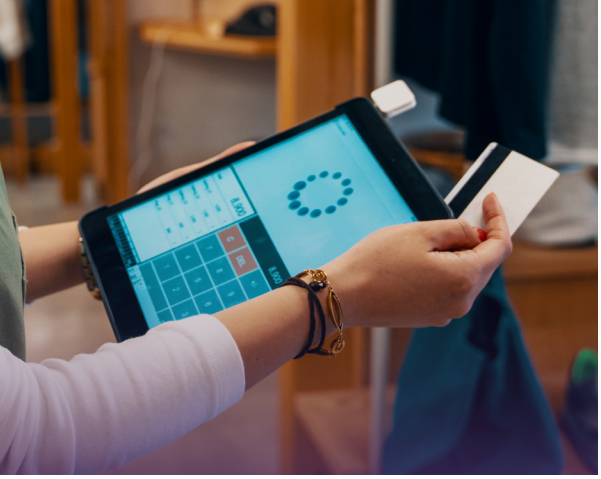

CASE STUDY

Square Deploys Entrust nShield HSMs to Fight Cyber Attackers on Its Own Terms

With a belief that everyone should have the opportunity to participate and thrive in the digital economy, San Francisco-based Square, Inc. is on a mission to build tools that make commerce easier and more accessible to all.

Square was founded in 2009, with offices in the United States, Canada, Japan, Australia, Ireland, and the UK. It offers sellers a broad range of payment acceptance options, complemented by reporting and analytics, next-day settlement, and chargeback protection. The company's point-of-sale (POS) software and associated business services are designed to help sellers succeed. For example, significant innovation through the use of Square-designed readers for smartphones and tablets enables merchants to accept card payments in a secure manner without the complexity and cost of managing traditional fixed POS devices. The origin of the now substantial global mobile POS (mPOS) card acceptance market can legitimately be traced back to Square.

As with all companies, data integrity and the security of transactions are mission-critical factors. However, Square has a rather unique philosophy in the way it approaches its security architecture. Most attackers try to exfiltrate data so that they can work in the seclusion of their own systems. Square's environment was architected from the very outset to prevent that from happening, incorporating hardware security modules (HSMs) as a required element.

Square

Performance, Reliability, and Protection

Business Need

- Contribute to the overall ease of attaining multi-agency compliance
- Absolute reliability

Technology Need

- Ability to handle throughput and scale to support business objectives
- Make crypto-anchor architecture a reality

Solution

- Entrust nShield Solo XC hardware security module

Result

- High cryptography throughput rates
- Elevated protection through crypto-anchor deployment
- Streamlined compliance process
- Rock-solid foundation for layered code

> We have used Entrust nShield HSMs for five years and they have always been exceptionally reliable. We've layered a lot of code on top of the HSM; it delivers the performance we need and has proven to be a rock-solid foundation.
>
> **NEAL HARRIS, SECURITY ENGINEERING MANAGER, SQUARE, INC**

Business Challenge

The numerous regulatory bodies in Square's sector dictated the need for the selected HSM to be compliant with a wide range of government and payment industry mandates that meet stringent security requirements. Square conforms to multiple standards, including the Payment Card Industry Data Security Standard (PCI DSS).

In addition to making reliability a primary objective, the Square team closely focused on the selection of any component in its architecture capable of compromising data integrity, performance or the seller experience.

Technical Challenge

The uniqueness and value proposition of Square's offerings have made the company a resounding success and this has influenced the design criteria for the infrastructure. Square opted to handle scalability at the application layer and this created the need to be able to conveniently move keys between HSMs.

A key factor for selecting the optimal HSM for the Square implementation was a module's ability to process vast amounts of data. Square profiled its software to understand how many authentication code operations and how many encryption calls were taking place, and replicated this to test HSM performance.

Solution

Square's technical team performed a rigorous evaluation of multiple vendors and selected the Entrust nShield® Solo HSM because of its compelling performance across the full suite of tests. The Entrust solution's inherent ability to scale – enabled by the seamless sharing of keys across HSMs without user intervention or complex key cloning activities – was another of the many standout features.

The success of the Entrust nShield Solo HSM in the crypto-anchor role has since paved the way for their use in injecting keys into Square's readers to authenticate the devices. Every hardware product has its own unique key and the Entrust products are a critical part of that process.

Results

The fundamental value of the HSM-centric crypto-anchor approach has remained sound over an extended period of time. Several years since Square decided to use Entrust nShield HSMs, the choice of Entrust as a partner continues to hold valid.

The requirement to regularly conduct both internal and external audits can frequently be very labor-intensive and time consuming. However, the presence of the FIPS-certified Entrust nShield HSM can contribute to streamlining the process.

During its Payment Card Industry Data Security Standard (PCI DSS) audit, for example, Square specifically highlighted that its data is protected by an encryption key, located in the Entrust nShield HSM. The inclusion adds to the volume of evidence provided to the auditors to demonstrate that any potential issues are being handled in a robust and compliant manner.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION