

# How to Choose the Right Encryption Architecture to Protect Your SaaS Data

## Author:

**Arnaud Treps**

Chief Information Security  
Officer at Odaseva

**odaseva**



# Table of Contents

**3** Executive Summary

**5** What is important to know about encryption?

**7** A breakdown of each encryption method's rating

**10** How do you choose the right encryption method for your needs?

**11** Conclusion

# Executive Summary

What type of encryption do you need to protect the SaaS data in your organization?

As enterprises continue to ramp up adoption of SaaS platforms like Salesforce, the data stored in them grows in volume, complexity, and importance. Encryption is one of the key security controls highlighted to protect this critical data.

But not all encryption methods are created equal. While some vendors may appear to protect data with identical methods of encryption like AES-256, there are important architecture factors to consider besides just the encryption algorithm and key length.

Understanding where the encryption and especially the decryption takes place is very important. You need to know where decrypted data is exposed to potential threat actors.

Is the data safe from malicious employees, rogue admins, or hackers? How do you determine which encryption method is appropriate for the risks your organization faces?

When choosing a SaaS solution, decision makers should understand what type of encryption is used and decide if the evaluated solution is offering the protection level adapted to the data sensitivity.

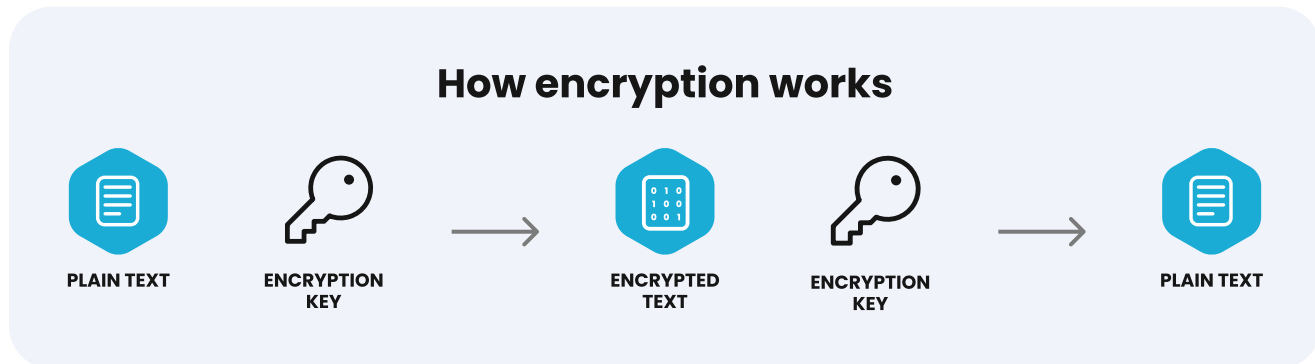
We propose the following rating, which ranks encryption methods from the easiest (but often weakest) methods, to the strongest approach where data encryption and decryption is only done on the data owner's device which eliminates most of the unauthorized access risks.

SECURITY GRADE	TYPE OF ENCRYPTION	USE CASE	EXAMPLE
A+	End-to-end encryption	Secret data, highest privacy level	Became mainstream with messaging applications (like Signal)
A	No view provider	Confidential data, zero-trust model, protection against malicious employees	Odaseva Enterprise Data Protection Platform - users of the platform can't see clear text data unless they have the encryption key
B+	Granular encryption with BYOK	Confidential data, protection against rogue database admins, enforced segregation of duties, audit logs	Salesforce Shield with BYOK option - database admin can't see clear text data, don't have access to the encryption key
B	Granular encryption	Confidential data, protection against rogue servers or database admins	Salesforce Shield - database admin can't see clear text data, segregation of duties is necessary to prevent access to the key
C+	Container encryption with BYOK	Auditability, capability to rescind key access	Cloud storage encryption (AWS S3, Azure Blob Storage, etc.) with BYOK
C	Container encryption	Basic needs, compliance driven	Transparent encryption in database servers, cloud storage, laptop or smartphone hard drive encryption
F	No encryption	Public, non-sensitive data	Clear text

## What is important to know about encryption?

Encryption is a mix of process and technology to convert sensitive data (clear text) into secret code (encrypted text).

