Versa CASB

Securing Web based and SaaS applications.

Introduction

Enterprises have steadily increased their adoption of Web based and SaaS applications for reasons ranging from improved productivity to adoption of OPEX based cost models. This is currently trending with enterprise cloud spending expected to exceed 45% of overall IT budgets by 2026 (Gartner, 2021). However at the same time, cloud adoption has significantly increased the attack surfaces and volume of threats enterprises are exposed to.

As services began originating in and shifting to the cloud, combined with distributed workforces, the enterprise perimeter has become more loosely defined making it challenging to enforce policies using traditional architectures. Cloud security now encompasses enterprise-wide protection. Unified SASE from Versa enables security teams to identify and manage the use of cloud applications, managed by IT or unmanaged/unsanctioned such as Generative AI applications.

In this article we describe Versa's Cloud Access Security Broker (CASB) offering and how it is used to improve application control and security when used in a Zero Trust architecture.

Concerns of Enterprises

Traditional Secure Web Gateways (SWG) or Firewall-as-a-Service (FWaaS) solutions often do not have the visibility and control to deal with the nuances of SaaS applications. SaaS in many cases may have dual use such as personal and enterprise accounts. Others (such as social Media) are essential for business use but at the same time present a data leakage risk to the business. Similarly, cloud based applications and their data are exposed and are a soft target for malicious attackers and insider threats.

How Versa CASB Works

Versa CASB is a cloud delivered security enforcement solution that sits either inline between cloud based applications and entities such as end users, or out-of-band with API based access to cloud applications and data. CASB is a key part of the SSE (Secure Service Edge) capabilities from Versa. SSE is defined by Gartner as the subset of SASE (Secure Access Service Edge) architecture that is focused on security services (i.e SASE without SDWAN).

Key Capabilities

Versa CASB is an essential tool in enforcing corporate policy for cloud applications access. Versa CASB leverages Versa's Unified Policy Engine. This ensures users benefit from a consistent policy language for all Versa SSE components i.e., DLP, SWG, ZTNA and more functions. Highlights include:

- Support for 300+ SaaS applications, and CASB profiles belonging to different categories.
- Inline discovery of applications being used and full visibility into who is using them.
- Assigns risk score based on application category, sanctioned vs. unsanctioned.
- Enforces policy based on user/group privileges, application risk, location, content, and more.
- Granular application usage control irrespective of where the data or user is located.
- Rich logging and audit trail of events, violations, and risky behavior.
- Anti-Malware protection for uploaded/downloaded content including files and attachments.
- Support for managed and unmanaged client devices.
- Seamless interoperability with Versa's Network DLP (Data Loss Prevention) function and other security functions.

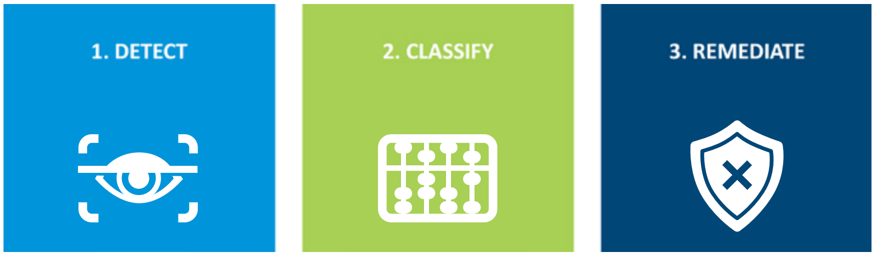
Deployment options

There are two ways to deploy Versa CASB. These are;

1. Inline CASB
2. Out-of-Band CASB

Inline CASB

It works in three phases:



1. DETECT

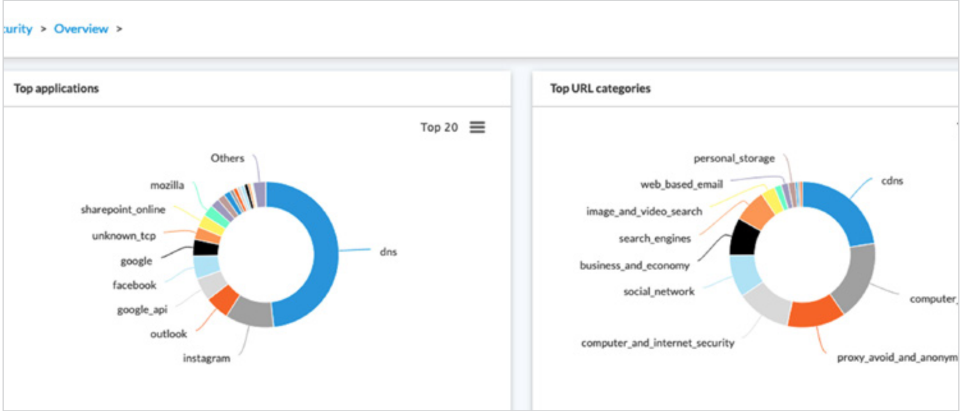
2. CLASSIFY

3. REMEDIATE

Detect Phase

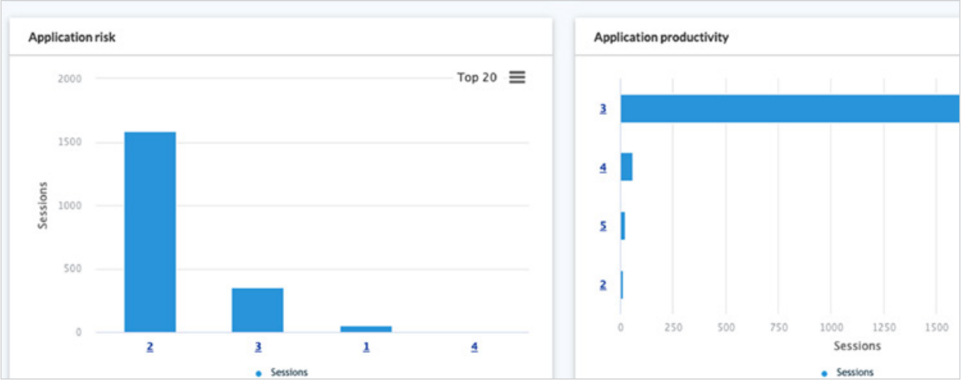
Application discovery is the process of identifying layer 7 information from the data flow. The Versa solution uses several advanced techniques to perform this function including DNS assisted detection from first packet and signature-based app matching. At the time of this publication, the Versa Cloud Gateways can identify 4000+ predefined applications. User defined custom applications are also supported.

This phase is also important for Shadow IT discovery by giving administrators visibility and insight into the inventory of unauthorized applications within the enterprise. Extensive dashboards and custom reports are available.



Classify Phase

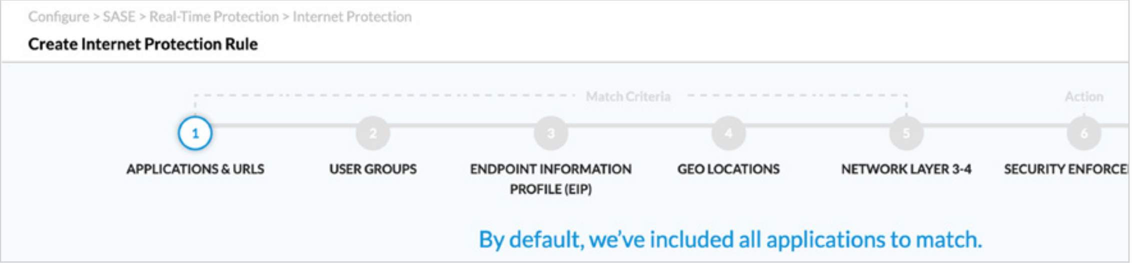
Once applications are identified, Versa CASB determines the risk level by class of applications. This includes Sanctioned vs Unsanctioned applications. Versa CASB then uses identity-based least privilege policies (i.e., user role and permitted privileges) to provide automated protection. This classification also provides powerful analytics insight to help administrators to fine tune their security policies.



