ManageEngine
Log360

CASB
For Cloud Security

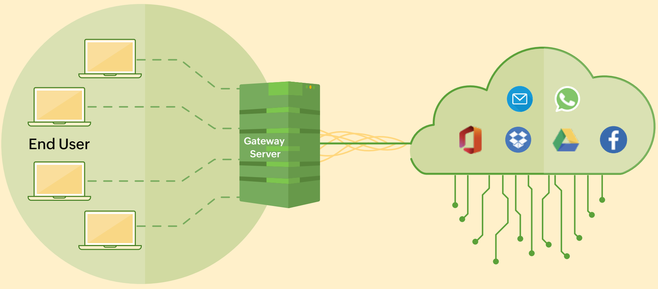
WHAT IS A CASB?

A cloud access security broker (CASB) serves as a policy enforcement point between enterprise users (both on and off the company network) and the cloud-based apps they wish to access. A CASB has three deployment modes

Forward proxy
Configured as a gateway server within the company network

Reverse proxy
Configured with the sanctioned app to validate user identity for unmanaged devices

API scanning
Configured to analyze the data-at-rest in the cloud via APIs



A forward proxy CASB

WHY DO YOU NEED A CASB?

254
The average number of cloud applications organizations have on average, according to Productiv

80%
The percent of end users who install software not sanctioned by IT, according to Cisco

10x
Shadow IT cloud utilization size is 10 times that of known cloud usage, according to McAfee

Shadow IT
- Lack of visibility over unsanctioned cloud apps
- Creates a security gap, because sensitive data can be leaked via third-party apps

Data exfiltration
- Unauthorized uploads to third-party cloud apps
- File sharing to personal or unknown cloud accounts

WHAT CASBs OFFER?

Visibility
Monitor traffic and volume by third-party apps and set custom alerts.

Insider threat mitigation
Sanction or block applications and track user activity in the cloud.

Data loss prevention
Detect suspicious uploads and data leaks in real time.

Deep packet inspection
Analyze HTTPS traffic for details such as file name, type, and size.

USE CASE