Versa Cloud Access Security Broker (CASB)

Cloud adoption brings significant benefits, including scalability, accessibility, and cost efficiency, with Accenture estimating a 40% reduction in total cost of ownership (TCO). As a result, organizations have rapidly embraced cloud-based SaaS applications and services. In fact, Gartner projects that 70% of workloads will be cloud-based by 2028.

This shift to the cloud also introduces critical challenges in management, security, and compliance. Versa's Cloud Access Security Broker (CASB), a core component of the VersaONE Universal SASE Platform, strengthens cloud security by extending Zero Trust principles to cloud apps and the data they store, allowing organizations to fully realize the benefits of cloud computing without compromising security.

Challenges with Cloud Apps and Services

While cloud apps offer scalability and flexibility, they also introduce complexities that traditional security models struggle to address. This shift exposes organizations to a broader attack surface and evolving regulatory demands. Without the right controls in place, businesses risk data breaches, compliance violations, and operational inefficiencies. As an enterprise adopts cloud apps and services, they must find solutions to these common challenges: the lack of visibility into cloud app usage, difficulty in ensuring robust security, and maintaining compliance across diverse cloud environments.

Lack of Visibility and Control

Since nearly anyone can register for a cloud service, organizations struggle to monitor and manage the cloud apps used by its employees. With no visibility into where company data lives outside enterprise perimeters, unmonitored cloud app use can put company data at risk, lead to potential data exposure, or defy compliance and data governance laws. Employees using unsanctioned apps (shadow IT) bypass corporate security measures, making it difficult to enforce policies that keep the organization and its data safe.

Security Concerns

Cloud apps store vast amounts of sensitive data, making them prime targets for cybercriminals. Cybercriminals can exploit cloud storage and collaboration tools to spread malware or encrypt data for ransom. Protecting cloud apps and services from cyber-attacks requires advanced security measures tailored for cloud environments. Without proper controls in place, organizations risk data breaches, account takeovers, and unauthorized access to sensitive information.

Compliance Requirements

Maintaining compliance with industry regulations such as PCI-DSS, HIPAA, and GDPR becomes increasingly complex as data moves across organization perimeters and multiple cloud platforms. Organizations must enforce consistent data protection policies and monitor for compliance violations to avoid regulatory fines and reputational damage. Specific auditing and reporting requirements are also part of meeting these mandates.

Versa CASB: Securing Cloud Apps and Data with Advanced Controls

Versa's CASB solution provides robust security and control for enterprise cloud apps. Leveraging Versa's Unified Policy Engine, it seamlessly integrates with other Versa security products, ensuring consistent policies are applied across the entire organization. Versa CASB supports various deployment modes for flexible, tailored security needs, and boasts capabilities including:

Enhanced Visibility

Versa CASB provides broad visibility into cloud apps used across the entire organization, enabling IT and security teams to track where company data lives and identify possible security gaps. It assesses cloud security posture with real-time monitoring, reporting, and analytics on cloud activity, and discovers shadow IT.

Advanced Security and Threat Protection

Versa CASB integrates seamlessly with Versa's Advanced Threat Protection to enforce robust security policies and safeguard cloud app use and data. Use Versa CASB with AI-driven threat detection, behavioral analysis, and anomaly detection to identify and prevent malicious activities targeting cloud services.

Compliance Enforcement

Ensure adherence to regulatory standards by enforcing DLP policies and monitoring compliance across all cloud services and on-premises. Versa CASB's automated compliance checks, audit logs, and customizable policy enforcement help organizations maintain regulatory requirements without disrupting business operations.

Common Use Cases and Examples

Versa CASB extends enterprise visibility, security, and data protection to cloud apps. Its seamless integration with the rest of the network as well as SaaS/IDaaS apps make it suitable for many use cases, including these below.

Shadow IT Prevention and Discovery

Detect unsanctioned cloud apps used within the organization, giving IT teams visibility into previously unknown security risks. Implement follow-up actions such as applying policies to prevent unauthorized app use or limiting actions within unsanctioned apps.

Examples:

- Find unapproved file-sharing apps.
- Prevent the sending of documents in unapproved file-sharing apps.
- Log users out of unsanctioned chat apps.

Cloud DLP Enforcement

Apply consistent DLP policies across the entire organization, including cloud apps, to eliminate data risk gaps. Enforce data policies to control what and how information can be shared in the cloud. Provides automated security controls and audit-ready reporting for common compliance standards such as PCI, SOC 2, HIPAA, and GDPR.

Examples:

- Redact SSN in documents uploaded to Box.
- Prevent the downloading of customer account lists from Salesforce by contractors.
- Schedule a recurring scan of Google Drive each quarter to tokenize sensitive financial information.

Threat Protection and Anomaly Detection

Detect potential malicious actions and threats within cloud environments, such as compromised user accounts, unusual data access patterns, and external attacks. Leverages Versa's Advanced Threat Protection (ATP) capabilities and rules.

Examples:

- Prevent malicious documents from being uploaded to Google Drive.
- Scan newly acquired share drives after a merger for malicious content.

Security Configuration and Compliance Monitoring

Continuously assess cloud app configurations to ensure compliance with security policies and industry standards. Includes monitoring for misconfigurations, enforcing security best practices, and generating compliance audit reports.

Examples:

- Periodically scan AWS for open storage buckets and excessive user permissions.
- Monitor that multi-factor authentication (MFA) is enabled for all cloud accounts; log when MFA is disabled on accounts.

Securing Unmanaged Devices

Apply consistent security and compliance policies even when users access cloud apps from unmanaged or personal devices.

Examples:

- Check users accessing Salesforce from personal mobile devices have the latest OS version before granting access.
- Restrict the downloading of files by users accessing Box from outside the EU regardless of what device they access from.

Monitoring Data-at-Rest and Post-Incident Forensics

Scan and monitor cloud data to detect and address potential security issues. Schedule scanning and or perform forensic analysis to investigate security incidents.

Examples:

- Automatically label files as sensitive if they contain SSN and birthdates.
- Periodically review file-sharing settings on Box and log setting changes.
- Log access to a specific folder to report file(s) accessed, modifications, sharing, and downloads.

Versa CASB Benefits

Versa CASB delivers comprehensive cloud security and is a seamless component of the VersaONE Universal SASE Platform. The platform uses Versa's Unified Policy Engine, ensuring consistent policy language across Versa SASE components, including ZTNA, DLP, ATP, and others. This unified approach simplifies security management and eliminates policy inconsistencies.

Versa CASB enhances visibility by detecting and assessing Shadow IT, helping organizations mitigate risks from unauthorized cloud apps. It employs automated risk level assignments and identity-based policies, enforcing least-privilege policies to reduce risks of insider threats and accidental data exposure. Granular application controls allow administrators to customize security policies based on user roles, devices, and locations, enabling dynamic protection against evolving threats.

Key Benefits

- Part of VersaONE Universal SASE using its Unified Policy Engine.
- Shadow IT discovery and risk assessment.
- Automated risk level assignment and identity-based policies.
- Granular application controls.

Flexible Deployment

Versa CASB supports the following flexible deployment options, making it suitable for any architecture. Many customers opt for multiple deployments to meet their different use cases and goals.

Inline Deployment

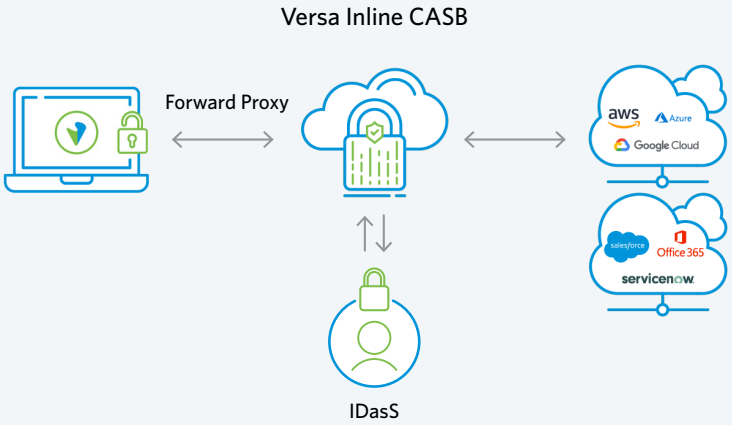
Inline deployment positions Versa CASB directly in the traffic path between user devices and cloud apps, enabling real-time monitoring and policy enforcement. As traffic reaches Versa CASB before the cloud app, inline deployment is ideal for analyzing data in transit and taking preemptive action (e.g. blocking a file from being uploaded, etc.).

Inline deployment can be configured via forward or reverse proxy.

Forward Proxy

Forward proxy is the simplest design approach with Versa CASB inline of the traffic flow. Traffic is tunneled from enterprise networks or remote devices to Versa CASB where policies are applied before reaching destination apps. This deployment requires the Versa SASE Client to be installed on devices and, as a result, is a good option for managed devices.

Versa Inline CASB deployed with forward proxy. Versa CASB is directly in the path of traffic. This deployment works for managed devices and requires the Versa SASE Client to be installed on endpoint devices.



An example flow of an inline forward proxy deployment would be the following scenario:

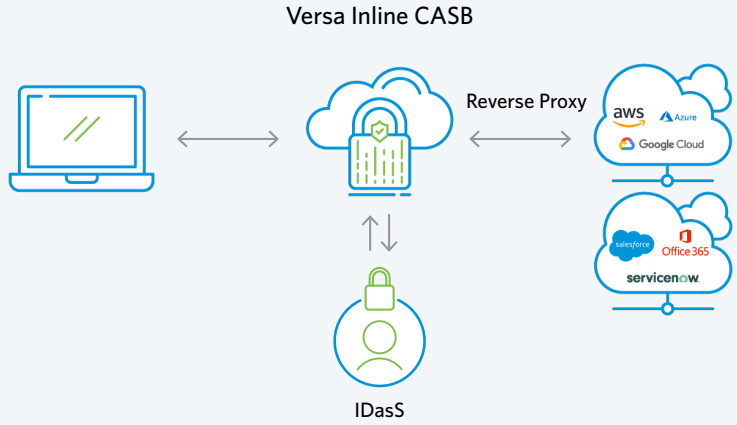
A remote employee accessing Salesforce from their laptop.

