Solution Showcase

# Securely Enabling the Use of Cloud Apps with Cisco Cloudlock

**Date:** November 2017 **Author:** Doug Cahill, ESG Senior Analyst

**Abstract:** While cloud applications have enabled new business opportunities, and streamlined workflows such as those required for external collaboration, their widespread unauthorized adoption has created a set of security and compliance challenges. Addressing those concerns requires a pragmatic approach, one that enables the secure use of cloud apps. Cloud access security brokers (CASBs), which provide insight into the risk associated with cloud apps and usage patterns as the basis for defining and applying policy, can provide the visibility and control required to implement such an approach. Cisco Cloudlock allows organizations to not only gain visibility into what cloud applications are being used, but also understand their associated risk to implement policies that protect data assets stored with these apps from compromise.

## The Dimensions of Shadow IT

The broader dynamic of shadow IT is not a new one. The consumerization of IT started with the personal computer and has expanded dramatically with the use of smartphones and tablets. More recently, end-users have become very comfortable adopting SaaS apps to assist them with their jobs and boost productivity. As a result, many large companies have hundreds of shadow IT SaaS apps in use within their environments. Although empowering departments and individuals to quickly adopt new apps can be beneficial, there are legitimate concerns about data security, malicious apps, and account compromise as well as cost and functionality overlap. While this type of activity can't and shouldn't be halted, there is an urgent need for better visibility to help promote, manage, and optimize healthy and efficient cloud adoption.

### Visibility Gap – Shadow IT Cloud Apps and Their Associated Data

The "visibility" and "control" constructs of many, if not most, cybersecurity disciplines also applies to securing the use of cloud apps and starts with the adage that "you cannot secure what you cannot see." When it comes to shadow IT cloud apps, organizations know very well the unauthorized use of cloud apps has run rampant. In fact, nearly two-thirds of organizations participating in research conducted by ESG indicated that they are aware of a significant or moderate amount of non-IT-sanctioned cloud applications in use in their organizations. Establishing cloud app usage policies has little effect on the prevalence of shadow IT apps, with 77% of participants who stated that they have a significant or moderate amount of non-IT-sanctioned cloud applications in use in their organization also indicating that they have a formal methodology they always follow for each sanctioned IT app. So, what's the issue?

Establishing cloud app usage policies has little effect on the prevalence of shadow IT apps…

The top concern cited by ESG research participants is storing sensitive data in the cloud, with 87% indicating they are very or somewhat concerned about this aspect of cloud security.[1] As such, the visibility gap borne out of the use of shadow IT apps extends to the sensitive data that is associated with that use and further extends into a lack of understanding about who has access to that data, with whom they are sharing sensitive data, and other factors about the overall integrity of those data assets.

> **…the visibility gap borne out of the use of shadow IT apps extends to the sensitive data that is associated with that use…**

One way in which some IT and security professionals have responded is to review the logs on network controls at the edges of their networks, their proxies/gateways, and firewalls. While these logs will provide some course-grained visibility into cloud apps in use, they will conflate web traffic with cloud app traffic since many websites use cloud services, such as graphics that are loaded from a cloud-resident object store. And this basic level of inspection provides no visibility into the data that is associated with cloud apps, who is accessing the apps, nor any additional context to establish a risk profile.

## Connected Apps Widen the Gap

Another important dimension of the shadow IT cloud app visibility gap relates to connected applications. Many software-as-a-service (SaaS) apps have an ecosystem of layered applications that add incremental value on top of their base functionality. Some of the SaaS vendors with such an ecosystem offer both a development environment and an app store to make browsing, procuring, and utilizing layered cloud apps easy. Salesforce.com, for example, provides force.com, a platform-as-a-service (PaaS) environment for third-party app development, and AppExchange to promote those apps and facilitate their consumption. It's an appropriate example, given the broad use of salesforce.com by many organizations as their single source of truth for one type of sensitive data: customer information.

