Hewlett Packard
Enterprise

Business white paper

Achieving PCI DSS 3.0 Compliance with HPE SecureData

Table of contents

Introduction

The Payment Card Industry Security Standards Council (PCI SSC) released an updated version of its Data Security Standard (version 3.0) in November of 2013, which became fully effective on January 1, 2015. Currently, only PCI DSS 3.0 assessments will be accepted. Utilizing HPE SecureData technologies can help your organization meet PCI DSS compliance in an effective and cost-efficient manner. If you have any concerns about how the new PCI DSS 3.0 standard may impact your organization, please contact your trusted security partner at HPE Security—Data Security.

HPE SecureData data-centric protection helps enterprises:
- Reduce the risk of data theft in the event of a breach
- Dramatically reduce PCI DSS burden and audit scope and fast-track compliance at least cost
- Achieve compliance and security with minimal disruption to existing IT and business systems and processes
- Enable best practices in end-to-end data protection across payment terminals, POS systems, merchant IT and host processing systems

Overview

The Payment Card Industry (PCI) Data Security Standard (DSS)[1] 3.0 dictates that organizations processing and storing credit card data, including magnetic stripe data, EMV data and Card Not- Present data, must comply with a set of well-defined audit requirements in twelve areas of cardholder data management and privacy.

Compliance with PCI DSS requirements can be expensive, challenging, time-consuming, and disruptive, as cardholder data is often stored, transmitted, and used in many different applications within an organization, sometimes even beyond the organization's IT firewalls. At the same time, being compliant is not enough to prevent data breaches—as many compliant organizations have suffered public breaches. The industry now recognizes that a data-centric approach to security solves both challenges effectively, and also achieves the objective of PCI DSS scope reduction.

By taking a data-centric security approach, the data itself is protected so that it can move between applications and devices without changes to existing processes and user experience. HPE SecureData's unique technologies enable such an approach to be adopted consistently across all PCI affected processes with the least impact and cost. Traditional or homegrown solutions with high key management overhead for encryption, difficult integration, or complex tokenization architectures in leading acquirers, card issuers, banks, and thousands of merchants have been replaced with the HPE SecureData. The results are dramatic: these companies are minimizing the cost and disruption of compliance in some cases by up to 95 percent, and enhancing their overall ability to comply with PCI DSS guidelines.

This document provides an overview of how HPE Security—Data Security, a leading data-centric security vendor today, can help consumer-transacting businesses in retail, financial services, transportation, payment card processing, and other industries to achieve PCI DSS compliance and reduce scope quickly, easily, and painlessly.

HPE SecureData Technologies

PCI DSS compliance is not a one-time effort. It is a continuous process with regular assessments that cover people, systems, and processes. Therefore, any solution for compliance must minimize the impact of managing data privacy and system integrity over time and across business domains and boundaries.

Patented technology innovations by HPE Security—Data Security, such as HPE Format-Preserving Encryption (FPE), HPE Identity-Based Encryption (IBE), HPE Page-Integrated Encryption (PIE), and HPE Secure Stateless Tokenization (SST), deployed within the HPE SecureData solution suite, enable companies to achieve PCI DSS compliance easily, quickly, and cost-effectively—while greatly reducing the scope of future PCI DSS audits. By providing end-to-end data-centric protection, HPE Security—Data Security helps mitigate the risks of data breaches across the entire data life cycle, wherever the data resides, is used, or moves.

[1] The PCI Security Standards Council, comprised of major credit card brands and strategic members, released version 3.0 in November of 2013, with new requirements phased in to 2015 to allow migration from the prior standard. HPE Security—Data Security is a member of the PCI Security Standards Council (**pcisecuritystandards.org**)

HPE Format-Preserving Encryption

The advent of PCI DSS has driven many organizations to look at methods for encrypting credit card numbers and other types of structured data in payment processes, including capture of card data in point-of-sale systems (POS), databases, applications, and acquirer processing environments. While this may seem like a straightforward application of traditional encryption algorithms, the resulting encrypted data typically has a different format from the plain text data, which necessitates changes to database schemas and re-architecting of business applications so that they can accept the new encrypted data format.