1. Employee logs onto their work-provided laptop
2. Employee logs into their SASE client
3. Employee accesses Salesforce
4. All Versa policies are applied

Reverse Proxy

Reverse proxy redirects traffic via an identity provider (IdP) to Versa CASB. A user accessing a cloud app first authenticates via single sign-on (SSO) through the IdP. Once the use is authenticated, the IdP directs the traffic to Versa CASB to apply policy checks before reaching the destination app. This approach enables policy enforcement for both managed and unmanaged devices without requiring endpoint agents, making it ideal for BYOD and third-party access scenarios.

Versa Inline CASB deployed with reverse proxy. Versa CASB is directly in the path of traffic. This deployment works for managed and unmanaged endpoint devices.



An example flow of an inline reverse proxy deployment would be the following scenario:

An employee accessing Salesforce from public wifi while at the airport.

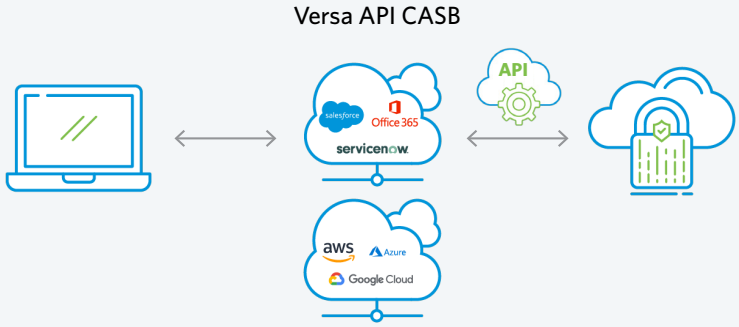
1. Employee connects to the internet via public wifi
2. Employee goes to Salesforce and tries to log in
3. Employee is redirected to their company's SSO
4. Upon successful login, employee is redirected back to Salesforce
5. All Versa policies are applied

API-Based Deployment

API-based deployment is an out-of-band deployment where Versa CASB is not in the flow of traffic. Instead, Versa API CASB connects directly to cloud apps via APIs, providing ultra-granular, application-specific controls without interfering with live traffic. As Versa CASB is not in the traffic path, action is taken in near-real-time via API. This approach is ideal for:

- Enforcing policies for both managed and unmanaged devices.
- Protecting cloud apps that use certificate pinning.
- Conducting scheduled scans and post-incident forensic analysis.
- Ensuring continuous monitoring and enforcement of data-at-rest security policies.

Versa API CASB is an out-of-band deployment. This deployment works for managed and unmanaged endpoint devices.



An example flow of an API-based deployment would be the following scenario:

An employee accessing their corporate AWS account from public wifi while at the airport.

1. Employee connects to the internet via public wifi
2. Employee goes to their corporate AWS account and logs in
3. All Versa permissions and policies are applied directly to AWS via AWS's API connector with Versa.

Summary of Versa CASB Deployment Modes

Deployment Mode	Best Used For
Inline – Forward proxy Requires SASE Client on endpoint devices	• Analyzing data in transit and taking preventive action (e.g. blocking a malicious file from being uploaded) • Use with managed devices
Inline – Reverse proxy Requires integration with an IdP	• Analyzing data in transit and taking preventive action (e.g. blocking a malicious file from being uploaded) • Maily used with unmanaged devices (but can also support managed)
API CASB Not in the direct flow of traffic	• Analyzing data at rest (e.g. scheduled scans, post-incident forensics) • Securing certificate-pinned apps • Use with managed *and* unmanaged devices

Versa's Cloud Access Security Broker (CASB) offers a comprehensive solution for organizations seeking to secure their cloud apps and data. With enhanced visibility, advanced threat protection, granular data protection, and flexible deployment options, Versa CASB ensures consistent policy enforcement and compliance across all cloud environments. Use Versa CASB for proactive threat prevention, real-time policy enforcement, or post-incident forensics to maintain a secure and compliant cloud infrastructure.

Schedule a demo to experience the robust capabilities of Versa CASB firsthand.

About Versa

Versa is a trusted leader in Secure SD-WAN, SSE, and SASE, delivering integrated networking and security to federal, defense, and public sector agencies. Our VersaONE platform – validated in the DISA Thunderdome initiative for ZTNA, SWG, NGFW, and CASB – is aligned with DoD Zero Trust architecture and proven across both enterprise and tactical environments. It's built to help you modernize with confidence, reduce risk, and achieve your goals with efficiency and clarity.

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