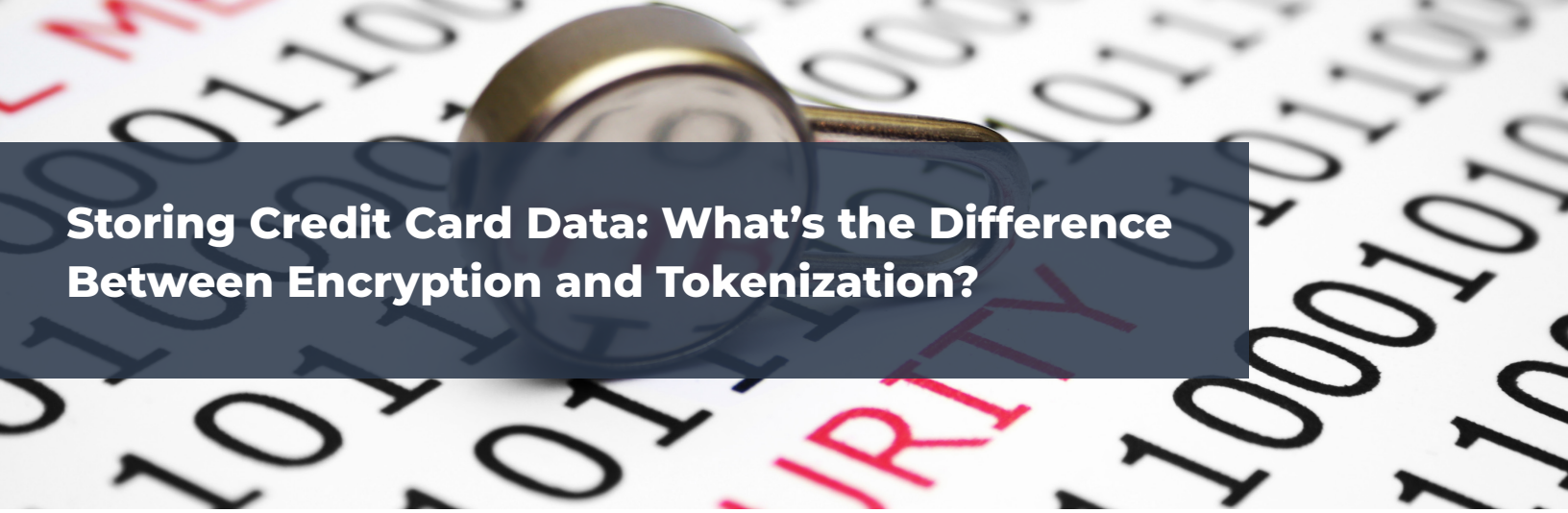

Storing Credit Card Data: What's the Difference Between Encryption and Tokenization?

There are two primary methods for capturing, storing, and sending sensitive data like credit card numbers and social security numbers. secure: encryption and tokenization.

Encryption changes the clear text data into a long string of characters. When needed, the data is decrypted using a "key." In its encrypted state, sensitive data is worthless to cyber criminals.

However, encrypted data is still a target for hackers, who have their own decryption software and are always probing for unlocked doors or the path of least resistance.

If they can't decrypt the data themselves, they'll try to find someone who has they "keys." If encryption is the process of building up high security walls around the sensitive data being stored, tokenization is the simpler strategy of storing data with no value to cyber criminals.

In this second method, credit card data is securely sent to an encryption server which creates and stores a "token" of that data. Payments are processed using that token, instead of the actual credit card data. This security method makes the data stored on the payment application network completely worthless to hackers.