Cloud Access Security Broker (CASB) Inline Proxy

Protect your cloud data with unparalleled visibility and control!

Introduction

The global pandemic situation has accelerated the adoption of cloud-based services at an unprecedented rate. As cloud solutions evolved, enterprises have extensively started using cloud-based applications and services as part of their post-pandemic operations, to meet their business needs. This has led to the rapid development of work from anywhere (remote workforce) concept as a new norm for employees.

While cloud technologies provide numerous advantages, they have also introduced new security challenges for organisations to address. As sensitive data is being stored, accessed, and handled in many new ways, it has become essential for organizations to build robust security measures covering all aspects of Zero Trust approach. Failure to do so, may result in an exposure to various cyber-attacks such as unauthorized access, data leakage, account takeovers and other malicious insider threats.

It should be noted with extreme caution that these risks can have a major impact on an organization's productivity, reputation, financial insights, and other areas which may typically go unseen or overlooked. As a result, an organization's efficiency and capability may become questionable for its risk exposures, which may lead to unexpected consequences.

This is where, Versa Networks CASB Inline proxy solution (SASE/SSE) helps enterprises in protecting their network and data from cloud-based risks and threats. Versa's solution addresses most of the security challenges that an organization faces today, ranging from identifying popular SaaS (Software as a Service) environments to Shadow IT discovery, granular application controls to visibility, preventing data leakage to compliance and much more.

The Challenge in Securing Cloud Application Access

Modern cyber-attacks have become more advanced and sophisticated.Nowadays, the focus has shifted towards targeting individuals and end-users rather than attacking the perimeter firewall devices. As a result, it has become critical for organizations to protect their most vulnerable and critical assets on cloud, including their data. However, most security teams face significant challenges while defining their strategy to improve their overall security posture. Some of these key challenges include:

1. **Securing Remote Workers and Distributed Teams**

   There has been a surge in employees accessing sensitive data and resources from a variety of devices (Laptops, PCs, Mobiles, Tablets) and geo-locations. Also, threats and attacks can originate from the devices the employees use. Often many times, security teams fail to identify, if the users logged in from a valid device/location that are deemed safe to access the data.

2. **Gaining Visibility of Application Activities**

   Traditional perimeter devices lack sophisticated features that can gain granular visibility of application activities and identify risky traffic based on ongoing transactions. Furthermore, gaining visibility of Shadow IT application is another major problem of concern in today's landscape. Lack of granular visibility has made security teams handicapped and are often forced to face the following challenges:

   a. Inability to identify the type of application actions that the users perform.
   b. Inability to identify/prioritize productive vs non-productive applications (Shadow IT discovery) at Organization level.
   c. Inability to apply granular effective controls based on different contexts.
   d. Inability to detect modern risks and threats.
   e. Inability to detect insider malicious actors.

3. **Data Loss and Compliance Monitoring**

   A major challenge in maintaining an effective data loss and compliance strategy is to ensure that sensitive data is not accessed or leaked by unauthorized parties. This requires organizations to implement monitoring and restriction

mechanisms that can scan, detect, and prevent unauthorized access and other data exfiltration activities on the fly. Most organizations still find this as a daunting task as data can reside on multiple cloud platforms and users can access from anywhere and from any device. Defining a strategic Data Loss prevention and Compliance procedure is key for any business, as failure to comply can result in serious reputation damage and hefty financial fines.

4. Unified Security Policies

   Disaggregated security policies add more complexity to identify, manage and mitigate security threats and exposures. This can result in a fragmented and disjointed approach to security management, making it harder for security teams to detect and respond to potential threats. Having a Unified Security policy that can span and apply actions based on Users, geo-location, device-compliance status, application actions (like, upload, download etc), data type etc across the organization, irrespective of where the user accesses these data, has become imperative. Without a centralized security policy framework, organizations may struggle to maintain compliance with industry regulations and standards and could face significant security risks that could compromise their sensitive data and assets.

Addressing the above challenges requires a proactive and holistic approach to security that leverages cutting-edge technologies, robust policies and procedures that adds extensive value to an enterprise. With this in mind, Versa Networks CASB Inline proxy solution continues to emerge as a game-changing innovation that would effectively address the ever-evolving security challenges faced by organizations. Versa solution offers an extensive range of features that can be seamlessly deployed and integrated within an organization's existing eco-system, providing the deepest level of protection. This makes it an ideal solution for organizations looking to enhance their security posture and mitigate potential threats with minimal deployment hurdles.

What is Cloud Access Security Broker (Inline)

With the rise of remote workforces and increased cloud adoption, the scope of cloud and data security challenges has grown rapidly. Addressing these challenges requires a comprehensive approach to security – starting from using existing foundational features to granular visibility and control, and a vision towards long-term security maturity that can evolve and adapt to new requirements. This is where Cloud Access Security Brokers (CASBs) helps to achieve the organization goals.

CASB solution can be deployed in different modes namely:

1. CASB – Inline Proxy
2. CASB – Reverse Proxy
3. API Based – Out-of-Band mode.

This document will predominantly cover the Inline Proxy CASB mode - its benefits, use-cases and more.

