

A 19th Century Company Meets 21st Century Challenges

CASE STUDY - MAJOR RETAIL & LOGISTICS COMPANY

This government-owned services provider has a history dating back to the early 19th-century—today it must confront urgent 21st-century challenges. Besides its traditional services, this company also has a broad array of financial services. These include online bill paying, personal banking, and money transfers.

Since it has enormous reach and an extensive range of fiscal operations, the company qualifies as a Tier One merchant under the Payment Card Industry (PCI) privacy guidelines. Recently, the organization's information security officers needed to boost IT security infrastructure and the overall approach in cardholder data protection.

“Implementation couldn't have been easier, we used a local integration team, consisting of one project manager and one developer. Voltage SecureData uses all standard components, so installation was a snap—it took just an hour to set it up and configure it.”

IT Security Manager

A Massive Business Challenge

The company accepts payment card transactions through a network of more than 3,500 retail locations, as well as online. These include simple payments for postage stamps, in-store retail purchases, and courier services, plus monthly payments for utility services like telephone, water and home heating/cooling. With its broad authorization, the company handles and stores credit card details of the country's population and many of its visitors. In a nation of over 21 million people, this number represents almost every household in the country.

Transactions handled at the retail location are uploaded through secure file transfer once a day, with the cardholder data ultimately stored in a data warehouse running Oracle. The company had basic security controls around the data warehouse but, under PCI regulations, it had to enhance data-management protocols, and improve data protection in storage and transit using strong encryption.

“Proposed solutions we considered included installing new database software, using third party tools, and building a proprietary public key encryption system,” the company's senior IT security manager explained. “These options, however, would have required enormous increases in IT spending, together with capital costs and ongoing staffing.”

Under the PCI rules, the company needed to encrypt the credit card numbers already in its corporate data warehouse, and encrypt new credit card numbers, captured daily and added each night through batch processing. The company also had to provide role-based and masked access to credit card numbers for customer service representatives and designated staff, through a web-based application on the intranet. Finally, while remaining PCI compliant, the organization had to let developers continue developing applications with masking, so that live credit card data was not used in testing and development environments.

A Hard Technical Challenge

This last requirement was very challenging, because conventional approaches to encrypting data within databases—such as encryption proxies, column encryption or look-aside databases—can be costly, cumbersome, and often impractical to use. The company had a very brief timeframe to meet compliance with the PCI rules. Even so, encryption vendors, who met with the IT decision-makers, insisted that completion of all three project phases required 18 months, at least. This prolonged timeline was a problem, because it could place the company at odds with PCI compliance deadlines.

“We run a TRU64 system—a legacy Digital Unix system,” the IT security manager noted. “Because of this architecture, we have very tight development windows. This is a big problem for us—finite processing times. We couldn’t be confident that installing software on the box wouldn’t impact existing processes. For instance, say encryption software impacted processing times by 30 percent—is that going to blow out my other windows? Couple that with the extended timeline for compliance using conventional encryption, we just couldn’t run the risk.”

Company managers decided to move in a different direction, and find a solution flexible enough to work within the existing IT environment. Basically, they were looking for a kind of policy engine or service they could use to offload their encryption requirements. This was a tricky proposition, because the company used its data warehouse to support so many different operations and systems.

