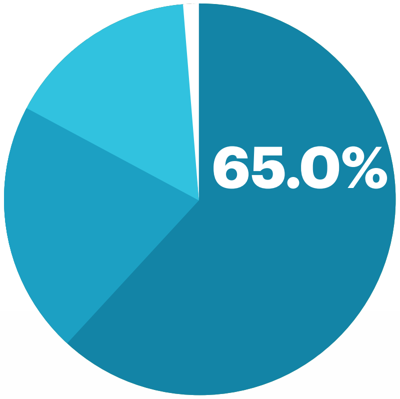
For cloud service category DLP violations this quarter, webmail remains the leader after jumping up to first last quarter with 43.3 percent of the violations. Cloud storage comes in at second with 30.6 percent. We call out collaboration services as a separate category – Slack and other collaboration services are fast-rising in popularity with Netskope customers and in general – making up 9.8 percent of the violations. Other cloud service categories combined to make up 16.3 percent. Collaboration services are increasingly replacing email functionality — organizations should remember to place DLP policies on these services as well as sharing files and collaborating within services like Slack and Microsoft Teams is easy and make employees more productive but lead to increased chances of sensitive data loss.

DLP violations by activity was similar as last quarter's trends with uploads making up the majority at 65.0 percent, followed by send 17.5 percent, download 16.2 percent, and other 1.3 percent. For types of DLP violations, we continue to see more widespread use of the Netskope GDPR DLP template. PII made the majority of type violations with 29.3 percent. PHI followed with 18.5 percent, source code 26.8 percent, PCI 3.6 percent, and other closed it out with 21.8 percent.



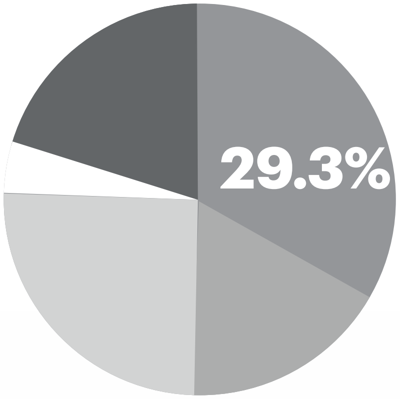
CATEGORY

- 🟥 Webmail **43.3%**
- 🟧 Cloud storage **30.6%**
- 🟫 Collaboration **9.8%**
- □ Other **16.3%**



ACTIVITY

- 🟦 Upload **65.0%**
- 🟦 Send **17.5%**
- 🟦 Download **16.2%**
- □ Other (including View) **1.3%**



TYPE

- ■ PII **29.3%**
- ■ PHI **18.5%**
- ■ Source Code **26.8%**
- □ PCI **3.6%**
- ■ Other (including Confidential and Profanity) **21.8%**

THREE QUICK WINS FOR ENTERPRISE IT

1 Secure users and devices against hybrid cloud and web threats with context-aware security solutions and controls.

2 Prepare for the impending GDPR deadline by understanding where all organizational data are and securing that data.

3 Evaluate popular collaboration services in use to enforce DLP controls and security policies.

netskope