Voltage security

Heartland PAYMENT SYSTEMS

Heartland Payment Systems

When Business Imperatives Demanded Moving beyond Compliance, Heartland Created a Highly Secure, Cloud-scale Solution — with Voltage End-to-End Data Protection

Leadership and Resilience through Business Challenges

Since its founding in 1997, Heartland Payment Systems® has been providing debit/prepaid/credit card processing, gift marketing and loyalty programs, payroll, check management and related payments solutions. The company processes more than 11 million transactions a day and more than $80 billion in transactions a year, making it the fifth-largest payment processor in the United States and ninth in the world. From the beginning, its business model has been to employ leading-edge technology and economies of scale to save its customers money on every transaction.

Although assessed as in compliance with the Payment Card Industry Data Security Standard (PCI DSS) and employing multiple layers of security to protect cardholder data, Heartland still suffered a costly data breach in 2008. The episode prompted Heartland to conduct an internal and industry-wide assessment of payment card security with the goal of providing the most secure and trusted services for Merchants and consumers.

Like many card processors and large retail organizations, Heartland performs credit card processing according to industry best practices. When the breach took place, Heartland was using several specific products to encrypt “data-at-rest”. One of the lessons learned was that protection of a whole database or a zone within the processing environment still leaves points of vulnerability or “air gaps” for cyber criminals to exploit. If data leaves a database in clear text as it travels to a designated application, an attacker can harvest clear text card values. According to Verizon’s 2010 Data Breach Investigations Report, these types of attacks (e.g. SQL injection) are one of the three most frequent attack techniques used to achieve illegal access to enterprise data and compromise enterprise applications.

About the Company

- **Public company: in business since 1997**
- **#9 worldwide in payment processing; #5 in the United States**
- **Handles more than $80B in bank card payments annually**
- **Leader in micro payments business (e.g., vending machines, gas pumps, washers/dryers)**
- **OneCard™ program used at 150 universities**

Situation Summary

Heartland wanted to establish market leadership by providing a highly secure and scalable solution that would protect cardholder data from from card swipe to and through the Heartland network.

Solution Summary

Heartland quickly achieved PCI compliance and established industry leadership with end-to-end encryption for Merchants. Using the Voltage Security data protection platform, Heartland exceeded all its goals for enterprise data protection and protection of payments from card swipe to and through the Heartland network.

Heartland takes Action

Heartland conducted an extensive evaluation of available technologies, including end-to-end encryption technologies from several vendors, tokenization-only products, and traditional encryption, to determine the most effective approach to achieve end-to-end data protection.

Heartland's vision was to bring to market a true end-to-end data protection payments solution that protected data starting at the card swipe through to Heartland's back-end systems. Also, Heartland required support for on-going PCI DSS compliance. Voltage Security helped Heartland swiftly achieve this goal while enabling Heartland to provide end-to-end encryption across all its transaction processing systems.

Heartland and Voltage Security collaborated to develop a more comprehensive and secure end-to-end encryption solution. Named E3™ and powered by Voltage SecureData Payments, the solution is designed to safeguard cardholder data at-rest and in-transit throughout the lifecycle of payments transactions - from the moment of card swipe, to and through Heartland's network.

Stamp of Approval for Heartland's E3 Encryption

Bank Technology News | November, 2010 | By John Adams

Heartland Payment Systems' E3 point-to-point encryption system has passed muster with Coalfire System, an independent PCI assessor, which in an audit found E3 to both increase security while reducing PCI scope.

E3 is designed to safeguard cardholder data through the entire payment process—from swipe or key entry to Heartland's network, then handoff to card brands. E3 does this by leveraging Voltage Security's AES methodology, which preserves the card's 16-digit number through encryption—allowing seamless integration with a firm's processing system as well as simplified key management.

Coalfire found that E3 reduces the cope of PCI compliance by 79 percent for merchants using dial up connections, and 69 percent for those using an IP connection. These rates are due to the product's use of cryptographic algorithms and identity based encryption. Coalfire's assessment includes technical testing, architectural assessment, industry analysis, compliance validation and peer review.

