THE DEFINITIVE GUIDE TO CLOUD ACCESS SECURITY BROKERS

WHITE PAPER

AUGUST 2014

bitglass

For many enterprises, security and compliance concerns hamper adoption of cloud applications. Furthermore, cloud applications are accessible from anywhere dragging mobile and BYOD security concerns into the picture. Cloud Access Security Brokers are a category of security tools that help enterprises safely enable cloud apps and mobile devices.

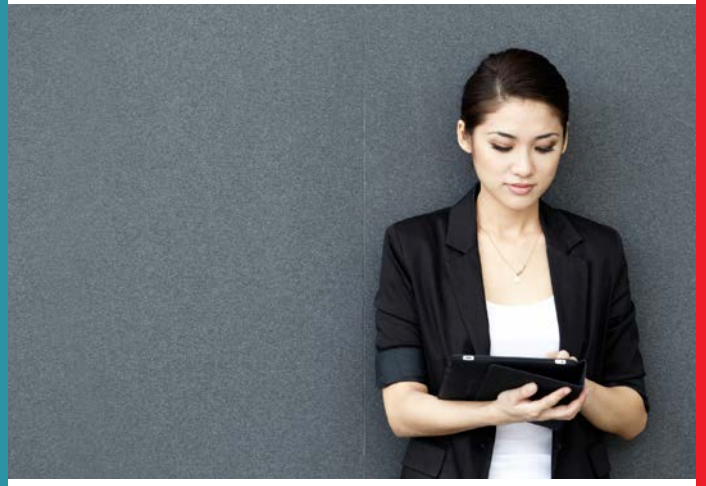
CASBs work by intermediating or "proxying" traffic between cloud apps and users. Once proxied, these tools provide:

- **Visibility—**audit logs, security alerts, compliance reports, etc.
- **Data Security—**access control, data leakage prevention, encryption, etc.

Together, these functions fill in the gaps otherwise encountered when an enterprise moves from internal, premises-based applications to cloud apps like **Salesforce**, **Google Apps**, or **Office 365**. For enterprises in heavily regulated industries, like Finance and Healthcare, use of a CASB might be the only practical approach to enabling cloud apps. More broadly, any organization with sensitive data to protect would be well served by considering this emerging solution category.

According to Neil MacDonald and Peter Firstbrook at Gartner,

"For business leaders and information security professionals looking to securely enable the use of cloud-based services from managed and unmanaged devices, CASBs offer a solution without compromising the need to ensure compliance with enterprise security policies."



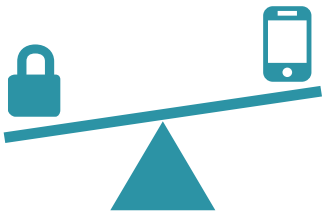
Aren't cloud apps already secure?

It's the job of SaaS application providers to ensure that their products are as secure as possible. After all, they're asking enterprises to trust them with their data, which is highly valuable. Many SaaS vendors hire the best and the brightest in IT Security, and buy the best security products in order to ensure the security of their customers' data. Through these efforts, most app vendors are focused on preventing breaches into their infrastructure—things like denial of service attacks, malware outbreaks and widespread data exfiltration events. These are the types of security events that land the cloud app vendor on the front page of the Wall Street Journal, and have a severe negative impact on their business.

There's another set of security risks that the cloud app vendors are less concerned with, the types of risks that land YOU on the front page of the Wall Street Journal, putting your company and your job at risk. These risks revolve leakage of sensitive corporate data. When sensitive data stored in SaaS apps is not properly controlled, the result can be inadvertent or malicious leakage of company data, theft of user credentials, regulatory compliance failure, and worse. These types of risks are outside of the control of the SaaS application provide and require you to enforce contextual access control policies on your users. In short, securing your data against such risks is your responsibility.

Effectively, the cloud app vendor is protecting against attacks that target the application and the underlying network infrastructure. What you need to protect against are attacks that target the data and your users.

Balancing IT Needs and Employee Demands



Some years ago, the user experience didn't really matter that much. Employees didn't have much of a choice and increased security always meant a poor user experience. Today, employees are quick to reject IT solutions that reduce their productivity.

