CipherCloud CASB+ Integration Ecosystem

CipherCloud CASB+ Solution at a Glance

- Universal cloud applications support
- Automated cloud usage discovery
- Cloud and user activity monitoring
- Adaptive access control
- Advanced policy engine
- Threat detection and prevention
- User and Entity Behavior Analytics
- Automated data classification
- Data Loss Prevention
- Encryption and Rights Management
- Continuous compliance monitoring
- Cloud Security Posture Management
- SaaS Security Posture Management

Customers

- From large to small enterprise
- Across every region and geography
- Representing nearly every vertical including:
  - Banking and Financial Services
  - Healthcare and Pharmaceutical
  - Manufacturing
  - Energy
  - Technology
  - Telecommunications
  - Education
  - Government

CipherCloud Integration Overview

The effectiveness of today's Cloud Access Security Broker (CASB) solutions is highly contingent on their abilities to integrate and analyze information provided by a wealth of adjacent platforms. In addition to the full breadth of cloud applications, CASB solutions must support integration with sources providing detailed, real-time information on factors ranging from identity and access to data classification and protection, along with event management, threat detection, network security, orchestration and response, and IT notification channels, among others.

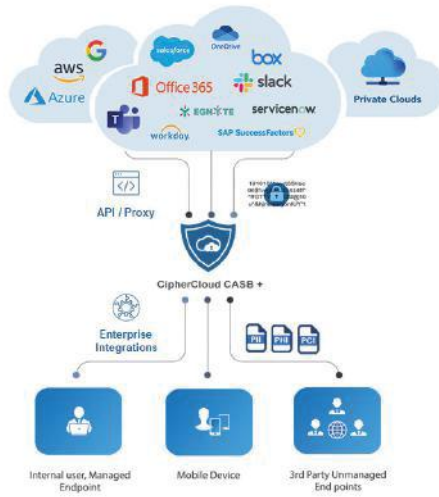
By delivering out of the box integration with cloud applications including Office 365, Slack, Box, G Suite, ServiceNow, SAP Cloud and Salesforce, among others - along with numerous solutions spanning every relevant aspect of IT security and management, CipherCloud CASB+ delivers the contextual and data-centric approach required by today's practitioners to address their most important cloud security and data protection requirements.

Building an Integrated Cloud and Data Security Ecosystem

CipherCloud CASB+ integrates directly with the full range of cloud, IT security and management solutions required to gain visibility and maintain control over applications and data across cloud, remote and enterprise deployments. By combining key contextual information regarding everything from leading cloud applications to broadly deployed security infrastructure, and beyond, CASB+ enables customers to constantly expand and optimize their cloud security processes. In addition to allowing organizations to better address evolving risks, CASB+ integration also increases the value of existing infrastructure and maximizes the ROI of current and future investments.

To support the broad ecosystem of capabilities and information that practitioners require to understand and address their most critical cloud security issues, while effectively managing their overall IT security strategy and operations, CipherCloud CASB+ specifically offers fully supported integration with capabilities including:

- Security Information and Events Management (SIEM)
- Single Sign On (SSO) and Multi-factor Authentication (MFA)
- Data Loss Prevention (DLP)
- Data Classification
- Identity and Access Management (IAM)
- Applications Access Control (AAC)
- Threat Prevention and Response
- Zero Trust Access (ZTA)
- Mobile Device Management (MDM)
- Security Orchestration and Response (SOAR)
- Secure Web Gateway (SWG)
- Notification Channels



CipherCloud CASB+ Architecture Diagram

Through both out of the box and customizable integration with nearly every form of security and IT management solution, CipherCloud CASB+ incorporates a huge range of advanced capabilities that enable organizations to execute their most strategic cloud security and data protection workflows. From the ability to secure the use of individual cloud applications to end-to-end monitoring and protection of organizations' multi-cloud deployments and data, CASB+ empowers practitioners to optimize their integrated cloud and data security ecosystem.

Leading CipherCloud CASB+ Integrations Include:

Security Information and Event Management (SIEM)

Integration with leading Security Information and Events Management (SIEM) solutions extends network log collection from on-prem devices to the cloud to provide in-depth analysis and control over security incidents across the enterprise, cloud, SaaS, and mobile environments. Using this highly strategic information, organizations can identify cloud security issues in near real time to inform response, while also feeding related data back into their existing SIEM platform for centralized analysis and reporting of related risk exposure and data protection.

