JUNE
2016

WORLDWIDE
VERSION

CLOUD REPORT

3 OUT OF 4 CLOUD APPS IN USE NOT READY FOR GENERAL DATA PROTECTION REGULATION

Eleven Percent of Enterprises Have Detected Malware in Sanctioned Apps

REPORT HIGHLIGHTS

- Three-quarters of cloud apps in use lack key capabilities to comply with the upcoming European Union General Data Protection Regulation.
- Malware continues its rise in enterprise clouds, with an average of 11.0 percent of enterprises detecting malware in their sanctioned apps.
- 26.2 percent of malware files discovered in sanctioned apps are shared with internal or external users or publicly.
- Enterprises have an average of 935 cloud apps in use, a slight rise from 917 last quarter. The Microsoft Office 365 suite continues to lead the pack in top-used business productivity apps, with Office 365 Outlook.com, OneDrive for Business, SharePoint, Yammer, and Lync in the number 2, 3, 12, 19, and 20 spots, respectively.
- Cloud Storage apps dominate cloud DLP violations, with 73.6 percent of the total.

EXECUTIVE SUMMARY

In this Netskope Cloud Report™, we've compiled the most interesting trends on cloud app 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, 2016.

The focus of this quarter's report is on cloud apps' readiness to comply with the European Union General Data Protection Regulation (GDPR). With the legislation now fully ratified by member states, both data controllers (enterprises that own or have control over users' private data) and processors (organizations that process data on behalf of the controllers) will need to start preparations (if they haven't already!) to comply. Not only will enterprises need to ensure proper geographic bounds and security and privacy controls for their data in the cloud, but they will also have to sign data processing agreements with cloud service vendors. In this report, we are previewing the GDPR-readiness score that we will release shortly in the Netskope Active Platform. Our early findings indicate that 75.4 percent of all cloud apps are not ready for the GDPR, meaning they lack proper geography, security, and privacy controls as well as industry certifications to be considered ready to comply with the requirements of GDPR. When assessing cloud apps, enterprises will increasingly have to do the due diligence on cloud apps in use by employees and compensate for the lack of native controls.

In this report, we expand on our cloud malware findings. Last quarter, we shared that 4.1 percent of enterprises had detected malware in their sanctioned apps. This number has grown to 11.0 percent this quarter. These include JavaScript exploits and droppers, Microsoft Office macros, backdoors, mobile malware, spy- and adware, and Mac malware. For enterprises that detected malware, the range was from a single instance to several dozen. JavaScript exploits and droppers led by 63.3 percent, followed by Microsoft Office macros at 21.3 percent, backdoors at 4.9 percent, mobile malware at 4.3 percent, and spy- and adware, Mac malware, and other rounding out the data at 3.2 percent, 2.7 percent, and less than one percent, respectively. The majority of these detections - 73.5 percent - were categorized as "severe." Of note is that the JavaScript exploits and droppers and Microsoft Office macros categories often deliver ransomware, which currently is top-of-mind for many organizations. Finally, a shocking 26.2 percent of the malware files detected in sanctioned apps were shared with either internal or external users or publicly.

