SECLORE

Extending Data Security for Cloud Access Security Broker (CASB) Solutions

Extending Data Security for Cloud Access Security Broker (CASB) Solutions

As a Cloud Access Security Broker (CASB), you are able to offer many values to an organization:

- Visibility – Offering quick insights and visibility into cloud usage, the flow of data, and identification of risks and gaps in policy enforcement.
- Threat Protection – Identify and remediate insider and privileged user threats in trusted cloud services.
- Compliance – Identity sensitive data in motion or at rest in cloud services and enforce data loss prevention policies across multiple cloud services.
- Data Security – Access control and data security via encryption.

However, the data security offered by stand-alone CASB solutions stops once a file is decrypted by the intended user. That's where Enterprise Rights Management comes into play.

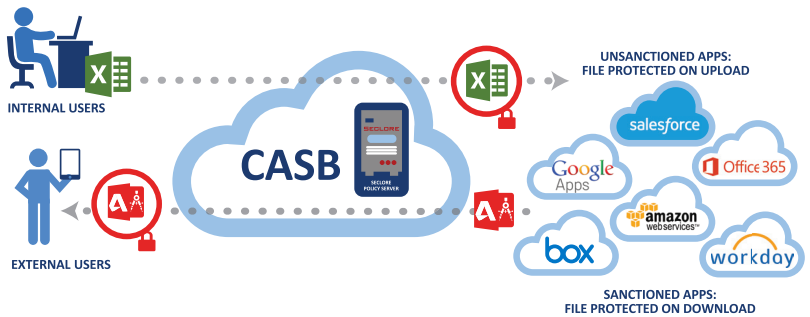
Securing the Last Mile: Protecting Files That Reach the Intended User

Once a file reaches an intended user, the CASB does not offer a way to control what actions the user can take on the file (view, edit, copy, print, screen capture e.g.). While the file may be encrypted until it reaches the intended user, once it is decrypted, that user can do anything with the file. Additionally, the organization will lack visibility as to what the user has done with the file, or if it was re-shared. As well, a business process can be disrupted if the only option is to 'grant access' or 'not grant access'. If the sender could share the file while maintaining control over what the recipient was able to do with the file, including time-bombing, then the collaboration would continue uninterrupted.

Where Seclore's Enterprise Rights Management Adds Value to CASB Solutions

Seclore's Enterprise Rights Management will enable you to extend the data security and compliance capabilities of your CASB offering. Specifically, Seclore's value propositions are as follows:

1. **Persistent, Granular Data Security**
   Seclore goes beyond standard data encryption with the ability to persistently control highly granular usage policies.
2. **Robust Compliance Reporting**
   Authorized and unauthorized file usage attempts and actions are automatically collected throughout the life of the protected file.
3. **Extending the Power of Data Loss Prevention**
   Persistent usage controls can be automatically applied to files that are detected by CASB DLP, ensuring sensitive content, originating from any source repository (EFSS, VDR, ECM, ERP) is secure.
4. **Policy Normalization**
   Leveraging Seclore's Policy Federation Framework, the policy is fetched via the CASB in real-time the moment the file is accessed. This allows the CASB to normalize policies across ALL cloud applications.



Seclore provides very granular and persistent file-centric usage controls which go beyond access controls and encryption. Our software can control what actions are taken against the content including: editing, printing, copying and pasting, as well as screen prints. We can even control when the content is available with configurable expiry dates or time-bombs, as well as where the content can be accessed – specifically IP ranges or the restriction of mobile access. Usage rights to content can be modified or even revoked after distribution no matter how many copies have been created by the authorized recipient.

One of the keys to reliable adoption of an ERM solution is ease of use. Recipients of Seclore-protected files can:

- Easily authenticate due to robust identity federation capabilities,
- Access protected documents from any device (Windows, MAC, Android or iOS)
- Open a protected document via a browser or light-weight agent (native application viewing)

To ensure an uninterrupted user experience, the file extension is maintained so the content opens in its native format.

Additionally, and perhaps most unique to Seclore, our Policy Federation Framework allows the inheritance of security policies from the source solution, which may be from an EFSS, ECM, ERP or any other Cloud solution, or from the CASB itself. The organization will not need to maintain and administer a separate 'rights' policy within Seclore's environment.

Lastly, Seclore's audit logs can extend your CASB compliance framework by automatically capturing both authorized and unauthorized usage activities across the distributed unstructured content. This audit trail can be easily consumed by the CASB in order to present a single dashboard for all compliance reporting.

Benefits of CASB + Seclore ERM

The combination of Seclore ERM with your CASB solution will offer your customers a more powerful way to manage, secure, and audit the information that is flowing between cloud applications and users. Some specific benefits include:

- CASB becomes the ERM file-centric security broker for all cloud applications
- Extend usage control policies beyond encryptionvwith the ability to control specific actions (view, edit, print, screen share, copy, etc.)
- Extend file-centric security to wherever the information travels, even while the document is at-work or at-rest outside of the organization's perimeter.
- Automated file-centric security; No user intervention is required to apply the usage controls
- Zero impact on business workflow; the seamless integration and ability to utilize any device and protect any file type makes it easy to engage in secure external collaboration
- CASB becomes the "policy of truth" across ALL cloud applications with centralized policy federation for information usage policies
- Robust file-centric audit data including detailed insights on authorized actions on files and unauthorized usage attempts

Ease of Integrating Seclore ERM with Your CASB Solution

Seclore is designed specifically for ease of integration with other enterprise systems and infrastructure. Our connectors have been built using our fully published API Library available in both Java and .NET. As such, we have found that connectors are typically built within a matter of weeks.

Summary

By enhancing and extending your CASB solution's data protection and compliance capabilities, you will be able to differentiate your solution from the competition, offer additional value to your existing customers, and attract new enterprise customers.

SECLORE