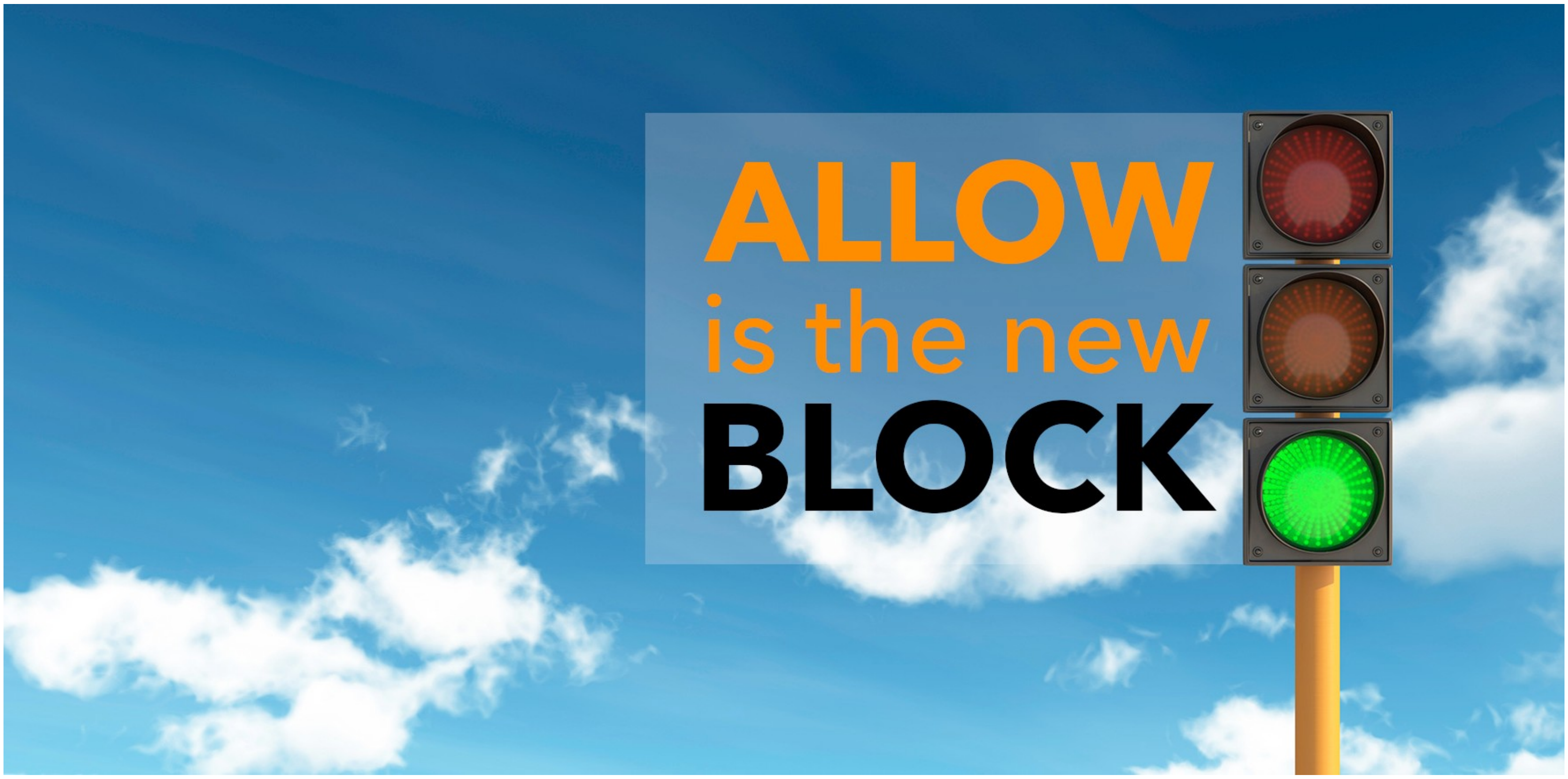
netskope



"Allow is the New Block" in Action: 10 Alternatives to Heavy-Handed Cloud App Control

“Allow is the New Block”

“Allow is the New Block” is a philosophy we live by at Netskope. It encapsulates our view on cloud enablement and reflects our product capabilities. But it’s more than just a glib catch-phrase. We believe in it and there’s real meaning and substance behind it.

For as long as the term “Shadow IT” has existed, technology vendors have encouraged IT professionals to uncover unsanctioned IT in their organizations so they can block it. And if you think about things from a purely security-oriented point-of-view, blocking makes a lot of sense. But we, and our customers, are taking a different tack. Our point of view is that blocking any useful technology doesn’t work and ultimately does the IT organization and the business a disservice. Cloud apps like Box, Dropbox, Jira, NetSuite, and Workday help people get their jobs done more efficiently and flexibly, and people will always find ways to use cloud apps, even if it means going outside of enterprise policy.