Other classification categories include Application Family, Sub Families, Risk (ranked 1-5, 1 is low risk and 5 high risk) and Productivity (ranked 1-5, 1 least productive and 5 most productive).

Remediate Phase

Versa CASB uses the information from the classification phase to set policies for the organization's data and user access to comply with security needs. Remediation automatically happens when a violation occurs. This is activated by using a protection rule to identify the interesting traffic then performing a specified CASB action.



Configure > SASE > Real-Time Protection > Internet Protection

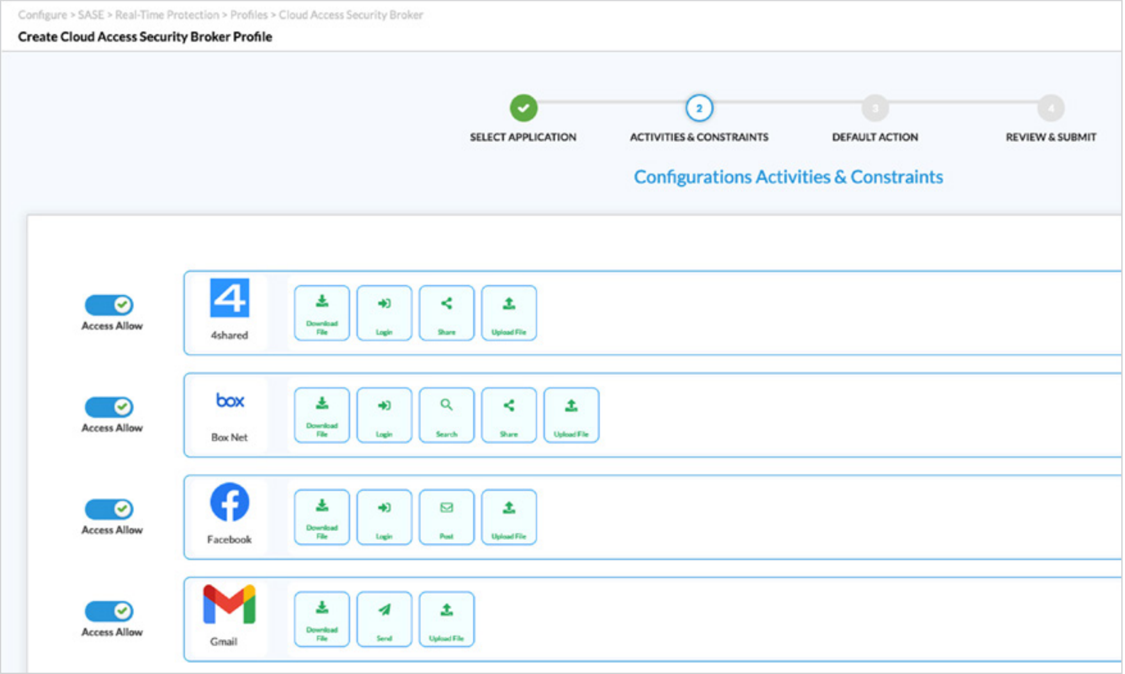
Create Internet Protection Rule

By default, we've included all applications to match.

The above shows the components of a protection rule. Versa CASB allows traffic to match based on the following options:

- Applications & URLS
- User and User Groups
- Device posture (EIP)
- Source and/or destination Geo-location
- Zone based Network Firewall (Layer 3 & 4)

CASB Enforcement Profiles are user defined granular application controls. This gives administrators the flexibility to allow access to the application (i.e. authorization policies to access an application) while maintaining security controls over activities within the application (i.e. access control policies within an application).



Configure > SASE > Real-Time Protection > Profiles > Cloud Access Security Broker

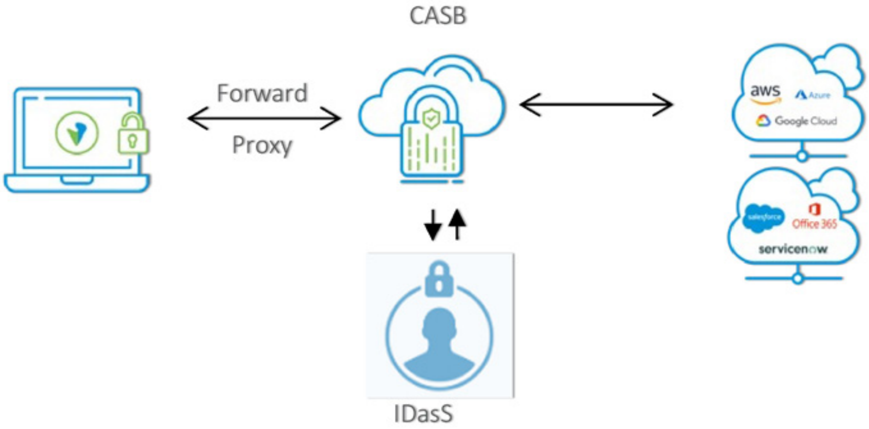
Create Cloud Access Security Broker Profile

Configurations Activities & Constraints

Inline CASB further supports Forward and Reverse Proxy methods. This works for both managed and unmanaged devices.

Forward Proxy Method

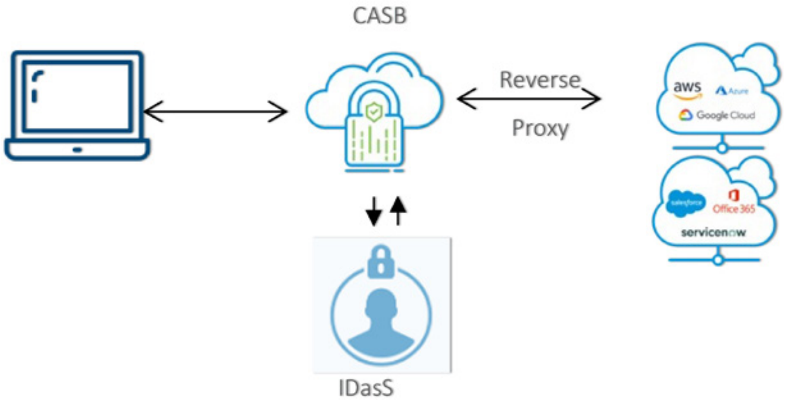
This is suited to devices that are under the administrator's network control. Appliances behind the enterprise network tunnel traffic to the Versa CASB enforcement point. Alternatively, the SASE Client is installed on remote worker devices to tunnel to Versa CASB.



Forward proxy with Versa CASB placed inline of the traffic is the simplest design approach.

