MICROSOFT OFFICE 365
CLOUD SOLUTION BRIEF

CipherCloud®

CipherCloud Cloud Access Security Broker (CASB+) for Microsoft Office 365®

Office 365

The CipherCloud CASB+ for Microsoft Office 365 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 Office 365, 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 Microsoft Office 365 with the confidence of keeping control and knowing your data will always be protected.

Important Use Cases for Office 365

Visibility. CipherCloud CASB+ provides deep visibility into every application within the Office 365 suite. This lets you better understand how data is being shared by Office 365 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 across your entire Office 365 suite and ecosystem so you can quickly validate non-compliant behavior.

Compliance. CipherCloud CASB+ enables your Microsoft Office 365 cloud to be compliant with a broad mix of current and pending global privacy and compliance regulations. This includes the controls necessary to support cloud-based applications under PCI, PII, HIPAA, GDPR, California Data Privacy, and much more.

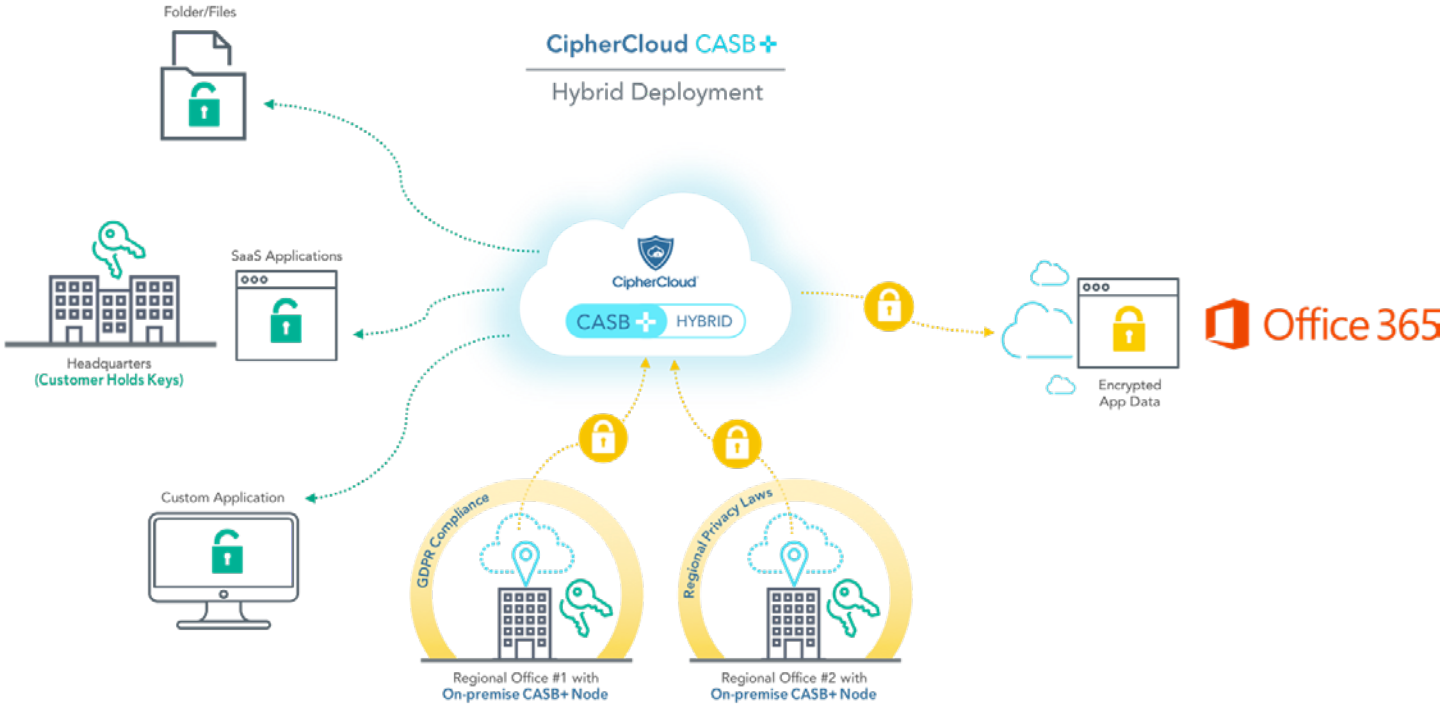
- Our Hybrid Deployment allows any multinational enterprise to manage one integrated secure deployment for key cloud applications across multiple countries with controls and key management configurable to address a broad variety of differing regulatory requirements.
- Each country may have different compliance controls for data privacy, data protection, data sovereignty, and data residency. The CipherCloud CASB+ platform for Office 365 can also support any combination of customer-controlled keys, for multiple applications, in configurations that can include one or more on-premise key management systems.