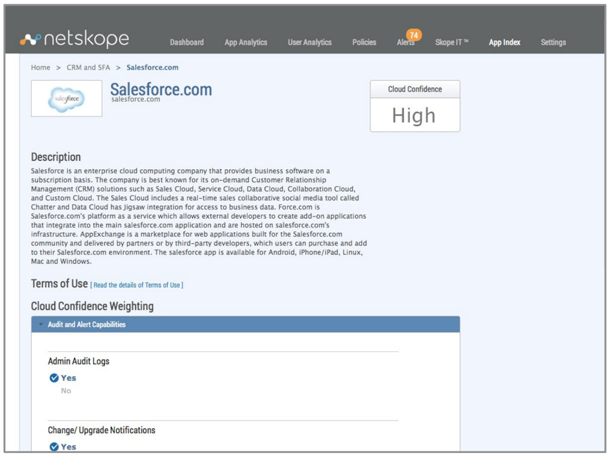
Our view is that with a little diligence, the right data, and the ability to enforce policy in a very precise manner, enterprise IT can eliminate the catch-22 of enabling the cloud while protecting the enterprise. By looking closely at cloud app usage, using granular policies to shape behavior, and using data to have a conversation with users and lines of business, they are eschewing heavy-handed controls for a more nuanced and effective approach.

10 Alternatives to Heavy-Handed Cloud App Controls

Below are ten best practices we generalize from the thoughtful and creative approach our customers are taking.

1. Evaluate app risk

After discovering cloud apps in their environment, many of our customers evaluate the risk of those apps. They use the Netskope Cloud Confidence Index™ (CCI) to give them an enterprise-readiness score based on objective criteria. For a low-confidence app, they then evaluate the app based on how it is used in the enterprise. Is it used for high-value or mission-critical activities or does it handle sensitive data? It is the combination of an app’s enterprise-readiness score and the organization’s unique usage of that app that defines that app’s risk. For risky apps, these customers may limit certain activities in the app or partner with the user or line of business to select a less-risky app that offers similar functionality. If not, they may simply let the app continue and monitor or exert mitigating controls. This is especially important for the apps they don’t procure or administer, but are still broadly used in the enterprise.



Home > CRM and SFA > Salesforce.com

Salesforce.com
salesforce.com

Cloud Confidence
High

Description
Salesforce is an enterprise cloud computing company that provides business software on a subscription basis. The company is best known for its on-demand Customer Relationship Management (CRM) solutions such as Sales Cloud, Service Cloud, Data Cloud, Collaboration Cloud, and Custom Cloud. The Sales Cloud includes a real-time sales collaborative social media tool called Chatter and Data Cloud has Jigsaw integration for access to business data. Force.com is Salesforce.com’s platform as a service which allows external developers to create add-on applications that integrate into the main salesforce.com application and are hosted on salesforce.com’s infrastructure. AppExchange is a marketplace for web applications built for the Salesforce.com community and delivered by partners or by third-party developers, which users can purchase and add to their Salesforce.com environment. The salesforce app is available for Android, iPhone/iPad, Linux, Mac and Windows.

Terms of Use [Read the details of Terms of Use]

Cloud Confidence Weighting

Audit and Alert Capabilities

Admin Audit Logs
✓ Yes
No

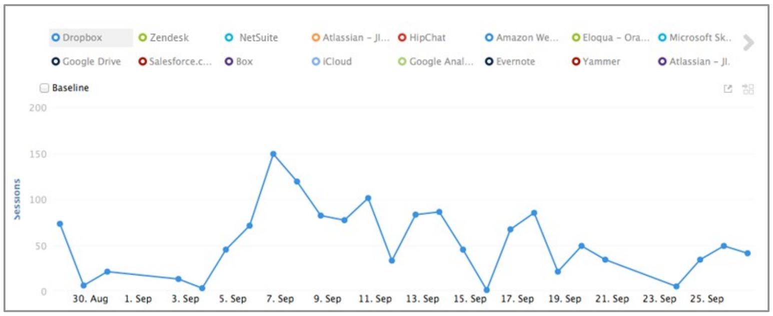
Change/ Upgrade Notifications
✓ Yes

2. Monitor usage

Many of our customers go beyond discovering cloud apps to understand what people are doing in them. One Netskope customer in the media industry employs a usage framework to evaluate the scope, business case, and risk of the app. IT measures app user counts and usage volume to ascertain scope. For heavily-used apps, they identify activities (e.g., sharing, downloading, editing, and administrative activities), and build a business case to either support the app or, in the case of app overlap, suggest consolidation. Finally, they look at usage through a risk lens, assigning each activity a risk level. When they find an app in which users are performing high-risk activities, they set a policy blocking the risky activity.

