CipherCloud®

CipherCloud® Cloud Access Security Broker (CASB+) for
SAP SuccessFactors®

The CipherCloud CASB+ for SAP SuccessFactors provides unparalleled protection for your users and data, giving you complete control over user access, their activities and data access. Deep visibility, end-to-end data protection, advanced threat protection, and comprehensive compliance capabilities ensure enable you to safely and securely embracing SuccessFactors, as well as many other cloud-based applications. The cloud-native CASB+ platform provides end-to-end data protection for enterprises adopting cloud services, ensuring confidential and sensitive data is protected at all locations - in the cloud and on users devices. The CASB+ capabilities enable you to adopt SAP SuccessFactors with the confidence of keeping control and knowing your data will always be protected.

Important CASB+ Use Cases for SAP SuccessFactors

VISIBILITY. CipherCloud CASB+ provides deep visibility into the SuccessFactors suite. This lets you better understand how data is being shared by SuccessFactors users. This visibility also helps you identify and protect sensitive and private regulated data so that you can prevent accidental disclosure or exposure.

+ CipherCloud CASB+ supports **Deep Forensic Analysis** and **eDiscovery** across your entire SuccessFactors suite and ecosystem so you can quickly validate non-compliant behavior.
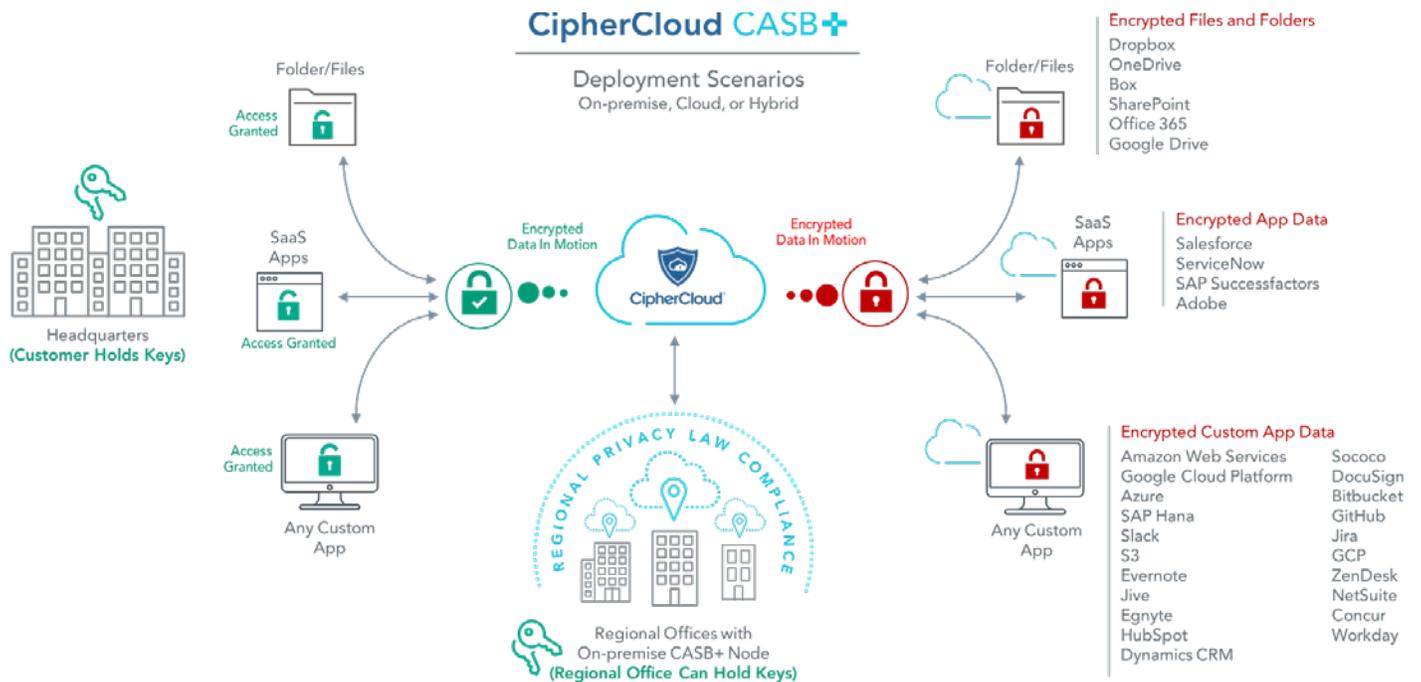
DATA SECURITY. CipherCloud CASB+ provides industry-leading end-to-end Zero Trust encryption, and comprehensive key management with the flexibility to address any mix of security requirements for your SuccessFactors suite. Our data protection, data loss prevention (DLP), native device management, secure offline data access, automated PII anonymization, and HSM support are available in one scalable platform.