HPE Security—Data Security's patented HPE Format-Preserving Encryption (FPE) takes advantage of the U.S. government standard AES encryption algorithm in an advanced mode called "FFX-mode AES" and allows organizations to encrypt data fields, including credit card numbers, government tax ID numbers, and names and addresses, so that the encrypted versions retain the format and integrity of the original data. Maintaining the original format avoids the need to change database schema, screens, and processing systems dependent on a given data format—such as POS processing systems, merchant store systems, loyalty schemes and payment processing engines. HPE FPE is a technique that has been independently verified with formal security proofs[2] and is recognized by NIST under the auspices of the AES modes process[3], and HPE FPE is NIST-standard FF1 AES Encryption.

HPE Identity-Based Encryption

HPE Identity-Based Encryption (IBE) is a breakthrough public key technique that enables keys and data to be securely exchanged, for example from payment terminals to processing hosts, without the burden of traditional PKI and certificates, while retaining the benefits of public key cryptography. HPE IBE can use any arbitrary string as a public key, enabling simplified key management, dynamic key rotation, and enables the elimination of key injection for Point-to-Point Encryption (P2PE) implementations, reducing cost and complexity.

When combined with HPE FPE, HPE IBE permits sensitive cardholder data to be securely encrypted in online or offline environments, allowing only the back-end host or processor to access the real data. All intermediate systems are unable to decrypt or access decryption keys, resulting in a dramatic PCI DSS scope reduction by as much as up to 80 percent as validated by leading QSA's. This stateless key management approach also enables retailers and other organizations to reduce PCI DSS scope and avoid live data in POS environments which are vulnerable to malware and memory scraping trojans. The combination of HPE FPE and HPE IBE enables protection at "point of card read" all the way to the payment host in either the payment processor or the merchant's hosting partner without changing payment streams and payment protocols.

> "The constantly mutating threat landscape requires new defensive measures, one of which is the pervasive use of data encryption technologies. In the future, you will encrypt data both in motion and at rest by default. This data-centric approach to security is a much more effective way to keep up with determined cybercriminals. By encrypting, and thereby devaluing, your sensitive data, you can make cybercriminals bypass your networks and look for less protected targets."
>
> - Killing Data, March 2012 Forrester Research Inc.

[2] "Format-Preserving Encryption", Mihir Bellare and Thomas Ristenpart and Phillip Rogaway and Till Stegers **eprint.iacr.org/2009/251**

[3] **csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf**

Customers including Heartland Payment Systems, Columbia Sportswear, Elavon, and ClickandBuy use HPE Security—Data Security data-centric approach to increase security of their sensitive data and achieve PCI DSS compliance. In many cases, PCI DSS scope is reduced by up to 80 percent with HPE FPE enabling point-to-point encryption from card reader to acquirer. Enterprise PCI DSS assessments are reduced from 6 months with 3 assessors to 3 weeks and 1 assessor.

HPE IBE is standardized in IEEE 1363.3 "IEEE Standard for Identity-Based Cryptographic Techniques Using Pairings", and in IETF 5091, 5408 and 5409. The method of HPE IBE Pairings is also defined in ISO Standard 15946-1 "Information Technology—Security Techniques—Cryptographic Techniques Based on Elliptic Curves—Part 1: General."

HPE Page-Integrated Encryption

HPE Security—Data Security patent-pending HPE Page-Integrated Encryption (PIE) technology allows merchants, payment processors and enterprises to encrypt sensitive data in the browser before it is seen by upstream web servers or load balancers. Employing a unique, use-once key, encrypted data can only be decrypted at the payment processor. HPE PIE assigns each user transaction (i.e., each browser page load) a unique key that is derived using a FIPS-based random number generator. At point of capture, the data is encrypted with a key used only for that single transaction, and the key is not available to any intermediate system before the data arrives at the payment processor.