Encryption prevents unauthorized persons from accessing sensitive data because a decryption key is required to transform data back from encrypted text to clear text.



## What are the risks of not having proper encryption?

Encryption is often complex and will be as strong as its weakest link. The strength of any given type of encryption is typically tied to:

1. The strength of the encryption algorithm
2. The implementation of the encryption module
3. The control and management of the encryption keys
4. The place where encryption and decryption occurs

If you don't have an effective encryption method in place, the security of your data is at risk. Examples of risks include:

**Exposed data:** If your organization stores sensitive or regulated data such as trade secrets, Personal Identifiable Information (PII), or health records, a breach can have serious consequences including business interruption, loss of revenue, and reputation damage.

**Non-compliance:** encryption is also a fundamental control in almost all compliance frameworks including NIST-800-53, PCI, HIPAA, GDPR and more. That means ineffective encryption can put organizations at risk of non-compliance – and the resulting legal and business implications.

**False sense of security:** Not having proper encryption is sometimes more dangerous than having no encryption at all because it creates a false sense of security that data is adequately protected.

## How to assess encryption capabilities







Overall, you want to select vendors that offer the right encryption method for your organization's needs.

Regarding encryption in transit, especially in web applications leveraging HTTPS, the encryption methods are now well standardized and can be easily assessed using online tools like Qualys SSL Labs. But when it comes to encryption at rest (i.e. how is data encrypted when stored or manipulated on the servers), more analysis is required.

The first step is to make sure the encryption methods are using state-of-the-art algorithms (refer to resources like the NIST Cryptographic Standards and Guidelines).

But many vendors may appear to offer the same encryption, with well-known algorithms like AES-256 symmetric encryption, or RSA 2048 for asymmetric. That's why the next step is to assess at which layer of the application the encryption and decryption takes place, and how it protects against the different threat actors.

Overall, the closer the end user is to where the encryption and decryption is performed, the fewer possibilities it gives to threat actors to access encrypted data.

	THREAT	EXAMPLE
	Unauthorized access to physical storage media	Accessing the hard drive or physical server and can read the content of the disk
	Malicious Employee	Intentionally decrypting data with the intention of misusing it
	Rogue admin	Administrators with access to sensitive information abusing their privileges
	Cloud vendor's rogue admin	Cloud vendor's administrators with access to sensitive information abusing their privileges
	Hackers	A malicious third-party gains access to encrypted data
	Government subpoena	A government agency demands access to encrypted data

## A breakdown of each encryption method's rating

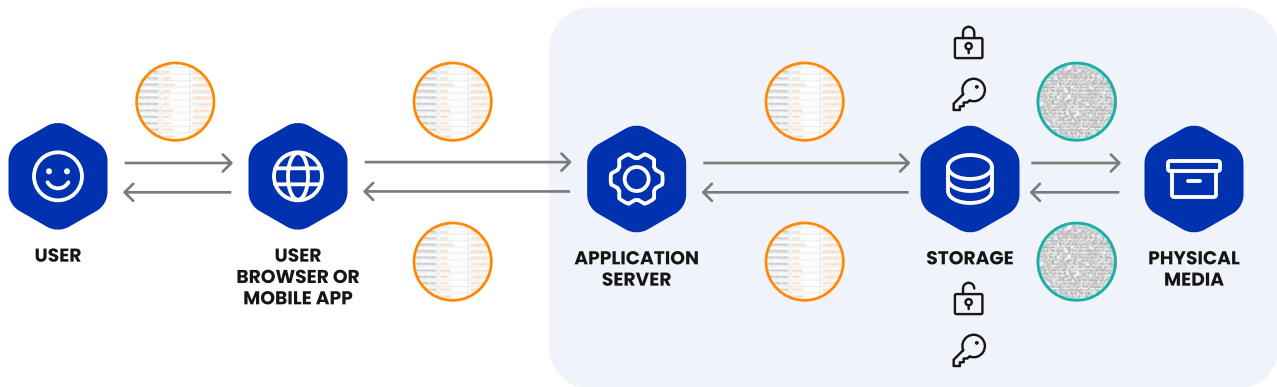
Here is a breakdown of each rating reference in the chart on page 3, from weakest to strongest.

