Five Must-Haves for a Cloud Access Security Broker (CASB)

CLOUD APPS: THE WAY PEOPLE WORK TODAY

People and organizations have moved to the cloud in a big way. Today growing at six times the traditional IT market, cloud computing has accelerated because it allows people to get their jobs done more quickly, easily, and flexibly than traditional computing tools. Software-as-a-Service (SaaS), the most visible and adopted segment of cloud computing, has proliferated in enterprises to such an extent that IDC predicts most software vendors will shift to a SaaS/PaaS code base by 2018. Forrester projects the SaaS market will reach more than $100 billion by the end of 2016.

Cloud apps are increasingly common in nearly every kind of enterprise. Sometimes this is because they are cheaper to buy and operate. Other times it's because people want to be nimble, deploying an app faster and taking advantage of the latest product features sooner than they would with on-premises software. And other times it's because people don't want to coordinate across the many gatekeepers—operations, hardware, networking, and security—required to make a software roll-out successful. Cloud apps have reached a level of maturity and feature richness that they are now mainstream. In fact, they are reaching a tipping point in organizations. IDC expects nearly a third of companies to source greater than half of their IT spend from the public cloud in 2016. Cloud Access Security Broker (CASB) leader Netskope™ counts more than 20,000 cloud apps being used in enterprises today, with more than 900 in use per enterprise. For most people and organizations, cloud apps are simply the way we work today.

AN OPPORTUNITY FOR IT AND THE BUSINESS

While IT has ownership or responsibility for some cloud apps, people and lines of business are now more than ever empowered to go outside of IT and deploy their own apps. This means they are procuring, paying for, managing, and using these apps without IT's involvement. This is a good thing for the business because it enables people to get their jobs done more efficiently. But it also means that there is no way for IT to consistently enforce security and compliance controls across all of the cloud apps in use across the organization, whether those apps are "shadow IT" or sanctioned.

Beyond "shadow IT," IT is often responsible for some portion of cloud app enablement. In some cases, deployment of a cloud app is a net-new project for the organization. In others, it's a migration from a traditional application.

Whether shadow or sanctioned, cloud app usage is growing and C-suites, boards of directors, and audit committees around the world are beginning to ask whether the cloud technologies in their environment are safe, compliant with business policies, perform according to vendor service-level agreements, are cost-effective, and are optimized for business usage.

When IT can confidently answer these questions and assuage these concerns, it can sanction cloud apps and deliver them optimally. IT can shine a light on "shadow IT," educate and inform cloud app stakeholders of the risks and opportunities, and safely bring cloud apps on board.

The time is now for you to get complete visibility into the cloud apps in your organization. Then, together with your security and line-of-business counterparts, you can make decisions and institute granular policies to make those apps safe and compliant.

SLEDGEHAMMER VS. SCALPEL

When confronted with an unknown technology, sometimes organizations are inclined to shut it down. That's because many of the tools IT has used to detect and remediate rogue technology are binary, so they allow you to say only "yes" or "no." But what if you could take a more nuanced approach?

Instead of taking a sledgehammer to the apps people and lines of business want to use, what if you could say "yes" to nearly all of their favorite apps, and then, like a surgeon, slice out certain activities or transparently protect certain data to make the usage of those apps acceptable to your organization from a security and compliance standpoint? This approach would put you in the position of partnering with and enabling the business rather than saying "no." And for the cloud apps that you have been championing but have had to slow roll because of security and compliance concerns, this approach will let you adopt them quickly. Taking a scalpel instead of a sledgehammer to the problem will pave the way to cloud confidence.

According to Gartner, Cloud Access Security Broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Organizations are increasingly turning to CASB as a way for them to address cloud app risks, enforce security policies, and comply with regulations, even when cloud apps are beyond their perimeter and out of their direct control. If you intend to use CASB to increase your confidence about your organization's cloud app usage, consider taking a granular approach to policy enforcement and data protection. In other words, consider using a scalpel rather than a sledgehammer for your cloud app security. Here are five steps you can take to achieve this.

CASB: FIVE STEPS TO CLOUD CONFIDENCE

What steps must you take to gain cloud confidence? We've identified the following five: 1. Find all of the cloud apps in use in your enterprise and assess their risk; 2. Understand how those apps are being used; 3. Protect against malware, detect threats and anomalies, and manage incidents; 4. Identify and prevent the loss of sensitive data; and 5. Enforce your security and compliance policies across any cloud app in real-time. We'll walk through each of the five steps and provide a short checklist within each step.

Let's set the stage with a use case.

