VERSA NETWORKS

WHITE PAPER

Cloud Access Security Broker

A New Strategy for Strong "Sensitive Information Protection"

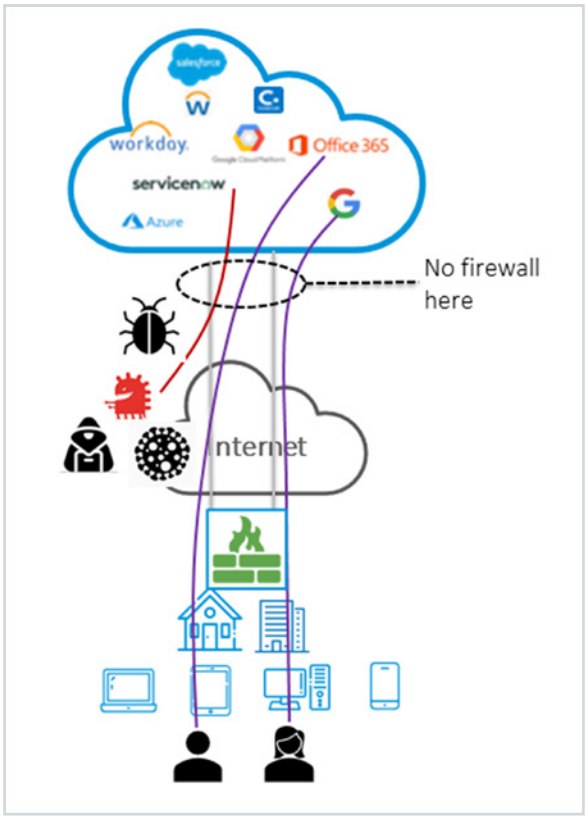
A Cloud Access Security Broker (CASB) is a cloud-based security function that controls access to cloud applications and data. A CASB enables enterprises to implement security policies governing which users and devices have access to cloud applications and information stored in the cloud.

Why Do You Need a CASB?

Enterprises must always safeguard their intellectual property and restrict access to sensitive customer information. Reasons for protecting information include maintaining competitive advantage, compliance with regulatory requirements, and meeting customer privacy expectations and regulations.

Historically, when enterprise information was kept on paper, company information was secured in a physical, locked location that restricted human access. With the advent of the computer networks, enterprises implemented perimeter security using firewalls to safeguard digital access to information in data centers located in enterprise-owned and secured buildings and networks.

More recently, the trend in cloud transformation means corporate applications, workloads and information are increasingly migrating to an inexact, non-enterprise-owned cloud location that limits the enterprise's ability to either physically or digitally safeguard its information. While enterprise IT staff retains system administrator privileges on their personal view of their own cloud-resident resources, they do not have any such privileges or visibility into the cloud platforms that the resources reside on. Enterprise IT also do not control which cloud platforms contain their applications and data, where these platforms are physically located, the access to these platforms, or how the platforms are shared with other enterprises' resources.



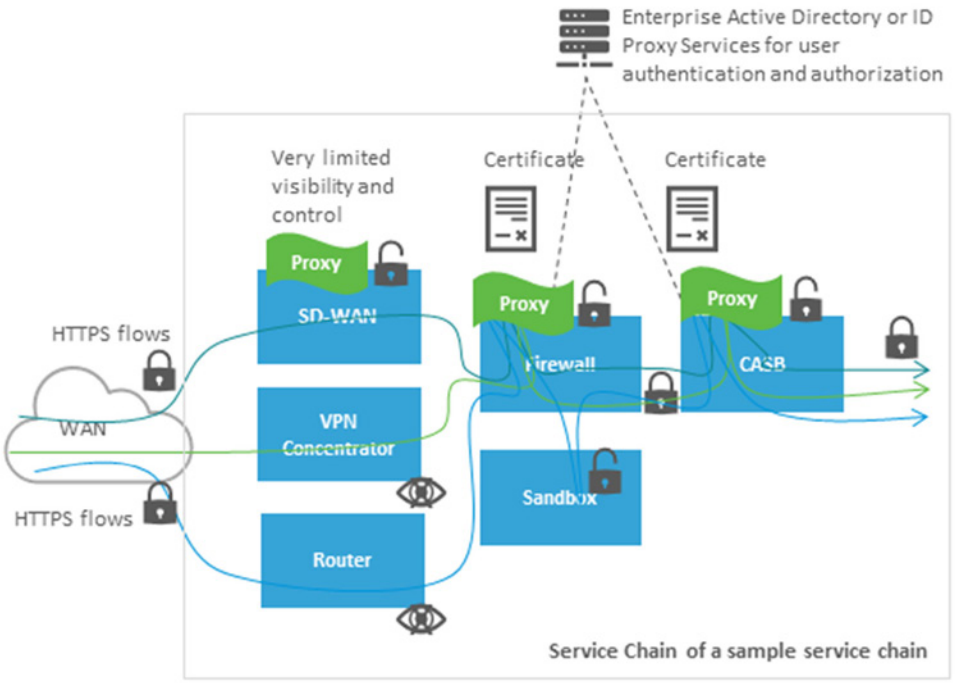
With on-prem data centers, perimeter firewalls determined what information could leave the company premises, and accessed by whom. With the information now resident in the cloud, it is suddenly accessible from anywhere and everywhere—the enterprise perimeter and its control have disappeared. Threats as well as legitimate access now come from any direction across the internet towards cloud-based applications and data.