+ **Data loss prevention (DLP)** protects your sensitive and regulated SuccessFactors content. CipherCloud CASB+ helps you discover sensitive content and then take necessary action based on compliance requirements and risk. CipherCloud CASB+ prevents the upload of sensitive and regulated content defined as containing PII, PCI, PHI or other sensitive or confidential material. This content can also be encrypted on-the-fly during the upload to ensure that it is compliantly protected.

+ Our comprehensive data security also includes our native **Digital Rights Management (DRM)**. Data that is downloaded from your cloud-based custom application to a user's device can be protected based on predefined policies, including defining what devices are allowed to access the data (for example, that users cannot use personal devices to access sensitive data). In the event that downloaded data needs to be protected from misuse (for example, former employees taking customer data), the administrators have the ability to retract access to the data, even if it was downloaded and copied to another device. Real-time key revocation can protect data on even lost and stolen devices.

THREAT PROTECTION. CipherCloud CASB+ brings advanced protection to identify and stop threats that are being shared through SuccessFactors services. This protection includes capabilities such as adaptive access control, user and entity behavior analytics, virus/malware protection, and our cloud access control.

✛ Our **Adaptive Access Control (AAC)** can also block access, even to what appear to be authorized users, based upon platforms used, time of day, originating location, and more that might suggest the theft, compromise of authentication credentials, or a sophisticated cyberattack. For example, if someone attempts to login in using your credentials, one hour after you have logged in from Detroit, Michigan, but they are located in Shanghai, China, AAC would immediately identify and stop this activity.

✛ Our **User and Entity Behavior Analytics (UEBA)** capability uses machine learning to monitor user activity, including time of day of activity, attempts at bulk file download, and other anomalous behavior. UEBA can make real-time decisions to flag unusual activity or block it based on variation from normal patterns. For example, if an employee starts downloading unusually large amounts of documents at 1 am, this would be flagged as anomalous behavior and stopped.

✛ Our **Virus/Malware (AVAM)** protection can defend against virus, malware, and ransomware to help keep SuccessFactors data safe. URL link protection and on-premise sandbox integration enable us to discover and remediate even the most challenging Zero-Day threats. For example, AVAM can detect and isolate an infected document before the malware spreads across your cloud documents.

✛ Our **Cloud Access Control (CAC)** brings layers of important controls to protect your SuccessFactors cloud during the upload and download of files. For example, CAC can scan and evaluate the content based on multiple parameters that may include: user name, user groups, managed versus unmanaged devices, risky IP addresses, locations (example - only allows office network connected upload), compromised or non-compliant devices, and the encryption of documents prior to upload or download to SuccessFactors.

✛ Our **Cloud Security Posture Management (CSPM)** brings continuous oversight and real-time guardrails to protect critical administrative and configuration controls in your many IaaS environments, including Amazon AWS, Microsoft Azure, and Google Cloud Services.

CipherCloud CASB+

Deployment Scenarios
On-premise, Cloud, or Hybrid

Headquarters
(Customer Holds Keys)

Folder/Files
Access Granted

SaaS Apps
Access Granted

Access Granted
Any Custom App

Encrypted Data In Motion

REGIONAL PRIVACY LAW COMPLIANCE

Regional Offices with
On-premise CASB+ Node
(Regional Office Can Hold Keys)

Encrypted Data In Motion

Folder/Files

SaaS Apps

Any Custom App

Encrypted Files and Folders
Dropbox
OneDrive
Box
SharePoint
Office 365
Google Drive

Encrypted App Data
Salesforce
ServiceNow
SAP Successfactors
Adobe

Encrypted Custom App Data

Amazon Web Services	Sococo
Google Cloud Platform	DocuSign
Azure	Bitbucket
SAP Hana	GitHub
Slack	Jira
S3	GCP
Evernote	ZenDesk
Jive	NetSuite
Egnyte	Concur
HubSpot	Workday
Dynamics CRM	

COMPLIANCE. CipherCloud CASB+ enables your SuccessFactors to be compliant with a broad mix of current and pending global privacy and compliance regulations, as well as any local data residency laws. This includes the controls necessary to support cloud-based applications under GDPR, HIPAA, PCI-DSS, GLBA, California Consumer Privacy (2020), Sarbanes Oxley Act, FISMA, ITAR, NERC CIP, and much more.

✛ The CipherCloud CASB+ platform provides the ability to protect data within SuccessFactors with you holding control of who has access to the data - even the provider's super administrators cannot see your data without your explicit permission and granting access. With the CASB+ platform, you can define a single set of security and compliance policies for SuccessFactors from a single console, eliminating per-application security complexity or security misconfigurations.