Acme's IT department has not been able to sanction the usage of or deploy key cloud apps for its business such as the Microsoft Office 365 suite, Box, Salesforce.com, or ServiceNow or even key line-of-business apps such as cloud-based HR management or next-generation financial reporting because it can't monitor the apps or enforce security policies in them. Moreover, as managers of a public company, Acme's executives must be able to attest, for compliance purposes, that only authorized personnel had contact with key systems and data, and any use or modifications were proper and accurate. With an increasing number of cloud apps coming onto the scene at Acme that contain an increasing amount of critical company data, management is concerned that it can no longer attest to the accuracy of these statements.

Find All Cloud Apps and Assess Risk

In order to lay the groundwork for cloud confidence, Acme IT must take the first step: use a CASB to find all of the cloud apps in use in the organization. This includes both apps that are sanctioned by Acme's IT department and any that are unknown. To get a complete picture, IT should find not only those apps accessed from desktops and laptops within the four walls of the workplace, but also from remote laptops and mobile devices, regardless of whether the apps are browser-based or native, such as a sync client. Once those apps are found, IT should evaluate each of the apps against a set of objective criteria in the areas of security, auditability, and business continuity as well as assess the app's risk based on its organization's use of that app.

- ✓ Find all cloud apps, whether sanctioned or "shadow IT"
- ✓ Include cloud apps that are running on-premises, remote, or on PCs or mobile devices
- ✓ Score apps on enterprise-readiness, as measured by security, auditability, and business continuity
- ✓ Evaluate those apps' risk based on your organization's usage of them
- ✓ Make risk-based decisions about whether to standardize on, monitor, govern, block certain activities in, or simply block each app

Understand Cloud App Usage and Context

After finding all of the cloud apps in use in the organization, Acme IT should use a CASB to drill down into the information surrounding those apps and understand how people are using them. This second step involves understanding contextual usage of those apps, including user identity or group, as well as the device the user is on, browser, geo-location, and time; cloud app, app instance, or app category; specific app activities, e.g., "download," "share," or "edit;" content type and file or object name; DLP profile, if applicable; and where and with whom content is shared.

- ✓ Drill down into usage context, including user, group, OU or BU, device, device classification or status, browser, geo-location, and time, answering questions such as "Who from our overseas support organization is logging into our CRM after-hours?"
- ✓ Understand the app, e.g., app, app instance, or app category, with the ability to monitor and ultimately enforce policy differently in, say, a sanctioned version of Box versus the hundreds or thousands of personal Box instances
- ✓ Ascertain cloud app activities, e.g., "download," "upload," "share," "edit," "approve," etc., or administrative

activities, as well as with whom content was shared, if applicable, answering questions such as "Is anyone outside of HR downloading data from any HR app to an unmanaged device?"

- ✓ See content details, e.g., content type, file or object name; and DLP profile, if applicable, to ascertain whether users are uploading, downloading, or sharing sensitive or regulated data such as personally-identifiable information (PII), intellectual property (IP) such as next-year's product designs, or confidential business data such as non-public financials
- ✓ e-Discover content at rest within an app, including against a DLP profile, understand its exposure within and outside of the organization, and review activity audit trails on sensitive content that may have been exposed

Protect Against Malware, Detect Threats, and Manage Incidents

Beyond understanding cloud app usage, Acme IT should use a CASB to protect against malware, detect threats and anomalies, and manage incidents. IT should take automated action on malware, such as quarantine and tombstone a file, whether suspected malware is at rest in a sanctioned app or en route to or from any app. Moreover, they should alert the rest of the organization's security infrastructure, including detonating the malware in a sandbox and alerting endpoint detection and remediation (EDR) systems so the EDR can take action such as isolate endpoints or kill processes. IT should also use CASB as an early warning system-of-sorts to pull indicators of compromise (IOCs) found in the cloud into their overall threat picture by combining cloud threat intelligence in the organization's existing threat platforms and incident management systems. Beyond threats entering the organization's cloud apps, Acme's CASB should detect and prioritize cloud app usage anomalies that can signal risky or non-compliant user behavior, data leakage, or account compromise. In the case of a high-priority incident, Acme IT should drill into forensic details to audit the activity leading up to the incident and outcomes of the incident, whether policy violation, data exposure, malware infection, etc. Finally, Acme should use a CASB to perform incident management tasks or integrate with their on-premises incident management solutions such as security information and event management (SIEM).