Versa Networks Cloud Access Security Broker (CASB) – Inline proxy solution, is a specific function of SASE/SSE that is deployed between Versa SASE (Secure Access Service Edge) Gateways and the cloud applications/Internet Services. As an intermediary broker between an end-user and the cloud services, Versa's CASB engine gains visibility of cloud applications usage (including encrypted TLS/SSL traffic) and apply differential treatment access controls for data in motion. Some of the unique benefits offered by Versa's CASB solutions include:

a. Visibility with Continuous Traffic Evaluation and Restriction – Monitoring and control of application activities such as uploading, downloading, and sharing of data through SaaS Cloud applications. This ensures that all user activities are tracked, and any unauthorized or suspicious behaviour is detected and acted upon in real-time.

b. Contextual Access Policies – Access restrictions to SaaS applications and other resources based on various contextual parameters. These contextual parameters can be in the combination of user identity, IP (Internet Protocol) addresses, URLs, location, device types, device posture, compliance status, etc. By enforcing contextual access policies, organizations can minimize the risks of unauthorized access and ensure compliance with security standards.

c. Data Security & Compliance - Data protection and regulation policies can be applied to protect sensitive information from unauthorized access or leakage. Different regulations like HIPAA, GDPR, and other federated services are considered to enforce data protection policies, ensuring compliance with relevant regulations, while preventing data leakage.

d. Integrated Threat Protection – Protection against several types of cyber threats by scanning all incoming and outgoing traffic. Malicious URLs, IPs, malware, viruses, exploits, and other vulnerabilities are detected in real-time and prevented from causing harm to the organization's infrastructure.

CASB uses multiple contextual data to evaluate traffic and follows Zero trust actions based on:

a. User Identity with MFA (Multi Factor Authentication)
b. User Location
c. Device type
d. IP Addresses
e. Application type
f. IP/URL risks
g. Device Compliance status
h. Device Posture
i. Operating Systems etc.

Cloud Access Security Broker (CASB) solutions have become a critical component of Secure Access Service Edge (SASE) and Secure Service Edge (SSE) architectures. Versa's CASB Inline proxy solution can easily fit into an enterprise's SASE/SSE deployment architecture. Such integrations via Versa's SASE solution allows enterprises to maintain consistent security policies across their entire network (both on and off net network users) and ensure that their cloud-based applications and services are secure and compliant.

However, before deploying a CASB solution, understanding the specific use cases that an organization is striving to solve is crucial. Such use-case analysis ensures that the solution meets the organization's needs and provides maximum ROI value.

We will now explore some of the most common use-cases for Cloud Access Security Broker (CASB) solutions and illustrate how Versa's CASB Inline proxy solution can effectively solve these challenges.

Securing Non-Corporate SaaS Tenants

It is common for employees to use both corporate and personal accounts of the same SaaS application (Google, Office365, dropbox etc.). However, this can increase the attack surface for an organization, as sensitive data from sanctioned accounts can potentially leak via unsanctioned personal accounts. Therefore, it is important for an enterprise to have critical controls over those unsanctioned personal accounts like personal Gmail, Microsoft and dropbox accounts.

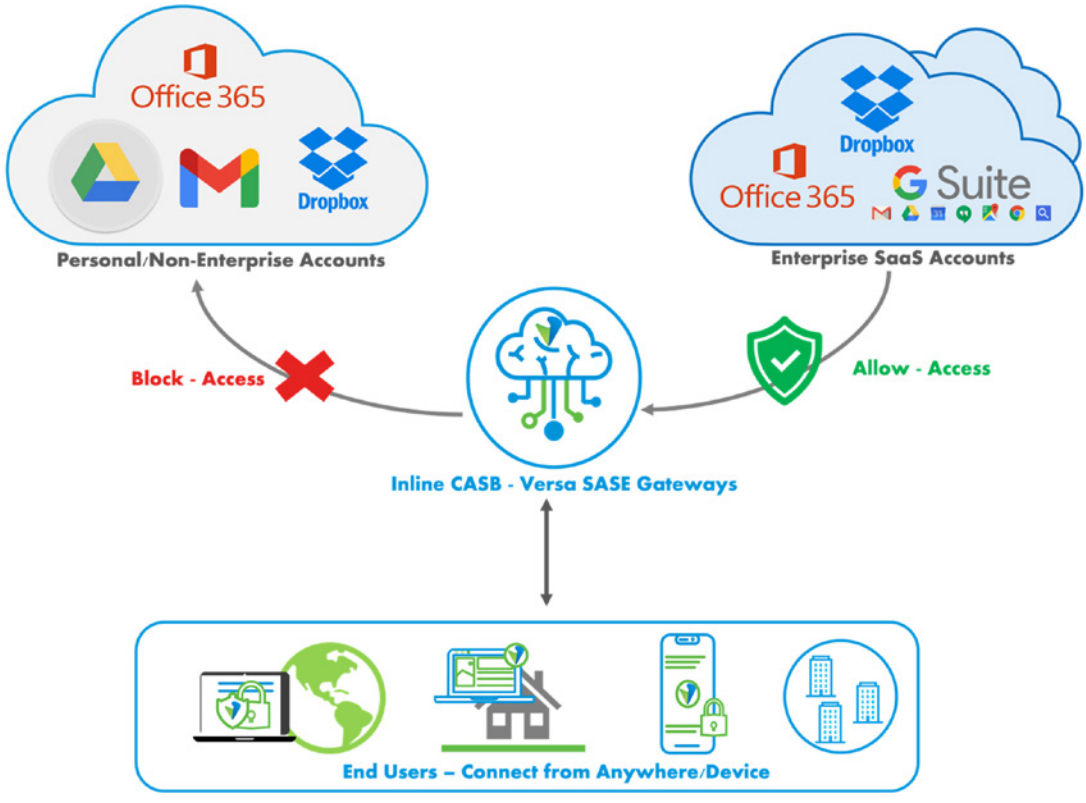

Figure 1: SaaS Tenant Access Controls

Versa's Inline CASB solution can provide an effective solution in identifying and restricting access to personal SaaS accounts. Its SaaS Apps Tenancy Control feature allows for real-time and automated remediation in restricting access to various non-corporate/personal SaaS application accounts.

