OCTOBER 2018

netskope

CLOUD REPORT

IDENTITY AND ACCESS MANAGEMENT TOP CATEGORY OF CONCERN FOR I/PAAS DEPLOYMENTS IN ORGANIZATIONS: A LOOK AT AMAZON WEB SERVICES (AWS)

71.5% of CIS Benchmark Violations in AWS Occur in Identity and Access Management Category

REPORT HIGHLIGHTS

- 71.5 percent of CIS Benchmark violations in AWS occur in Identity and Access Management category
- 64.1 percent of DLP activity violations in cloud infrastructure occur with downloads
- Enterprises have an average of 1,246 cloud services in use, an increase from 1,181 last report

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 Security Cloud™. Report findings are based on usage seen across millions of users in hundreds of accounts globally.

In average number of cloud services in use per enterprise, there was an increase to 1,246 from 1,181 last report.

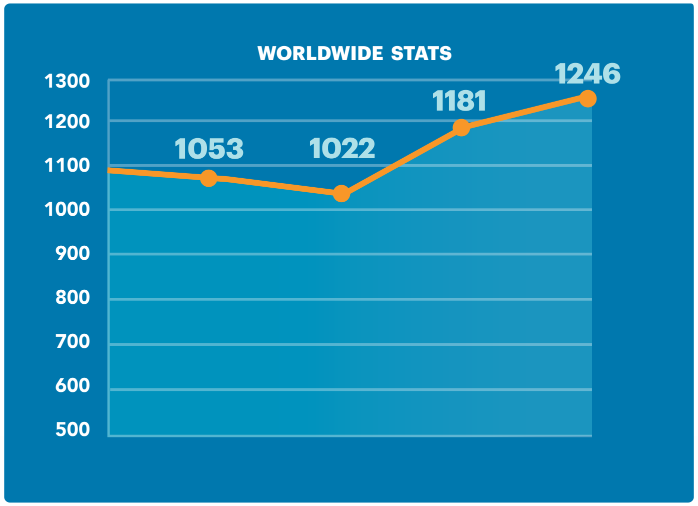
Cloud infrastructure (e.g., IaaS, PaaS) was the focus of this report. We found that 71.5 percent of violations were in the Identity and Access Management category, Monitoring followed with 19.0 percent, Networking with 5.9 percent, and Logging with 3.6 percent. Common violations in the IAM category involved role access to resources and their configurations. EC2 led the way in the resource cut of violations at 66.2 percent of the violations, followed by CloudTrail 15.2 percent, S3 10.9 percent, IAM 4.5 percent, and "other" 3.2 percent. In severity, 86.3 percent of violations were of medium severity, 9.1 percent high, 4.0 percent critical, and 0.6 percent low. Netskope categorizes severity of violations across the CIS benchmark with a custom framework to help administrators prioritize which violations to address first.

Log in, send, edit, create, view, download, share, upload, view, and delete, were the top cloud activities this quarter respectively. By cloud service categories, the results were similar to previous reports with activities involving sharing, uploading, and downloading an important focus for security teams when crafting policies to reduce risk for the organization.

In DLP violations, 54.0 percent of violations were in cloud storage services, webmail 35.3 percent, collaboration services 10.1 percent, and other (including cloud infrastructure) 0.6 percent. Of note is that cloud infrastructure DLP policies are on the rise across our customer and prospect base due to the rise in use of these services. We separate out cloud infrastructure DLP violations this quarter to show the areas and activities in which security teams are focusing their DLP policies. Similar to the entire category, download and upload were the major activities with violations with 64.1 percent and 35.7 percent, respectively. Other rounded the numbers out at 0.2 percent.

ENTERPRISES USE AN AVERAGE OF 1,246 CLOUD SERVICES

This report had an increase of 5.5 percent in average amount of cloud services in use per enterprise, compared with 1,181 in our last report. 92.7 percent of these services are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence Index™ (CCI).