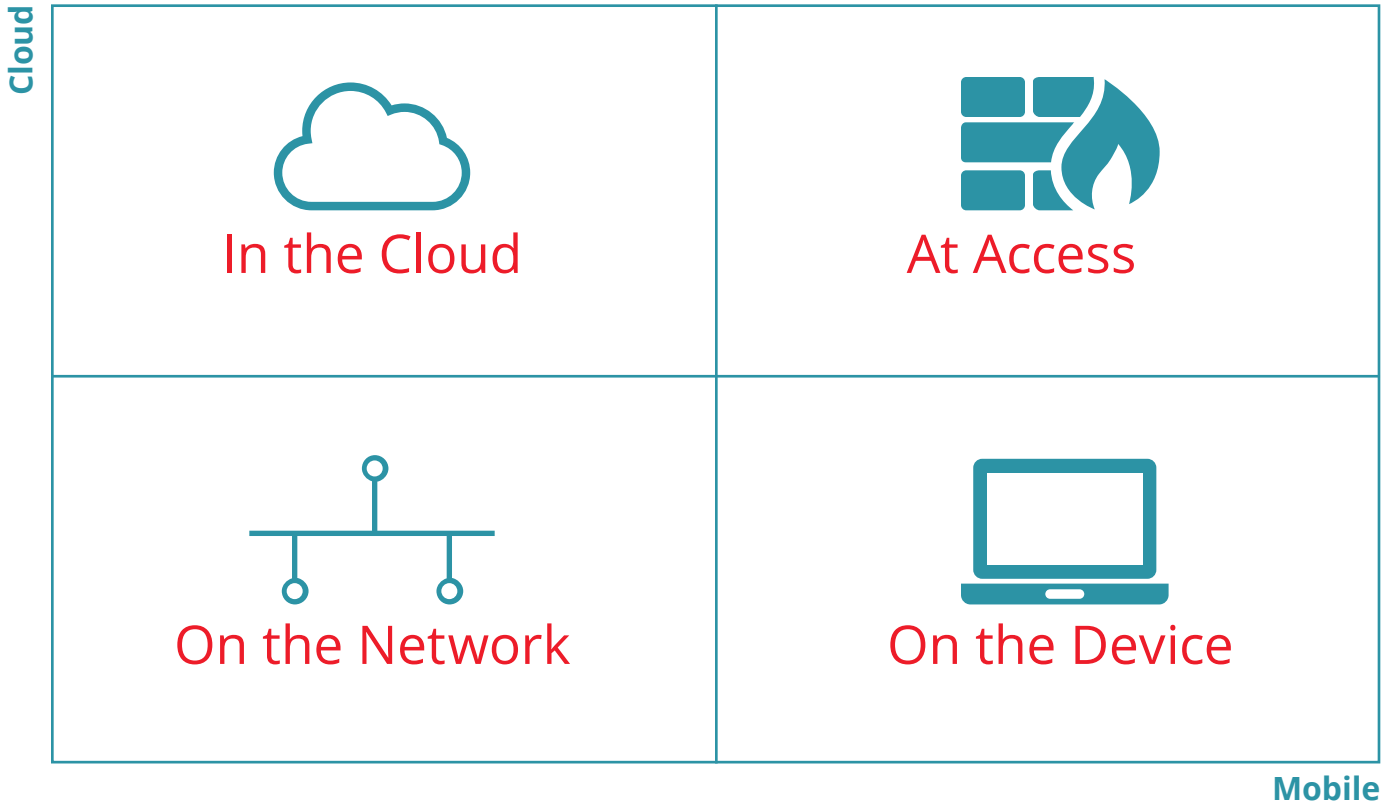
Enterprises must choose security solutions that does not hamper productivity.

- **Privacy—**Employees have not only an expectation, but a right to privacy. Gone are the days when it is acceptable for IT to capture personal traffic in the security dragnet.
- **Transparency—** Usability has been a key adoption driver for many cloud apps and mobile devices. Employees are familiar with these technologies and have come to expect the same great experience with corporate applications that they enjoy in their personal applications.
- **Mobility—**Employees want to be able to go out and buy the latest and greatest device and connect to their work data and applications with no restrictions.