Coalfire also determined that E3 meets all Visa Data Field Encryption guidelines as well as other industry standards. Coalfire president and COO Kennet Westby said that as a payment processor, Heartland has a unique advantage in that it can protect data through its own network. Other large processors, including Fifth Third, have also recently introduced point-to-point encryption.

Successfully Managing Reputation and Business Risk

Heartland acted quickly and decisively to reassure merchants and consumers the company was a trusted provider of payment card transaction processing. Like other large enterprises that have successfully managed potential damage to their brand and business operations, Heartland communicated clearly and openly about its plans to remediate both the technical and business issues that contributed to the data breach.

Heartland needed to quickly demonstrate PCI compliance to continue servicing Visa and MasterCard merchants. Visa cardholders (1.7 billion cards worldwide) and participating merchants (29 million merchant outlets worldwide) are ubiquitous, and retailers are obligated under the terms of their Visa agreements to use PCI-compliant service providers. As a publicly traded company, Heartland had to show tangible results in securing card data regardless of where that data traveled or was stored. In addition, Heartland's ambitious goals went well beyond remediation to deliver a new value-added service that would change the perception of the level of security merchants should expect from a service provider. As a leader in the payments industry, Heartland committed to establishing security as an integral part of its operation, not just an add-on option for merchants.

All of the above challenges had to be accomplished rapidly and convincingly in order for Heartland to implement its plans to rebuild its brand image and continue to accelerate growth for shareholders and leadership with merchants.

The Hard Cost of Data Breaches

"According to the Mercator Advisory Group, as hackers continue to breach payment networks, the average cost per data breach now exceeds $6.65 million per year."

Protect Cardholder Data from Card Swipe through the Heartland Network

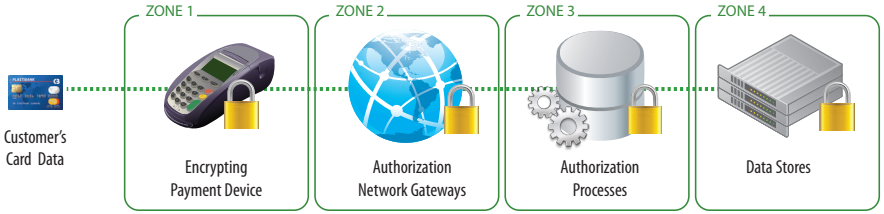
Industry standards and regulations such as PCI DSS do not guarantee security. They are a set of rules designed to serve as guidelines to help organizations protect sensitive information.

The PCI DSS contains 12 highly detailed requirements that address core principles for network architecture, cardholder data protection, vulnerability management, access controls, network security, and information security policies. The requirements include numerous details such as policies for the storage of card data, reports and receipts, physical access to data, and passwords.

Heartland wanted a security solution that would not leave any cardholder data in the clear at any point in the transaction flow. This was the best way to ensure the highest level of protection for merchants and meet PCI compliance objectives. The technical challenges to achieve protection from the card swipe through the processing network meant Heartland could not rely on technology that only addressed limited parts of the transaction flow.

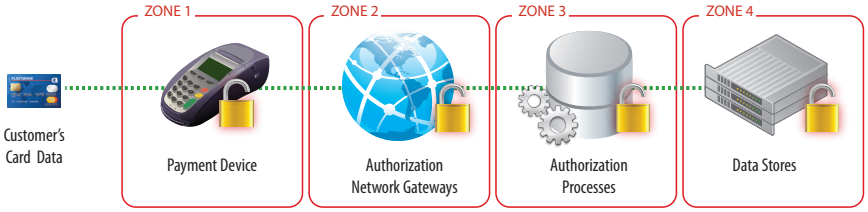
Encrypted data Unencrypted data

End-to-End Encryption



Data is protected by encryption while stored in every zone in addition to being encrypted in transit between zones.

Point-to-Point Encryption



Though data is encrypted in transit between zones, data stored in each zone is unencrypted and thus potentially vulnerable.

