CipherCloud

Operationalizing Security for Office 365 Collaboration in Remote Work Environments

Solution Brief

Office 365

Overview

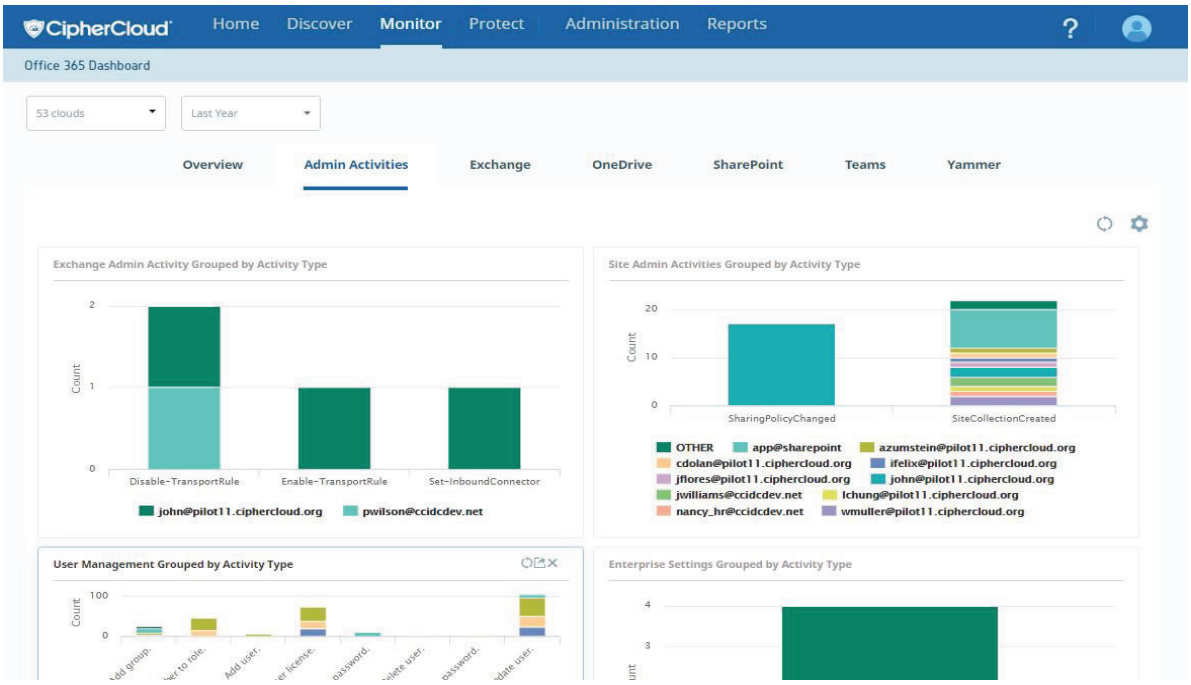
Rapid expansion of the remote workforce has massively increased demand for SaaS collaboration applications that enable employees to partner and communicate from any location in the world to ensure business continuity. More than any other such platform, Office 365 has emerged as a leading enabler of remote workforce environments based on its wide range of its productivity and collaboration capabilities, from Outlook to Teams, to OneDrive and Sharepoint. Amid the ongoing remote workforce transformation, these cloud capabilities have allowed organizations to better communicate and collaborate via email, shared documents and chat channels to keep the productivity meter ticking.

At the same time, the tremendous benefits delivered by Office 365 create their own sets of security and data protection challenges. From attempting to maintain a clear picture of who is accessing data in Office 365, to understanding precisely where in the world company data is being accessed and how all of this impacts mandated compliance, O365 generates numerous security concerns that organizations are required to address. With the sudden surge in active users exchanging a huge volume of data online, it has clearly never been more important to enforce strict security guardrails that serve to identify and protect sensitive information uploaded into Office 365 and prevent it from falling into the wrong hands due to any number of accidental and nefarious events.

To help address this specific set of growing requirements, CipherCloud CASB+ enables advanced security monitoring and control for Office 365, allowing secure collaboration between users accessing these applications from any remote location, using any device - managed or personal - while providing unparalleled data protection. By facilitating organizations to more effectively adopt Office 365 as part of their digital transformation and remote collaboration strategies, CASB+ answers the following questions faced by most organizations as they seek to secure O365 collaboration:

- How do you identify and classify all data being uploaded into O365, across all apps?
- How do you gain full visibility into Office 365 user activity and data risks to prevent data loss and breaches?
- How do you enable secure access to Office 365 apps from unmanaged, BYO devices?
- How do you enable classification and protection of sensitive content shared through Office 365 emails, files, and messages?
  How do you protect sensitive information during downloads and offline shares?

By empowering a 'Zero-Trust' security approach, CASB+ provides deep visibility into all the activities ongoing across your Office 365 suite, further supported by end-to-end data protection with adaptive access controls, advanced threat protection, and compliance monitoring capabilities that ensure your data remains protected across all locations - in the cloud, and on users' desktop and mobile devices. CASB+ specifically allows you to adopt O365 with every confidence that your organization is maintaining complete control over its data, knowing that information will always be protected while being shared between Office 365 and other popular cloud collaboration apps, such as Slack, Box and Dropbox.