Layered applications often need administrative access to their underlying base applications, which is at odds with the least privileged best practice of granting the least amount of entities access to the least amount of assets with the least amount of privileges. The prevalent implementation of the OAuth authentication standard to link applications by using a shared set of credentials and resulting tokens is common for both business and consumer applications, and is in direct conflict with a least privileged approach. As such, while OAuth effectively facilitates connecting cloud apps it can also result in granting the layered application access to sensitive data. Given this, bad actors exploit OAuth as an opportunity to fool users into providing access to a cloud app that can, in turn, inadvertently provide access to sensitive data. As a result, the attacker is unwittingly granted privileged access to resources.

While inline network-based controls can detect the use of some cloud apps, they lack visibility into layered applications since those apps do not directly cross the network those controls monitor. That is, because those connected apps are accessed via the base app, they are invisible to on-premises controls.

## The Moving Target Nature of Shadow IT App Discovery

> **…the discovery of shadow IT apps needs to be an automated, ongoing process.**

The other shortcoming of a manual log inspection approach is it provides partial visibility for just a point in time. IT and security teams are inevitably surprised to learn just how many SaaS apps are in use in their organizations. And because end-users are regularly signing up for new apps, gaining visibility into the use of shadow IT apps is a fluid situation. A partner in the supply chain may, for example, send a file via yet another file sharing service. As such, the discovery of shadow IT apps needs to be on an automated, ongoing process.

[1] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

## The Context and Control Requirements for the Safe Use of Cloud Apps

When it comes to addressing the visibility gap and protecting cloud-resident sensitive data, there is broad recognition that cloud access security brokers (CASBs) are essential. When asked how important using a CASB is to gain greater control over an organization's use of cloud applications, two-thirds of ESG research respondents stated that CASBs were either critical or very important.[2] Organizations evaluating a CASB should consider the following requirements:

### Contextual and Continuous Visibility

The simple discovery of the cloud apps in use in an organization in and of itself is not enough as it does not provide a full picture of whether there are connected apps, the relative trustworthiness of the cloud apps in use, and the types of sensitive data associated with the use of each cloud app. As such, visibility needs to be continuous and actionable, as follows:

- Multidimensional Discovery – In addition to discovering what shadow IT apps are in use, a CASB should discover associated connected apps and whether they have been granted escalated privileges. Sensitive data based on out-of-the-box profiles, such as personally identifiable information (PII) and customized profiles, should also be discovered.

- Risk Assessment – Risk is also multidimensional, since the risk associated with an app and the risk profiles of app users are important elements to understand. CASBs should consider multiple factors in assessing risk, including business-criticality, compliance with regulations, adherence to best practices such as those prescribed by the Cloud Security Alliance (CSA), threats associated with the IP address(es) of the app, and the behavior of users.

- Classification – App and data classification allows for such groupings to be used for both the definition and enforcement of policy and ongoing monitoring.

- Usage – Establishing a baseline of who is accessing what sensitive data, via what cloud apps, at what time of day, and from what location(s) helps establish a baseline of normal usage patterns from which anomalous and potentially malicious activity can be detected.

- Continuous and Retrospective – A multi-mode implementation that employs both network-based visibility and integration with native cloud app APIs enables the discovery of both apps that can be seen on the wire and those that are connected to each other. This deployment model also provides continuous visibility into current use and allows for the retrospective application of new policies.

With this context, organizations can get to work on establishing a policy lexicon.

### Pragmatic Policy Framework

A CASB should enable the implementation of policies to govern not only what applications are allowed and tolerated but also who has access with what privilege levels to different classes of data, as follows:

- Application Access Controls – The spectrum of policies extends beyond blocking those cloud apps that are prohibited and allowing those that are explicitly sanctioned to a nuanced approach of tolerating certain applications by monitoring the data types being used in conjunction with such apps.

[2] ibid.

- Data Loss Prevention (DLP) – A complete DLP policy lexicon will allow for the application of course- and fine-grained policies to control access to and use of data stored with cloud apps. For example, a general policy that a CASB should support is whether data can be uploaded and/or downloaded to/from a specific cloud app or class of cloud app. More specific policies allow for controlling which specific users are allowed to perform certain actions on specific classes of data. A CASB will also maintain an audit trail of activity and alert on attempted policy violations.