Moving beyond Compliance

Heartland's challenge was to improve on baseline requirements to prevent a costly data breach or any other type of penetration that would jeopardize its customers' businesses and its own business. It could not afford to wait for clarifications to standards. It took matters into its own hands and outlined an approach to dramatically increase the level of security available to merchants, consumers and business partners by adopting a two-pronged strategy:

1. **Use end-to-end encryption to secure the payments stream and internal systems and achieve compliance.**
2. **Move beyond compliance requirements to establish a more robust barrier against and deterrent to attacks on sensitive customer and corporate data.**

Heartland began by evaluating its business-critical systems, applications, and business processes to identify existing or potential vulnerabilities.

Key focus areas included:

- **Customer service applications from which cardholder data was emailed to merchants**
- **Dispute handling applications that shared PDF files of customer dispute data and transaction reversal information from stores**
- **Internal communications that included sharing of sensitive email for day-to-day business**
- **Internal file sharing between automated systems and desktops**
- **Other automated systems (e.g., systems in which files arriving as scans from fax machines were emailed to customer service representatives)**

An In-depth Evaluation

Because PCI DSS requires encryption of any cardholder data, Heartland had to identify all of the places and ways in which cardholder data resided and determine how to protect that data. This mandate applied to structured data and unstructured data such as email and files. Intent on protecting all sensitive data, Heartland looked beyond what was strictly considered cardholder data to include all personally identifiable information (PII) such as social security and tax ID numbers. Doing so served the dual purpose of going beyond PCI DSS requirements and providing a data security infrastructure that could be extended beyond payment processing to other Heartland applications.

To achieve true end-to-end encryption and ensure data protection from the card swipe through to its back-end systems, Heartland realized it would need to adopt a fundamentally new approach to data encryption and to deliver a new offering to its hundreds of thousands of merchant customers.

Based on its comprehensive review, Heartland determined it needed solutions that could reliably provide the following capabilities:

- **End-to-end encryption from card swipe to transactional payment systems**
- **Internal data protection for structured sensitive data found in internal databases at Heartland**
- **Protection of sensitive email between partners, customers, and internal employees, including mobile Blackberry users and roaming field staff**
- **Protection of sensitive data found in files (PDFs, Microsoft Office documents and faxes) in which scanned credit card information may be contained**

Heartland also concluded that to meet these criteria, it needed a technology partner with extensive industry experience in the payments space and a proven track record of success.

"Heartland's objective was simple: Protect cardholder data at all stages of a transaction — from card swipe through the Heartland network — and ensure that internal systems and processes were secure."

Voltage Security Solution Helps Put Heartland in the Lead

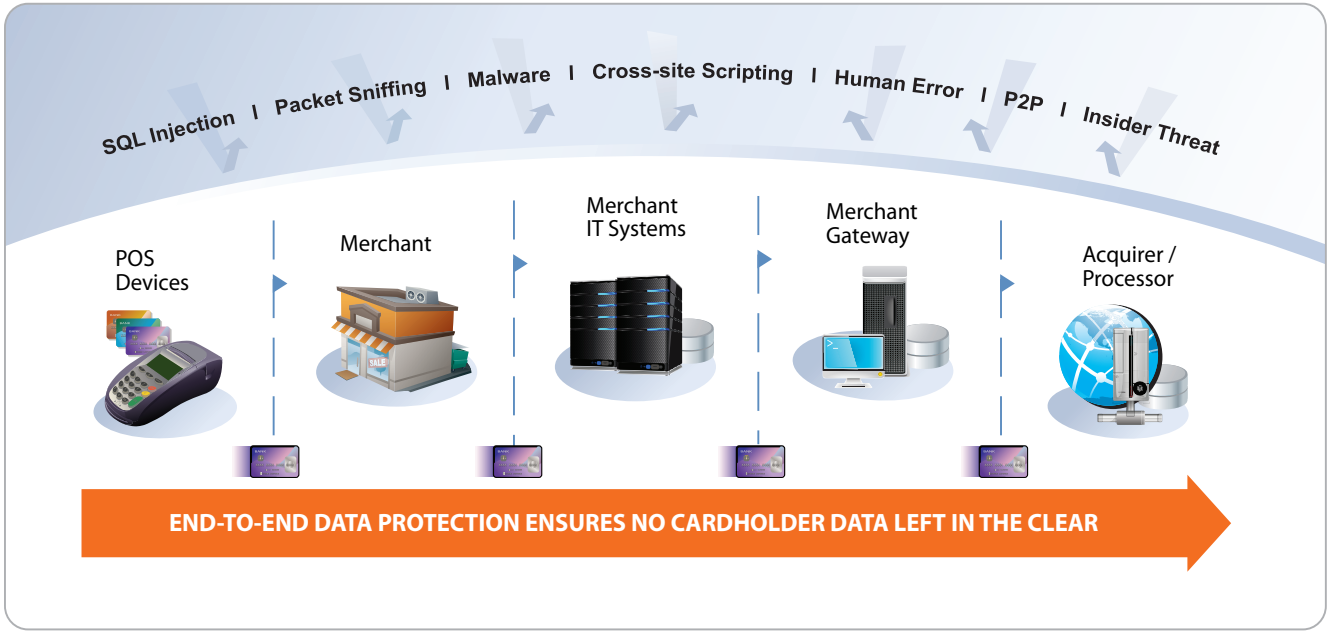
Warding Off Cyber-Crooks with End-to-End Encryption