The CipherCloud CASB+ Office 365 Dashboard

For instance, O365 tools such as OneDrive allow employees to share large volumes of data with collaborators both internally and externally -- including suppliers, distributors, vendors, and customers. Without proper controls, OneDrive could thereby easily enable either mistaken or malicious distribution of sensitive company data. However, using the CipherCloud CASB+ solution security practitioners can define centralized policies that:

- Inspect the content and the type of file is being shared, by leveraging content-aware data analysis
- Automatically detect external users and remove their access from specific shared folders meant for internal consumption
- Alert security teams of potential risks, allowing targeted response by either addressing involved users or misaligned business processe

Leading CASB+ O365 Use Cases

Securing Teams collaboration between internal and external users

CipherCloud CASB+ allows users to securely communicate, collaborate, and share information virtually from anywhere using Microsoft Teams. CipherCloud's advanced Data Loss Prevention (DLP) policies scan and protect any form of data posted to Teams, and files moved across Office 365 apps in real-time, both via inline mode and fast API integration, offering near real-time controls. This capability includes masking of sensitive content such as SSN or credit card numbers, with policies that can be designed to restrict external members from accessing specific channels that contain sensitive or confidential information.

CASB+ Hosted Deployment Architecture

Identifying and classifying sensitive content in SharePoint and other file shares

CipherCloud CASB+ offers an integrated DLP that performs deep scanning of all documents uploaded across the Office 365 suite, including SharePoint and other file shares, then automatically classifies sensitive files by applying AIP labels. Once again enabling advanced protection via application of centralized policies, this capability enables full visibility into and protection of data wherever it is shared, including other popular applications such as Box, securing intellectual property and other protected information from unintended data exposure.

Protecting sensitive content shared through Outlook and other email

CipherCloud CASB+ offers the industry's first Secure Email Gateway delivered in a CASB that integrates directly with Office 365 and Outlook. This unique capability allows customers to extend existing DLP policies to cloud-native email, enabling seamless collaboration across O365 emails and other apps. CASB+ routes all email sent from any client device, managed or unmanaged, through a dedicated email gateway to provide detailed visibility into corporate messaging and protect sensitive content in the email subject line, body, and attachments, as well as preventing forwarding to unintended or unauthorized external domains.

Securing O365 access from unmanaged, personal devices

CipherCloud CASB+ can automatically classify any remote user device attempting to connect to Office 365 apps using digital certificates and further secure device access using contextual Adaptive Access Controls. Involved context may include device type, location, time of the day and user role, among other factors Based on the involved policy access to thick apps can subsequently be enabled or blocked from personal devices, or users can be provided with limited, read-only access via web browser. This function allows users to access O365 apps from any device, while enforcing the correct security controls.

Preventing cloud data breach from compromised account or insider threat

CipherCloud CASB+ also delivers integrated User and Entity Behavior Analytics (UEBA) that leverages advanced machine learning to monitor user activity in O365 and prevent insider threats by calculating a risk posture for each user. UEBA enables deep visibility into various user actions in the cloud and automatically flags unusual or anomalous activity, based on variation from normal patterns. Anomalous user behavior may include actions including logins during off-hours, an attempt at performing a bulk file download, or many other such improper activities.

Protecting data shared outside the Office 365 environment

CipherCloud CASB+ offers native Rights Management that protects data downloaded on personal devices, subsequently encrypting any files containing sensitive information. Only users with valid keys are able to decrypt and view the content using this model, thereby enabling secure offline collaboration. Using this approach, keys can also be revoked in real-time to protect data on any lost or compromised devices. CASB+ also enables step-up authentication as an additional verification, such as when a user attempts to download documents with sensitive information from the cloud using unmanaged devices CipherCloud further integrates with Microsoft ActiveSync to discover mobile devices, applying controls for real-time Sync, and for Send activities for Office 365 email, along with the ability to wipe sensitive data from mobile devices.

CASB+ Customer Success with Office 365

Major healthcare university in North America

Quick facts

- Industry: Healthcare Provider, Medical Research
- 40,000+ staff including Researchers, Doctors, Nurses and Clinical professionals
- More than 500,000 patients
- Opted for Office 365 to enable remote collaboration, requiring complete visibility and control over regulated information (PII, PHI, PCI) to maintain compliance

Customer Challenges

- Rapidly address expanding work from home environment for numerous staffers
- Securely standardize on cloud apps for file sharing, remote meeting, and company-wide collaboration
- Protect PHI data across files and endpoints, and ensure compliance with HIPAA

Solution

CipherCloud CASB+ provided an integrated stack and single pane of glass for security services required to protect healthcare data across multiple Office 365 apps and email service. Specific capabilities utilized include data loss prevention policies with ethical firewalls, securing of user access through adaptive access control, protection against malicious behavior by internal or external parties, and threat protection against malware in the cloud apps.

Customer Success

- Rapid deployment - the entire solution was securel integrated and launched for 40,000-plus end-users within 2 weeks.
- Delivery of secure access for any user, any device from anywhere
- Increased flexibility and productivity across all apps
- Met HIPAA privacy laws to protect patient's PHI

CipherCloud Differentiation

- One-stop solution: The only CASB vendor enabling data protection and governance across the entire Office 365 suite
- Deployment scale: CipherCloud has the experience (9+ years) in delivering security solutions at scale to service tens of thousands of cloud users who are constantly engaged in mission-critical work
- Business-ready security: Best-in-class cloud security, preserving overall O365 user experience and cloud functionality

Conclusion

Remote work has become the new normal for many workers, and, as such, organizations must focus on data-centric security capabilities to tighten their visibility and control over cloud-based collaboration. CipherCloud CASB+ empowers security operations teams to identify and protect data across the Office 365 suite, offering a single pane of glass for email and collaboration security, along with ensuring compliance with related data privacy laws such as PCI, GDPR, and HIPAA, among others. With CASB+, organizations can securely adopt and extend their use of Office 365 to collaborate and communicate seamlessly from anywhere in the world to better support worker productivity.

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.

CipherCloud

Headquarters

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

+1 855-5CIPHER
(+1 855-524-7437)

info@ciphercloud.com

