Success Story

One of the World's Largest Fashion Retailers Chooses Tokenization

Encryption is an effective and secure tool for protecting data, but its usefulness in high-volume, real-time payment environments is compromised by the stress it puts on IT infrastructure. This high-profile fashion retailer used comforte to implement a tokenization solution to provide both speed and security.

Customer Profile

In most retail stores, whenever a customer uses a payment card, the transaction details are stored in a central computer system to facilitate the exchange of money for the items sold. Unless the retailer outsources their payment processing to a service provider, storing transaction details is a normal business operation.

This major fashion retailer in the US is no exception. With close to 900 stores in North America, accepting payment cards has long been a staple as part of their customers' experience: the firm has accepted payments from all major card labels (Visa, MasterCard, Amex, and Discover) for more than 30 years.

Challenges

Stored transaction details contain payment card data, which is a huge target for bad actors and hackers looking to steal valuable data. On the dark web and underground websites, stolen credit and debit card details are sold for large sums of money, used to purchase illegal items, and exploited for other criminal purposes.

This is exactly what happened to this highly-recognized and trusted retailer. They experienced a data breach of an undisclosed amount of customer records. The attackers exploited gaps in their data security program, which prompted decision-makers at the board level to invest in a more robust data security solution.

As part of their existing data security program, the retailer already used encryption to protect the payment card numbers, as well as an internal reference number associated with every payment card. However, personal information (names, addresses, birthdates, etc.) of their valued customers remained unprotected. The high possibility of suffering another data breach due to unprotected data was not something the company wanted to risk.

Activating encryption for all customer data across their complex landscape would have overburdened their hybrid infrastructure. Encryption is excellent for protecting data, however, to use the actual data for standard business purposes (like back-office processing, disputes and reconciliation, settlement, and customer loyalty programs), decryption needed to occur. Encryption and decryption processes take up computing power and may impact transaction speed and performance. During peak times when customers visit their stores, the transaction volumes may reach over 100 transactions per second collectively from all the registers in the stores as well as online transactions. The last thing this retailer wanted to do was slow down authorizations happening at their registers. This would harm their world-renowned customer service.

Quick Facts

- Data protection extended beyond PANs to include personal data
- Same level of security as encryption but with reduced burden on IT resources
- Time and resources saved by taking sensitive data out of scope of PCI audits
- Encryption key management no longer required for tokenized data
- New data protection tools will facilitate cross-regulatory compliance

Secure your Growth with comforte

With more than 20 years of experience in data protection on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data. comforte's Data Protection Suite, SecurDPS, has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers, and continuous technology disruptions. We are here to help secure your growth by providing expertise, an innovative technology suite, and local support.

To learn more, get in touch with a comforte representative today by visiting: **www.comforte.com/contact/**.

"We are thrilled to work with comforte on expanding our data protection systems. Their dedicated team of professionals has taken the time to fully understand our requirements and is always ready to go the extra mile to get this project done right."
– CISO at a Major Fashion Retailer

Encryption and decryption also increase IT operations, specifically the management of encryption keys. As a common practice in encryption processing, encryption key management responsibilities require refreshing and replacing encryption keys every so often (also called rotating keys), as to reduce the possibility of data exposure should the encryption keys be lost or stolen. The retailer expects its volumes to grow year over year; therefore it was natural for them to expect their operations and key management functionality to grow as well. To put this effort into perspective, based on the annual volume from this retailer, rotating encryption keys on one billion payment cards every year was not a task they wanted to continue.

This company was also working on ways to minimize risk, not increase it. So, the concept of adding more sensitive data to a huge encryption program was unattractive: the more sensitive data under encryption, the higher the risk of encryption key exposure. Security professionals know that hackers typically do not attempt to break the encryption algorithms; they attempt to steal encryption keys. Therefore, counter-intuitively, more sensitive data protected with encryption could be seen as increasing their risk, rather than minimizing it.

Solution

Tokenization

Tokenization was the data protection method the retailer chose to secure its sensitive data throughout its enterprise. Tokenization of sensitive data uses cryptography to generate a surrogate value (also called a token) of the original data. Tokenization differs from classic encryption because tokenization does not use an encryption key as part of the cryptography process. Tokenization is a data protection method with less risk of sensitive data exposure since no encryption keys exist and less operational impact since no encryption key management needs to be planned and resourced.

Preserve Referential Integrity

However, there was one more major requirement the retailer mandated before finalizing their decision. They wanted to be sure that when sensitive data was tokenized, they could still use the protected data throughout their enterprise and receive the same results. This requirement is called 'maintaining referential integrity.' In simple terms, if card number "4444 4444" is tokenized into value "9876 5432" and the same card is used again one year later, the tokenization process will still tokenize the original card value as "9876 5432". Referential integrity allows the retailer to maintain data usability throughout the lifecycle of each customer, throughout their applications and services, and provide the data security and privacy necessary to stave off data exposure incidents or data breaches.

No other approach provided data protection, privacy, and referential integrity while maintaining the lowest level of risk tolerance provided by tokenization. Therefore, the retailer was completely convinced and committed to securing its enterprise with tokenization.

Proof of Concept

The retailer required a small, focused Proof of Concept (POC) project, which our solution was able to meet on-time and with all requirements met. Due to the sensitive nature and the specificity of their requirements, the details for the POC are not in the public domain.

Going Forward

As one may expect of an organization with 30 years' history of accepting payment cards, and over one billion payment cardholder records, the project to improve its data security has the full attention of each department involved. The retailer is in full project mode and has already completed the first milestone towards getting fully implemented with tokenization.

In summary, the keys to success were convincingly met:

- Minimize the existing risk of cardholder and customer data
- Present negligible transactional impact on retail stores or online services
- Maintain referential integrity thus allowing tokenized data to operate as if it were the original data
- Extend data protection beyond payment card numbers to include personal info from customers

Benefits

The retailer was already in compliance with PCI DSS requirements. The switch to tokenization had no impact on their PCI DSS compliance stance, as tokenization is recognized by the PCI Security Standards Council as a strong approach to payment cardholder data protection.

Reducing PCI Audit Scope

Two added benefits resulted from the switch to tokenization as the data protection method. First, the retailer can potentially reduce the scope of the security audits they are subjected to each year. Typically, the security audits for PCI DSS compliance require the scope of audit to include all systems which contain the original payment cardholder data. Since the tokenization process replaces the original data with a surrogate (token) value, some systems can be taken out of the scope of the security audit, since the original data no longer exists. A complete study has not yet been completed, but it is anticipated that the retailer may save more than 60% in time and resources as a result of Audit Scope Reduction due to tokenization.

Cross-regulatory compliance

Secondly, tokenization positions the retailer to be ready to respond to other data privacy laws surrounding the processing of personally identifiable information (PII). In the US, each state has come out with – or will be coming out with – data privacy laws that protect customer data. Based on how the retailer uses personal data from its customers, it may be subject to some of these data privacy laws. Tokenization fulfills the act of replacing sensitive data with surrogate values, which puts the retailer in a strong position when looking to comply with additional data privacy laws.

"At comforte, our mission is to provide solutions to protect the data that organizations have been entrusted with. We are very excited to continue that mission by enabling this major retailer to keep their loyal customers' data safe."
– Michael Deissner, CEO at comforte AG

comforte