### Container encryption

Security Score



When encryption is only done at the storage level, anyone such as a rogue admin can access decrypted data by connecting to the database engine without being blocked by the encryption, since the database engine transparently decrypts data. This method, called container encryption, is very popular since it's easy to implement, but it's only protecting against the risk of physical access to the storage media.



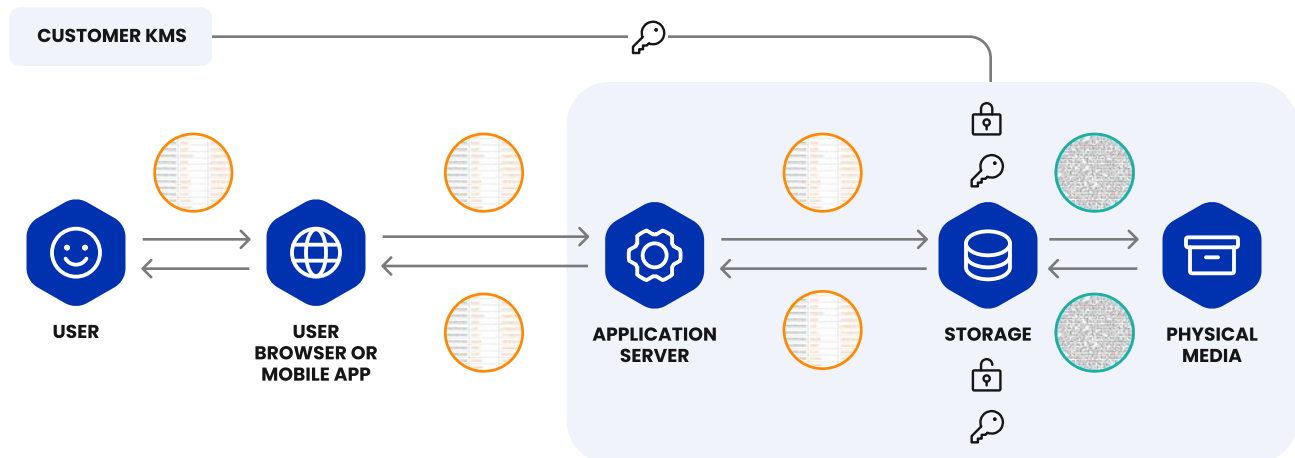
### Container encryption with BYOK

Security Score



Another type of container encryption is "Bring Your Own Key" (BYOK), which introduces a key management system that is managed by the customer. This approach gives the customer the ability to better control and track access to the encryption key, however in normal operations it's not drastically changing the level of security: the storage engine has access to the key to decrypt, and all actors connected to the storage or the application will see data in clear text.

The main benefit is the ability to remove access to the encryption key, in case of an incident or at the end of the relationship with the vendor.



## Granular encryption

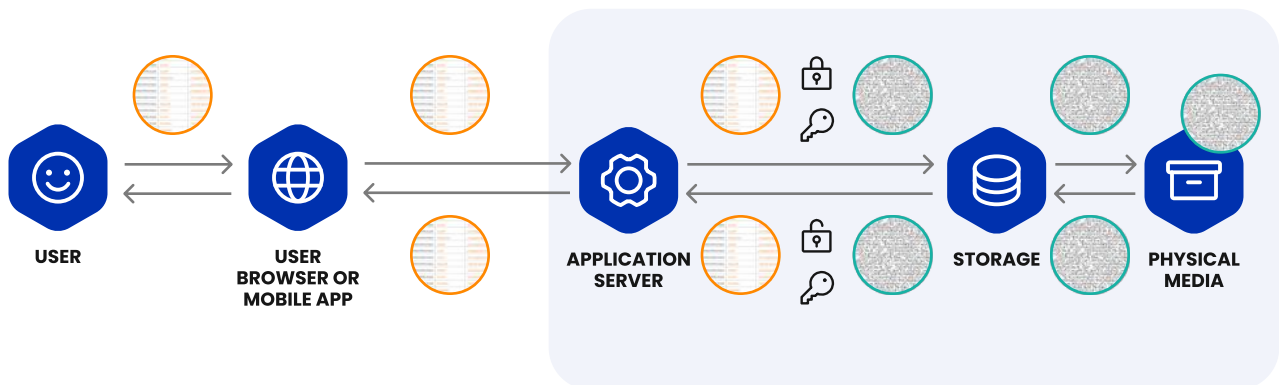
Security Score

B

Granular encryption means the encryption and decryption is performed by the application server.