Finding a CASB that can meet these key requirements will help to stop employees from "going rogue" and working around IT.

Requirements of a CASB Solution

As an emerging market, Cloud Access Security Broker capabilities vary from one vendor to the next. A complete solution protects corporate data throughout its life cycle—in the cloud, at access, on the device, and on the corporate network.



In the Cloud

Many cloud app vendors encrypt data-at-rest in their cloud infrastructure. However, the application vendor controls the encryption key, effectively reducing the value of such encryption to each customer. Furthermore, data residency requirements in many countries require that sensitive data never leaves the country.

The advantage of using a CASB for cloud encryption is that it allows the enterprise to control their own encryption keys, ensuring that nobody can gain access to corporate data without the knowledge of the enterprise.

The downside of using a CASB for cloud encryption is that some application functionality may be affected. Specifically, encrypted data cannot be processed by the SaaS application servers. For example, if you encrypt a field with monetary values, the cloud app is not able to report on sum totals of those dollar values appropriately.

Another issue with using a CASB for cloud encryption is that encrypted data cannot be searched. To overcome this limitation, first generation CASB solutions watered down the encryption to cyclic ciphers. In such solutions, searching the plaintext data for a keyword is accomplished by searching the encrypted data for the encrypted form of the keyword.

Unfortunately, cyclic ciphers are weak and easily cracked via chosen plaintext attack. Some products enhance cyclic ciphers with 256-bit AES encryption, but limit the number of initialization vectors in order to maintain searchability. For example, one cloud encryption vendor advertises “millions” of initialization vectors. One million is approximately 220, i.e, 256-bit AES encryption with one million initialization vectors is effectively 20-bit encryption, which certainly doesn’t pass the requirements of any security conscious organization.

One thing to review with any vendor you assess is resiliency in the face of constantly changing cloud applications. First generation cloud encryption CASB products rely on large teams of engineers that scramble to update their software whenever cloud application providers update their apps. This can be a daily occurrence, resulting in poor availability and negative continuity. The challenge is that modern SaaS applications use client-side AJAX for most of their UI. First-generation CASB products rely on hand-coded logic for such applications, and frequently break when the application is updated.

At Access

Since CASBs act as a proxy between cloud apps and users, they have the ability to see all traffic to/from those cloud apps, and to inspect and secure data. At access, CASBs provide visibility, identity, access control, and data protection.

VISIBILITY

CASBs are able to provide visibility into user behaviors and activities across all cloud applications. Typically, visibility comes in the form of a complete audit log with higher-level analytics, reports, and alerts on that data. Analytics and reports can help you to observe trends and insights into deviations from normal behavioral patterns. Alerts can keep you apprised of potential security and compliance issues, such as inappropriate data access, user account compromise, etc.

Since CASBs intermediate all of your cloud apps, they can provide visibility that spans your entire cloud deployment. For example a CASB should be able to alert you when a user logs into Salesforce from San Francisco and then someone claiming to be that user logs into Box from New York at the same time.

IDENTITY

Identity is a key challenge for many enterprises that have moved to cloud applications. In many cases, enterprises have created separate and distinct accounts for new cloud applications as they have added them. This causes huge problems with password management, user account updates, employee termination, etc.

A CASB should help you to ensure that all cloud apps leverage a single identity store, either by

authenticating users directly against your corporate directory, or through a third party cloud identity provider. This eliminates redundant accounts and allows you to more effectively enforce password policies. Some CASBs are able to act as a cloud identity provider, eliminating the need to purchase a third party solution.

At Access

ACCESS CONTROL

Access Control answers the question of who is allowed to access a particular cloud app, and under what conditions and context. A CASB should enable you to define policies by applications, or even by functionality within an application. These policies should be based on:

- **Group or role in the organization:** Typically as defined in Active Directory. For example, Executives and members of the Finance team might have access to this quarter's financial results but nobody else should be able to access that data.
- **Device type or operating system:** Many organizations have policies on what can be accessed on a corporate managed Windows Laptop versus a personally owned mobile device, as an example.
- **Geography:** Physical location of a user may indicate suspicious or rogue behavior for some organizations, so they want to limit access to sensitive data from certain regions or countries

DATA PROTECTION

At access, CASBs are responsible for identifying and classifying sensitive information, and then allowing the customer to create policies that determine what should be done with that data. These capabilities are similar to Data Leakage Prevention capabilities typically found inside of a corporate premises network or on managed endpoint devices.

