

# Cloud Access Security Broker Features Datasheet

## Move to the Cloud without a Care

Organizations are transforming and taking up innovative approaches to provide faster, reliable, and robust service to their customers. Changes from the traditional software infrastructure to the cloud are imminent but it still poses a lot of security risks and mismanagement issues. miniOrange CASB is here to help you tackle these challenges and help you smoothly transition to the cloud.

## Why do you need miniOrange CASB?

Businesses need to work with a fleet of cloud apps and managing how data is shared between users and these apps is a strenuous process. To ensure data security, integrity and business continuity, the miniOrange CASB sits at the core of your infrastructure safeguarding your data and ensuring cloud security.

## Product Features



### Granular Access Control

Enable restrictions down to the most granular level within your cloud apps with the miniOrange CASB to control access based on the user groups.



### Threat Protection

Once a threat is detected, isolate it and discreetly purge it from your cloud infrastructure without disrupting the working of your other cloud app processes.



### Device Restrictions

Enable device restrictions for office security by allowing users access to cloud apps from company-issued devices and prevent them from accessing business-critical data stored on your Cloud SaaS apps.



### Download Restrictions

Stop users from exporting or downloading data from any of your cloud apps in order to stop unauthorized downloads that could result in serious security breaches.



### Network based Restrictions

Allow access to users only if they are on whitelisted IP addresses, set by the security admin before they can access your cloud apps in real time. If a user switches their network, their access is instantly revoked at runtime.



### Shadow IT

Detect Shadow IT practices early on in your company with CASB to prevent users from accessing company data and resources from unmanaged and risky devices.



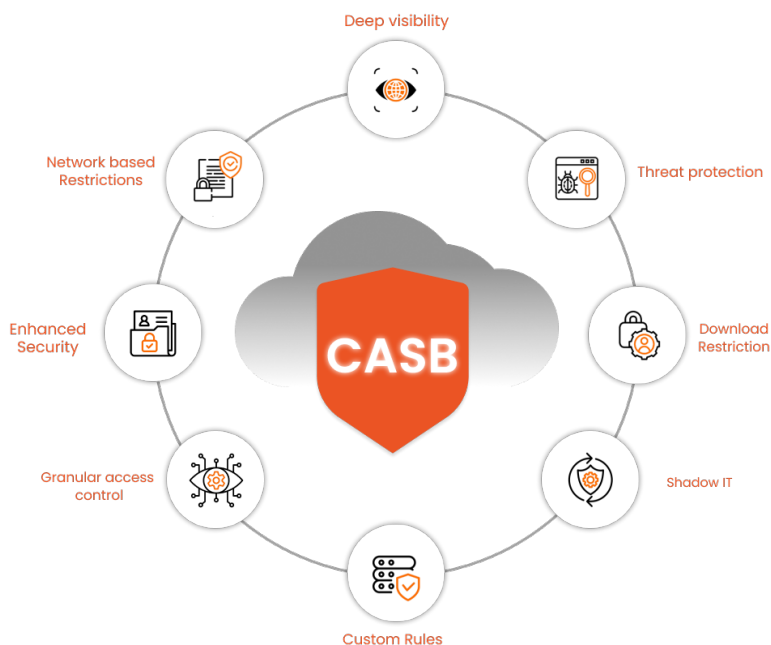
### Deep Visibility

You can monitor individual user actions and keep a log of their activity as well. This allows you to monitor and track malicious user activity and prevents any attempt at data infringement within the company.



### Custom Rules

Set custom access for individual user groups and set their permissions for individual cloud app security for improved flexibility to cover all security gaps your business may face.



## Cloud Apps Supported



Any Cloud App

