FORCEPOINT CASB

OFFICE 365 SECURITY

Enforce BYOD access rules

The automatic data synchronization (auto-syncing) feature of Outlook, OneDrive for Business, or ActiveSync mobile email app poses serious risk. Forcepoint CASB enables granular access control from BYOD, allowing you to block auto-syncing of email and files to unmanaged devices without the need to install agents on the unmanaged device. This prevents data proliferation and ultimately enhances Office 365 security.

Prevent data leakage

Forcepoint CASB identifies sensitive or regulated data stored in OneDrive to ensure compliance with regulations such as PCI, SOX and HIPAA. Forcepoint CASB inspects content in real-time, applying comprehensive Office 365 data loss prevention (DLP) policies. Forcepoint CASB includes an ICAP interface to integrate with Forcepoint DLP or 3rd-party DLP solutions.

Control data and file sharing

Forcepoint CASB enables organizations to control the sharing of sensitive data and files through granular file-sharing policies. For instance, you can allow sharing for specific users or departments, enforce whitelists or blacklists of external users and domains, or block sensitive files from being shared. You can also apply controls on file sharing outside the organization based on various criteria (by user, destination, type of content, and more).

Protect against cyber threats

Stealing login credentials is one of the most popular techniques to get access to sensitive data stored in Office 365. Forcepoint CASB has pre-defined, sophisticated algorithms to fingerprint devices and learn user behaviors in order to detect data access anomalies (indicating a possible external or insider threat). If an anomaly or account takeover is detected, Forcepoint CASB provides several remediation options, including blocking access or requiring stronger identity verification.

Monitor activities

Forcepoint CASB monitors all Office 365 activities in real-time, including uploads, downloads and shares. It lets you see what users are doing all the way down to the individual action and data object. If a policy threshold is triggered, you can display an alert, block the specific action or account, or require two-factor authentication to verify someone's identity.

Identify security & compliance gaps

Forcepoint CASB gives you complete visibility into all of your Office 365 users, even contractors and ex-employees that might still have access to your Office 365 instance. Benchmark how your Office 365 security settings stack up against industry best practices or relevant compliance requirements.

CONTACT
www.forcepoint.com/contact

[DATASHEET_OFFICE365_ENUS] 100067.051917