By using Versa Networks SASE/SSE with CASB tenancy controls, an organization can gain greater control over their employees' access and actions regarding personal/non-corporate SaaS accounts, thereby reducing the risk of data breaches and unauthorized access to sensitive information.

Preventing Data Leakage via Shadow IT applications

Security teams have always faced a daunting task in controlling unsanctioned applications activities, also known as Shadow IT. This is because employees may intentionally or unintentionally upload or share sensitive corporate files from approved, sanctioned applications to unsanctioned application repositories. Such activities can pose a significant threat and provide a covert venue for malicious insiders to leak data.

For example, an organization may need to prevent the upload of sensitive files from Office365 to Gdrive account which may be non-sanctioned app as part of their data leakage strategy. Here is how Versa's SASE integrated inline CASB can help prevent such data leakage scenario:

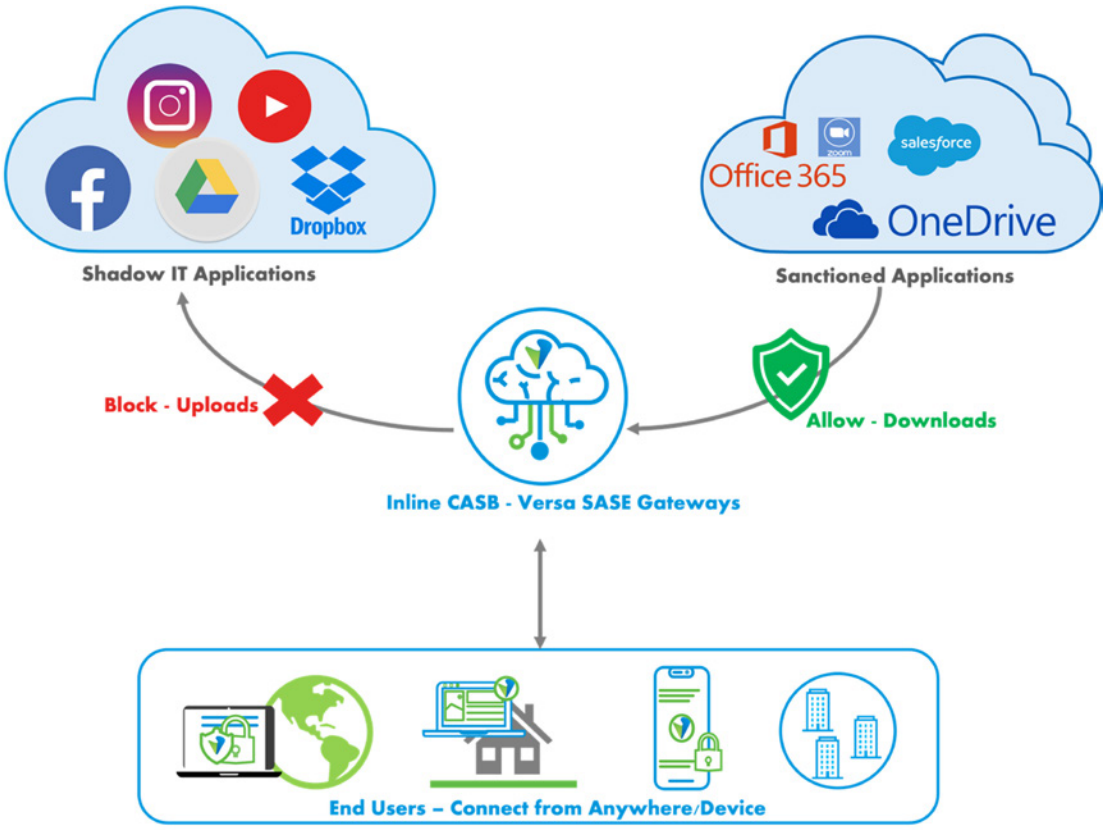

Figure 2: Restricting Shadow Applications Usage

1. All user traffic goes through the Versa SASE cloud gateways via Versa SASE client.
2. Versa SASE gateways are enabled with SSL inspection/decryption to gain granular visibility of user traffic, providing valuable insights into user behavior.
3. CASB engine scans the traffic and uses its app engine database to identify granular actions and risks involved in each of the user transactions (Continuous implementation of Zero trust approach at transaction/flow level). In this case, Versa's CASB discovers the following:
    a. A download action has been done by a user via OneDrive application.
    b. An upload action has been done by the same user via Gdrive application.