CATEGORY	# PER ENTERPRISE	NOT ENTERPRISE-READY
HR	175	96%
Marketing	170	98%
Collaboration	110	83%
Finance/Accounting	76	94%
CRM	76	93%
IT Service/Application Management	31	93%
Cloud Storage	28	67%
Social	26	92%

IDENTITY AND ACCESS MANAGEMENT A DIFFERENT BEAST FOR CLOUD INFRASTRUCTURE

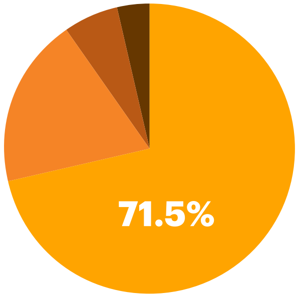
The focus of this report is on public cloud infrastructure or I/PaaS, as its use across organizations has been growing rapidly. DevOps teams are using various I/PaaS to rapidly deploy apps and services across the organization. Amazon Web Services, Google Cloud Platform, and Microsoft Azure are the main three in use across Netskope customers and prospects. And with resources being created and also spun down constantly across public cloud infrastructure, we recommend security teams put tools in place to continuously monitor their deployments to ensure proper security settings are in place to protect sensitive data, defend against threats and breaches, and ensure compliance. While we see many organizations going with the multi-cloud approach and using combinations of cloud infrastructure vendors, we focus on AWS in this report with statistics based on the CIS Benchmark for AWS.

By category in the CIS benchmark for AWS, the majority of violations was in the Identity and Access Management category at 71.5 percent. Monitoring followed with 19.0 percent, Networking with 5.9 percent, and Logging with 3.6 percent. This may indicate that while many organizations have controls around cloud services and implemented things like multi-factor authentication (MFA) and single sign-on solutions, I/PaaS identity and access policies still need to be set. Many of the IAM violations involve instance rules and access to resources or password policy requirements—simple fixes that may not have been a focus when first setting up roles and instances. There has been a lot of focus on micro-segmentation security technologies for I/PaaS workloads, but of note are simple IAM policies that can be addressed directly in AWS without an external security solution.

In resource type violations to the CIS benchmark for AWS, EC2 led the way at 66.2 percent of the violations, followed by CloudTrail 15.2 percent, S3 10.9 percent, IAM 4.5 percent, and other 3.2 percent. This relates to the previous numbers—EC2 instances should have proper IAM roles for access.

IDENTITY AND ACCESS MANAGEMENT A DIFFERENT BEAST FOR CLOUD INFRASTRUCTURE (CON'T)

Finally, in severity, 86.3 percent of violations were of medium severity, 9.1 percent high, 4.0 percent critical, and 0.6 percent low. Netskope categorizes severity of violations across the CIS benchmark with a separate framework to help customers and prospects identify which areas to focus on first. The critical violations mostly focus on networking violations like ensuring no security groups allow ingress from 0.0.0.0/0 to port 22 and the like to prevent data exposure risks such as having security buckets open to the world.



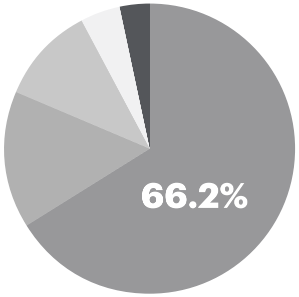
BY CATEGORY

■ Identity and Access Management **71.5%**

■ Monitoring **19.0%**

■ Networking **5.9%**

■ Logging **3.6%**



BY RESOURCE

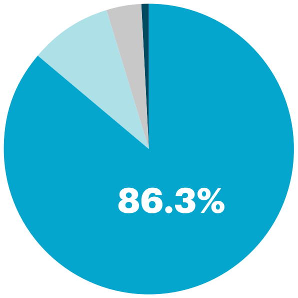
■ EC2 **66.2%**

■ CloudTrail **15.2%**

■ S3 **10.9%**

■ IAM **4.5%**

■ Other (config., KMS, RD, CloudWatch) **3.2%**



BY SEVERITY

■ Critical **86.3%**

■ High **9.1%**

■ Medium **4.0%**

■ Low **0.6%**

TOP CLOUD ACTIVITIES

The top cloud activities this quarter were log in, send, edit, create, view, download, share, upload, view, 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. Invite
2. View
3. Share

