![CipherCloud logo]

At a Glance

- Founded in 2010 and Headquartered in Silicon Valley
- Over 10 years providing advanced cloud security and data protection solutions
- 23 granted and pending CASB and cloud security patents
- Investors: Andreessen Horowitz, Transamerica Ventures, Delta Partners, Deutsche Telekom.

Customers

- Trusted by enterprises of all sizes
- Across every region and geography
- Representing nearly every vertical including:
  - Banking and Financial Services
  - Healthcare and Pharmaceutical
  - Manufacturing
  - Energy
  - Technology
  - Telecommunications
  - Education
  - Government

CipherCloud CASB+ Cloud and Data Security Solution

Solution Overview

CipherCloud CASB+ is the market's most advanced, data-centric CASB solution, encompassing the widest range of dedicated capabilities required by today's security practitioners to gain centralized visibility into and control over their cloud applications and data. The cloud-native solution ensures that sensitive data is protected both in the cloud and on users' devices, providing a unified solution that enables enterprises to safely utilize diverse multi-cloud environments.

More than any other available solution, CASB+ delivers integrated Zero Trust access control, data protection, threat prevention and policy compliance across leading cloud applications including Office 365, Slack, Box, G Suite, ServiceNow, SAP Cloud and Salesforce, among others. By directly supporting these applications and the full array of adjacent IT security solutions, CASB+ delivers context-aware protection of any cloud application, accessed by agentless devices, from unauthorized upload, download, access, and data sharing to meet corporate governance, compliance, information technology, and cybersecurity requirements.

Data-Centric Cloud Security Protection

As organizations have experienced the need to employ more effective cloud and data security controls, based on the increased use and complexity of cloud applications, demand for more adaptive and encompassing CASB capabilities has also been amplified. Accelerated by widespread adoption of intricate processes including cloud-based collaboration among both remote workers and external partners, along with an endless array of business processes involving PII, PHI and other highly sensitive information, today's practitioners actively seek CASB solutions that offer a truly data-centric approach to managing related risks.

To provide the full breadth of integrated monitoring, data protection, threat prevention and governance safeguards sought by today's practitioners to address their leading cloud security challenges, CipherCloud CASB+ delivers critical solutions capabilities including:

- **Deep Visibility:** into all cloud usage, data availability, data handling and user behavior
- **Zero Trust Adaptive Access Control:** for every cloud connected user and device
- **Powerful Information Protection:** to prevent data loss and information exposure
- **Zero Day Threat Prevention:** against malware and account compromise
- **Governance and Compliance:** in accordance with global privacy regulations

By consolidating every core component of a leading-edge CASB solution, augmented by innovative capabilities including integrated Data Loss Prevention (DLP), Enterprise Digital Rights Management (E-DRM) and Cloud Security Posture Management (CSPM), among others, CipherCloud CASB+ offers uniquely powerful cloud security and data protection. CASB+ further provides integrated Zero Trust Network Access (ZTNA), directly supporting organizations' continued adoption of Secure Access Service Edge (SASE) methodology.

As a fully cloud native solution featuring multiple flexible deployment modes, CASB+ also offers the ability to scale to fit any enterprise, engineered with the elasticity necessary to support increased demand without impacting customer service, cost or manageability.

Key CipherCloud CASB+ DLP differentiators include:

1. Integrated data discovery, DLP, E-DRM, data protection and encryption
2. Zero Trust adaptive access applications control
3. Advanced policy engine and compliance management
4. Dedicated cloud email security and protection
5. Out-of-the-box deployment for every popular cloud application
6. Full breadth integration with adjacent IT security platforms
7. Agentless design for rapid deployment and efficient operation
8. Integrated Cloud and SaaS Security Posture Management
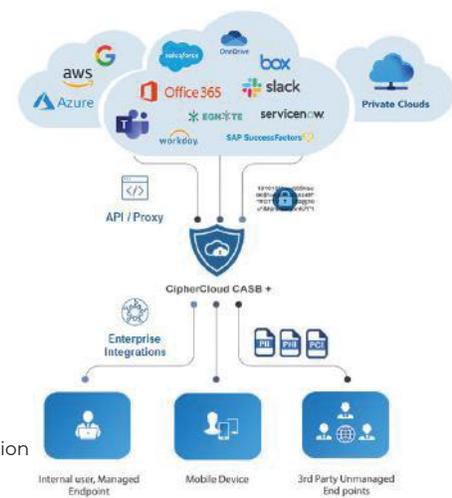
CipherCloud CASB+ Architecture Diagram