- **Integrations:** **HP ArcSight, IBM QRadar, Intel Security, LogRhythm, Splunk, FireEye Helix, McAfee SIEM**

Single Sign On (SSO) and Multi-factor Authentication (MFA)

CASB+ integrates with leading SSO and MFA platforms to ensure the utilization of advanced access controls and authentication during every session, thereby defending against improper data exposure, potential compromise and threat propagation. By providing centralized oversight of both individual and cross-cloud access policy enforcement, CASB+ also logs all authentication activities across the entire ecosystem providing consistent and unified controls throughout the multi-cloud environment.

- **Integrations:** **Okta, Thales Safenet Trusted Access, Ping Identity, Akamai EAA, Azure AD, Microsoft ADFS, IBM TFIM, SiteMinder, OneLogin, Oracle Access Management**

Data Loss Prevention (DLP)

In addition to a native built in DLP capability including image support via OCR scanning, CipherCloud CASB+ also seamlessly integrates with enterprise Data Loss Prevention (DLP) to extend existing data protection and policies to the cloud, enabling consistent enforcement across enterprise, cloud, and remote environments. The CASB+ DLP integration offers organizations the ability to scan data through native cloud DLP, external DLP, or to augment data protection using multi-level scanning wherein data is inspected through native DLP with final scanning performed by external DLP engine. Through this strategic combination of capabilities, organizations are enabled to invoke consistent policies and protection across all data - both on premise and in the cloud, making the most of their DLP investments.

- **Integrations:** **Symantec DLP, ForcePoint, or any ICAP enabled DLP system**

Data Classification

CipherCloud CASB+ extends data classification and governance to any document in any cloud, providing full visibility into and protection across multiple apps, users, and devices - securing intellectual property and other protected data from unintended exposure. Advanced policies executed via integration with leading data classification solutions including Microsoft Azure Information Protection (AIP) enable organizations to implement enterprise standard classification on unclassified data, prevent the inappropriate use of sensitive data (such as sharing, upload, download) or reclassify documents based on the context.

- **Integrations:** **Microsoft AIP and Titus Data Classification Suite**

Identity and Access Management (IAM)

CipherCloud CASB+ integrates with leading IAM solutions to help implement and apply strong cloud and data access policies that enable Zero Trust access to cloud applications and services, while protecting sensitive information and maintaining standards compliance. Combining the strong identity controls of IAM solutions with CASB+ cloud and data security capabilities provides fine-grained access control over all login activities over SaaS and IaaS applications, dictates appropriate access to specific assets and enables 360-degree protection across applications and data, from initial user log-in to log-out.

- **Integrations:** **Okta, Thales Safenet Trusted Access, Ping Identity, Akamai EAA, Azure AD, Microsoft ADFS, IBM TFIM, SiteMinder, OneLogin, Oracle Access Management**

Applications Access Control (AAC)

By integrating with market leading AAC solutions, CASB+ empowers context-aware cloud applications and data access controls that continuously calculate related risks and enable more efficient access management, without impacting user experience. The unique combination of AAC and CASB enables performance of continuous risk assessment of users, devices, apps and locations, monitoring user activity and risks throughout each cloud session while protecting against data loss and threats in SaaS apps and emails.

- **Integrations:** **Akamai Enterprise Application Access**

Threat Prevention and Response

In addition to built in Antivirus/Antimalware (AVAM) protection, CipherCloud CASB+ also integrates with advanced threat prevention solutions to secure against Advanced Persistent Threats (APTs) and enable real-time detection of malware, including zero-day threats, viruses, spyware, ransomware, worms, and bots. CipherCloud has also partnered with FireEye to offer the industry's first real-time protection of zero-day threats across the enterprise, cloud, SaaS, and mobile environments. This integrated solution offers 360-degree visibility by aggregating and correlating threats from the enterprise networks, cloud, and end-user devices to uniquely address the new wave of cybersecurity threats facing today's remote workforce.