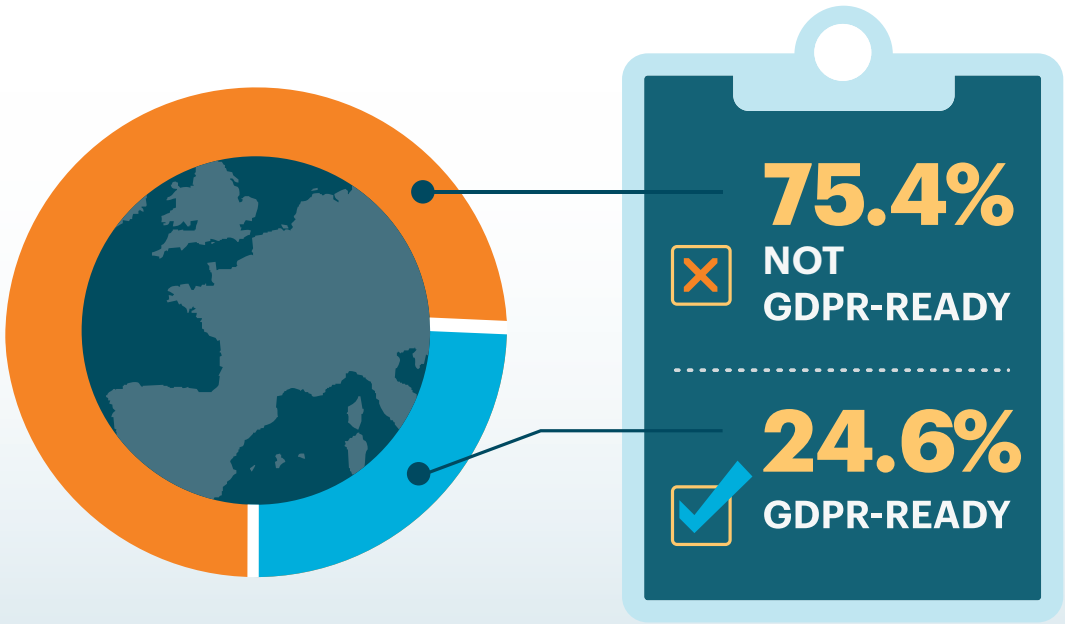
The average number of cloud apps in use per enterprise increased slightly to 935, compared with last quarter's 917. The Microsoft Office 365 suite continues to lead the pack in top-used business productivity apps. Office 365 Outlook.com, OneDrive for Business, SharePoint, Yammer, and Lync took the number 2, 3, 12, 19, and 20 spots, respectively. Similarly, the number of apps that are not enterprise-ready increased slightly from 94.0 percent to 94.6 percent.

Share is the top activity in the Cloud Storage and Business Intelligence cloud app categories, while edit is the leading activity in Finance. In HR, the top activity was create, but it was followed closely by edit, and download. Finally, create was the top activity in Collaboration. Knowing what activities are most common in each app category helps organizations know where their risks may lie, and where to start with policy creation. For example, after reviewing sharing in Cloud Storage and Business Intelligence apps, IT may choose to create a watchlist for all sharing outside of the organization. Similarly, after reviewing edit activities in Finance, a risk and compliance officer may choose to enforce a policy requiring user justification for any data modification within any Finance app.

In which app categories and for which activities did the policy violations occur? Cloud Storage drove the most violations by app category, contributing 73.6 percent, followed by Webmail, at 22.1 percent. Download was the most popular violating activity, at 53.0 percent of all violations, followed by upload and share at 24.0 percent and 22.7 percent, respectively. Adding an additional layer of policy visibility - whether those violations also involved data loss prevention (DLP) - personally-identifiable information (PII) violations accounted for 43.7 percent of all DLP violations. Protected health information (PHI) contributed to 29.4 percent, source code 24.1 percent, and “confidential” and other regular expressions 2.8 percent.

THREE QUARTERS OF CLOUD APPS NOT READY TO COMPLY WITH THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)

This spring, European Union member states fully ratified the EU General Data Protection Regulation (GDPR). With two short years to comply or face stiff penalties (of up to four percent of annual worldwide revenue or 20 million Euros, whichever is greater), organizations are now starting to get serious about complying. For many organizations, a significant hurdle is cloud app usage. Because most organizations have no visibility into the hundreds (or thousands) of apps that are being used in their organization - much less controls over those apps - they will have difficulty even taking their first steps toward GDPR compliance. Netskope's R&D team evaluates more than 22,000 cloud apps and publishes an enterprise-readiness score across 55+ parameters adapted from the Cloud Security Alliance's Cloud Controls Matrix. Beyond a more general enterprise-readiness score, Netskope will begin publishing a GDPR-specific readiness score based on metrics across the following eight requirements: 1. Geographic requirements; 2. Data retention; 3. Data privacy; 4. Terms of data ownership; 5. Data protection; 6. Data processing agreement; 7. Auditing; and 8. Certifications. For each question, we assign rewards and penalties for the inclusion or lack of each capability, and normalize the score to a total of 100 points. Below is a sneak peek at this analysis. We grouped apps into those scoring below 50 (which we define as low), 50-70 (defined as medium) and above 70 (defined as high) to give readers of this report a sense for the relative readiness of cloud apps when it comes to GDPR compliance. We acknowledge this is not a perfect measure; it doesn't take into account an organization's use of an app or countermeasures that they may have in place, and our scoring process and weightings may not be appropriate for every environment. That said, it is a useful starting point for determining apps' relative readiness for EU GDPR compliance, and where the gaps exist.



