How to Boost CASB Security for Your Agency

zscaler™

A cloud access security broker (CASB) extends an agency's security policy to third-party cloud services. It provides visibility into the cloud services an agency uses and then builds policies to control the usage of sanctioned vs. unsanctioned cloud apps.

As such, a CASB is a critical cloud security tool. In some situations, it may be enough on its own, although those situations are increasingly rare. Why? CASBs do not provide security protection features, such as (but not limited to) web content filtering and advanced threat protection.

For that level of security, the CASB needs to be bundled with a secure web gateway (SWG).

What is an SWG?

An SWG protects enterprises and users from cyberthreats while enforcing corporate policies and may include a range of features incorporated as an integrated platform, such as:

- Web-content filtering
- Cloud-app discovery and management controls (in the CASB)
- Data loss prevention (content inspection and action)
- Advanced threat protection (against malware, phishing, and more)
- SSL inspection
- L4-L7 firewall
- DNS traffic management
- Bandwidth management
- Logging

A cloud-delivered SWG may also implement functionalities found in CASB through its inherent deployment model—inline visibility provides protection and enforcement for cloud apps. But, the optimal scenario for complete security protection is an SWG that includes CASB functionality. Zscaler™ provides that solution.

An in-depth look at CASB

How do you decide whether CASB alone will meet your agency's needs, if you need an SWG that includes CASB functionality, or you need to work with a CASB provider that partners with SWG vendors?

The first step is to look at the four implementation areas for CASB solutions in the market today.

1 Forward proxy.

- Supports all apps (sanctioned and unsanctioned)
- Works with browser and native apps
- Provides real-time discovery and governance
- Often requires an agent

2 Reverse proxy.

- Supports only sanctioned apps
- Works only with browser apps
- Provides real-time discovery and governance
- Does not require an agent
- Includes a rewrite engine that can break an application

3 Out-of-band CASB.

- Supports only sanctioned apps
- Has no network changes and no agents
- Works well with browser or native apps
- Is compatible with all device types and locations
- Provides near real-time discovery and governance

4 Log parsing.

- Supports visibility for all apps (sanctioned and unsanctioned)
- Is frictionless, avoiding a change to the traffic flow
- Features a parsing architecture that can frequently break when vendors change traffic feed or have excessive log volume
- Often requires a complex deployment, needing to organize traffic feeds from all sources that could discover cloud apps in use
- Does not provide enforcement functionality as it is purely logging and visibility

How stand-alone CASB performs in relation to these implementation areas

Stand-alone CASB does not support forward proxy. There is no forward proxy service that exists as part of a platform to provide active blocking and protection. Some CASB providers partner with an SWG security vendor to provide and integrate with the log parsing scenario.

For example, Microsoft partners with Zscaler to provide the SWG for its Microsoft Cloud App Security (MCAS). In 2019, Zscaler was awarded the Microsoft Technology Partner of the Year in part because of the integration we built with MCAS.

Because Zscaler is an inline protection engine doing SSL inspection as a function of the platform, it not only discovers cloud apps, but can also control interaction with them.

Zscaler enables the following granularity of control as a forward proxy. A few examples include:

- Upload/Download-level control based on the cloud app (for example, allowing downloads from Box but blocking uploads)
- Read/Post content (for example, allowing users to read Twitter but blocking the posting of new tweets)
- File type control (for example, blocking the download of EXE and ZIP files from unapproved cloud services)
- File size control (for example, blocking the upload of ZIP files greater than 5 MB)
- File content control (for example, blocking the downloading of password protected ZIP files)
- Data loss protection in transit (for example, blocking the upload of web traffic, including files that contain PII, financial data, HIPAA information, source code, Salesforce data, weapons, gambling, drugs, adult content, restricted handling tags, RegEx/pattern matching, etc.)
- Protocol-level control (for example, only allowing SSH to approved cloud apps)

Stand-alone CASB does not support reverse proxy. There is no reverse proxy capability as part of a CASB service.

Zscaler enables this use case through the identity proxy functionality, in which Zscaler acts as a SAML IdP proxy between the user and supported cloud app services. This capability enables an agency to build policy from within Zscaler that prevents a user from signing on to a protected cloud application unless the traffic to the cloud application is sourced from Zscaler. The Zscaler approach does not rely on a rewrite/reverse proxy engine because it is integrated on the authentication side.

Stand-alone CASB does not support out-of-band CASB. Out-of-band CASB is accomplished through an API-based approach for connecting to supported cloud app services and scanning the content at rest, as well as through activity indicators associated with supported cloud apps. This encompasses four different functions:

- Login authorization (who can access what cloud apps using the cloud provider's API)
- Login activity (for example, a cloud provider API indicating a high number of logins, password failures, unexpected country of access)
- Analysis and discovery of cloud applications in use (for example, an alert is triggered when a new unsanctioned cloud app is used) through log data that is fed to the CASB via third-party log collection (see log parsing)
- Data loss prevention (PII, financial data, HIPAA, and RegEx only) of content at rest via a scanning engine that runs on a schedule (for example, an alert is triggered if PII is stored in a supported cloud provider or if a file containing SWIFT codes is shared with a third party)

Blocking capabilities are subject to the limitations of the supported cloud service partners. That means only a subset of integrations may support the functions listed above.

While Zscaler does not yet support out-of-band CASB for federal customers, this functionality is in beta testing in our commercial cloud and will be available in the FedRAMP cloud in late 2020 or early 2021. Zscaler will use the same security and protection engines as those found in our forward proxy engine to perform enforcement and provide centralized policy control for data in rest and in transit.

Stand-alone CASB and log parsing. MCAS covers log parsing via the use of a log ingestion service. This is handled through one of the following approaches:

- A log connector VM in a Docker container in which web traffic logs are forwarded via syslog/CDF/ etc. to the log connector VM
- An FTP ingestion service where logs are uploaded
- Manual log import through their web portal

Log parsing only provides visibility into traffic violations (for example, users accessing an unsanctioned cloud app) and configuration of governance policies around what cloud apps are blocked. There is no actual blocking of the traffic (enforcement) function. A technician, such as a SOC resource, needs to perform that function manually to correlate cloud app usage and identify violations—based on the log data fed to the CASB—to a policy (block script) on a third-party traffic inspection device, such as a web content filter or firewall. There is no way to correlate and validate that a third-party device has all the blocks that are configured in the CASB without doing a manual audit. That enforcement/blocking function would need to be scripted manually if the CASB vendor does not have out-of-the-box integrations for third-party tools.

When Zscaler is integrated with a CASB, it automatically ingests the blocked cloud app governance policies from the CASB and creates block rules to prevent users from interacting with the unapproved cloud apps. This occurs automatically without user intervention through an API, so there is no need to manually audit whether services or engines are in sync.

Conclusion

CASB is a fantastic tool that every federal agency should be using to make data more secure. However, CASB alone does not meet all of an agency's security needs. When sourcing a CASB solution, make sure your vendor of choice has an integrated SWG or is partnering with a provider that does. See how **Zscaler's CASB** solution can help secure your data.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com