The security level is significantly improved with granular encryption. Rogue database admins or hackers gaining access to the storage layer will only see encrypted data. One needs to hack into the internals of the application server to decrypt data.

However, any user of the application will see data in clear text. It could be legitimate users, but it could also be viewable by hackers who successfully steal credentials through a phishing campaign or a rogue application admin.

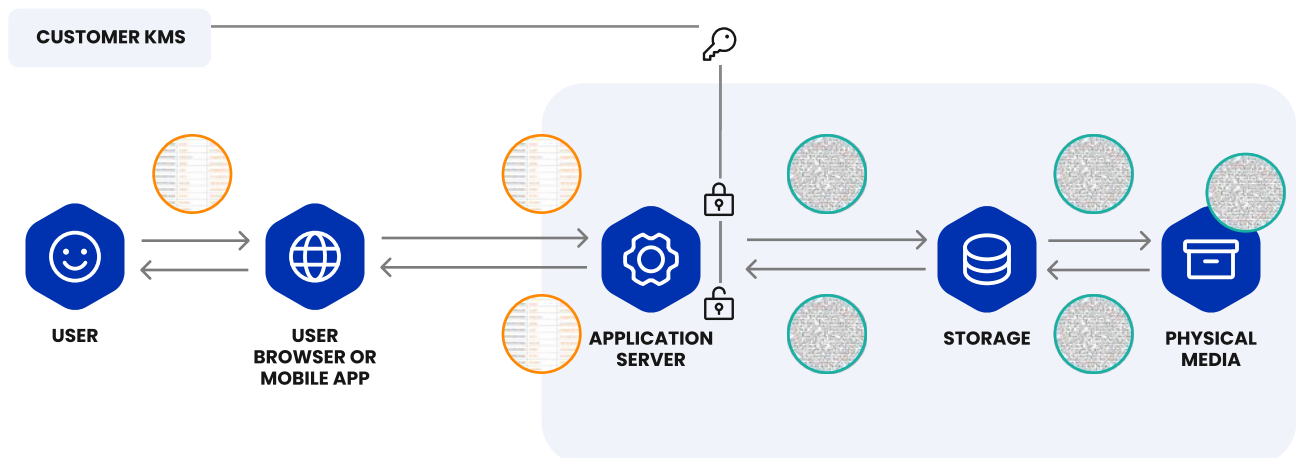


## Granular encryption with BYOK

Security Score

B+

Granular encryption is also possible with BYOK, giving more control to key access.





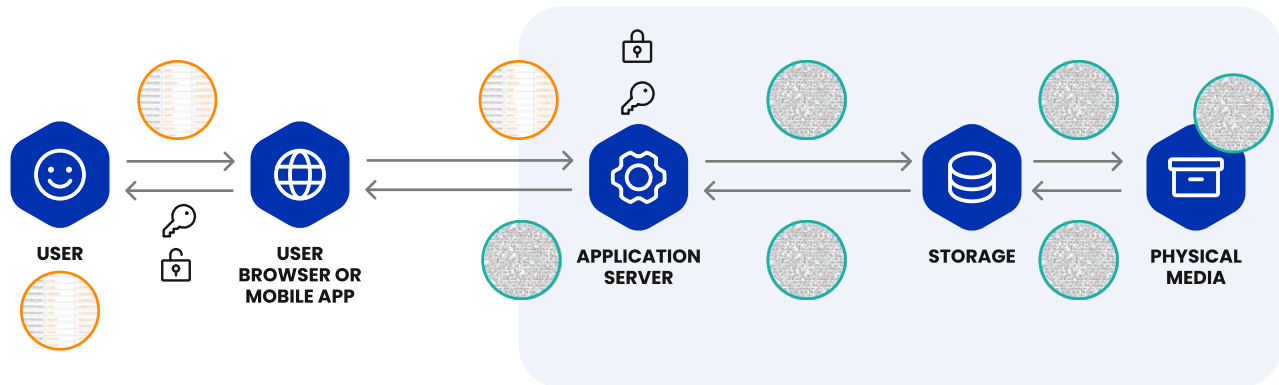
## No view provider

Security Score



No-view provider is the best approach for use cases where data can't be encrypted at the client-side.