GDPR-READINESS METRICS AND WHAT THEY MEAN

- **Geographic requirements.** Does the cloud app ensure that EU citizens' PII is kept in data centers in the EU?
- **Data retention.** When a customer discontinues use of the cloud app, does the app make the data available for customer download, and then fully and quickly erase the data?
- **Data privacy.** Does the cloud app have mechanisms in place to protect data privacy, such as assurances that data won't be shared with third parties?
- **Ownership terms.** Does the cloud app clearly state that the customer owns the data in its terms of service?
- **Data protection.** Does the cloud app have data protections in place, such as strong encryption and key management?
- **Data Processing Agreement (DPA).** Is there a Data Processing Agreement in place between the data processor and controller?
- **Audit.** Does the cloud app make data access audit logs available?
- **Certification.** Does the cloud app have data center certifications in place, such as SOC-2?

Based on this framework, we find that 24.6 percent of cloud apps fall into the "high" GDPR readiness group, 47.6 percent into the "medium" group, and 27.8 percent into the "low" group. Said another way, three-quarters of cloud apps are not ready to comply with GDPR. This tells us that, beyond cloud-consuming organizations having their work cut out for them, cloud app vendors themselves have a long way to go to comply with the new law.

It's worth noting that even a "high" GDPR-readiness level may not mean an app 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 apps are being used in a compliant manner. Remember, there is a shared responsibility between cloud app 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 apps. For example, a Cloud Storage app 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 app cannot protect against that compliance violation.

Overall GDPR Readiness:

27.8%
LOW

47.6%
MEDIUM

24.6%
HIGH

SAMPLE GDPR-READINESS METRICS, AND HOW APPS STACK UP

DATA EXPORT REQUIREMENTS

11.6% of cloud apps don't support data export upon termination of service

DATA RETENTION REQUIREMENTS

46.4% of cloud apps keep data for longer than one week upon termination of service

DATA OWNERSHIP TERMS

62.3% of cloud apps do not specify that the customer owns the data in their terms of service

STATE OF CLOUD THREATS AND MALWARE

In last quarter's Netskope Cloud Report, we shared our preliminary analysis of malware in the cloud. This quarter, the percentage of enterprises that have sanctioned apps containing malware increased from 4.1% to 11.0%. As we augment our scanning of sanctioned cloud apps to include unsanctioned ones, we expect this number to increase in future cloud reports.

What malware did we detect in enterprises' sanctioned apps? We've classified them into six main categories.

1. **JavaScript exploits and droppers.** These attacks arrive by web exploit kits or are sent through email or cloud services. An executable is downloaded and run on the user's machine. Increasingly, these executables are used to deliver ransomware, which encrypts users' files or entire systems, and encrypted data can propagate via sync clients.
2. **Microsoft Office Macros.** These can arrive via email or a cloud service with a deceptive attachment or link in the form of Microsoft Word or Excel files such as "resume.doc" to trick a user into opening them. When the file is opened, an option to "Enable Macro" pops up. Once enabled, malware is downloaded onto the device.
3. **Backdoors.** These executables give attackers full, unauthorized access to users' devices and applications.
4. **Mobile malware.** Mobile devices can be infected with malware designed to disable a mobile device, allow a malicious user to remotely control the device, or to steal personal information stored on the device.
5. **Spy- and Adware.** These types of malware steal passwords and account credentials, as well as monitor user activity and serve spam ads to the user.
6. **Mac malware.** These malware instances were a surprise to us. Apple's popularity means that the device is increasingly a target for hackers.