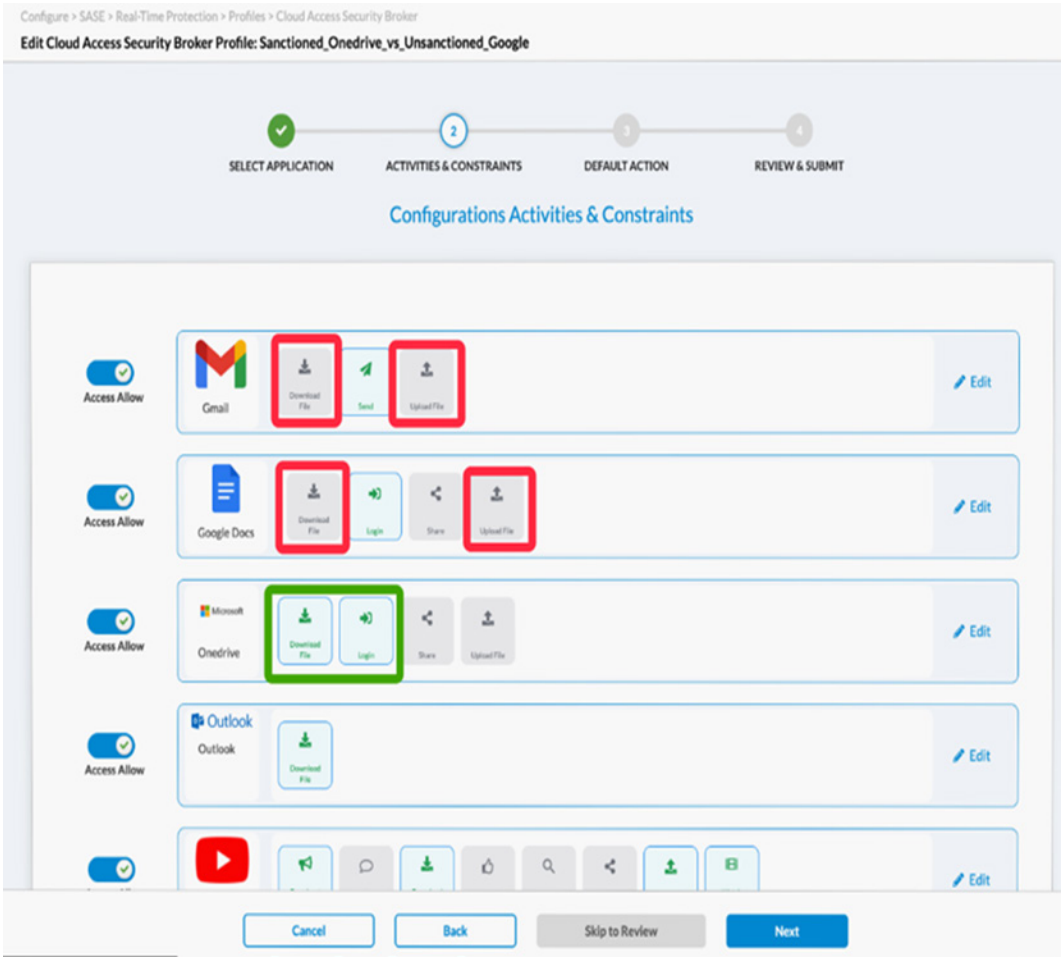

Figure 3: Application Activities & Constraints

4. Based on the above discovered application actions, security teams can decide if both or one (Upload to Gdrive) of the actions should be classified as an unsanctioned activity.
5. Security teams can create policies using CASB app signatures to block or allow access to the entire application usage(Gdrive) or have granular blocking actions inside a specific application to restrict either upload (to Gdrive) or/and download(from OneDrive and Gdrive) or/and share (to OneDrive and Gdrive) to the document.

Controlling Data Leakage within Approved IT applications

Preventing data leaks to Shadow IT applications may not always suffice. There are situations where specific sensitive files should not be accessed, shared, or viewed by a particular set of enterprise users or departments.

For instance, to comply with regulatory and compliance requirements, it may be necessary to restrict all Office365 departments/users, except for Finance and Accounting Departments/users, from accessing, downloading, viewing, or sharing sensitive files such as customer details, transaction details, and account information.

Versa's SASE/SSE solution supports integration of inline CASB (Cloud Access Security Broker) and DLP (Data Loss Prevention) capabilities, to help prevent such granular data leakage. The following example, reflect the effectiveness of our solution:

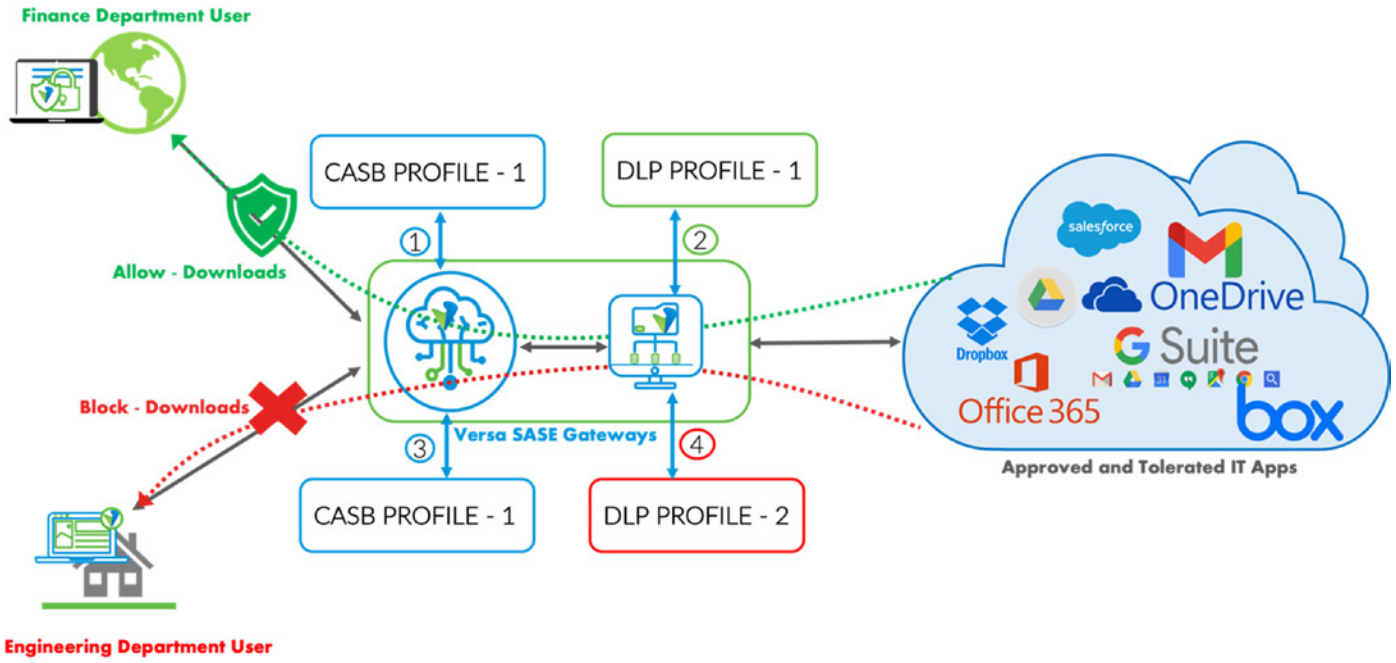

Figure 4: CASB Data Leakage Controls over Approved IT Apps

1. Office365 Administrators can assign sensitivity labels to all sensitive documents of the Finance/Accounting departments using Microsoft Purview Information Protection (MIP).
2. All user traffic directed through Versa SASE cloud gateways via the Versa SASE client, provides a centralized point for security inspection.
3. Versa SASE gateways are equipped with SSL inspection/decryption to gain granular visibility into user traffic and user behavior.
4. The following profiles shall be activated on the Versa SASE gateways:
    a. CASB Profile-1 - Allows download of files from office-365 suite applications such as web Outlook.
    b. DLP Profile-1 - To classify documents based on sensitivity labels assigned by MIP (Microsoft Information Protection) and allow Access.
    c. DLP Profile-2 - To classify documents based on sensitivity labels assigned by MIP and block Access.
5. The above profiles are tied to the access policies as below:
    a. The first access policy is configured to match traffic from users in the Finance/Accounting departments. This is achieved by tying the DLP Profile-1 and CASB Profile-1 together. The policy ensures that only users from the Finance/Accounting department, who have been authenticated (via MFA) and are subject to Zero Trust policies, are able to download files that have been labeled as sensitive. Both the DLP Profile-1 and CASB Profile-1 are allowed to perform their respective functions in this scenario.
    b. The second access policy is configured to match traffic from users in departments other than Finance/Accounting and ties the DLP Profile-2 and CASB Profile-1 together. This policy allows for application activities to continue without restriction unless the user attempts to access a file that has sensitive labels assigned. If the user attempts to access a sensitive file, the assigned DLP Profile-2 and CASB Profile-1 will work together to restrict access to the file and prevent any unauthorized actions that could compromise the security of the file or the organization's data. However, if the user is attempting to access a file that does not have a sensitivity label assigned, access will be allowed without any restrictions.

Match Component	Action	Pattern	Data Profile	Profile Name	File Name	File Type	File Size	File Transfer Direction	Verdict	File Rule Name	User
FileLabelMatched	alert			DLP-Rules_Finance	Versa-General.pdf	pdf		download	Payload	File-Label	finance-user1@acsecurity.com
FileLabelMatched	block			DLP-Rules	Versa-General.pdf	pdf		download	Payload	File-Label	engin-user1@acsecurity.com
FileLabelMatched	alert			DLP-Rules_Finance	Versa-General.pdf	pdf		upload	Payload	File-Label	finance-user1@acsecurity.com

Figure 5: Analytics Logs – Data Leakage Monitoring & Visibility

The above strategy shall work for other applications as well depending on an enterprise's security requirements. By effectively integrating other security modules like DLP along with CASB, organizations can prevent data leakage and ensure that sensitive data is only accessed by authorized users, in compliance with regulatory requirements.

Securing Unmanaged Devices

As users increasingly access IT applications from multiple devices/endpoints, the risk of security threats also increases. As countless users use their own mobile phones, bring-your-own-device (BYOD) devices, or corporate devices for data and application access, it has become essential for security administrators to ensure that only authorized devices or endpoints can interact with the respective approved cloud IT applications. This security posture check strategy can significantly reduce attack gaps and make it more challenging for attackers to infiltrate corporate data and steal information.

An enterprise can implement different posture check strategies based on endpoints, to ensure only devices that pass their security posture check are granted access. Versa Networks supports multiple endpoint/device authorization features, that helps enterprises to safely grant access to cloud applications and control actions based on individual device/endpoint status or platforms.