Enterprises must implement protected access to their applications and information stored in the cloud. With the dissolution of the enterprise network perimeter, the remedy must be cloud-based and must focus on the verifiable credentials of users, devices, applications and data rather than physical buildings or locations. The solution must determine if any request for cloud access should be granted, which authentication and policy functions must first be satisfied, and how and when to permit information to be uploaded or downloaded from the cloud.

Why Using Enterprise-located Proxies doesn't Work

When cloud solutions first became a trend, enterprises adopted a complex configuration of on-prem proxies to ameliorate cloud access security gaps. A virtual private network (VPN) proxy could allow an enterprise to authenticate and secure a connection for access control purposes. A firewall proxy could enforce a policy to restrict what information could be accessed.

Proxies operate by being in the traffic path, which means all sessions must be backhauled to a fixed corporate location, steered from one proxy to the next, and then exit towards the cloud. This traffic architecture violated stringent delay and jitter requirements to the detriment of application performance and user experience. It also introduced massive traffic scalability bottlenecks in the location where the proxies were located. Further, the solution required multiple proxies, with attendant operational complexity. An on-prem proxy solution also imposed increased network and compute capacity as both the traffic to and from the requestor, as well as the traffic to and from the cloud resource, had to be transported over the same connections.



It quickly became apparent that a cloud-based solution was imperative to provide feasible, scalable and secure cloud access, while at the same time minimizing delay, distributing traffic patterns for better scalability, and preserving an acceptable user experience.

The Cloud Access Security Broker (CASB) Solution

A CASB is a cloud-based security policy enforcement function that authenticates access to cloud applications and data based on the identity of the user, device and application. A CASB implements enterprise policies to govern who is granted access to cloud applications and information stored in the cloud: it integrates with the enterprise's Identity Provider (IdP) to authenticate the identity of the user, or device, with the application or data to be accessed.

A CASB:

- Is application-aware to integrate with the SaaS application provider
- Must intercept, or have visibility into, the activity that the user wants to perform in the specific SaaS application
- Makes access policy decisions to allow/deny the transaction or information request

An optimal CASB solution offers granular policy definitions to enable an enterprise to control access at many levels, including file, application, individual, device, or organization.

CASB architectural models allow several different modes of operation. Some choices may be better suited to your needs than others. It's important to choose an architecture that fits well into your network's overall architectural strategy.

- Agent-based and Agentless
- Inline and Out-of-Band
- Real-time and near-real-time

Agent-Based and Agentless CASB Architecture

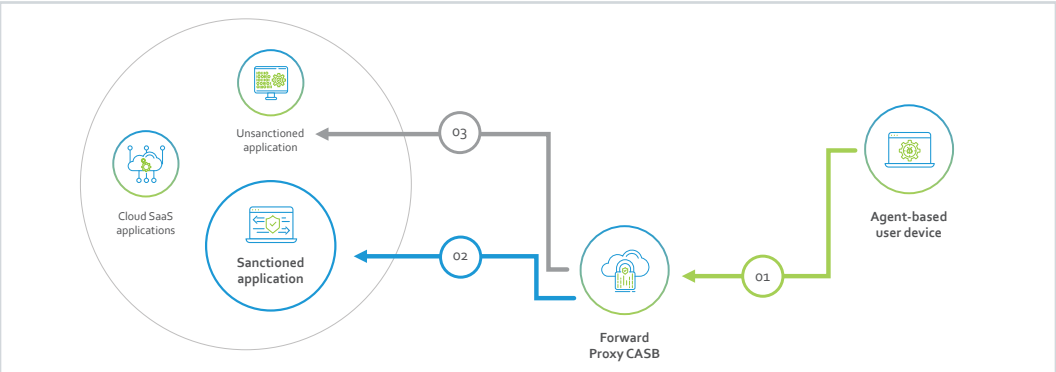
An **Agent-based CASB** uses a software agent installed on the user device to steer cloud-destined traffic originated by the device to the CASB. The Agent applies identity policy decisions at the point of access on the device. Additional policy and security can be implemented in the CASB itself, or via cloud security.