Top Activities in HR

1. Download
2. Create
3. Edit

Top Activities in Business Intelligence

1. View
2. Download
3. Share

Top Activities in Finance

1. Create
2. Edit
3. Upload

Top Activities in Collaboration

1. View
2. Edit
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, 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	4 !	3 !	1	8 !	9	5	6 !	2
Customer Relationship Management	8	5 !	4	1	7	9	2	6 !	3
Finance/ Accounting	4	6	3	1	–	–	7	5	2
HR	5	3 !	4	1	–	–	7	6 !	2
I/PaaS	6	2 !	4 !	1	–	–	–	5 !	3
Social	6	7 !	5	2	3 !	–	–	4 !	1
Webmail	6	4 !	2	8	–	1 !	7	5 !	3

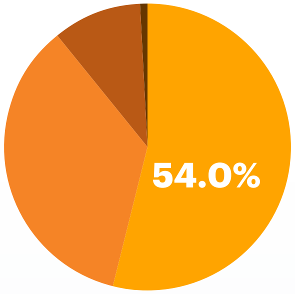
! Policy violation included in data loss prevention profile

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

CLOUD DLP POLICY VIOLATIONS

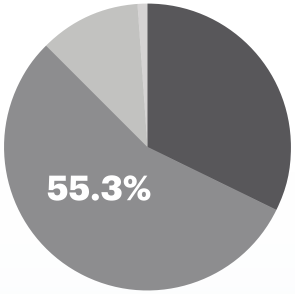
For now, most DLP violations still occur across cloud storage services and webmail, but IaaS solutions have increasingly become a focus for DLP policies across organizations due to the sensitive data stored in places like S3 buckets or Azure Blob storage. Besides misconfigurations across CIS benchmarks, Netskope customers have increasingly placed DLP and threat policies across the storage components of I/PaaS to ensure the organization is compliant and has additional protection against hackers. With an increasing amount of hacks and malware related to I/PaaS, we recommend security teams evaluate current security solutions to see if they're enough protection and to simplify with platform solutions that can be used across SaaS, I/PaaS, and web to reduce operational overhead and complexity. This report has 54.0 percent of cloud DLP violations from cloud storage, webmail 35.3 percent, collaboration services 10.1 percent, and other (including I/PaaS) 0.6 percent.

In DLP violations by activity, uploads made up the majority with 55.3 percent, followed by downloads with 32.4 percent, send 11.2 percent, and other 1.1 percent. We separate out I/PaaS DLP violations this quarter to show the areas and activities in which security teams are focusing their DLP policies. Similar to the entire category, download and upload were the major activities with violations with 64.1 percent and 35.7 percent, respectively. Other rounded the numbers out at 0.2 percent.



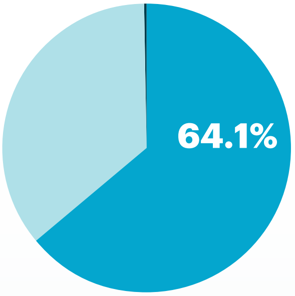
CATEGORY

- 🟧 Cloud Storage **54.0%**
- 🟧 Web Mail **35.3%**
- 🟫 Collaboration **10.1%**
- 🟫 Other (including I/PaaS) **0.6%**



ACTIVITY

- ■ Upload **55.3%**
- ■ Download **32.4%**
- ■ Send **11.2%**
- ■ Other (including View) **1.1%**



IAAS ACTIVITY VIOLATIONS

- 🟦 Download **64.1%**
- 🟦 Upload **35.7%**
- 🟦 Other (including edit) **0.2%**

THREE QUICK WINS FOR ENTERPRISE IT

1 Place DLP policies and security controls over activities like downloading sensitive information from IaaS solutions to secure increasing use of the public cloud.

2 Assess the security of your IaaS environment continuously against best practices so you can quickly identify and remediate risks and potential vulnerabilities.

3 Consider using the same security profiles, policies, and controls across SaaS, IaaS, and web services to reduce complexity.

netskope