The following features are supported:

1. Secure Endpoints – Granular Gateway Connectivity controls that enable administrators to define policies based on a user's device platform or endpoint type. (Windows, MAC, Android, Ubuntu etc.)
2. Endpoint Information Profiles (EIP) - Collect crucial data from various endpoints as part of the security posture check before granting access to both gateways and applications.
3. Microsoft Intune MDM (Mobile Device Management) Integration – Effectively manage and secure devices of employees by validating the device managed compliance status, before granting access to the gateways.

A combination of these features can be used along with CASB as part of the ZTNA (Zero Trust Network Access) strategy. For example, for an enterprise user, to provide differential context-based access for Dropbox and Slack applications connecting from different Windows devices, the following Zero Trust approach can be implemented using the Versa SASE solution, which involves verifying the identity of both the user and the device for each of the application actions:

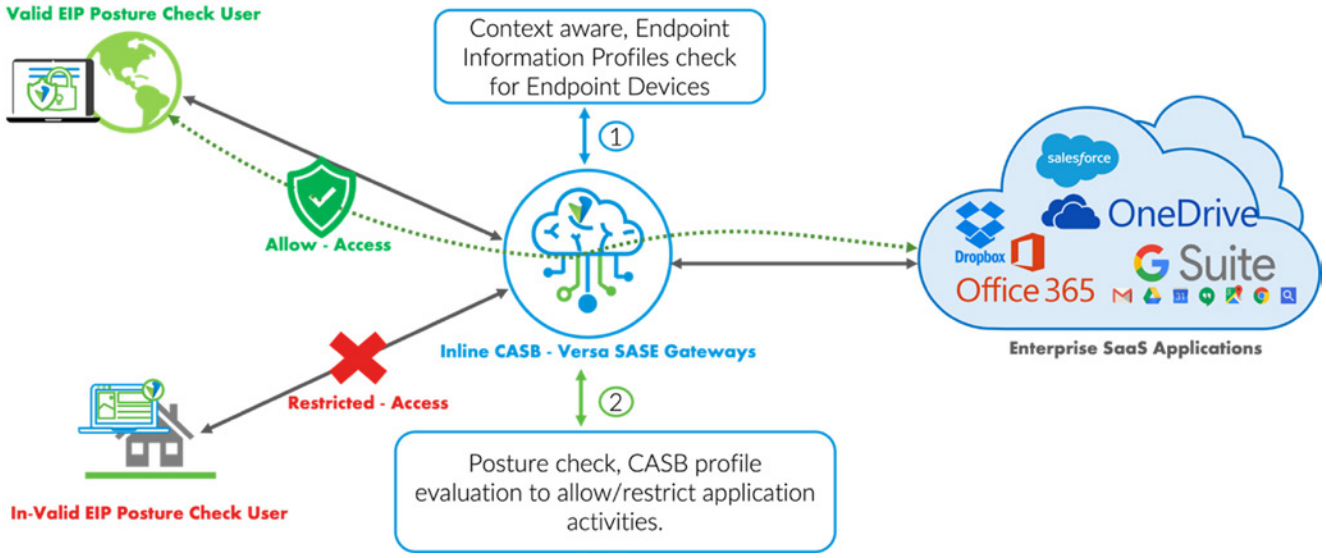

Figure 6: Context aware CASB controls based on Posture Checks

1. Context aware Gateway policies are enabled on the SASE gateways for granting access (1st level of defense):
   a. Users/User-Groups are defined as per the IAM (Identity Access Management) procedure available.
   b. All devices (Windows OS) will use EIP (Endpoint Information Profile) information to be validated before granting connectivity to SASE gateways.
   c. These EIP profiles can be customized based on individual endpoints and may include checks for operating system versions, patch levels, antivirus software, and other security settings.

2. Following the above validation filter, for the valid users a security administrator can enable differential context aware CASB action controls (2nd level of defense):
    a. If the EIP profile evaluation succeeds for a device, all application activities to Dropbox and Slack are allowed. This means that the user can upload, download, share, and perform other actions on these applications without any restrictions.
    b. If there is a deviation in the EIP profile evaluation for a device, CASB application activities such as upload, download, share, etc. are restricted on Dropbox and Slack, this means that the user will not be able to perform any of these activities on the applications until the deviation is resolved.