An **Agentless CASB** does not require software to be installed on the individual's device to access information in the cloud.

The Agent-Based CASB Model

The Agent-based CASB model allows significant control over all cloud access because the CASB is aware of all cloud applications and sees all cloud-destined traffic. However, this model is limited in scope in the number of individuals and devices that can be secured. Enterprises can easily install the Agent on all enterprise-owned devices. The enterprise may also require employees to install the Agent on employee-owned devices, if the device is used to access enterprise cloud applications or data.

In the diagram below of an Agent-based CASB model, all cloud application access from the device's Agent is directed to the CASB which acts as a forward proxy. This enables the CASB to see all application traffic and therefore control access not just for enterprise-sanctioned SaaS applications (1, 2), but also for "unknown" SaaS applications (1, 3).



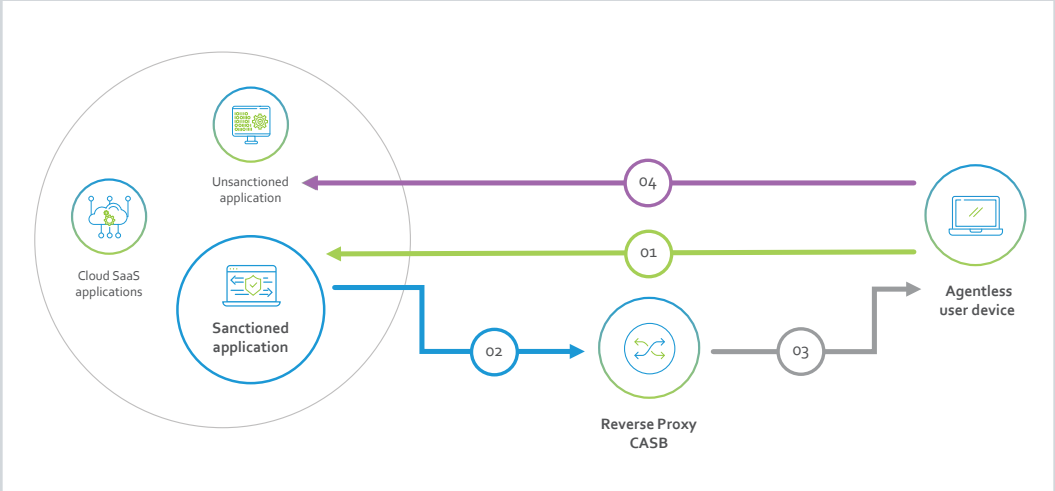
A drawback of the Agent-based model is that requiring partner and contract workers—with a non-exclusive relationship with the enterprise—to install an Agent on their devices may clash with other CASB Agents for other enterprises they do work for. This may make an Agent-based CASB solution difficult or impossible to implement for non-employee workers. Additionally, IOT devices typically do not allow for any type of Agent software to be installed.

While the Agent-based CASB model provides excellent coverage for all types of cloud applications (enterprise-sanctioned and "unknown"), restrictions regarding full device support limit the scope of an Agent-based CASB solution.

The Agentless CASB Model

The Agentless CASB model requires no specific software to run on the device accessing the cloud, and therefore allows access to enterprise cloud information from any device, anywhere: all enterprise-owned devices, individual-owned devices, IOT devices, as well as customer, partner and contractor devices. However, use cases remain where this CASB model cannot properly secure access to some cloud resources.

The Agentless CASB model readily protects enterprise-sanctioned SaaS applications: the application is configured to redirect requests either to the CASB (which acts as a reverse proxy), or to the IdP which in turn redirects to the CASB (1,2,3 in the diagram). The scenario where an Agentless CASB model cannot provide protection is when unsanctioned SaaS applications are accessed as no CASB redirection configuration exists on these "unknown" applications (4).



