Cloud Encryption

How platform encryption compares to CASB encryption

bitglass

Public cloud applications like Salesforce and Office 365 have quickly become mainstream, with many of the world's most security conscious and heavily regulated organizations jumping into the fray. In an effort to keep security and compliance concerns from inhibiting adoption, Cloud Service Providers (CSPs) and third-party Cloud Access Security Brokers (CASBs) have responded by offering cloud encryption products that allow enterprises to encrypt sensitive cloud data. Many view this promise as a panacea - the flexibility and accessibility of the public cloud, with the security of a private data center.

This document breaks down how both CSP-provided platform encryption and CASB-provided encryption work, and the pros and cons of each approach.

Key Cloud Encryption Questions to Consider

Does the cloud encryption solution work across cloud applications?

This is a critically important question to address. Even if you're only focused on a single cloud app today, that is highly likely to change in the near future. Managing different encryption policies and different approaches to encryption becomes very difficult as your organization extends to 3, 4, or more cloud apps in the future.

Don't forget to consider other apps that connect to the initial cloud app(s) you are protecting. An app like Salesforce, for example, is almost always tied integrated with an ecosystem of both premises and cloud applications - the chosen encryption solution must take those apps into account as well, or you'll end up with encrypted data in Salesforce, but with the same data in cleartext in several other applications.

Does the solution support both field and file level encryption?

Some encryption solutions encrypt only fields in structured data, or only complete files. Even apps that mostly center around structured data often include an ability to store files in the application itself. Ensure that your solution supports encryption of both types of data.

Does the solution allow for complete separation of duties?

Separation of duties in the encryption context means that the person or people that control the application don't also control the data. This takes two forms - cloud provider versus enterprise and application team versus security team. In the former, the cloud provider controls the application and the enterprise maintains full control over the data. The latter example deals solely with internal teams - many enterprises wish to ensure that no single party has the ability to control both the application and the data. With platform encryption, the applications team has full admin access to the application, and also full access and control over the data. For many organizations, control over the data should be in the hands of the security team, not the applications team.

Does the solution allow you to meet data residency requirements?

If you do business in a country that requires that data like personally identifiable information (PII) remains within the geographic bounds of the company, you'll need a solution that allows that level of control. Some CASBs allow you to encrypt data and store it on your premises or in your private cloud, rather than in the cloud app. This gives you control over data residency.

Does the solution encrypt data end-to-end?

Encrypting data-at-rest in a cloud application won't be very effective if you allow all users to download and access that data in cleartext, especially from unmanaged devices. The ability to encrypt data from cloud-to-device is critical. Ensure that the solution you choose lets you not only encrypt data-at-rest in the cloud, but also apply features like file encryption or digital rights management upon download, especially if the app is being accessed from an unmanaged device.

Does the solution give your organization full control over the encryption keys?

The only way to fully control encrypted data is to control the encryption keys themselves. Solutions that offer encryption, but where the provider either owns or has access to the keys also allow the provider to access the data. This means that rogue admins, government subpoena, hackers, and a broad range of other miscreants can potentially access your organization's data. So why have you encrypted at all?

Does the solution allow you to achieve your full range of control and visibility goals for the cloud?

Managing security policies across several platforms can result in high overhead and mismatched policies, yet encryption is far from the only data protection function that most organizations will need. Other features like data leakage prevention, access control, and user behavior analytics are also critical. Ensure that the solution you choose covers not only encryption, but your full spectrum of cloud security needs.

How Does CSP Platform Encryption Work and What Problems Does It Solve?

Platform encryption is becoming more popular amongst major SaaS applications, with vendors like Box and Salesforce starting to support encryption. With this approach, data is transmitted to the cloud provider and is encrypted upon being stored at-rest. Encryption keys are typically owned and managed by the cloud vendor and shared across customers. A minority of CSPs have begun to support bring-your-own-key (BYOK) mechanisms, where the customer manages their keys. In a BYOK architecture, the CSP must still retain access to the keys (typically holding them in memory) in order to access the data.

The goal of platform encryption is to encrypt data-at-rest - it protects against breach-theft of the cloud provider's physical storage. In order to continue to operate properly, the data is always accessible to the CSP in cleartext so that the application, admins, users, ecosystem apps connected via API, and other external systems can access the data. Additionally, search indexes are typically in cleartext.

Since very few attacks target the physical storage, and instead attempt to target the application or users, platform encryption is very limited in its effectiveness against unintended disclosure.

How Does CASB Encryption Work and What Problems Does It Solve?

CASBs are a category of security solutions that provide data protection in a number of areas, including data leakage prevention, access control, mobile data protection, identity, user behavior analytics, and, of course, encryption. CASB encryption works by encrypting data before it travels to the CSP, typically via proxy (for user upload/download) and API (for existing data-at-rest and for data being uploaded to CSP from other premises and cloud applications). CASBs are either deployed as a cloud service, or on the enterprise premises or private cloud, and support BYOK schemes that leverage the enterprise's existing key management systems.

The goal of CASB encryption is to ensure that sensitive data never leaves the control of the enterprise. Data remains encrypted at all times as it is accessed by users, transferred to other cloud applications, and accessed by the application. Only when allowed by policy is data decrypted. Many CASBs also support the ability to encrypt data that is downloaded to endpoint devices, ensuring end-to-end encryption.

The key challenge that CASBs have had to solve is how to preserve application operations such as search and sort once the data has been encrypted. CASBs do this by recreating key functions of the application within the CASB architecture. For example, a CASB might create an encrypted search index on the customer premises and transparently use this index since the CSPs index cannot search across the encrypted data.

CASBs are best-suited to organizations that need to support multiple cloud applications, have premises or cloud-based integrations with other applications, and that recognize that they are responsible for security of their sensitive and regulated data, regardless of where it goes.

CASB vs Platform Encryption Checklist

	Bitglass Harbor (CASB Cloud Encryption)	Platform Encryption
Data in control of enterprise at all times?	Yes	No
Multiple app support?	Yes	No
Application/business team vs security team separation of duty?	Yes	No
Meet data residency requirements?	Yes	No
Data encrypted cloud-to-device?	Yes	No
Enterprise control/management of keys?	Yes	No
Broad control/visibility beyond encryption?	Yes	No
Controlled access from any device?	Yes	Yes