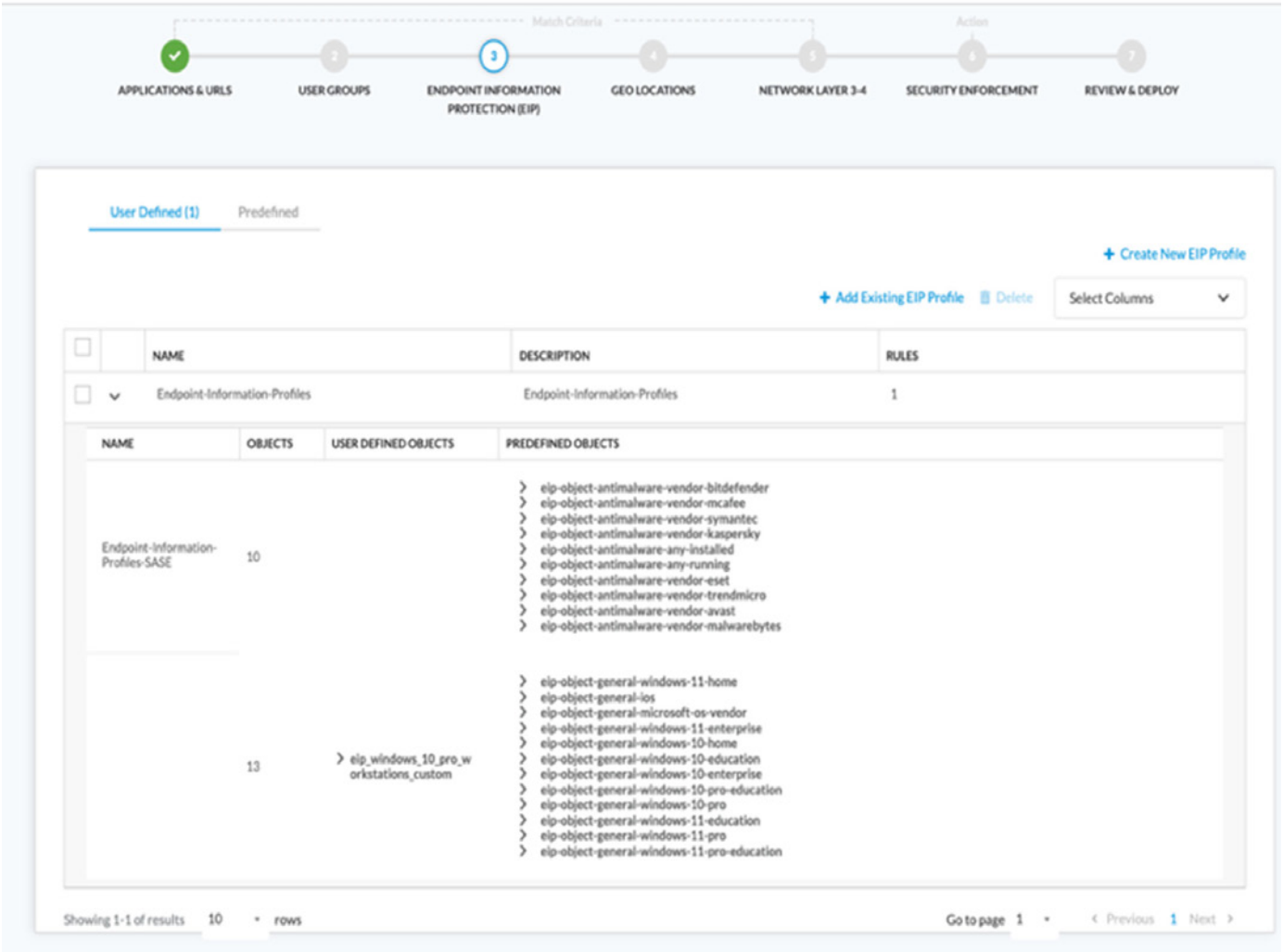

Figure 7: Endpoint Information Profiles (EIP)

By leveraging Versa Networks' endpoint/device validation features and CASB, organizations can effectively manage the security of their cloud applications and data, while enabling flexible and unified secure access for users coming from a variety of devices/endpoints.

Malware Defense

Cloud applications are often used as a medium for storing and sharing files, making them a prime target for cyber-attacks. To address this issue, Versa Networks SASE gateways can inspect, detect, and block malware, ransomware, trojans etc. in transit to and from cloud services by decrypting SSL/TLS connections based on individual application activities.

Even if a user is allowed to upload a file as part of the CASB profile, Versa SASE Gateways can still block malware files from being uploaded/downloaded. This continuous evaluation of CASB activity transactions is essential in implementing a Zero Trust approach, as any loopholes can lead to network-wide infections.