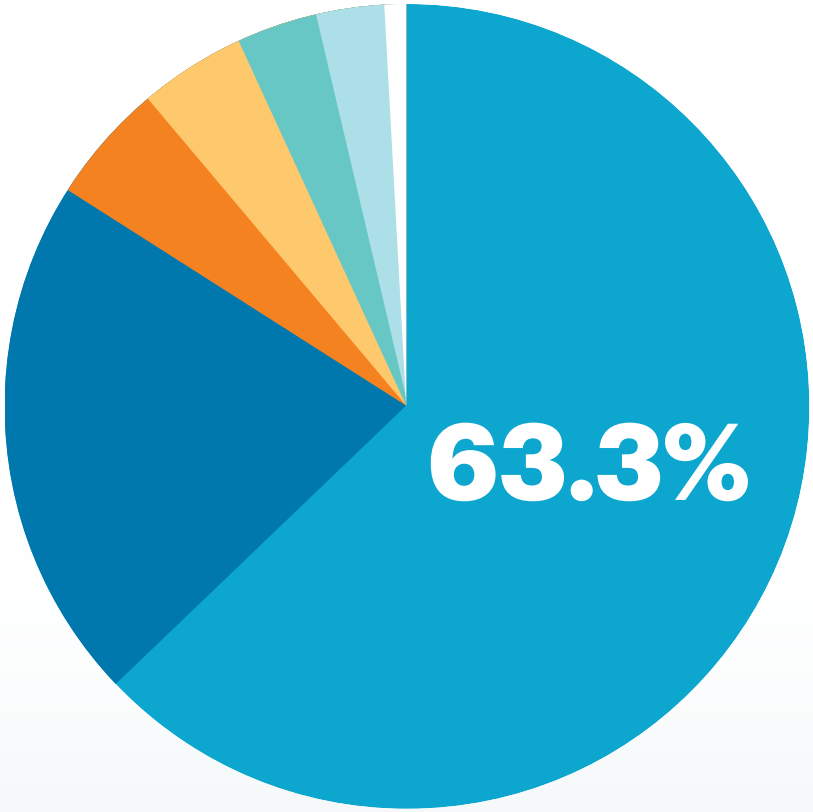
What's interesting is that a full 26.2 percent of the detected malware files were in folders that were shared (whether publicly, across the enterprise, or with at least one other person), demonstrating the ease of propagation and risk of malware in the cloud.

Beyond detecting malware in enterprises' sanctioned apps, we have also assigned those detections a severity level based on the extent to which they affect user privacy and computer security and cause damage. 73.5 percent of detections were categorized as "high" severity, 8.3 percent were "medium," and 18.2 percent were "low."

11% OF ENTERPRISES HAVE SANCTIONED APPS THAT HAVE AT LEAST ONE INSTANCE OF MALWARE

Malware Detection Types

- JavaScript exploits and droppers **63.3%**
- Microsoft Office Macros **21.3%**
- Backdoors **4.9%**
- Mobile malware **4.3%**
- Spy- and adware **3.2%**
- Mac malware **2.7%**
- Other **>1%**



Severity

73.5 percent high severity

8.3 percent medium severity

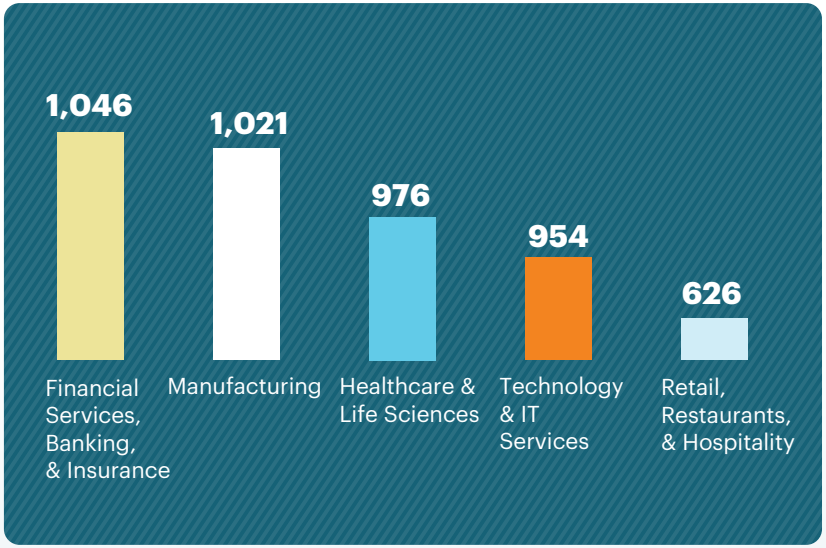
18.2 percent low severity

A shocking **26.2** percent of malware detected in sanctioned apps were files that had been shared with others, including internal or external users or publicly.

