Encryption Software For The Financial Industry

Encryption & Data Security

Financial institutions are among the top targets for data thieves and cyber-attacks. With enormous amounts of sensitive data to protect, the consequences of a data leak and the loss of unprotected data can be catastrophic for financial organisations and their customers.

Securing data with an encryption solution retains customer confidence, and ensures that financial institutions comply with national and international industry directives. Organisations also need to establish security protocols that are easy-to-use and do not interfere with customer service, communication or other business requirements.

What Data Should Be Encrypted?

As one of the most regulated industries in the world, the Finance Sector deals with large amounts of Personally Identifiable Information (PII), such as names, addresses and social security numbers, as well as more sensitive data including income details, credit scores and Non-public Personal Information (NPI).

Most financial institutions are required to:

- Ensure customer information is held securely and confidentially.
- Protect this information from any anticipated threats.
- Protect this information from any unauthorised access.

This is the type of information that should be protected with encryption software in the financial sector:

- Any sensitive information that the customer provides, including names, addresses, income, social security numbers.
- Any information received about an individual when a transaction takes place between the individual and the financial service provider. This includes information such as account numbers, payment history, loan or deposit balances and credit card purchases.

Industry tested encryption algorithms should be employed by financial institutions. Encryption technology with long key lengths is essential, an example of an industry-tested, FIPs approved encryption standard is AES 256-bit. The same encryption standard used by the Military and Government sector.

The Different Levels Of Encryption

ENCRYPTION FOR DATA AT REST

This means adding encryption to the data before storing it in a database, cloud storage, the server, etc. This is considered one of the most secure ways to protect data, and allows access controls and time-stamping to be set up, as well as other security parameters.

This also applies to any sensitive information that is stored on portable devices such as laptops and smartphones. These portable devices should also have their hard drives encrypted, including all external hard drives.

ENCRYPTION FOR DATA IN MOTION

With the increased use of mobile devices to do their banking, customers and businesses alike need a secure way to communicate with their financial services provider. Ensuring that all emails, text messages, apps and websites are securely encrypted end-to-end is a must for the financial sector.

This way, any data that is being shared is protected while it's in transit, meaning that it cannot be read while it is on route to its final destination.

The Importance Of Effective Key Management

Encryption keys are the way to unlock and read all of that encrypted data that has been stored or shared. How these keys are managed is just as important as the sensitive data itself.

Losing an encryption key means losing access to the data. The importance of retaining control over who has access and holds the keys to the data is crucial. The Financial Sector stores some of the most sensitive data there is and there are strict controls over data storage and sharing.

How WinRAR Can Help

Financial institutions need to be able to stop a data leak before it even begins. Every day they move sensitive data across the globe and at the speed of light, navigating multiple IT infrastructures and storing sensitive information in multiple repositories. One relatively small breach can cause a huge deal of damage.

WinRAR uses AES 256-bit encryption. The industry standard and FIPS certification for encryption technology, simply set your RAR archives and files with a password, and WinRAR will not only encrypt the archive, but all of the metadata too. This is perfect for sending data across servers, with emails and for storing important data in the cloud.

With WinRAR, admin rights can be established, protecting files from unwanted viewing and taking control of those encryption keys. With data and time stamps, administrators have full control over who and when sensitive data is viewed and by whom.

WinRAR's built-in Password Manager also helps with control of encryption keys and the numerous passwords that organisations need to use to keep data protected.

With more than 25 years' experience and a dedicated Sales & Support Team, WinRAR is the ultimate software for Financial Institutions. Out-of-the-box and easy to use, WinRAR can do everything that organisations need to stay compliant with privacy regulations such as the GDPR and CCPA.

<- Back to: Industry Sectors

DownloadSupportNewsPartnersIndustryPrivacyContact