HPE PIE uses HPE FPE to encrypt data without changing the format or length, thereby enabling quick deployment with minimal changes to existing applications, databases and other systems. Because encryption is selective, meaning some portions of the data can remain in the clear if required, HPE FPE preserves existing processes, such as bank identification number (BIN) routing or verification of the last four digits of the card. HPE PIE technology is ideal for reducing risk for e-commerce payment transactions while giving the merchant full control over the customer checkout process. HPE PIE eliminates the need for redirects while also protecting sensitive Card-Not-Present data.

HPE Secure Stateless Tokenization

Tokenization replaces data values with a "token", or a random equivalent in its place. Tokenization has a special advantage for credit card numbers: the PCI Tokenization guidelines note that systems that only hold tokens can benefit from scope reduction, thus greatly reducing audit costs. HPE SST technology is an advanced, patent-pending data security solution that provides enterprises, merchants and payment processors with a new approach to help assure protection for payment card and sensitive corporate data. The HPE SST technology is "stateless" because it eliminates the token database and removes the storage of card data from the solution. This dramatically improves speed, scalability, security and manageability over conventional tokenization solutions. HPE SST technology is available natively on secure processing platforms including IBM z/OS, HPE NonStop, and from the virtualized HPE SecureData Appliance.

HPE SST includes Token Multiplexing, a unique innovation that permits multiple, unique tokens to be mapped to one primary account number without the need for additional databases or mapping tables for each merchant. For example, an acquirer may service many merchants but want to ensure that tokens from one merchant cannot be inadvertently used in another merchant's system in the event that tokens are stolen. A merchant may want two outsourcers to have different token sets for loyalty analytics but which uniquely map to the same customer card at the merchant or acquirer. Token multiplexing enables this easily, without the increasing costs of unique databases as required by traditional tokenization systems, and avoids the problem where tokens may be considered financial instruments, and thus come under PCI DSS scrutiny.

HPE SST is ideally suited to reducing PCI DSS audit scope, both for the merchants and acquirers. It can also be applied to use cases outside of PCI DSS requirements and combined with HPE FPE for increased ROI from a deployment perspective.

HPE SecureData and PCI DSS Compliance

All products within the HPE SecureData solution suite are based on one or more of the company's patented technologies listed above. With the goal of providing end-to-end data protection for a variety of deployment environments, HPE Security—Data Security products help organizations ensure compliance with and reduction of overall PCI DSS scope. The following sections describe how each product in the HPE SecureData solution suite fits into a comprehensive PCI DSS compliance strategy.

HPE SecureData Enterprise

HPE SecureData Enterprise delivers data-centric encryption, tokenization, data masking and key management to protect structured and unstructured data without the cost and complexity of traditional solutions. Files and bulk data batch files and image scans containing cardholder data can be easily encrypted and shared between business processes.

Both encryption and tokenization are available within the HPE SecureData Enterprise platform. The platform strictly controls what functions applications are permitted to perform through central policy that is enforced independent of the application—some applications may only be able to tokenize, others can partially de-tokenize, and trusted applications can completely de-tokenize. Because the data format is unaltered, only "trusted" applications need a minimal change, typically with only one or two lines of code. Most components can just use the encrypted or tokenized value "as is" without change.

By taking advantage of identity infrastructure such as LDAP, AD, and identity management systems, HPE SecureData Enterprise enables role-based access to data—the whole data field or partial field such as the last four digits of a credit card number. Only the systems and users with the business "need-to-know" requirement and appropriate permissions can access the full data. For example, customer service representatives using merchant or payment processor applications might see only the last four digits of an account or credit card number, whereas fraud investigators or other applications (such as a payments gateway for credit card processing) might need the full field. Limiting accessibility to the original data by making only the essential partial fields visible effectively reduces the PCI DSS scope of the organization.

HPE SecureData Enterprise dramatically reduces the cost and complexity of issuing and managing keys because keys are generated on-demand as needed, reducing risk, complexity, and management costs. Combining stateless simplified key management and full audit capabilities with consistent policy-controlled data protection, merchants and enterprises can easily add encryption and tokenization to existing applications without the operational and management headaches prevalent among traditional solutions.