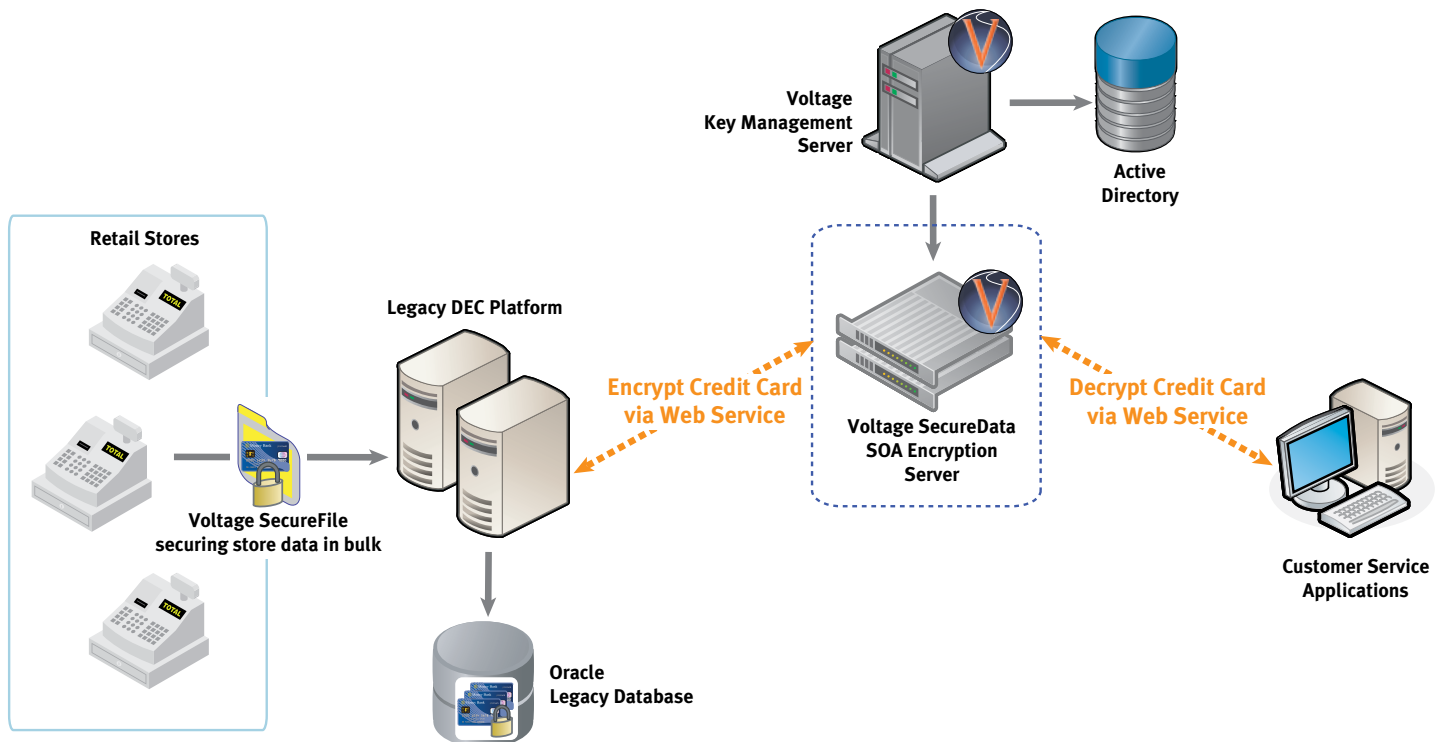
In fact, using native Oracle encryption wasn’t an option because—besides the data warehouse—the company maintained older legacy systems to support development, testing and disaster recovery operations. Since PCI requires segregation of duties, the native approach wouldn’t satisfy policy goals in such a diverse environment. Widening its search for encryption solutions beyond conventional technologies, the company hired a global consulting firm

and made contact with Voltage Security. With Voltage, the company discovered that it was possible to implement encryption as a service, and to apply it in other flexible ways.

A Flexible Solution

The company chose to implement a PCI-compliant encryption solution, based on **Voltage SecureData** and **Voltage SecureFile Command Line**. Unlike traditional database and network layer approaches mandating database re-architecture, **Voltage SecureData** uses Format-Preserving Encryption (FPE). FPE is an advanced encryption mode of AES that secures data while preserving its original format. With FPE, it is possible to integrate seamless data-level encryption into legacy business application frameworks, which were difficult or impossible to address—as was true of the company’s data warehouse and web-based customer service applications.

Unlike traditional encryption algorithms, which expand data into binary fields, FPE allows encrypted data to retain its original format. This means encrypted data “fits” in existing fields and removes the need for database schema changes. For example, a 16-digit credit card number can be encrypted with the output in the same 16-digit format, but with the strength of 256 bit AES. The credit card checksum



can still be maintained or leading digits can be preserved. FPE also allows indexed fields to be encrypted while keeping referential integrity. Through the use of FPE, Voltage SecureData provides highly efficient, robust data encryption, and data masking that—typically—can be executed with a fraction of the effort required by competing systems.

Voltage in Action

After a week of integration across five critical applications, the company used the **Voltage SecureData Command Line**—a scriptable tool for bulk encryption operations—to perform a one-time encryption of all cardholder data in its data warehouse. Additionally, the company installed the **Voltage SecureData SOA Encryption Server**. This is a centralized Web services encryption option for SOA environments. It was ideally suited to the organization’s legacy environment, since it could transparently encrypt updates to the data warehouse, which runs on the legacy TRU64 system. Plus, it could be used by the customer service applications.