While Heartland's objective was simple enough to state, the technology challenges it faced in achieving its objective were not quite as simple.

Recognizing that compliance with the PCI DSS—even with incremental improvements in the standard—would not adequately address its overall objectives, Heartland decided to take a different tack: end-to-end encryption.

"These guys are the 21st century bank robbers… they are calling themselves the 'dons' of the IT theft world," says Steve Elefant, Chief Information Officer at Heartland. "There is no such thing as secure software…and malware is so sophisticated that it is no longer possible to achieve security without strong encryption."

With that understanding, Heartland determined that the most efficient and effective way to develop and deploy its solution would be to partner with an expert in the use of end-to-end encryption for data protection.



Voltage Security Solution Benefits

The following list of capabilities shows Heartland's rationale for choosing Voltage Security and the benefits it achieved.

Proven Voltage Security solutions, including: Voltage SecureMail™, Voltage SecureData™, Voltage SecureFile™

Benefits:

- Achieved compliance and Visa certification within 60 days
- Encryption of email, structured data, and files meant that Heartland improved protection for both PCI and PII data
- Implementation of a complete data protection solution for all types of internal processes and business applications

True end-to-end protection vs. point protection through Voltage Security's innovative technology approach to encryption: Identity-Based Encryption™ (IBE), Format-Preserving Encryption™ (FPE)

Benefits:

- Eliminate key injection processes
- Support off-line devices from card swipe through the Heartland network
- Support multiple devices and systems to meet the maximum number of merchant use cases

Industrial-strength security based on the Advanced Encryption Standard (AES) and full HSM support

Benefits:

- Delivers higher standard than the card industry Triple Data Encryption Standard (TDES)

High-performance, small-footprint implementations for multiple devices with embedded point-of-sale (POS) software developer kit (SDK). FPE and IBE functions and IBKEEP protocol require less than 70K ROM, 30K RAM

Benefits:

- Portable to any embedded processor such as ARM CPUs common in POS/Pin Pad
- Transparent to transactions
- Support for hardware Advanced Encryption Standard (AES) accelerators or optional tamper-resistant security modules (TRSMs)

Heterogeneous support for acquirer/processor or merchant applications and systems

Benefits:

- Available on Linux, IBM z/OS , HP NonStop, Stratus, Solaris, Teradata and more
- Fast-tracked deployment in back-office payment infrastructure
- Support for hardware security modules (HSMs), which are essential in payments processing

Voltage Security's innovative end-to-end encryption ensures card data is never left in the clear

Benefits:

- By encrypting PANs, Heartland established leadership and raised the bar on best practices for data protection in the payments industry

E3 Brings End-to-End Encryption Standards to the Payments Industry

Working together, Heartland and Voltage Security team developed E3™, an end-to-end encryption solution that protects sensitive cardholder and payment account information from card swipe through the Heartland network. Using Voltage SecureData Payments and its core technology — Format-Preserving Encryption and Identity-Based Encryption — the solution was developed and implemented in 60 days (from a standing start to production-ready transactions).