935 CLOUD APPS PER ENTERPRISE

The average number of apps per enterprise increased slightly from last quarter, growing from 917 to 935. 94.6 percent of those apps are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI).

The Marketing app category leads the pack with 97 apps per enterprise, followed by Collaboration and Finance at 64 and 56, respectively. Most categories have greater than 90 percent of non enterprise-ready apps, per the Netskope CCI. This is true of Finance, which may hold sensitive financial data and user personally-identifiable information (PII). This is of note for companies that must comply with Sarbanes-Oxley; keeping a cloud audit trail of who is accessing, trying to access, editing, and deleting data that can impact financial results is critical for compliance. Not surprisingly, the Cloud Storage category contains the greatest amount of enterprise-ready apps as Cloud Storage apps are often heavily scrutinized by large enterprises.



CATEGORY	# PER ENTERPRISE	% NOT ENTERPRISE-READY
Marketing	97	97%
Collaboration	64	90%
Finance / Accounting	56	97%
Productivity	53	99%
HR	48	97%
CRM / SFA	35	96%
IT/Application Management	29	95%
Software Development	28	92%
Cloud Storage	27	76%
Social	23	90%

MICROSOFT MAINTAINS LEAD IN PRODUCTIVITY APPS

Microsoft has solidly emerged as the top vendor in terms cloud productivity app usage within enterprises. As with last quarter's Netskope Cloud Report, Microsoft has seven apps on the top 20 apps list, five of which are from the Office 365 suite. Office 365 Outlook.com, OneDrive for Business, SharePoint, Yammer, and Lync took the number 2, 3, 12, 19, and 20 spots, respectively. This has implications for ecosystem apps, or apps that integrate and share data with the Office 365 suite. If security teams monitor and enforce policies in the Office 365 suite, they should extend those policies to the myriad apps that integrate with it. Facebook, per usual, is at the top of the list, we believe primarily for personal use.

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

TOP CLOUD ACTIVITIES

The top activities in the Netskope Active Platform are send, create, edit, login, download, view, share, post, upload, and invite, respectively. Netskope normalizes more than 50 possible cloud activities across apps within categories and even across categories, so whether a user shares a file from a Cloud Storage app 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 app activities in the context of the app category, we call out the top three activities besides login for each of five important business app categories, Cloud Storage, HR, Business Intelligence, Finance, and Collaboration.

Top Activities in Cloud Storage Apps

1. Download
2. Share
3. View

Top Activities in HR Apps

1. Create
2. Edit
3. Download

Top Activities in Business Intelligence Apps

1. Share
2. Upload
3. View

Top Activities in Finance Apps

1. Edit
2. Create
3. Upload

Top Activities in Collaboration Apps

1. Create
2. Download
3. View

TOP POLICY VIOLATIONS IN THE NETSKOPE ACTIVE PLATFORM

Beyond measuring usage and activity, we also look at policy violations within cloud apps. Policies can be enforced based on a number of factors, including user, group, location, device, browser, app, instance, category, enterprise-readiness score, DLP profile, activity, and more. Through data abstraction and normalization of those factors, we're able to discern the apps, 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 apps with someone outside of the company, and blocking unauthorized users from modifying financial fields in Finance apps.