HPE SecureData Enterprise supports native data-centric security across IBM z/OS, HPE NonStop, Stratus VOS, AWS, Azure, Windows, Unix and Linux open systems, Teradata, Hadoop, and any platform supporting SOAP API's. It is in use for PCI DSS compliance and scope reduction in Fortune 50 banks, top US acquirers, credit card processors, and Level 1, 2, 3 and 4 merchants. HPE SecureData can be implemented at the network edge, internally, or by a hosting provider.

HPE SecureData Web

Breaches involving payment data are the most common manner of data theft, with online transactions offering attractive targets for hackers. Between the web browser where a user enters a credit card number to the payment processor, existing security gaps between systems present opportunities for hackers. In desktop and mobile web browsers, the card number can be protected while in transit between systems using Secure Socket Layer (SSL) encryption, but the number is “in the clear” when stored in application servers, back-office systems, and databases. Database encryption can help protect data at rest, but it is still exposed as it enters and leaves each system, providing tantalizing targets for hackers, increasing compliance scope, and increasing risk of non-compliance.

To secure payment data in online transactions, HPE SecureData Web, built on HPE PIE technology, encrypts payment information at the browser and keeps it protected until it reaches the payment processor. By shielding the data from theft in all the merchant and intermediary systems, HPE SecureData Web helps merchants and payment processors tighten their defenses while also protecting their brand and reputation.

HPE SecureData Payments

Web browsers are not the only place where users enter credit card numbers for purchases, and brick and mortar businesses are not the only locations with credit-card terminal systems. Today, everything from handheld credit-card terminals to downloadable apps for your smartphone along with a small physical reader device attached—can initiate the payment process.

However, in most payment systems, credit card data is left unprotected during the authorization and settlement processes. At the backend of the payment stream, cardholder data is also commonly left in the clear during routine business processes, such as loyalty programs, chargebacks or recurring payments. In order to comply with PCI DSS requirements, merchants, processors, and acquirers must take steps to protect this credit card data at rest and in transit within their environments.

HPE SecureData Payments protects cardholder data at all points in the end-to-end payment stream, from point of card terminal through to the processor. A complete payments transaction security platform, HPE SecureData Payments is built on HPE Security—Data Security patented HPE FPE and HPE IBE technologies, providing a solution that uniquely addresses the complexity of high-transaction retail environments. Payment processors, such as Elavon and Heartland Payment Systems, and payment device manufacturers, such as Ingenico and Equinox Payments, have implemented HPE SecureData Payments in their infrastructure to provide enhanced security in merchant payment transactions. These partners can deploy a proven, end-to-end encryption solution that protects cardholder data at all stages of a transaction—from card terminal through delivery to the acquirers’ processing environment via existing payment networks.

For example, Heartland Payment Systems has implemented HPE SecureData Payments in response to the impact of advanced threats, becoming the world’s first end-to-end payment data protection based on HPE Security—Data Security solutions and technology in 2009, recognized as having “the greatest potential of any new product to impact the security of America’s financial system” and winning “kudos for reacting expeditiously to both save the company and set a standard for the rest of the industry to follow”[4]. By encrypting the data at the point of origination, Heartland Payment Systems protects customer data from the merchant’s card readers all the way to the payment processor and every point in between. Whether in transit or at rest, HPE SecureData Payments ensures that cardholder information is always encrypted and protected, reducing PCI DSS scope by up to 80 percent, as assessed by a leading QSA.

[4] Ref.: **americanbanker.com/btn/22_9/1-heartland-payment-systems-1001434-1.html**

A global outdoor apparel, footwear, accessories, and equipment maker, Columbia Sportswear, uses HPE SecureData Payments to ensure the highest level of service and security for its customers and to reduce PCI DSS scope. Together with MerchantLink and Equinox Payments, HPE Security—Data Security created a comprehensive payment solution for Columbia that protects cardholder data in flight and at rest, thus reducing scope and breach risk without impacting the customer checkout process or performance.