- **Integrations:** **Juniper Sky ATP, FireEye Detection On Demand**

Awards

Integration Partner Logos

Awards

Integration Partner Logos

LogRhythm
The Security Intelligence Company

okta

IBM Radar

Microsoft AIP

onelogin

CORTEX

FIREEYE

Zero Trust Access (ZTA)

In today's remote workforce environment, when employees, partners, and customers are increasingly connecting to company assets and data using any device, from nearly any region, it is critical to invoke stringent controls over access to data and applications. CASB+ integrates with leading Identity and Access Management (IAM) solutions to create a layered approach to monitoring and enforcement, ensuring appropriate access to sanctioned SaaS apps. The combined solution, driven by the strong identity controls of IAM and the CASB+ solution's adaptive access controls, enables end-to-end Zero Trust access to cloud data and services, across every approved session, user and device.

- Integrations: **Okta, Thales Safenet Trusted Access, Ping Identity, Akamai EAA, Azure AD, Microsoft ADFS, IBM TFIM, SiteMinder, OneLogin, Oracle Access Management**

Mobile Device Management

With a wide array of managed and unmanaged personal BYO devices connecting to the cloud from outside the enterprise perimeter, organizations require visibility into each device type to control access to data and other resources. CipherCloud CASB+ integrates with Mobile Device Management (MDM) solutions to monitor information on endpoints connecting to the cloud and use that intelligence to help enforce access to critical cloud apps and data - for example, allowing read-only access via web browsers or stepping up authentication for access through unmanaged devices. Connecting devices can be classified as managed or unmanaged through the installation of digital certificates on the devices.

- Integrations: **VMware AirWatch, Microsoft Intune**

Security Orchestration and Response

With the increasing number of endpoints (managed or unmanaged devices, distributed servers), organizations need deeper intelligence into user and device activity across all the connected entities for effectively responding to online security incidents and threats. CipherCloud CASB+ integrates with SOAR solutions, collecting data about threats and vulnerabilities while automatically responding to the security events. Using API integration, CASB+ provides the user risk intelligence to the SOAR platform for blocking risky users and for orchestration with other security tools.

- Integrations: **Palo Alto Cortex XSOAR platform**

Secure Web Gateway

Today's growing remote workforce requires a consistent, frictionless experience while connecting to cloud applications and services while ensuring inline threat protection to guard against attacks and prevent potential data loss. CipherCloud CASB+ integrates with Zscaler Internet Access (ZIA) and other SWGs, firewalls and proxy systems to identify ongoing cloud utilization and secure access to data in any SaaS application from any device and location, without requiring any agent software installation. The combined solution enables full visibility and control over users, data, and connections, allowing organizations to leverage cloud applications in a secure manner.

- Integrations: **Zscaler Internet Access (ZIA) or any SWG, firewall or proxy**

Notification Channels

Driven by the need to inform numerous IT security and management workflows with the detailed cloud and data security information necessary to trigger response and remediation, including ticketing systems, CipherCloud CASB+ integrates with any business communication and notification system, including incident response and IT Service Management platforms. Detailed information about specific conditions and exposures can be used to dictate any form of response from recommending necessary changes in access to highlighting emerging threats and detailing specific remediation requirements.

- Integrations: **ServiceNow Incidents, Slack or any email system**

About CipherCloud

CipherCloud delivers the market's leading approach to integrated CASB, SASE, and Data Privacy, addressing the full scope of customer requirements across cloud access, discovery, monitoring, data protection, policy enforcement and compliance. CipherCloud CASB+ has been named SC Magazine Cloud Security Product of the Year, Overall Leader in the CASB market by KuppingerCole, and a Visionary by Gartner, while counting numerous global 1000 companies among its rapidly growing customer base. CipherCloud is backed by Andreessen Horowitz, Transamerica Ventures, Delta Partners and DTCP, the venture arm of Deutsche Telekom. For more information, visit **www.ciphercloud.com** and follow us on **Twitter @ciphercloud.**

CipherCloud

CipherCloud, Inc.
4353 North 1st Street
Suite 100, San Jose CA 95134
USA

+1 855-5CIPHER
(+1 855-524-7437)
Info@ciphercloud.com