Reverse Proxy Approach

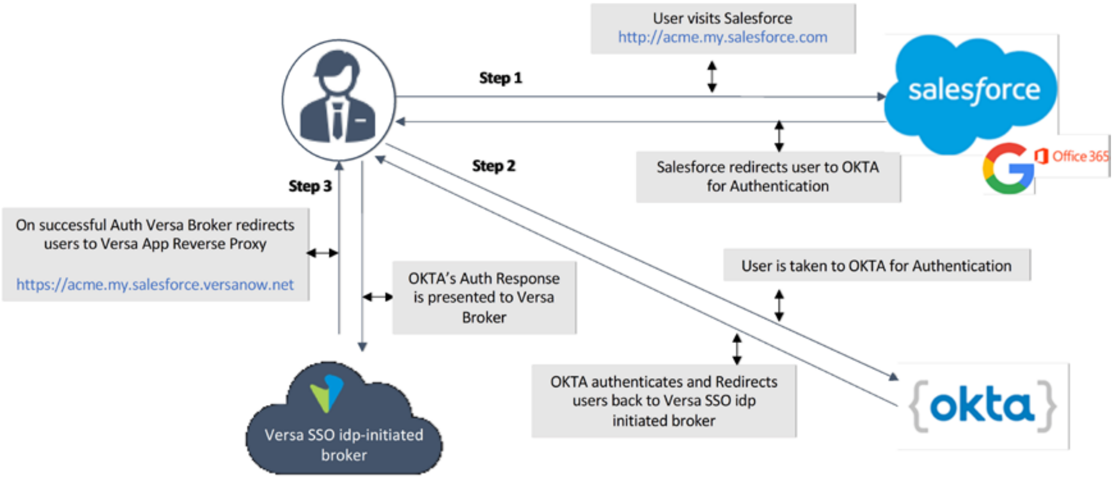
Application reverse proxy protects direct access to SaaS application from unmanaged devices or devices outside an organisation's network and security purview. The goal is to bring this traffic in line with the Versa CASB for inspection.



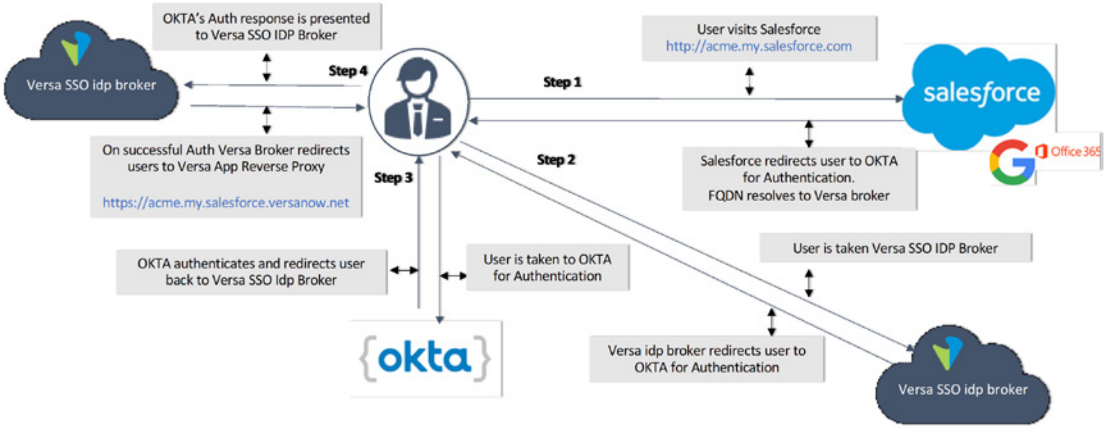
This leverages Single Sign On (SSO) authentication to redirect the connection via Versa CASB. Once the IdP (Identity Provider) authenticates the user, the IdP directs the traffic to the application's reverse proxy FQDN (Fully Qualified Domain Name). As this is the FQDN for the CASB service, traffic between end user and application passes through the CASB service. This permits the enforcement of real-time protection policies, based on the application and the user's context.

Versa CASB supports both IdP initiated, and SaaS application initiated reverse proxy flows.

- IdP initiated SSO – The SaaS application is configured to authenticate directly with the 3rd party IdP such as OKTA. When an endpoint accesses a SaaS application, the SaaS provider redirects the endpoint to the IdP for SSO. After successful authentication, the IdP presents the SAML assertion to the Versa IdP broker. As a result, the Versa reverse proxy comes in the path to SaaS application and enforces Zero Trust Network Access (ZTNA), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and other Versa SSE capabilities.