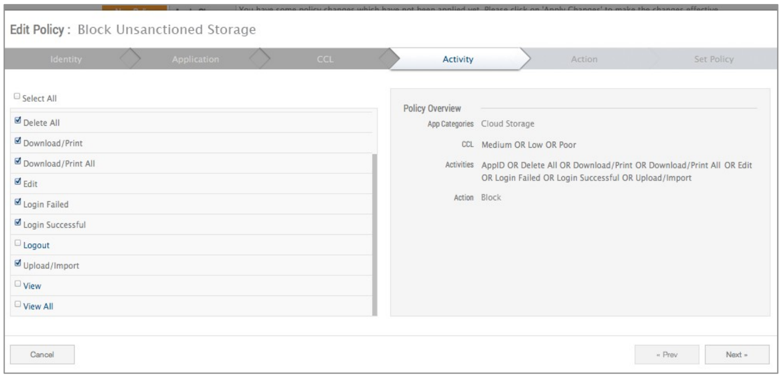
3. Look for anomalies

The above example highlights the importance of looking at behaviors within apps, not just the presence of an app. Some questions our customers ask when they use our solution is: What is the usage baseline of this app, and are there spikes in usage or activity? Are there more sessions than normal in a given time period? Excessive downloading? People logging in from locations they shouldn't be, or from two locations at once? These behaviors can signal risky behavior or even an external attack.



4. Block an activity, not an app

Some technology vendors encourage IT to uncover unsanctioned apps so they can shut them down. This sledgehammer approach rarely works and pits IT against the business in a negative way. Rather than block an app wholesale, several of our customers analyze the activities within the apps that represent the most risk (e.g., downloading to a mobile device, sharing with someone outside of the company) and block them. This lets them shape the activity to mitigate risk. Key to this is that they do this for not just the apps they manage but especially for the ones they don't.


You have some policy changes which have not been applied yet. Please click on 'Apply Changes' to make the changes effective
Identity
Application
CCL
Activity
Action
Set Policy
Cancel
« Prev
Next »

Edit Policy : Block Unsanctioned Storage

☐ Select All
☑ Delete All
☑ Download/Print
☑ Download/Print All
☑ Edit
☑ Login Failed
☑ Login Successful
☐ Logout
☑ Upload/Import
☐ View
☐ View All

Policy Overview

App Categories Cloud Storage
CCL Medium OR Low OR Poor
Activities AppID OR Delete All OR Download/Print OR Download/Print All OR Edit OR Login Failed OR Login Successful OR Upload/Import
Action Block

5. Protect data in context

Adopters of data leakage prevention solutions – or any detection technologies for that matter – know full well that too many false positives erode the value of a solution. As our customers think about cloud data loss prevention, they are being smart about context. Rather than just detect patterns or key words, they are using Netskope to define granular contextual situations incorporating user, group, app category, location, device, and activity (such as upload or share) that help narrow the scope of where a data breach is likely to occur. This helps them increase their accuracy when they do apply data loss prevention techniques such as blocking or encrypting.

6. Have a conversation

One of our e-commerce customers needs to keep a close eye on PCI DSS compliance. But the organization also has an enabling philosophy when it comes to cloud apps. So, when IT finds an app that does not facilitate PCI compliance or identifies a behavior within an app that could hurt their compliance status, they learn how the app is being used, come up with a few options to improve their compliance status, and then have a conversation about it with the user or line of business. Tapping someone on the shoulder and having a data-driven conversation increases the chance of an optimal outcome for both IT and the business.

7. Provide alternatives

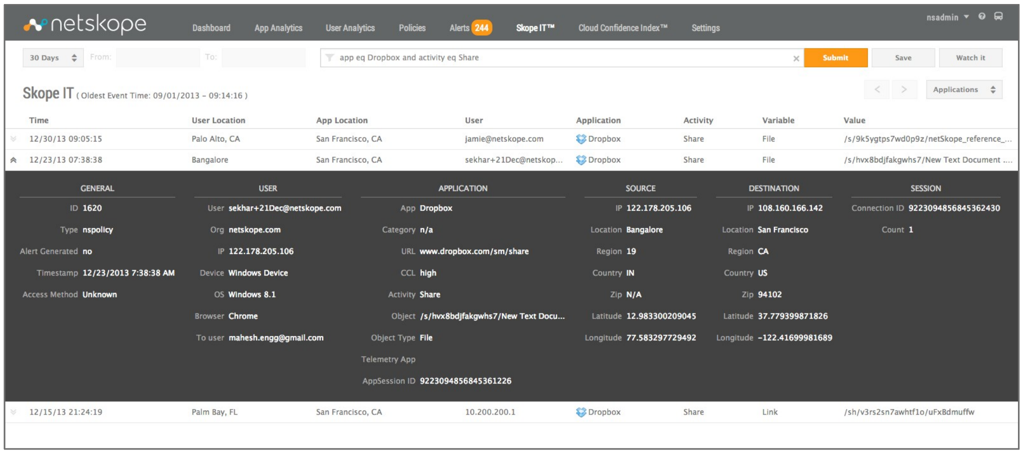
One of our healthcare customers is all about coming to the conversation not just with data, but with alternatives. They use the CCI to identify apps that have similar features and functionality to riskier ones the business may be using. In the conversation, IT points out why the apps in use put the business at risk (e.g., poor auditability or lack of HIPAA compliance) and offer choices that have a higher confidence score. This positions IT as a problem-solver and increases the chances that users will solicit IT's input before procuring a cloud app the next time around.