✛ Our unique **Hybrid Deployment** allows any multinational enterprise to manage one integrated secure deployment for key cloud applications across multiple countries with controls and key management configurable to comply with any industry regulatory requirement or local privacy law. Each country may have different compliance controls for data privacy, data protection, data sovereignty, and data residency. The CipherCloud CASB+ platform can do this by supporting any combination of customer-controlled keys, for multiple applications, in configurations that can include one or more on-premise key management systems.

✛ With the CASB+ platform, you can greatly simplify SaaS application licensing and administration with a global deployment, while controlling user and regional access to restricted data.

Enterprise Integration

All of your SuccessFactors traffic can be integrated with your security information and event management (SIEM) system to improve the probability of identifying critical incidents of compromise (IOCs). Further, we integrate with other important enterprise applications and infrastructure to include data loss prevention (DLP) systems such as Symantec, mobile device management (MDM) systems such as Airwatch, Sandbox engines such as Juniper SkyATP, and more.

Benefits for SAP SuccessFactors Users Include:

Accelerate Cloud Adoption. Move to the SuccessFactors cloud faster by overcoming cloud security, data privacy, and compliance obstacles.

Increase Cloud Visibility. Discover SuccessFactors cloud usage, data movement, and user activity to minimize data loss and compliance risk.

Reduce Cost of Ownership. One centrally controlled, easy-to-deploy hosted or hybrid platform to address all enterprise cloud requirements, provide end-to-end data protection, and minimize the scope of compliance audits.

Minimize Data Breach Risks with Powerful Data Protection. End-to-end data protection and other key features ensure data is never stored in cloud applications or cloud platforms unprotected, minimizing the risk of data breach, financial loss, and reputational and legal impact.

Prevent Forced Third-Party Disclosures and Be in Control. CASB+ brings a unique and powerful encryption key management capability to SuccessFactors that is always in the customer's jurisdiction. No matter who requests access to the data, from third parties to the cloud provider, only the customer can grant or deny access.

Enhanced Collaborative Governance. CASB+ provides a full solution for the collaborative sharing of data with third parties, including full control over sensitive content, full monitoring, and logging of all cloud activity.

The Most Comprehensive Solution for Global Compliance Requirements. The CipherCloud CASB+ architecture can uniquely address any mix of global compliance requirements and local privacy laws to simplify your cloud-based application adoption and reduce costs.

CipherCloud CASB+ is the Best Cloud Security Solution for SAP SuccessFactors

Unified. One Single Integrated CipherCloud CASB+ Platform provides all of the key CASB components.

Total Cloud Control. CipherCloud CASB+ provides total control of any user, any device, managed or BYOD, anywhere in the extended enterprise, and enforces policies to mitigate risk.

Seamless. CipherCloud CASB+ extends data protection transparently to the user experience, ensuring application workflows are not affected.

End-to-end or Zero Trust Encryption. Zero Trust Encryption completely protects data in the cloud from the enterprise "edge" and back. Data remains encrypted at rest (database), in motion (middleware, API's, network), and in use.

Native Digital Rights Management. Built-in DRM completely controls devices that access sensitive encrypted data. DRM tracks all movement of data, and restricts access in real-time, and secures documents even when offline.

Secure and Simple Collaborative Governance. Secure Collaboration without cumbersome portals or other 3rd party tools.

Agentless - Built for Speed. CipherCloud CASB+ does everything you need without the unnecessary overhead of yet another agent sitting on your endpoints.

No Reconfiguration of Your Network. CipherCloud CASB+ blocks unsanctioned clouds using your existing network infrastructure. No complex network reconfiguration or traffic routing required.

Unique Hybrid Architecture. CipherCloud CASB+ supports multiple on-premise KMS. Data encryption keys are retained exclusively by the customer.

The Largest Multinational Companies in the World Use CipherCloud

+ 5 of the Top 10 U.S. Banks
+ 6 of the Top Banks Worldwide
+ 3 of the Top 10 Insurance Firms
+ 3 of the Top 10 U.S. Health Care Firms
+ 3 of the Top 10 Pharmaceutical Firms
+ 2 of the Largest Telecommunications Firms
+ Government agencies in the United States, United Kingdom, Canada, Australia, and beyond

About CipherCloud

CipherCloud, a leader in cloud security, provides an award-winning cloud security platform delivering powerful end-to-end protection for data resident in the cloud, threat prevention, visibility, and compliance for enterprises to adopt cloud with confidence. Uniquely, CipherCloud provides the deepest levels of data protection in real time to provide an immediate solution for challenging cloud security and compliance requirements. The world's largest global enterprises and government institutions in over 25 countries protect and secure their cloud information with CipherCloud.