The first step is to identify corporate data. All CASBs should include an ability to define templates or policies that classify corporate data into different risk or sensitivity levels. For example, an organization that handles personally identifiable information (PII) for its customers must be able to identify all files that contain PII, and then take action to protect it from leaking outside of the organization.

Policy actions range from lightweight visibility mechanisms to outright blocking. A lightweight CASB action might be to allow data to be downloaded, but either encrypt or track that data (see "On the Device" section for more detail). More aggressive actions would include redacting sensitive data from a particular transaction, or blocking a file from download altogether. Every organization must make judgments and create policies around what type of actions to take based on applications, users/groups, and data.

On the Device

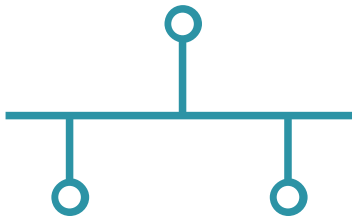
When most people think about cloud app security, they think about controlling access to apps like Salesforce and Office 365, providing visibility into who's doing what in ServiceNow and Workday, and even encrypting data at rest in Box and Google Apps. These are all solutions to protecting data in cloud applications.

An even bigger challenge for many enterprises is the point of consumption—the devices from which employees are accessing and downloading data from these cloud apps. In order for Box to really be effective, employees need to be able to download files to their myriad mobile devices. And once those files are on the mobile devices, a whole new set of security concerns arises.

CASBs must protect not only data stored in the cloud and access to the cloud, but cloud data on the consumption device as well. Capabilities must include:

- Client-side file encryption of sensitive corporate data. CASBs should offer the ability to tie data classification policies to data transferred through the CASB, encrypting the most sensitive data on the fly so it is accessible only to the authorized user downloading that data. This eliminates the possibility of sharing sensitive data outside of the organization.
- Selective wipe of cloud data from mobile devices. Employees lose devices or leave the company on a daily basis. Since most MDM/MAM solutions can't provide comprehensive solutions for third party cloud apps like Google Apps or Office 365, your CASB must take on the responsibility of removing corporate data from devices when necessary.
- Data Tracking and Fingerprinting. Some corporate data may be judged as not so sensitive that it should be encrypted upon download, but should still be tracked. CASBs offer the ability to embed fingerprints into corporate data that can identify who removed a particular file from the cloud application. This capability provides an ability to track the source of leaks, should they occur, and also acts as a deterrent to employee malicious behavior. Some CASBs have combined this capability with callback mechanisms so that the enterprise gets notification when and where corporate data is being accessed outside of the enterprise. This can provide advance warning or notification of a potential leakage event.
- Enforcing basic device security policies. Any device on which corporate data is synchronized must have basic security measures in place, including passcodes and encryption. At a minimum, your CASB must verify that these policies are in place before allowing access to cloud data. Some CASBs provide the ability to enable these policies as well.

On the Network



"Shadow IT" is a concern for many enterprises, as they don't always know which cloud applications are in-use in their organization. It is important to be able to identify the cloud apps in use on your corporate network, and then take the appropriate action.

Using a log analyzer, analyze the access logs on your firewall or DNS service to extract list of all apps in use at your company. If you have a next-generation firewall or secure web gateway, you already have a source for this data. You can also use free or paid commercial services, some of which are offered by CASB vendors as an ancillary service, for identifying cloud apps via log analysis.

Keep in mind that not all cloud apps are "Shadow IT." Many employees use cloud apps like Twitter, Facebook or Dropbox for their own personal use. Inspection of personal use apps can run afoul of employee privacy concerns and should be carefully thought through before proceeding.

Recognize that inspecting and restricting data flowing into cloud apps is not a good way to control Shadow IT. If the app is useful for business, then you don't filter it. If the app is not useful for business, then you either block it or leave it be. Even blocking itself is not always feasible—if you block an employee on a corporate network, they can generally find an unrestricted Wi-Fi network elsewhere on which to connect to the blocked app(s).

