Financial Services Industry Brief

A1LOGIC

At-A-Glance

- Protect Confidentiality, Integrity and Authentication of Financial Files of any File Type
- Protect Confidentiality, Integrity and Authentication of important columns in SQL tables, such as “Credit Card Number” or “Account Balance”
- Assume attackers will steal data, but make clear text available only to authorized physical computers within the enterprise

The Situation

In the financial services industry, companies hold data that literally has financial value, such as bank account numbers, credit card information and account balances. Theft of such data is equivalent to bank robbers breaching a safe and walking out with bags of money.

The finance industry assumes that customers will be deceived and their account or credit card numbers will be stolen. Fraud due to such theft is considered a cost of doing business and accounted for accordingly. Given the fact that it is not provable whether the computers and networks that hold financial data are compromised or trustworthy, it is wise to similarly assume infrastructure is compromised. However, with A1FILO, data breaches do not have to be considered a cost of doing business.

We have seen finance use cases storing sensitive data in 2 main ways: in files and in databases, and A1Logic can protect both.

Protecting Files

In the case of files, A1FILO opens your files in a reverse sandbox, isolated from the rest of the world. The files could be residing anywhere and on any storage medium that is unaware of the encryption, such as a file server, cloud, or a USB drive. An example would be a spreadsheet of bank account numbers which is stored on a file server within the company. If an employee wants to open the spreadsheet, they would simply double click the file on the file server, and it would be opened by A1FILO in a reverse sandbox by the desktop's spreadsheet software. Due to the way A1FILO locks down files to the organization's physical computers, even if the spreadsheet was leaked to the internet maliciously or by accident, it could not be decrypted on a physical machine that is not known to the company. Additional integrity checking and authentication of the spreadsheet can also be done to make sure it was not modified at rest on the file server or in transit to/from the file server since the last time an authorized employee manipulated it on their authorized machine.

> A1FILO locks down files to authorized physical computers in an organization.

Protecting Databases

In the case of a database, servers contains SQL tables, where the Credit Card Number (CCN) is the sensitive column. Existing database software can encrypt database columns, but those columns are only encrypted "at rest" by the database server and are decrypted when queried and

returned. What happens if an employee's desktop computer that is querying the database is compromised? What happens if your organization is hit with SQL injection and the CCN column is accidentally returned to an attacker outside the organization? What happens if an attacker manipulates cells in other SQL columns such as "Account Balance"?

A1Logic can protect the columns in all three cases.

The database stores data "at rest" with all the necessary column(s) encrypted. An authorized employee queries the records of the database from their authorized desktop, and the database server returns the encrypted CCN cells. The employee's desktop runs the finance application and decrypts the CCN cells only in a reverse sandbox, where they are protected "in use" from malware and Malicious Insiders. The CCN cells stay encrypted both when stored "at rest" in the database server and "in transit" to the employee's desktop over the network. If SQL Injection did occur and an attacker was able to dump the CCN column from the database, the attacker would only get the encrypted CCN column, and would not be able to decrypt it, because their physical computer is not known to the organization. This is how A1Logic can protect whole database columns "at rest", "in transit", and "in use", preventing SQL Injection attacks from resulting in a Data Breach.

> A1Logic can protect SQL columns from SQL Injection by protecting columns "in use", "at rest" and "in transit".

Another danger is attackers manipulating sensitive SQL columns such as “Account Balance”. A1Logic can additionally enforce integrity and authenticity of columns, guaranteeing that data was not manipulated at rest in the database or in transit to/from the database since the last time an authorized employee last manipulated the cells on their authorized computer.

www.A1Logic.com

info@A1Logic.com

+1-202-888-7765