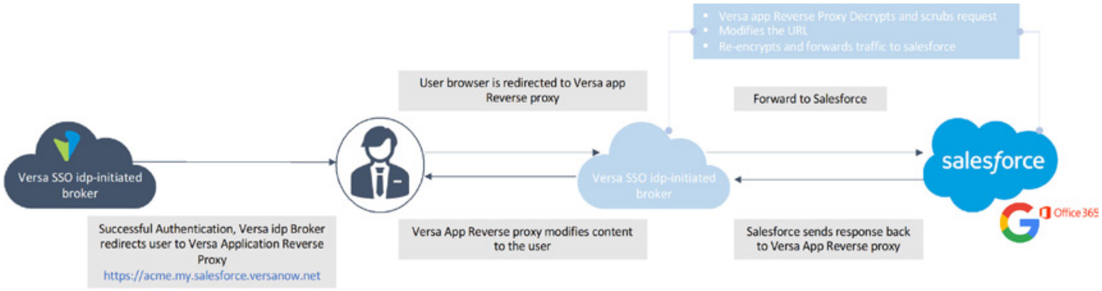

User visits Salesforce
http://acme.my.salesforce.com
Step 1
salesforce
Office 365
Step 2
Salesforce redirects user to OKTA for Authentication
Step 3
On successful Auth Versa Broker redirects users to Versa App Reverse Proxy
https://acme.my.salesforce.versanow.net
OKTA's Auth Response is presented to Versa Broker
User is taken to OKTA for Authentication
OKTA authenticates and Redirects users back to Versa SSO idp initiated broker
okta
Versa SSO idp-initiated broker

- **SP (Service Provider) initiated SSO** – The SaaS application is configured with the FQDN of Versa Broker as its IdP. Therefore, when a user accesses an endpoint SaaS application, the SaaS provider redirects the endpoint to Versa IdP broker which after applying policies redirects the endpoint to endpoint's real IdP (for e.g., Okta or Azure AD).


OKTA's Auth response is presented to Versa SSO IDP Broker
Versa SSO idp broker
Step 4
User visits Salesforce
http://acme.my.salesforce.com
Step 1
salesforce
Office 365
On successful Auth Versa Broker redirects users to Versa App Reverse Proxy
https://acme.my.salesforce.versanow.net
Step 3
Step 2
Salesforce redirects user to OKTA for Authentication. FQDN resolves to Versa broker
User is taken Versa SSO IDP Broker
OKTA authenticates and redirects user back to Versa SSO Idp Broker
User is taken to OKTA for Authentication
okta
Versa idp broker redirects user to OKTA for Authentication
Versa SSO idp broker

A key advantage of the SP Initiated SSO is that the Versa CASB can enforce ZTNA policies even before the authentication attempt is made to the IdP. Therefore, if a user group is not permitted access to a particular SaaS application, their request will be denied from the initial attempt.

In both IdP initiated and SP Initiated methods, the Reverse Proxy always remains in the path of the session. Users cannot bypass the proxy.


Versa app Reverse Proxy Decrypts and scrubs request
Modifies the URL
Re-encrypts and forwards traffic to salesforce
User browser is redirected to Versa app Reverse proxy
Forward to Salesforce
Versa SSO idp-initiated broker
Versa SSO idp-initiated broker
salesforce
Office 365
Successful Authentication, Versa idp Broker redirects user to Versa Application Reverse Proxy
https://acme.my.salesforce.versanow.net
Versa App Reverse proxy modifies content to the user
Salesforce sends response back to Versa App Reverse proxy

Out-of-Band CASB

In this model, no attempt is made to insert Versa CASB inline of the traffic path. This model uses APIs to communicate to SaaS applications, inspects user activities and content, enforces security policies, and provides granular access control for SaaS applications. No enforcement happens on the Versa gateways, instead the Versa CASB engine signals the access levels and privileges a particular user is permitted to have on a SaaS application and also remediates the violation on SaaS applications.

