VERA SECURITY SOLUTIONS BRIEF

HOW VERA EXTENDS FILE PROTECTION IN CLOUD ACCESS SECURITY BROKERS (CASB)

Introduction

Cloud Access Security Brokers are a relatively new entrant to the enterprise security stack. As the name implies CASBs help to secure organizations accessing cloud applications. Gartner defines CASB as:

“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.”

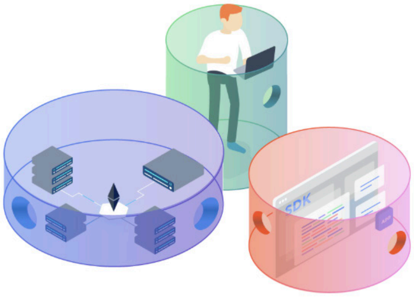
CASBs have proven to be highly valuable to enterprises on a variety of fronts. At their core, a CASB is able to extend security policy to an enterprise’s cloud applications in much the same way a traditional firewall would protect on-premise applications.

Organizations can control who should get access to a cloud-based app, what features they should be able to use within that app, and so on. A CASB can also give an organization insight into what applications are being used so that they can better understand user needs and their attack surface. With this similarity to traditional firewall functionality, it’s no surprise that most firewall vendors have acquired or integrated CASB functionality into their offerings. This similarity to firewalls also begins to highlight the differences between VERA’s content-based security and CASB. In fact, VERA closely partners and integrates with CASBs as opposed to competing with them. One of the major differences can be found in the definition of a CASB itself.

Revisiting the definition above, a CASB is an enforcement point when cloud resources are accessed. Once again, this is a point-in-time, localized approach to security. It effectively extends the physical perimeter of a local network to a new perimeter specifically for cloud applications.

What we see is that a CASB can lose control over data after it has been accessed. Users can still copy the content, store it in insecure personal drives, share it with other parties, or have it compromised by malware or attackers. While a CASB can help illuminate an application blind spot, it does not ensure that data itself remains safe.

This is where VERA compliments a CASB solution.



How VERA + CASB Works

VERA protects unstructured data, and a CASB allows you to fulfill the gaps in structured data. From an unstructured data perspective, when VERA encrypts a file in Box, it can break some of the functionality of Box, namely search. You can use a CASB to protect the file as it's sent to Box, and gives the ability to use that file while it's unencrypted, so you have the benefits under their infrastructure. However, when that file starts to egress and leave the company, that's when the CASB would call on the VERA API to extend their protection, encrypt the files, and maintain that ownership of the file, once it leaves the protection of the CASB sphere.

VERA + CASB gives organizations a chance to open up their ruleset so they can be more flexible and still stay secure. With any system, you can lock down information such that it becomes difficult for employees to do their jobs. This is one of the more powerful things VERA offers when we work with CASB solutions - we can give customers the best of both worlds.

Capabilities

CONTENT INSPECTION AND APPLY POLICY

Documents residing in a OneDrive folder are sensitive. CASB can run DLP on those files and detect sensitive content. A policy has been defined to protect sensitive documents in VERA, and the CASB solution protects the document by calling the VERA API to encrypt the document.

INHERIT APP PERMISSIONS

Documents in Box folders which are shared for collaboration with external parties are also protected by VERA + CASB solutions. When the CASB detects sensitive documents, VERA policy is executed and the permitted users are inherited from the Box folder collaborators. For example, users that have view-only rights get a policy that is different from the policy that is applied to users that have read-write permissions.

REVISE VERA POLICIES BASED ON CONTENT

When documents are already protected, the CASB can decrypt the content to be able to apply DLP on the document. When the content scanning is complete and the CASB determines that the VERA policy should be escalated, the CASB will re-apply a new VERA policy based on the sensitivity level of the document.

VISIBILITY AND ANALYTICS ON PROTECTED DOCUMENTS

When customers use the CASB's analytics engine to report on VERA protected content, they can see that certain documents are protected with VERA. Administrators can run reports on protected vs. non-protected documents to understand the risk exposure.