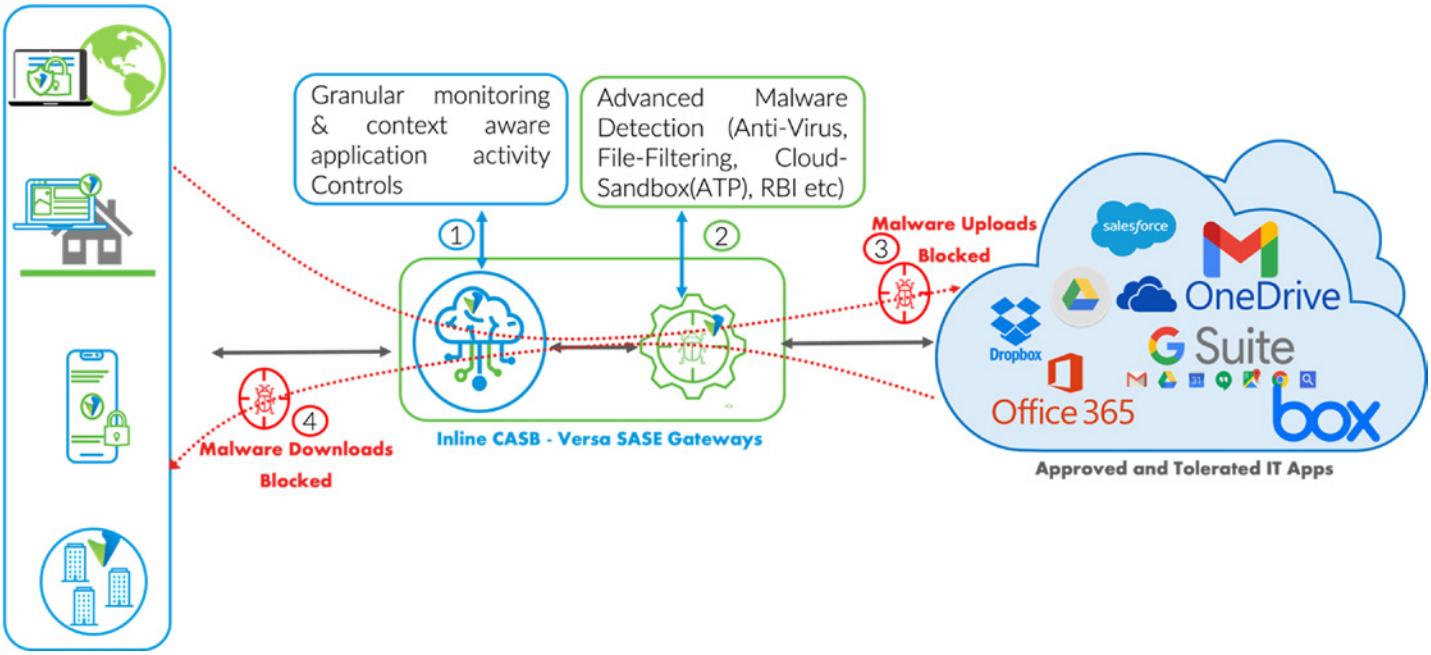

Figure 8: Inline CASB Malware Protection

Versa Networks' SASE Inline CASB solution not only identifies known malware using its anti-virus, file-filtering features but also detects zero-day malware using its ML based malware detection and sandboxing (ATP) feature. Along with this, an organization shall also enable Intrusion Prevention System (IPS) engine to detect other exploits for the respective application traffic/flow. By tying all these features under one roof an organization can safeguard their businesses against a wide range of potential threats that can compromise their cloud applications and services without worrying about performance degradations.

The Versa Advantage

1. Versa's CASB enabled SASE gateways provides complete visibility of all application traffic consumed by an organization, including sanctioned and unsanctioned apps, allowing better identification and management of potential security risks.
2. Continuous scanning of all web traffic via CASB-enabled SASE gateways allows for quicker detection and prevention of unsanctioned activities or applications that may pose security threats.
3. Comprehensive security feeds, covering wide classification of CASB APP signatures and threat Signatures allows IT teams to quickly respond to any potential attacks.
4. Centralized & consistent management of all Security policies spanning across Gateways/On-prem devices under a single pane of glass.
5. Tenancy controls for SaaS Apps restrict access to non-corporate and personal SaaS accounts. This ensures that only authorized users have access to sensitive data reducing the risk exposure.
6. Versa's Inline CASB can seamlessly integrate with Data Loss Prevention (DLP) to identify and stop potential data leaks in real-time, helping organizations from data compromises and leakages.
7. Safeguard an organization from a wide range of potential threats by defending against known malware, ransomware etc. along with new zero-day exploits.
8. Versa's Inline CASB solution can be integrated with any device type such as BYOD, Unmanaged, Windows, Mobile etc., making it easier to manage and maintain the organization's security posture across all data and resources.
9. Frequent security feed updates ensure round the clock-protection of all traffic via Versa SASE/SSE gateways.

Other Considerations

While the Solution brief has discussed the benefits of the Inline CASB mode, it is also critical for enterprises to carefully evaluate their specific use-cases before selecting a CASB vendor or deployment mode.

Major factors such as a unified single pane of glass across all SASE/SSE features for effective management and automation, a granular reporting/analytics platform, authentication integration services such as LDAP/SAML should be on top priority to simplify their Management and Operations. Such Unified solution would help achieve an organization's security goals on the longer run, thereby making the network immune to potential threats.

Other log export functionalities to existing SIEM/Threat Intelligence/OSS/BSS platforms and other integrations support that can co-exist on a single unified solution should also be considered.

Support for frequent and automated security updates of updated signatures across all security suites should be a critical consideration in providing maximum protection.

Versa Networks SASE solution by default satisfies all the above requirements and is in line with industry standards as defined by Gartner on "Unified SASE/SSE" architecture.

Versa Networks SASE solution can also inspect TLS 1.3 traffic which is widely deployed across all web traffic thereby giving a comprehensive coverage for effective detection and prevention for the future.

Conclusion

In Conclusion, Versa Networks Inline CASB solution is one of the few solutions in the market that can help an organization's network immune to potential risks and threats. While some organizations may be tempted to choose a multi-vendor solution, doing so could result in more complexity, loss in traffic visibility and can open potential blind spots for attackers to exploit the network.

But, Versa Networks Unified Inline CASB solution provides a rich set of APP signatures, state-of-the-art security control and threat feeds, all delivered on a single unified platform for all SASE functions through its simplified management and orchestration "Concerto" platform. Also, the platform simplicity makes it easy for security teams to not only prevent and optimize against existing threats but also helps in discovering emerging new threats to stay ahead in the game.

To summarize Versa's Inline CASB solution makes it an excellent choice for organizations looking to achieve their future security goals.

For more information on Versa Networks, please visit https://versa-networks.com, contact us at https://versa-networks/contact or follow Versa Networks on Twitter @versanetworks

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