Voltage SecureData Payments works by encoding cardholder data so it cannot be read by unauthorized users. This end-to-end encryption safeguards information from the moment a card is swiped at a point-of-sale (POS) system, and through the payment processor's network. This approach is particularly effective because by encoding the data across the complete flow of a transaction, it renders the data useless to anyone who might succeed in penetrating a network or system.

Heartland PAYMENT SYSTEMS™

End-to-End Encryption powered by Heartland Payment Systems

Princeton, N.J. – Heartland Payment Systems (NYSE: HPY), one of the nation's largest payments processors, has selected Voltage Security as a partner to develop end-to-end encryption (E3) software specifically suited to payments processing. Voltage is a global leader in information encryption.

"Heartland is developing a complete end-to-end encryption solution designed to protect cardholder data at all stages of a transaction – from card swipe through delivery to the card brands," said Bob Carr, Heartland's chairman and chief executive officer. "Together with Voltage, we are developing a comprehensive solution that currently does not exist."

Heartland's new E3 solution will significantly enhance the security of payment card information throughout the processing lifecycle. The Voltage SecureData™ product line, based on its Format-Preserving Encryption™ and Identity-Based Encryption™ approaches, will power the software component of Heartland's E3 solution. Heartland also employs Voltage SecureMail™ and Voltage SecureFile™ to protect personal information throughout its corporate and extended business network.

Heartland E3 - Industry Leading Payments Protection

E3 is rolling out to all of Heartland's merchant customers making security an integral part of the Heartland service and not an expensive option. This is a huge benefit to merchants of all sizes and underscores a key advantage to all participants in the payment processing chain. The solution delivers card data protection from the card swipe through the Heartland payment network, helping merchants reduce the costs of PCI compliance.

"Tier I merchants need to protect cardholder data, achieve compliance and reduce scope. There are huge risks if compliance is the sole focus. We are talking about reducing scope by systems never seeing card data and never having access to keys," says Steve Elefant.

Get more detailed information at:

http://www.e3secure.com
http://www.voltage.com/end-to-end/index.htm

> *"Only end-to-end encryption delivers a sufficiently robust approach to security. It does this by treating the payments system as a chain of potential vulnerabilities that must be addressed as a whole. E3, powered by Voltage SecureData Payments, provides a single solution for systemically protecting cardholder data as well as assisting merchants and POS application providers with PCI DSS compliance."*
>
> — **Mark Bower, VP Products, Voltage Security**

Covering All Types of Sensitive Data: Voltage Security for the Enterprise

In parallel with E3 development, and with remote configuration and installation help from Voltage, Heartland was able to quickly encrypt the multiple business processes and applications where sensitive data might be exposed. By incorporating the full suite of Voltage Solutions—Voltage SecureMail, Voltage SecureFile, and Voltage SecureData Enterprise—Heartland locked down credit card data and PII data in its enterprise.

	Commercial Business Service	Credit Card Reconciliation	New Merchant Recruitment
Product	**Voltage SecureData**	**Voltage SecureMail**	**Voltage SecureFile**
Description	Business services supporting thousands of customers	High-traffic email system for credit card reconciliation	PII data encryption to enable agents to sign new merchants without storing information on their laptop
Benefit	Protect PII data such as social security numbers and tax ID numbers	Meet PCI requirements more efficiently and more transparently	Protect PII data such as social security numbers and tax ID numbers
Details		Integrated with data loss prevention (DLP) content scanner to avoid slowing down system and Symantec eVault system for electronic discovery	Information filled out in forms, faxed, converted to PDF, and stored on shared drive; files encrypted en-route and at rest

PCI Compliance in 60 days; End-to-End Encryption to Merchants in 60 days

Enterprise Data Protection

January '09	February '09	March '09	April '09	May '09
Heartland approves remediation plan initiates breach action plan	Solution evaluation begins with the following vendors: ▪ **SafeNet** ▪ **nuBridges** ▪ **Protegrity** ▪ **RSA** ▪ **Semtek/VeriFone** ▪ **Vormetric** ▪ **Voltage Security** Voltage enters Proof of Concept with Voltage SecureData, Voltage SecureMail, and Voltage SecureFile.	Heartland selects Voltage Security, development and implementation begins.	Heartland completes enterprise implementation of Voltage SecureData Enterprise, Voltage SecureMail and Voltage SecureFile. Heartland achieves PCI certification on April 30.	Visa certifies Heartland on May 4th.