Inline vs. Out-of-Band CASB

An **inline CASB** is located directly in the traffic path between the device accessing the information and the cloud where the information is stored or where the cloud application is running.

An **Out-of-Band (OOB) CASB**—also referred to as an offline or API-based CASB—allows the CASB to enforce security policies without being in the traffic path.

Inline CASB Model

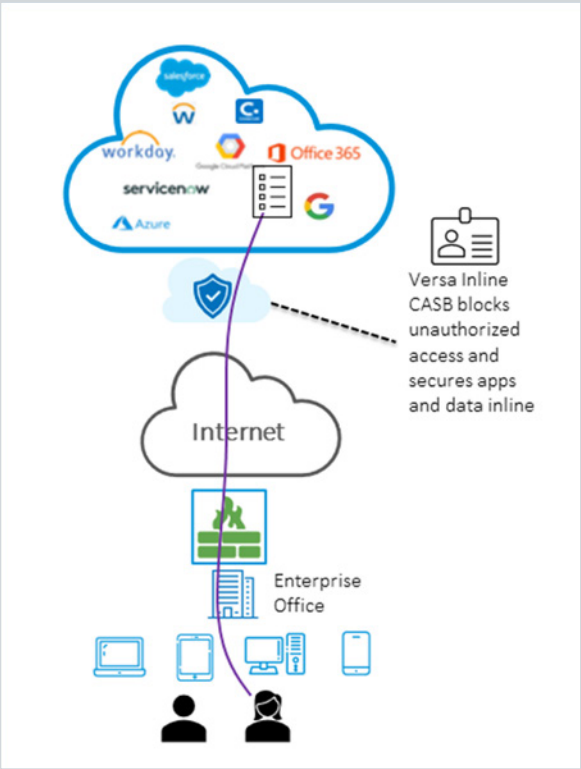
In the inline CASB model, the CASB operates as a full proxy (both forward and reverse), meaning that the traffic passes through the CASB and can therefore be inspected. As a proxy, an inline CASB exerts access control by:

- Integrating with the enterprise's IdP to authenticate the individual/device requesting the access
- Enforcing corporate policies that determine if access is authorized
- Ensuring that there is no deviation from the authorized policy

The inline CASB evaluates different parameters to ensure compliance with corporate policies governing information access, including:

- How to authenticate the requestor
- Applying various criteria such as location, access-method, device used, or the classification of the information
- Whether the data accessed is allowed only to be read, or also to be modified

The inline CASB model provides the enterprise with full control over access to enterprise cloud applications and information because all traffic flows through the CASB.



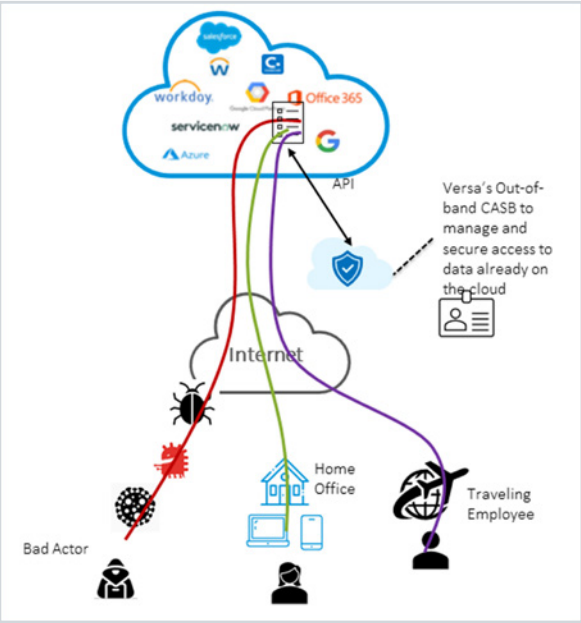
Forward Proxy Operation

A forward proxy is generally used in the Agent-based CASB model, but can also be used for the Agentless model. The forward designation means the enterprise forwards the traffic to the CASB and then on to the cloud.

A forward proxy can be instantiated by a proxy PAC (Proxy Auto-Configuration) file installed on the web browser, via DNS redirection, or by an enterprise tunnel solution. The tunnel architecture allows legacy routers/firewalls or an SD-WAN solution to participate in the CASB solution. For example, an enterprise router or perimeter firewall can be configured with a VPN tunnel to direct all traffic to the CASB for inspection and access policy enforcement. The tunnel method additionally allows Agentless devices (devices that do not, or cannot, run a CASB agent, such as IoT devices) to benefit from CASB security.