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. 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 content. CipherCloud CASB+ helps you discover sensitive content and then take necessary action based upon 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 integration with Microsoft's Digital Rights Management (DRM). Data that is downloaded from Office 365 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 to new companies), 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. We also provide our own native DRM in the event that you do not use Microsoft's product.

Threat Protection. CipherCloud CASB+ brings advanced protection to identify and stop threats that are being shared through cloud-based services. This 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



Accelerate Adoption of Your Office 365 Cloud

Increase Office 365 Cloud Visibility

Reduce Cost of Ownership

Minimize Office 365 Data Breach Risks with Powerful Data Protection

Prevent Forced 3rd Party Disclosures and Be in Control

Enhanced Collaborative Governance

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 upon 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 Office 365 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.
- Finally, our Cloud Access Control (CAC) brings layers of important controls to protect your Office 365 cloud during the upload and download of files. For example, CAC can scan and evaluate the content based upon 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 Office 365.

Enterprise Integration

All of your Office 365 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. CipherCloud CASB+ for Office 365 also includes a first class integration with Azure information Protection to leverage your other cloud data protection capabilities.

Benefits for Microsoft Office 365 users include:

Accelerate Adoption of Your Office 365 Cloud.
Move to cloud faster by overcoming cloud visibility, security, data privacy and compliance obstacles anywhere on the globe.

Increase Office 365 Cloud Visibility. Discover cloud usage, data movement and user activity to minimize data loss, minimize compliance risk, and support necessary forensic audit.

Reduce Cost of Ownership. One centrally controlled, easy-to-deploy hosted or hybrid platform to address all of your Office 365 cloud requirements, providing end-to-end data protection, and minimize the scope of compliance audits.

Minimize Office 365 Data Breach Risks with Powerful Data Protection. End-to-end data protection and other key features ensure data is never stored in Office 365 unprotected, minimizing the risk of data breach, financial loss, reputational and legal impact.

Prevent Forced 3rd Party Disclosures and Be in Control. CipherCloud's CASB+ for Microsoft Office 365 brings a unique and powerful encryption key management capability that is always in the customer's jurisdiction. No matter who requests access to the data from 3rd parties, to the cloud provider, only the customer can grant or deny access.

Enhanced Collaborative Governance. CipherCloud's CASB+ provides a full solution for the collaborative sharing of Office 365 data with 3rd parties, including full control over sensitive content, full monitoring and logging of all cloud activity.

Improved Compliance Readiness. One solution will help your Office 365 cloud meet global compliance requirements such as GDPR, California Data Privacy, HIPAA, and more. The CipherCloud CASB+ architecture can address any mix of global compliance requirements and local privacy laws to simplify your Microsoft Office 365 adoption and use.

The Largest Multinationals 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

CipherCloud

CipherCloud, a leader in cloud security, provides powerful end-to-end protection for data resident in the cloud. Our award-winning cloud access security broker delivers comprehensive visibility, data security, threat protection, and compliance for cloud-based assets. Uniquely, CipherCloud provides the deepest levels of data protection and real-time data access control to provide an immediate solution for challenging cloud security and compliance problems. The world's largest global enterprises and government institutions in over 25 countries protect and secure their cloud information with CipherCloud.