Checklist

What you need
to know while evaluating a

CASB

When it comes to **cloud adoption, security** is a
big !ssue
that IT teams face.

In addition to this, organizations are rapidly moving to cloud-based applications and allowing employees to work from anywhere, leading to increased use of shadow IT applications, or the use of IT systems deployed by non-IT teams without prior approval from the IT team.

CASBs act as an intermediary between an organization's on-premises, remote, or hybrid framework and their cloud applications, continuously monitoring the traffic between them.

Here's a checklist
of requirements that organizations should consider while
looking to adopt a CASB.

Assess your
security needs

Before deploying a CASB, it is crucial to understand your organization's security requirements. Evaluate your organization's security needs and look for a CASB solution that caters to those specific needs.

Look for the
four key functions

Visibility, data security, threat protection, and compliance are the four main functions of a CASB. A good CASB solution should offer all the four.

Consider
shadow IT

Since cloud solutions are widespread, anyone can access the cloud without the IT department's knowledge. This is called as shadow IT. A CASB should give you full insights into what apps are being used without the knowledge or approval of your IT team.

Check for
activity analytics

A good CASB solution should provide activity analytics in the granular level, including options to break down users by their location, department, endpoint type, etc. Your CASB should also be able to easily export these analytics to your SIEM solution for further validation.

Evaluate how easy
the solution is to use
and its affordability

Choose a CASB solution that fits your budget. It's important to keep in mind that a solution may be easy to use but unaffordable. Evaluate the solution to see if your security team will spend a lot of time validating its accuracy. This can help your organization save money.

Check out Log360 Cloud

A unified SIEM solution with integrated DLP and CASB capabilities, to investigate, detect, and respond to security threats.

Sign up for free