- ✓ Protect against malware at rest in a sanctioned app or en route to or from any cloud app
- ✓ Alert security infrastructure such as your sandbox and EDR so they can take action to protect the rest of the enterprise
- ✓ Detect and prioritize usage anomalies that could signal risky or non-compliant behavior, data leakage, or compromised accounts
- ✓ Perform forensic analysis on user activity leading up to an incident or breach
- ✓ Perform incident management in CASB or integrate cloud incidents into your on-premises incident management system

Cloud Data Loss Prevention

Beyond understanding cloud app activity and potential data loss, Acme IT needs to understand whether sensitive or regulated data are in the cloud, where they are, and whether they are exposed. In some cases, those data are in the cloud and shouldn't be and in other cases, they are in the cloud but aren't adequately protected, are exposed to unauthorized individuals or external parties, or are being moved where they shouldn't be (e.g., downloaded to an unmanaged device). To deal with any of these situations, Acme IT should use a CASB that features advanced, enterprise cloud DLP. That means cloud DLP that works for both content at rest in sanctioned apps or content en route to or from any cloud app, sanctioned or unsanctioned. It also means cloud DLP that features such enterprise capabilities as support for thousands of language-independent data identifiers, custom keyword dictionaries, hundreds of file types, true file type detection, metadata extraction, proximity analysis,

volume thresholds, international support including double-byte characters, document fingerprinting, content exact match, "and" and "or" rules, and validation mechanisms such as Luhn check for credit cards to get the most accurate and comprehensive detection of sensitive information. Beyond DLP features, Acme IT should use its CASB to wrap DLP profiles in contextual policies (e.g., in conjunction with user groups, app categories, or activities such as "share," "upload," or "download") in order to ensure fewer false positives and higher accuracy. Finally, since Acme IT has an on-premises DLP solution in which it has invested time and resources to create efficient, highly-tuned policies, it should consider integrating its cloud DLP with that system, taking advantage of its CASB filtering and using secure ICAP to shuttle potential violations on-premises for final detection and to take advantage of existing incident management processes.

- ✓ Create relevant DLP profiles for your cloud apps, including personally-identifiable information (PII), payment card industry information (PCI), protected health information (PHI), custom fingerprint and exact match profiles, and more
- ✓ Take advantage of advanced, enterprise cloud DLP features such as fingerprinting, exact match, proximity rules, and more
- ✓ e-Discover content at rest within your sanctioned apps and en route to or from any app, and initiate workflows such as quarantine, legal hold, change ownership, reduce sharing permissions, encrypt, and more
- ✓ Enforce cloud DLP policies that take effect in not just one app, but across an entire category or globally, if you need them to integrate your cloud DLP with your on-premises system to take advantage of highly-tuned policies and efficient incident management processes

Enforce Policies in Real-Time

Once Acme IT analyzes the organization's cloud usage against its policies, protects against cloud-based threats, and finds data violations, it can start enforcing policies that take place in real-time. Let's revisit our contention that using a scalpel, not a sledgehammer, to enforce policies is the way to cloud confidence. Acme IT realizes this, and not only wants to say "yes" to the apps that are already in use, but wants to move even more of its applications (such as productivity, storage, and collaboration, as well as ones serving functions like HR, Finance, and Marketing) to the cloud. Acme wants to be able to set sophisticated, precise policies based on the same contextual factors it's able to pivot on and analyze. For example, Acme wants to:

- ✓ Enable the use of collaboration apps, but prevent sharing of data with people outside of the company
- ✓ Disallow file uploads to cloud storage apps that contain highly sensitive data or intellectual property that, if ever leaked, stolen, or modified, could cause serious damage to the company
- ✓ Allow people in the HR and finance groups worldwide to access HR or finance/accounting apps, but block anyone outside of headquarters from downloading salary information
- ✓ Encrypt sensitive content in context as it's being uploaded or when it's already resident within cloud apps
- ✓ Enforce granular, activity- or data-level policies on any of the contextual factors described above
- ✓ Set policies once and have them enforced in real-time in any app, at the app-, app instance- or category-level, or globally, as well as whether users are on-premises, remote, on a laptop or mobile device, and accessing the app via a browser or working in the native or sync client
- ✓ Enforce policies whether or not you have administrative privileges to, or even sanction or know about, the app
- ✓ Enforce policies in real-time, before an undesired event or behavior happens
- ✓ Coach users on policy violations to educate them about risky behaviors and to create transparency

These five steps make up the framework for cloud confidence and the ability to take these five steps would mean that Acme IT can say "yes" overall to the cloud apps that Acme Corp. wants to use, while limiting certain risky or non-compliant behaviors within the apps:

1. Find all of the cloud apps in use in your enterprise and assess their risk
2. Understand how those apps are being used
3. Protect against malware, detect threats and anomalies, and manage incidents
4. Identify and prevent the loss of sensitive data
5. Enforce your security and compliance policies across any cloud app in real-time

SUMMARY CLOUD CONFIDENCE CHECKLIST

Find All Cloud Apps and Assess Risk	• Find all cloud apps, whether sanctioned or "shadow IT" • Include cloud apps that are running on-premises, remote, or on PCs or mobile devices • Score apps on enterprise-readiness, as measured by security, auditability, and business continuity • Evaluate those apps' risk based on your organization's usage of them • Make risk-based decisions about whether to standardize on, monitor, govern, block certain activities in, or simply block each app
Understand Cloud App Usage and Context	• Drill down into usage context, including user, group, OU or BU, device, device classification or status, browser, geo-location, and time, answering questions such as "Who from our overseas support organization is logging into our CRM after-hours?" • Understand the app, e.g., app, app instance, or app category, with the ability to monitor and ultimately enforce policy differently in, say, a sanctioned version of Box versus the hundreds or thousands of personal Box instances • Ascertain cloud app activities, e.g., "download," "upload," "share," "edit," "approve," etc., or administrative activities, as well as with whom content was shared, if applicable, answering questions such as "Is anyone outside of HR downloading data from any HR app to an unmanaged device?" • See content details, e.g., content type, file or object name; and DLP profile, if applicable, to ascertain whether users are uploading, downloading, or sharing sensitive or regulated data such as personally-identifiable information (PII), intellectual property (IP) such as next-year's product designs, or confidential business data such as non-public financials • e-Discover content at rest within an app, including against a DLP profile, understand its exposure within and outside of the organization, and review activity audit trails on sensitive content that may have been exposed
Protect Against Malware, Detect Threats, Manage Incidents	• Protect against malware at rest in a sanctioned app or en route to or from any cloud app • Alert security infrastructure such as your sandbox and EDR so they can take action to protect the rest of the enterprise • Detect and prioritize usage anomalies that could signal risky or non-compliant behavior, data leakage, or compromised accounts • Perform forensic analysis on user activity leading up to an incident or breach • Perform incident management in CASB or integrate cloud incidents into your on-premises incident management system
Cloud Data Loss Prevention	• Create relevant DLP profiles for your cloud apps, including personally-identifiable information (PII), payment card industry information (PCI), protected health information (PHI), custom fingerprint and exact match profiles, and more • Take advantage of advanced, enterprise cloud DLP features such as fingerprinting, exact match, proximity rules, and more • e-Discover content at rest within your sanctioned apps and en route to or from any app, and initiate workflows such as quarantine, legal hold, change ownership, reduce sharing permissions, encrypt, and more • Enforce cloud DLP policies that take effect in not just one app, but across an entire category or globally, if you need them to integrate your cloud DLP with your on-premises system to take advantage of highly-tuned policies and efficient incident management processes

Enforce Policies in Real-Time	• Enable the use of collaboration apps, but prevent sharing of data with people outside of the company • Disallow file uploads to cloud storage apps that contain highly sensitive data or intellectual property that, if ever leaked, stolen, or modified, could cause serious damage to the company • Allow people in the HR and finance groups worldwide to access HR or finance/accounting apps, but block anyone outside of headquarters from downloading salary information • Encrypt sensitive content in context as it's being uploaded or when it's already resident within cloud apps • Enforce granular, activity- or data-level policies on any of the contextual factors described above • Set policies once and have them enforced in real-time in any app, at the app-, app instance- or category-level, or globally, as well as whether users are on-premises, remote, on a laptop or mobile device, and accessing the app via a browser or working in the native or sync client • Enforce policies whether or not you have administrative privileges to, or even sanction or know about, the app • Enforce policies in real-time, before an undesired event or behavior happens • Coach users on policy violations to educate them about risky behaviors and to create transparency

ABOUT NETSKOPE

Netskope™, the leading cloud access security broker (CASB), helps enterprises find, understand and secure sanctioned and unsanctioned cloud apps. Through contextual awareness and a multi-mode architecture, Netskope sees the cloud differently. This results in the deepest visibility and control, the most advanced threat protection and data loss prevention and an unmatched breadth of security policies and workflows. The world's largest companies choose Netskope, the only CASB that ensures compliant use of cloud apps in real-time, whether accessed on the corporate network, remotely or from a mobile device. With Netskope, enterprises move fast, with confidence. To learn more about the Netskope Active Platform, visit our website.