When the web-based customer service application draws on cardholder data from the data warehouse, the **SOA Encryption Server** ensures that regulated content—like card numbers—is transparently decrypted and, based on user roles and permission policy, only the permitted last four digits are shown—the remaining fields are masked on the fly. This way, customer service representatives can access the information allowed by their jobs, but the first twelve characters of credit cards are not visible, ensuring that cardholder information is always protected. The **SecureData SOA Server** greatly reduces the scope of the PCI audit to one place where data is processed, so compliance costs are reduced to a minimum.

Voltage SecureData provides fully automated key management, with keys automatically and securely generated on demand. Its unique technology removes the need for key storage, escrow or archiving. This eliminates data loss problems, simplifies disaster recovery and business continuity, and integrates directly with existing Authentication and Identity Management infrastructure—in this case, Active Directory. This allowed complete control of existing roles, entitlement and authentication policies without change. Central policy management and auditing also assure minimal audit and compliance costs, with one point of management for authentication, reports and policy control. Voltage’s stateless key management also greatly

reduces the scope of audit for PCI compliance. For instance, PCI requires keys to be rolled annually; with Voltage key management, this key rollover is painless and automated. In this particular case, the keys are rolled every quarter to align with backup cycles. Now, when keys are rolled, past backups are virtually “shredded,” in accord with existing data shredding policy, and without any changes to backup processes—although now, all backups are encrypted.

Voltage SecureFile Command Line was also installed to protect bulk files containing cardholder data in transit and at rest prior to processing for complete PCI compliance. **Voltage SecureFile** provides seamless file encryption of bulk unstructured data, such as card data at rest when in file stores. The integrated key management provides a PCI-ready audit trail, in sync with the audit reports on database activity. This capability provides a complete 360-degree view of the audit trail over cardholder data protection.

“If we’re going to buy a solution, it needs to be an enterprise solution. If we’re going to do encryption on such a large scale, I don’t want a product that just encrypts on one application. And since **Voltage** makes key management so easy, we can do just that—implement encryption as a service anywhere we need it.”

IT Security Manager

When it comes to de-identifying credit card data used by developers in test and QA environments, **Voltage SecureData** made it very simple to meet the PCI requirements, and allow developers to work as before. Since data formats are preserved, including credit card checksums, developers can now use the encrypted data straight away—as masked data—and develop applications without any risk of data leakage.

“Implementation couldn’t have been easier,” the IT security manager said. “We used a local integration team, consisting of one project manager and one developer. **Voltage SecureData** uses all standard components, so installation was a snap—it took just an hour to set it up and configure it.”

Far-Reaching Results

The business implications of **Voltage SecureData** for this retail and logistics company were profound and far-reaching. Instead of a costly 18-month deployment, in less than two months, the business was able to implement **Voltage SecureData** and pass a PCI-compliance audit conducted by a qualified security assessor, a major Bank. The technical implementation itself was completed in three weeks.

Moreover, **Voltage SecureData** has numerous flexible deployment options, and the company took advantage of them in tackling compliance priorities in a complex IT environment.

Briefly, the Voltage solution removed the company's needs for expensive system re-engineering or re-architecting. Because the organization could keep using its existing systems, costs of the compliance efforts were significantly reduced. Furthermore, these costs will stay low due to the much-reduced scope of PCI audit. Besides this, the organization could expand this enterprise platform to meet encryption needs for additional new and existing legacy applications. In fact, with an enterprise encryption platform already in place, it will be much easier to meet new policy compliance challenges.

As the organization's IT security manager noted, "If we're going to buy a solution, it needs to be an enterprise solution. If we're going to do encryption on such a large scale, I don't want a product that just encrypts on one application. And since Voltage makes key management so easy, we can do just that—implement encryption as a service anywhere we need it."

Unlike a point solution which only addresses single policy challenges, a Voltage encryption platform supports the installation of additional services as needed. In the same way, through persistent encryption of information, the Voltage platform lets the company extend its business to external customers and partners, easily and safely.

Finally, but most importantly, Voltage allowed the company to have strong encryption for full PCI compliance—and without the high costs and long development lead times of older legacy approaches. Voltage was the difference in allowing the organization to meet the mandated PCI compliance timeline in two months—instead of accepting an unfeasible timeline of 18 months.