Reverse Proxy Operation

The reverse proxy is generally used in the Agentless CASB model. The reverse designation means traffic initially flows from the device requesting access directly to the cloud, and the cloud SaaS application redirects (based on configuration) the traffic to the CASB, or more commonly to the enterprise's IdP which in turn redirects traffic to the CASB. Because the reverse proxy model requires SaaS application participation (via configuration), only enterprise-sanctioned SaaS applications can support a reverse proxy deployment. However, this model requires no device-specific client, and therefore allows any and all devices to participate in the enterprise's CASB security solution.



Out-of-Band CASB Model

There are scenarios where enterprise-sanctioned SaaS applications do not provide a method of traffic redirection to the CASB. Without redirection, an inline CASB does not see the traffic and cannot provide security protection. For this use case, an OOB (or API-based) CASB can be deployed.

There are also scenarios where the cloud service does not allow a proxy (such as an inline CASB) to act on behalf of the requestor. This is commonly referred to as certificate pinning: a security method that assures the cloud platform that the entity accessing the information is only that entity and not an imposter. From an enterprise's point of view, an inline CASB is helpful as it provides the enterprise with oversight into what cloud information is accessed. But from the cloud service's point of view, the CASB proxy (representing the end user/device) is indistinguishable from the appearance of a malicious man-in-the-middle attack on the cloud service. An OOB CASB can help cover these types of scenarios.

The OOB CASB uses API calls between the OOB CASB and the cloud/SaaS provider. This enables the cloud service to query the CASB when a user makes an information request, a new file is uploaded, or a file modification is made. The OOB CASB determines if the access is permitted, and communicates back to the cloud service whether the access request (and associated action) is to be granted or denied. Once granted, the traffic flows directly between the user device and the cloud without a proxy in the path.

This OOB type of deployment does not generally provide as good application performance as an inline CASB (proxy). However, a high-caliber CASB solution uses multiple mechanisms to ensure near real-time performance of any type of request.

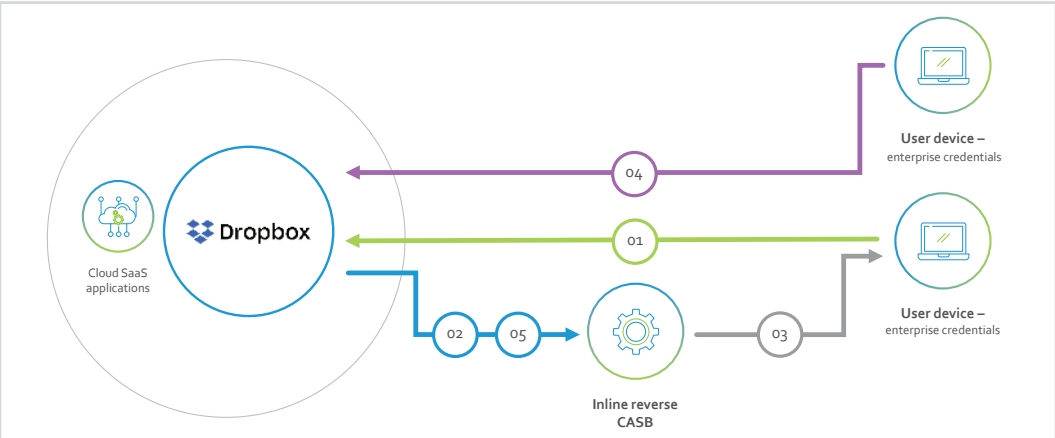
Contrasting Inline and OOB CASB Models

Both the inline and OOB CASB deployment models provide good coverage for many, but not all, uses case. Each method is also limited in some use cases that cannot be covered.

Accessing a SaaS Application with Redirection

The diagram below shows a redirect access scenario from an enterprise-sanctioned SaaS application where the inline CASB is implemented via a reverse proxy. The appropriate enterprise credentials must be supplied to access the enterprise-sanctioned SaaS application, so the reverse proxy CASB uses associated information to detect and prevent the use of personal or non-enterprise provided credentials.

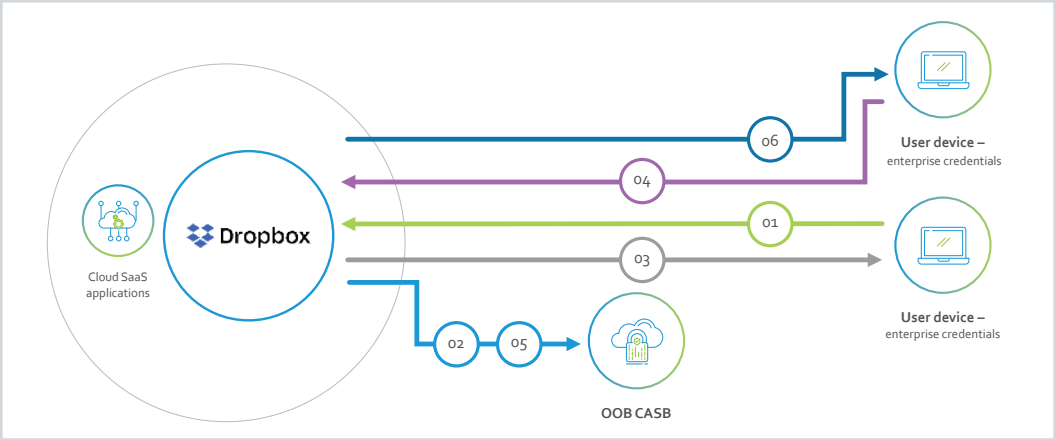
For example, if an enterprise sanctions the use of Dropbox and a user accesses the enterprise version of Dropbox (perhaps to upload files) using enterprise credentials (1, 2, 3) then the access is granted. However, if they access Dropbox with their personal credentials, then access can be detected and denied (4,5).



Accessing a SaaS Application that does not Support Redirection

In a scenario where the user session goes directly to a sanctioned SaaS application, but no redirection is supported to enlist a reverse proxy inline CASB, all traffic bypasses the CASB. This could happen if the sanctioned SaaS application does not offer a mechanism to redirect traffic, or if the communication is pinned in a manner that does not allow the insertion of a proxy.

Following on from the previous Dropbox example, the user now first accesses the enterprise version of Dropbox using enterprise credentials (1, 2, 3) using an OOB CASB, and the access is granted. If the worker now goes home and accesses Dropbox with their personal credentials, the OOB CASB can still provide protection (4,5,6), remediate uploaded files, and prevent files from being downloaded or shared. For this scenario tight integration with the enterprise SaaS application is required: the OOB CASB must have system administration privileges into the enterprise SaaS application.



Accessing Sanctioned and Unsanctioned SaaS Applications

An OOB CASB does not offer any protection for "unknown" and un-integrated SaaS applications: these "unknown" applications are not configured to query the CASB before granting access. If a user initially goes to their private SaaS application ("unknown" or unsanctioned) and subsequently goes to the sanctioned SaaS application, an OOB CASB can neither detect nor prevent this. However, any information that might have been downloaded from the unsanctioned SaaS application, and is subsequently uploaded to the sanctioned SaaS application, can still be remediated by the OOB CASB during the upload action.

Data Access Protection in a SaaS Application

While an inline CASB can protect actions (such as a file upload) in a SaaS application in real-time as they are performed, an inline CASB does not have the ability to inspect information already previously stored in the SaaS application. This scenario typically happens when the CASB solution is adopted after the cloud-based SaaS application or data repository has already been established.

Since an OOB CASB uses APIs to communicate with the SaaS Application, an OOB CASB is able to scan all the data at rest in the application—regardless of when it was stored—and can therefore identify, remediate, or isolate sensitive or malicious information.