Enforcement policies should be implemented in phases, starting with a "monitor and alert" mode via which policies can be tuned over time to mitigate against false positives that could impede end-user workflow and overwhelm the IT team.

## Gaining Visibility for Practical Control Over Cloud Apps with Cisco Cloudlock

Cisco's Cloudlock cloud access security broker meets these requirements with a multi-mode implementation that enables both visibility and control use cases.

### Actionable, Risk-based Shadow IT Discovery

Not all cloud apps are created equal with respect to their relative importance to the business and the risk their use may introduce. The Cloud App Security Index is built and maintained by the Cisco Cloudlock CyberLab and it considers multiple factors to provide a relative benchmark of trustworthiness. These factors include whether the cloud service provider (CSP) is known to have experienced a cybersecurity data breach, whether they comply with the most relevant industry regulations such as SOC-1 and SOC-2, whether they are financially viable, and whether they adhere to accepted industry guidelines and best practices. Many of the apps also have a community trust rating, which is compiled from feedback that is provided by actual app customers.

By integrating with APIs exposed by SaaS providers, Cisco Cloudlock can also discover whether other applications are connected to the base cloud app via OAuth authorization. And because risk can be ephemeral, Cisco Cloudlock treats risk dynamically by updating ratings as the disposition of a cloud app changes.

> …Cisco Cloudlock can also discover whether other applications are connected to the base cloud app via OAuth authorization.

Cisco Cloudlock extends discovery beyond shadow IT apps to the types of sensitive data stored with such apps as well as who is accessing that data.

### Malicious Connected App Prevention and Remediation

The Cisco Umbrella - Secure Internet Gateway (SIG) can be used to prevent users from accessing a malicious domain, in turn preventing a new OAuth token from being generated, and effectively blocking the malicious connected app from accessing the base app. In other situations when an OAuth token is generated, Cisco Cloudlock, upon discovering the connected relationship between the cloud apps, and determining that the layered app is malicious, can revoke the OAuth token, eliminating the ability of the layered app to access the resources, including sensitive data, associated with the base app.

### User Behavior Analytics to Detect External Attacks and Provide Insider Threat Protection

> Cisco Cloudlock employs user behavior analytics to then identify anomalous activity that could be indicative of an active insider threat…

The ability to discover not only the shadow IT apps that are in use, but also the data associated with those apps, and which users are taking what actions with the data, establishes a baseline of what constitutes normal behavior. Cisco Cloudlock provides a set of customizable user behavior policies to detect abnormal activity that is indicative of a compromised account (external attack) or an active insider threat (an attack perpetrated by a company employee with privileged access to sensitive data).

### Data Loss Prevention Engine

The DLP policy engine provided by Cisco Cloudlock allows for the application of general data usage policies associated with cloud applications such as whether data can be uploaded and/or downloaded by a class of application, such as enterprise file sync and share (EFSS) services. More specific policies can also be created to control what individual users, or groups of users, are allowed to do with classes of sensitive data.

## The Bigger Truth

Addressing the security concerns borne of the prevalent use of shadow IT cloud applications requires a pragmatic approach to safely enable the use of those apps that have become core to how many businesses now operate. Such an approach starts with gaining a clear understanding of the apps in use; the types of data assets that are used in conjunction with, and stored by, cloud apps; and the users who access those apps to establish a risk-based assessment. A cloud access security broker that can enable these practices will do so by providing contextual, and thus actionable, visibility into the use of cloud apps, a rich data loss prevention policy engine, and continuous monitoring of both the use of known cloud apps and the discovery of new shadow IT apps, including those that are connected to each other via OAuth. Cisco's Cloudlock CASB offering employs a multi-mode implementation to provide the level of visibility and set of controls required to securely enable an organization's ongoing use of cloud-delivered applications.

**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.