No-view provider is similar to granular encryption with one important specificity: the application server does not transparently decrypt data. This means that hackers who managed to steal user credentials or a rogue application admin won't have access to the data.



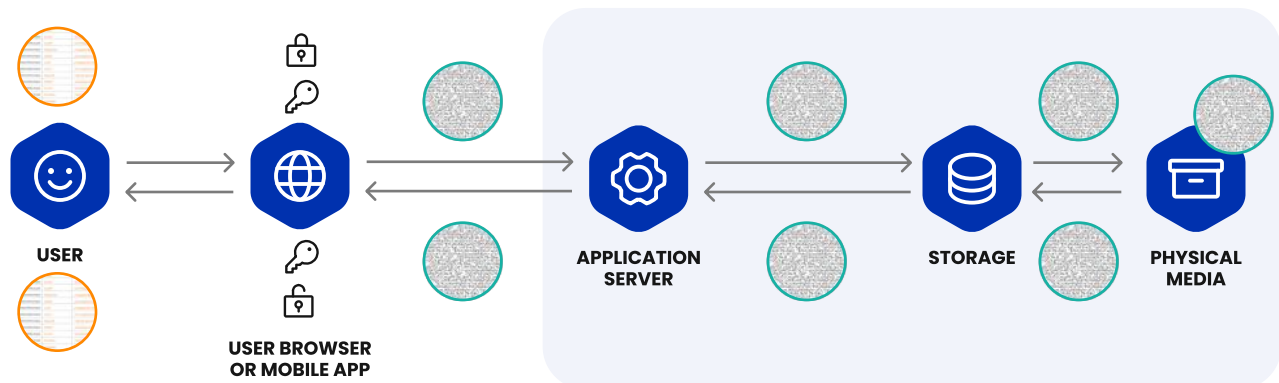
## End to end encryption

Security Score



Finally, end-to-end encryption completely removes the need to trust the cloud vendor or application admins, since data is encrypted and decrypted at the client side by the data owner.

The application, storage, and physical media only manipulate encrypted data and don't have access to the encryption key. With this approach most of the threat actors are eliminated, even the risk of third-party government intervention, because the data owner (not the SaaS vendors or other actors in the data protection program) has sole technical access to the data.



## How do you choose the right encryption method for your needs?

When you see that some methods of encryption are far superior to others, it's easy to wonder why every organization doesn't just use the highest level of encryption for all their data.

The answer is that there's a trade-off between usability and security.

When security features increase, usability typically decreases as a result. For example, applications with granular (or stronger) encryption typically have difficult or slow search functionality.

Another difficulty when using very strong encryption is that if you lose your decryption keys, it will be almost impossible to recover data.

Enterprises must find the right balance that suits their specific needs - a solution that secures data with the appropriate level of encryption, while preserving the features that employees and customers require.

The balance can be found by selecting a vendor that doesn't sacrifice usability for security and vice versa, but rather balances both. Investing in the right vendor should enable you to retain usability, even when protecting critical data with high levels of encryption. So find the "best of both worlds" solution that meets your needs.

# Conclusion

Encryption is one of the fundamental security controls used to protect sensitive data.

But not all encryption methods are created equal, and enterprises must choose the appropriate type of encryption for their needs.

It's not just the algorithm and key length that matters - key management is a critical consideration, especially when dealing with very sensitive data.

Even if two vendors provide the same encryption tech, the overall data protection can vary considerably, depending on where the decryption is performed.

For these reasons, it's important to understand the distinctive features between the various types of encryption.

Odaseva has been protecting Salesforce data for some of the world's largest companies for more than a decade. Our customers entrust Odaseva with critically important data. That's why our commitment to data security exceeds the requirements of even the most complex, highly regulated businesses in the world.

**Do you need to protect your enterprise's Salesforce data? Discover all the ways Odaseva can help.**

**Contact us today [odaseva.com](https://odaseva.com)**