8. Trust but verify

One of our media customers is reluctant to put onerous policies in place. Their culture centers on trusting people, and their risk profile enables them to make the tradeoff of permissiveness with potential data leakage. They balance this by auditing cloud app usage on a periodic basis as well as setting watch lists for particular behaviors that can signal a potential data breach or malicious activity.

9. Do forensics in the cloud

In addition to cloud audits, several of our customers perform forensic analysis after a suspected breach. In one example, a departing employee of one of our customers stole proprietary content to take to a competitor. IT identified the data breach as well as the events leading up to it, giving the company enough evidence to approach the competitor and recover the content. As a result of the accurate, thorough forensic audit trail, the employee in question lost his job not only at our customer, but also at the competitor.



app eq Dropbox and activity eq Share

Skope IT (Oldest Event Time: 09/01/2013 - 09:14:16)

Time	User Location	App Location	User	Application	Activity	Variable	Value
12/30/13 09:05:15	Palo Alto, CA	San Francisco, CA	jamie@netskope.com	Dropbox	Share	File	/s/9k5ygtps7wd0p9z/netSkope_reference_...
12/23/13 07:38:38	Bangalore	San Francisco, CA	sekhar+21Dec@netskop...	Dropbox	Share	File	/s/hvx8bdjfakgwhs7/New Text Document ....
12/15/13 21:24:19	Palm Bay, FL	San Francisco, CA	10.200.200.1	Dropbox	Share	Link	/sh/v3rs2sn7awhtf1o/uFxBdmuffw

GENERAL
ID 1620
Type nspolicy
Alert Generated no
Timestamp 12/23/2013 7:38:38 AM
Access Method Unknown

USER
User sekhar+21Dec@netskope.com
Org netskope.com
IP 122.178.205.106
Device Windows Device
OS Windows 8.1
Browser Chrome
To user mahesh.engg@gmail.com

APPLICATION
App Dropbox
Category n/a
URL www.dropbox.com/sm/share
CCL high
Activity Share
Object /s/hvx8bdjfakgwhs7/New Text Docu...
Object Type File
Telemetry App
AppSession ID 9223094856845361226

SOURCE
IP 122.178.205.106
Location Bangalore
Region 19
Country IN
Zip N/A
Latitude 12.983300209045
Longitude 77.583297729492

DESTINATION
IP 108.160.166.142
Location San Francisco
Region CA
Country US
Zip 94102
Latitude 37.779399871826
Longitude -122.41699981689

SESSION
Connection ID 9223094856845362430
Count 1

10. Get specific

Many of the above examples point to the benefit of specificity. Our customers are running analytics and setting policies based on combinations of app, category, user, group, location, device, OS, browser, time, app confidence score, activity, and content. This specificity allows them to, for example, be alerted when people in Investor Relations share content from a cloud app during the company's quiet period, block downloads of sensitive documents to mobile devices, prevent HR employees from accessing salary data outside of work, and limit content uploads for people in Germany to apps hosted in the United States.

The above are ways our customers are taking a lean-forward approach to cloud adoption and enablement while also mitigating risk and keeping their businesses compliant with their policies. What's cool is not one of the ten examples above includes an outright "no" to a cloud app. While some of our customers conclude that blocking an app is the right approach, it is with the right usage data, the right information about app risk, and the granularity to shape usage with a fine scalpel versus a sledgehammer.

ABOUT NETSKOPE

Netskope™ is the leader in safe cloud enablement. Only the Netskope Active Platform™ provides discovery, deep visibility, and granular control of sanctioned and unsanctioned cloud apps. With Netskope, IT can direct usage, protect sensitive data, and ensure compliance in real-time, on any device, and with the broadest range of deployment options in the market. With Netskope, businesses can move fast, with confidence.