HPE SecureMail

PCI DSS Requirement 4 requires encryption of cardholder data when transmitted over open public networks. HPE SecureMail is an ideal solution to encrypt email when it is used to communicate cardholder data for processes, such as merchant disputes and chargebacks.

HPE SecureMail allows the sender to seamlessly secure emails and attachments as part of the workflow that is already familiar, and only decrypt the communication after authenticating the identity of the intended recipient. Compliance with PCI DSS Requirement 4 can therefore be achieved easily, without impeding user productivity.

HPE SecureMail is used by the largest credit card issuers, merchants, and banks around the world.

HPE SecureFile

HPE SecureFile protects files and documents, regardless of where they go or how they get there. Unlike information security offerings that use complex keys or can only protect certain file types, transport mechanisms or storage locations, HPE SecureFile encrypts the data within the file itself. HPE SecureFile persistently protects all file types, enabling secure payment data exchange workflows such as merchant disputes and chargebacks between groups without the risk of data loss or policy violations. Powered by HPE IBE, HPE SecureFile encrypts to individuals and groups without the need to exchange certificates or memorize passwords.

The Twelve PCI Requirements and HPE SecureData

The fundamental principles of PCI DSS compliance are based on twelve tenets representing established best practices in handling sensitive data. Compliance programs and enterprise policies developed to address PCI can also be extended to embrace wider enterprise encryption requirements as a framework for encryption best practices beyond PCI. HPE SecureData solutions apply to many of the twelve tenets and can also reduce compliance scope in addition to protecting cardholder data. The following section provides a high level summary of how HPE Security—Data Security products, including HPE SecureData and HPE SecureMail, can address PCI DSS compliance requirements.

PCI DSS TENET	PCI DSS REQUIREMENT	HPE SecureData
Build and Maintain a Secure Network	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data	These requirements focus on the management, maintenance, and configuration of traditional network perimeter and segmentation firewall systems. These sections are not strictly applicable to HPE SecureData, although
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	HPE SecureData does not introduce any additional network complexity and uses standard ports and communications protocols for network communications (SSL), so network and firewall changes are minimized during HPE SecureData implementation.
Protect Cardholder Data	**Requirement 3:** Protect stored cardholder data	HPE SecureData meets and exceeds all requirements of Section 3. 1. Data is persistently encrypted or tokenized from the point of capture (POS, Web form, data warehouse load, etc.) to the point of consumption by applications (lookup, payment, reversal, investigation, discovery, etc.). This meets PCI DSS and PCI Point-to-Point Encryption (P2PE) requirements, including from POS to processor. 2. HPE Format-Preserving Encryption, or AES FFX-mode, encrypts data without changing field formats or schemas, minimizing change and thus implementation costs. Any intermediate system that transmits or processes credit card PAN data does not need to change—the encrypted data retains the full format of a valid credit card field, strongly encrypted per PCI DSS requirements. 3. Tokenization provides a method by which to replace live PAN or other data with a disassociated and randomly generated alias, with the reverse (de-tokenize) process performed by strictly controlled APIs via an independent and unrelated secure token mapping database. This removes applications from scope that do not need live card data. 4. HPE FPE is a published, proven, independently reviewed method of using AES in a mode that retains field format without sacrificing strength or security. HPE FPE was developed through ten years of cryptographic research and public scrutiny, and is NIST recognized, and HPE FPE is NIST-standard FF1 AES Encryption. 5. HPE Identity-Based Encryption (IBE) and HPE FPE can be combined for one-way data capture at the POS “swipe”—preventing access to cardholder data and eliminating the ability to decrypt data outside the back-end acquirer or card processor. This removes payment stream and merchant back-end systems from scope. 6. HPE SecureData APIs also provide traditional strong AES encryption, SHA hashing, and random number generator per NIST and FIPS standards. The HPE SecureData cryptographic toolkit has been FIPS validated on Windows, Linux and z/OS. 7. HPE SecureData also creates test (synthetic) data that cannot be reversed to eliminate live cardholder information from test and QA systems while still permitting full testing on valid format data that is realistic and preserves the important integrity characteristics of the source data without exposing the real data. 8. HPE Key Management is stateless and transparent, including automation of key rollover tailored to any business and operational requirements. Full separation of duties (data and keys) and PCI compliance reporting are standard with HPE SecureData. Hardware Security Module (HSM) support is provided as standard for optional FIPS 140-3 rated hardware key protection for root keys. 9. HPE SecureData’s service-oriented design also aligns to network segmentation best practices, ensuring minimum audit costs and simplification of PCI compliance by abstracting the applications away from keys and live data through strictly policy controlled API. 10. HPE SecureData is agnostic of underlying databases and application infrastructure, with a choice of integration options based on performance, architecture, and distribution requirements of components and legacy systems. 11. HPE SecureData provides a robust, highly scalable, and easy to manage redundant infrastructure without complex networking.