Timeliness of Malware Detection or DLP

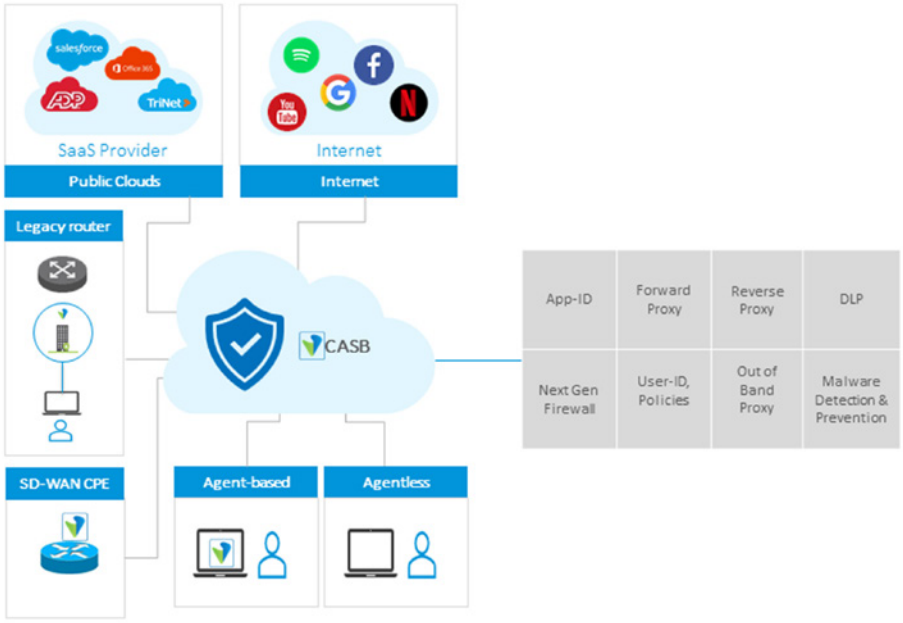
An inline CASB (which sits in the traffic path) can apply security functions such as Malware or Data Leak Protection (DLP) in a real-time manner. As a packet passes through the inline CASB, the packet is scanned and evaluated against policy and only forwarded if the security checks pass. When Malware is detected, the file can be either blocked or remediated.

In contrast, an OOB CASB is not in the traffic path, meaning there is a time delay between a file being uploaded to a cloud service and the time when the file can be scanned for Malware or DLP. This creates a small period of time in which the file can be downloaded by another user prior to a scan being completed.

Effective CASB solutions use multiple CASB methods to reduce the time gap in OOB CASB implementations.

CASB Data Protection

When accessing cloud services, a CASB protects the information stored, accessed, or shared from/by an enterprise cloud application. Typically, two types of data protection are performed by a CASB solution: DLP and Malware Detection. A high-caliber CASB solution allows several other additional security functions to further secure interactions with cloud workloads.



Data Loss Prevention (DLP)

DLP enables the enterprise to identify sensitive information such as Personally Identifiable Information (PII), financial information, health information, or enterprise proprietary information. DLP policies determine who has access to sensitive information, with whom it can be shared, and where and how it is stored.

- DLP can be supported by both the inline and OOB CASB deployment models.
- An OOB CASB uses DLP to scan data already stored in the cloud to determine which files contain what types of sensitive information.
- Both inline and OOB CASB models use DLP to control active use of enterprise information containing sensitive information.

Malware Detection

Malware Detection and Removal is another security function commonly supported with CASB solutions. Malware Detection and Removal enables the enterprise to scan information to ensure that no malicious content is included or embedded.

- An OOB CASB can scan enterprise information already stored in the cloud service.
- Both inline and OOB CASB models can scan information being uploaded or downloaded from the cloud service for malicious content.

Since an OOB CASB requires API integration between the CASB and the cloud, this method is only deployable for a select set of enterprise applications. However, an OOB CASB is also the only method able to scan pre-existing cloud information at rest when migrating to a CASB solution.

An inline CASB deployment is able only to protect future information, as well as information actively accessed, after the CASB solution is deployed. An inline CASB cannot review information that was at rest prior to the implementation of the inline CASB.

Versa Cloud Access Security Broker (Versa CASB)

The Versa Cloud Access Security Broker (Versa CASB) is a component of Versa Network's SASE Solution. Versa CASB functionality is available in either:

- The Versa SASE Service (SASE-as-a-Service), or
- The stand-alone Versa Secure Internet Access Service (SWG-as-a-Service)

Both solutions include:

- Inline and OOB CASB options
- Agent-based and Agentless options
- An extensive suite of additional security services

The Versa SASE solution contains more network and security services than the stand-alone SWG, version, for example the ability to use the SD-WAN for network connectivity.

The Versa Client can connect to multiple CASBs anywhere in the world. This approach is resilient and provides optimal uptime as it does not have to re-establish a connection to the SASE Service in the event of a network failure. The Versa SASE Client selects the best available CASB by using performance metrics of network connectivity as well as the CASB itself.

The Versa SASE Client is available for:

- MacOS
- Windows10
- iPhone
- Android
- Linux

The SASE Client is the first policy enforcement point that captures data regarding the connecting device and the user requesting the access.

The Versa CASB solution integrates with more than 1000 SaaS applications.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com