PCI DSS Compliance in 60 Days

End-to-End Encryption

February '09	March '09	April '09	May '09	June '09
Heartland details ambitious plan to offer the industry's first end-to-end encryption as a standard feature for all Heartland merchants.	Voltage SecureData POS SDK integrated into Heartland terminals.	Voltage SecureData Payments is selected for the Heartland end-to-end encryption initiative named E3.	Voltage SecueData Payments Host SDK deployed in Heartland IT environment. Successful pilot of E3 terminals with Voltage SecureData Payment and all major card brands. E3 availability announced on May 24th.	Voltage SecureData Payments enables E3 - the industry's first end-to-end encryption on a POS solution. Heartland establishes industry leadership - "We will pay any fines if you have a breach when using our new E3 terminals."

End-to-End Encryption in 60 Days

Heartland Achieved Goal... and More!

Heartland acted rapidly and with leadership to protect its merchants, consumers, shareholders, reputation, and long-term survival and growth. The company has established a roadmap for security for others in the payments industry to follow.

The results of its actions in the aftermath of the data breach have exceeded the company's expectations:

The Voltage Advantage

- **Heartland is on Visa's list of PCI DSS validated service providers.**
- **Heartland's reputation has been enhanced, as evidenced by its inclusion in the 2010 InformationWeek 500 as one of the nation's most innovative companies and most creative and effective users of information technology.**
- **Heartland's E3 end-to-end encryption solution, powered by Voltage SecureData Payments, has raised the bar for what constitutes comprehensive and robust data protection in the payment card industry. To date, Heartland's E3 has been enthusiastically received by its merchants and business partners as they look to secure their businesses.**
- **Voltage Security solutions not only protect sensitive cardholder information, but also save merchants money by enabling them to reduce audit costs by removing data from regulatory scope.**
- **Voltage Security solutions are emerging as the model for the next generation of payment card security standards.**

> *"We believe the marketplace will accept this higher level of payments security, and we are willing to share our knowledge and lessons learned with all industry stakeholders via the Payment Processors Information Sharing Council, FS-ISAC, and Secure POS Vendor Alliance organizations."*
>
> — Bob Carr, Chairman and CEO, Heartland Payment Systems

About Voltage Security

Voltage Security, Inc., an enterprise security company, is an encryption innovator and global leader in enterprise data protection for data residing both inside and outside the cloud. Voltage solutions provide cloud-scale encryption and simplified key management for protecting sensitive information wherever it is stored and processed, on-premise or in private and public clouds. Voltage solutions are in use at almost 1,000 enterprise customers, including some of the world's leading brand-name companies in payments, banking, retail, insurance, energy, healthcare and government.

Voltage solutions reduce the risks associated with theft of sensitive and private information, support privacy guidelines including PCI DSS, HITECH, U.S. Data Breach Disclosure laws and European Data Privacy directives, and uniquely provide security of data coupled with unmatched usability which results in significantly lowered total cost of ownership.

Harnessing award-winning cryptography and key management, including Voltage Identity-Based Encryption (IBE) and a breakthrough innovation in data usability, Format-Preserving Encryption (FPE), Voltage solutions have changed how enterprises protect their most valuable asset, their customer data. Offerings include Voltage SecureMail, Voltage SecureData, Voltage SecureFile and Voltage Cloud Services which provides cloud scale encryption and key management for businesses, partners and their customers. The Company has been issued several patents based upon breakthrough research in mathematics and cryptographic systems. To learn more about Voltage customers please visit **voltage.com/customers.**

For more information please visit:
http://www.voltage.com

Voltage
security

To learn more about Voltage Security and the Voltage Family of products, please visit:
http://www.voltage.com

Or contact us at:
http://www.voltage.com/contact/index.htm

For more detailed information on Voltage SecureData, please see our online information resources:
http://www.voltage.com/products/data_protection.htm