Here are the top activities globally that constituted a policy violation per cloud app category, with DLP violations noted where they apply. Just as activities can vary between apps, 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	Download	Upload	Post	View	Login	Send	Share	Delete	Edit
Cloud Storage	1!	5!	8	4	2	–	3	7	6
Collaboration	1!	4!	8!	2	7	9	3	6	5
CRM and SFA	5!	7!	3!	4	1	9	2	8	6
Finance/ Accounting	6	3	–	7	2	–	5	4	1
HR	3	4	–	5	1	–	7	6	2
Productivity	2	6!	–	7	1	–	4	5	3
Social	7!	6!	3!	2	1	9	8	5	4
Software Development	1	5	9	2	4	–	7	6	3
Webmail	4!	6!	3!	7	9	1!	8	5	2

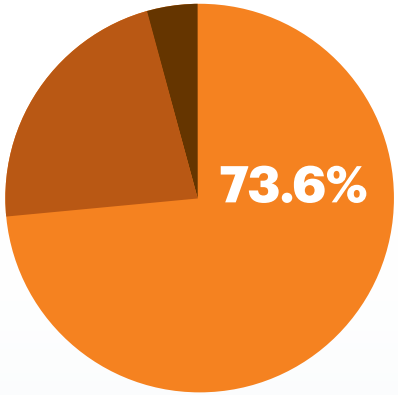
! Policy violation included in data loss prevention profile

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

CLOUD DLP POLICY VIOLATIONS

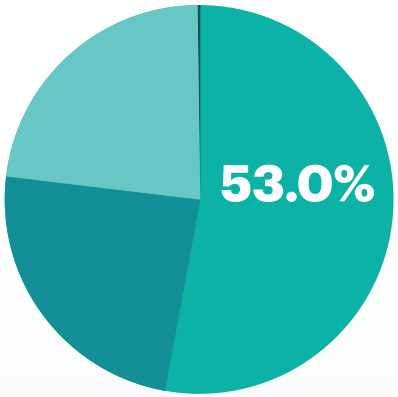
Cloud Storage apps dominate cloud DLP violations, making up 73.6 percent of all of the violations. Webmail follows this at 22.1 percent, with the other app categories behind in much lower percentages. In terms of activities, download triggers the most DLP violations at over 50 percent, followed by upload and share. This is expected as the top three activities are among the most risky in terms of leaking sensitive data and our customers craft policies around these major activities to ensure safe consumption of both sanctioned and unsanctioned cloud apps.

Finally, in the type of DLP violations, PII makes up the highest number at 43.7 percent, followed by protected health information PHI at 29.4 percent, and, finally, source code at 24.1 percent. In prior quarters, PHI made up the bulk of the violations. We believe that, as organizations' use of cloud security matures, they are enforcing policies on multiple data profiles. Since PII is common across many regulatory regimens, we aren't surprised to see it represented as the top violation type, and expect to see it in even greater numbers in the future. We also believe that as organizations move beyond low-hanging fruit of protecting regulated data to protecting intellectual property, we will see broad "confidential" violations as a larger part of the overall mix.



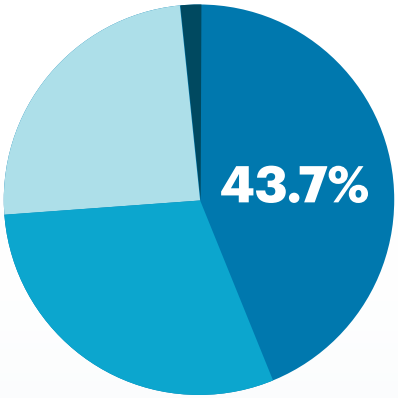
CATEGORY

- Cloud Storage **73.6**
- Webmail **22.1%**
- Other (e.g., CRM/ SFA, Social, and Collaboration) **4.3%**



ACTIVITY

- Download **53.0%**
- Upload **24.0%**
- Share **22.7%**
- Other (e.g., View) **.3%**



TYPE

- PII **43.7%**
- PHI **29.4%**
- Source Code **24.1%**
- Other (e.g., Confidential, Profanity, PCI) **2.8%**

THREE QUICK WINS FOR ENTERPRISE IT

1. With the EU GDPR ratified and compliance expected by 2018, enterprises must discover the cloud apps in use in their organization, and ensure that those apps meet key requirements of the regulation.

2. Threats and malware propagate in the cloud. Enterprises should gather threat intelligence about their cloud environments as well as scan for and remediate malware in cloud apps.

3. With DLP violations occuring in Cloud Stoage, Webmail, and several other app categories, enterprises should e-discover their regulated or sensitive content in those and other business-critical apps.