CASB Architectures and Deployment

PROS:

- Can be used for all application types, including client-server apps with hard-coded hostnames.

CONS:

- Difficult to deploy in a distributed environment with a mobile workforce.
- Reduced end-user privacy—both personal and corporate traffic are captured and inspected by the proxy.
- Requires installation and user-acceptance of self-signed digital certificates at each point of use.

CASB architectures vary from one vendor to the next. Most vendors have a primary proxy mechanism upon which their architecture is built—either a forward proxy or a reverse proxy. It is important to consider how each architecture is deployed and managed, as it can have a big impact on the application and device types that can be supported, and on the amount of operational overhead associated with managing the system.

Also keep in mind that web/HTTPS traffic is only a piece of the overall puzzle. For example, a cloud-based email system like Office 365 can be accessed via the web, but also via Microsoft Outlook, Mac OS X Mail, and just about every smartphone and tablet via Activesync. If your CASB can't secure these alternative access types, your coverage is incomplete.

FORWARD PROXY FOR CLOUD APPLICATIONS

When deploying a forward proxy for cloud applications, the IT administrator must ensure that every firewall or browser through which the application may be accessed is configured to proxy the traffic for the cloud applications. This requires modifying proxy settings on user devices and firewalls across the company, which can be a substantial administrative burden.

Since the proxy terminates and inspects SSL traffic for application domains owned by third parties, the proxy must also carry self-signed digital certificates that masquerade as the original domain. For example, a forward proxy that handles salesforce.com must masquerade as salesforce.com via a self-signed digital certificate for salesforce.com. Any browser used to access the application must also install and accept such a self-signed digital certificate. Distribution and installation of certificates is an additional administrative burden. In summary, here are the pros and cons of the forward proxy approach for cloud applications.

CASB Architectures and Deployment

REVERSE PROXY FOR CLOUD APPLICATIONS

A reverse proxy deployment for cloud applications is similar to an SSL VPN in that the proxy presents modified URL's for each application, e.g. http://www.salesforce.com may be reachable via the proxy as http://www-salesforce-com.proxy.net Users may login to the proxy from any browser to land on a portal page of applications to which they have access. To effectively enforce access control policies, bypassing the proxy for direct access to the cloud application is disabled.

Use of a reverse proxy architecture is the superior choice for proxying cloud applications, and should be employed wherever feasible. In specific use cases where deploying a reverse proxy might be technically infeasible, a forward proxy may be used. Specifically, client/server application such as native mobile applications with hard-coded hostnames may require a forward proxy.

PROS:

- Accessible from any device or location, making it suitable for a mobile workforce.
- End-user privacy—only corporate traffic is sent via proxy. Users may access a personal version of a cloud application directly. e.g., corporate Gmail is proxied but not personal Gmail.
- Simple to deploy and use, no configuration on mobile devices or firewalls required.

CONS:

- Not applicable to client-server applications with hard-coded hostnames.

Summary

Cloud Access Security Brokers are quickly emerging as a must-have security solution for organizations looking to adopt cloud-based applications. These technologies fill in the gaps that cloud app vendors have left to the enterprise to solve—visibility and data security. Look to solutions that can secure cloud data wherever it goes—from the cloud to the device. If you have deployed cloud apps or are planning to, you should educate yourself on the offerings available, and ensure that your budget includes a CASB deployment to coincide with your rollout of cloud apps. These technologies fill in the gaps that cloud app vendors have left to the enterprise to solve—visibility and data security. Look to solutions that can secure cloud data wherever it goes—from the cloud to the device.

Want to hear what the analysts are saying about Bitglass and CASBs? Reach out to Neil MacDonald or Peter Firstbrook at Gartner.

bitglass

About Bitglass

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they were developed to secure the corporate network perimeter. The Bitglass Cloud Access Security Broker solution transcends the network perimeter to deliver total data protection for the enterprise—in the cloud, on mobile devices and anywhere on the Internet.

For more information, visit
www.bitglass.com

Phone: (408) 337-0190 | Email: info@bitglass.com