CipherCloud CASB+ Key Solutions Features

▶ Zero Trust Adaptive Access Control

CipherCloud CASB+ Adaptive Access Control performs a Zero Trust, continuous risk assessment of users connecting to cloud applications from any location or device, ensuring context-driven access control to applications and data. Adaptive Access Control monitors behavior and continuously adjusts access privileges in real-time based on factors including device, location, user risk and other details, securing every user action from login to logoff to ensure proper enforcement while effectively mitigating risks.

▶ Integrated Data Loss Prevention

CipherCloud CASB+ Data Loss Prevention (DLP) enables organizations to apply consistent data security policies and controls across all of their cloud applications - ensuring the protection of sensitive information across every key process including upload, download and collaboration. Directly informed via Zero Trust Adaptive Access Control, CASB+ DLP offers centralized policy management and enforcement, multi-mode data inspection, data classification, data matching and Optical Character Recognition (OCR) help deliver full-scope cloud DLP, along with supported integration for traditional on-premise DLP solutions.

▶ Enterprise Digital Rights Management

CipherCloud CASB+ Enterprise Data Rights Management (E-DRM) protects sensitive data as it moves across the cloud and even when it's shared externally, offering integrated data protection controls and encryption based on a wide range of contextual factors including user, device, content, classification and activity. Based on the level of sensitivity, E-DRM automatically envelops data with advanced encryption, providing data and user-centric protection. Customer controlled encryption key management ensures protection, even on lost or stolen devices.

▶ User and Entity Behavior Analytics

CipherCloud CASB+ User and Entity Behavior Analytics (UEBA) enables continuous monitoring of user, device and application activities for real-time detection and remediation of anomalous user behaviors and insider threats. Monitoring includes geolocation, source IP addresses, and devices used. User behavior analysis includes monitoring of activities such as content uploads and downloads, edits, deletes, logins, and logouts. Behavioral context also supports analysis and compliance management via the CASB+ Insights Investigate incident response capability.

▶ Zero Trust Network Access

CipherCloud CASB+ Zero Trust Network Access (ZTNA) delivers critical Zero Trust access control to applications and resources to offer context appropriate access to nearly any application. This enables organizations to isolate business critical applications through micro-segmentation and dictate appropriate, real-time access across applications and data from any device and location - providing the ability to facilitate secure, flexible, and scalable remote workforce deployments that meet their specific requirements.

▶ Cloud Security Posture Management

CipherCloud CASB+ Cloud Security Posture Management (CSPM) monitors cloud security configurations via an extensive list of templates and rule sets, enabling protection of infrastructure, applications and data while enforcing remediation for SaaS and IaaS applications. This unique, integrated CASB and CSPM capability offers a centralized security solution for all cloud services and infrastructure - preventing cloud misconfigurations that can lead to data loss and enabling consistent compliance.

▶ Secure Access Service Edge (SASE)

CipherCloud CASB+ provides a powerful combination of data-centric Secure Access Service Edge (SASE) components across applications and data discovery, DLP and data protection, threat prevention and UEBA, and ZTNA, among others. This array of capabilities immediately enables organizations to define unified policies to secure all of their enterprise apps across SaaS, IaaS, and on-prem, laying the foundation for future SASE adoption.

Customer Case Study

Profile:
Large US Healthcare and Medical Research Provider

Challenges:
- Rapid expansion of remote workforce
- PII and PHI used in cloud collaboration
- Seeking to securely standardize on clouds
- Stringent HIPAA and PCI compliance reqs

CASB+ Benefits:
- Rapid deployment supporting all users
- Integrated DLP and IRM enforcement
- Secure access for any user on any device
- Integrated compliance monitoring
- Successful and secure migration

"
CipherCloud allowed us to get a much better handle on collaboration. Now we can auto classify data, adapt controls for different users and mask specific records when necessary
"

For more information on CipherCloud CASB+ visit:
https://www.ciphercloud.com/ciphercloud-overview/

Awards

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®

Headquarters
CipherCloud
4353 North 1 Street,
Suite 100, San Jose CA 95 134,
USA

📞 +1 855-5CIPHER
(+1 855-524-7437)

✉ info@ciphercloud.com