This works in two phases – Scanning and Remediation

Scanning

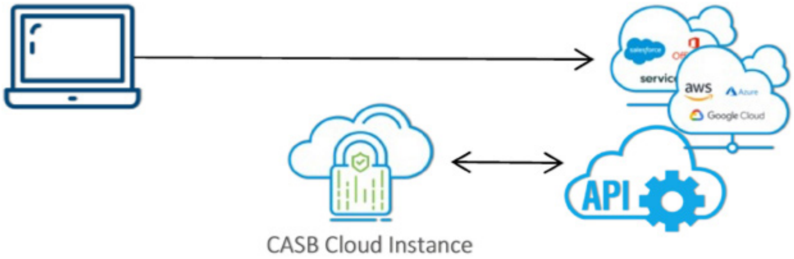
Real-time information about various objects may be sent as webhook events from SaaS applications to refresh and update Versa CASB. Examples of events include user login activity, file-upload etc.

Similarly, data-at-rest objects within the SaaS application may also be scanned periodically.

Versa CASB uses the information from the scanning phase to set policies for the organization's data and user access to comply with security needs.

Remediation

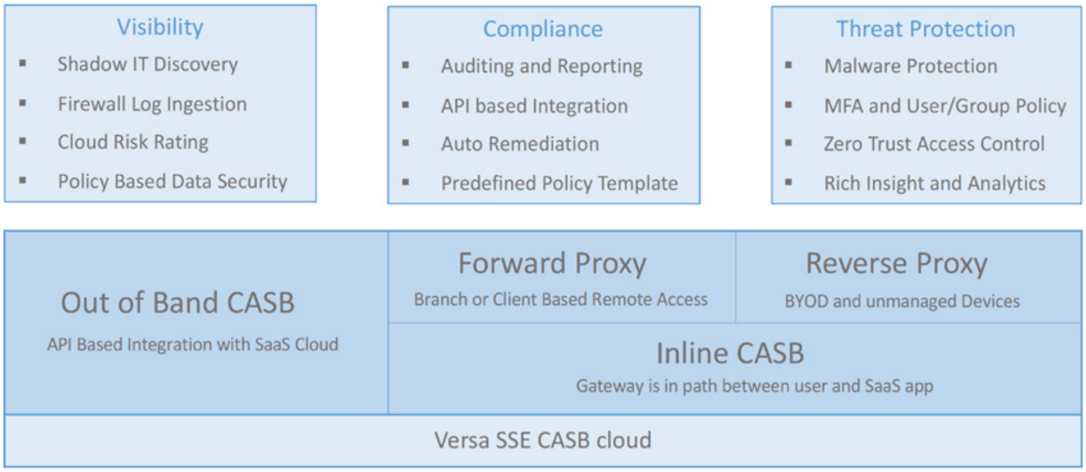
Remediation automatically happens when a violation occurs. Vulnerable data can be redacted, encrypted, quarantined, or deleted.



API based Out-of-Band CASB offers visibility into data and threats in the cloud, as well as quicker deployment and comprehensive coverage.

Summary

Versa CASB is a powerful tool that enables administrators with granular control over the use of cloud-based applications. At a high level its function can be classified into providing: 1) visibility features that provide insight into what resources are being accessed in the cloud; 2) a compliance step where we ensure that only acceptable behavior and access is allowed, and 3) malware protection against viruses that may be embedded in files downloaded or uploaded from a cloud-based application.



Visibility
- Shadow IT Discovery
- Firewall Log Ingestion
- Cloud Risk Rating
- Policy Based Data Security

Compliance
- Auditing and Reporting
- API based Integration
- Auto Remediation
- Predefined Policy Template

Threat Protection
- Malware Protection
- MFA and User/Group Policy
- Zero Trust Access Control
- Rich Insight and Analytics

Out of Band CASB
API Based Integration with SaaS Cloud

Forward Proxy
Branch or Client Based Remote Access

Reverse Proxy
BYOD and unmanaged Devices

Inline CASB
Gateway is in path between user and SaaS app

Versa SSE CASB cloud

In conclusion, we discussed the drivers for CASB and why a traditional firewall is no longer sufficient to secure cloud based SaaS applications.

We also looked at how Versa CASB can be deployed, and the various use cases it can address.

For more details visit www.versa-networks.com

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