PCI DSS TENET	PCI DSS REQUIREMENT	HPE SecureData
	Requirement 4: Encrypt transmission of cardholder data across open, public networks	HPE SecureData meets and exceeds all requirements with its unique data-centric protection approach. By encrypting at the moment of capture, data remains encrypted at all times, removing the need for additional data-in-motion solutions, and reducing costs. In addition, for bulk unstructured data such as Card Data Warehouse load arrays arriving from partners, bulk retail store data, and payroll information, the same unified key management architecture for HPE SecureData manages keys for bulk unstructured data using HPE SecureFile. This provides a complete solution under a single, enterprise encryption framework, including a single point for policy enforcement, auditing and reporting, management, and monitoring. HPE SecureMail can easily and quickly accommodate PCI compliance for transmission of cardholder data over end user messaging systems over open networks.
Maintain a Vulnerability Management Program	**Requirement 5:** Use and regularly update anti-virus software	This requirement does not apply to HPE SecureData, though meeting this requirement is not inhibited and HPE SecureMail and other solutions for protecting data exiting an organization over SMTP (in scope of PCI if email contains even a single credit card number), are unique in their ability to work with DLP, AV, and content inspection tools for electronic supervision.
	Requirement 6: Develop and maintain secure systems and applications	HPE SecureData is engineered by security experts with Secure Software Development Life Cycle methods. The core technologies are independently validated by well-known cryptographers, and the products are developed with secure coding best practices, automated security testing and scanning by leading scanning tools. If required, the customer's own cryptography specialists may review HPE Security—Data Security advanced cryptographic designs.
Implement Strong Access Control Measures	**Requirement 7:** Restrict access to cardholder data by business need-to-know	HPE SecureData meets and exceeds this requirement. HPE SecureData inherently addresses separation of duties. Data remains persistently encrypted or tokenized at all times stored in the production database, as it travels, and stored in logs and files until the data is needed by authorized applications or staff. HPE SecureData takes advantage of existing identity and access management systems to provide role-based access to data while key management is fully separated from the data, enforcing separation of duties at all times as the data, the key management, the tokenization interfaces, and the authorization and entitlement systems permitting access to data are completely independent.
	Requirement 8: Assign a unique ID to each person with computer access	HPE SecureData indirectly assists in meeting this requirement, since access to data can be driven optionally by existing identity and access management infrastructure used to manage unique IDs. HPE SecureData provides role-based access to the data itself, allowing existing investment in RBAC models and technology solutions to be re-used immediately.
	Requirement 9: Restrict physical access to cardholder data	This requirement is not applicable to HPE SecureData, although HPE Security—Data Security recommends best practices for data center access, such as vetting, dual physical controls, and physical access controls that have separation of duties themselves, in locations where HPE SecureData systems are deployed.

PCI DSS TENET	PCI DSS REQUIREMENT	HPE SecureData
Regularly Monitor and Test Networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data	HPE SecureData provides complete audit records in a PCI DSS-ready format for rapid audit and investigation compliance. When cardholder data is persistently encrypted or tokenized, access to data is only permitted by policy-based access, which simplifies meeting this requirement.
	Requirement 11: Regularly test security systems and processes	This requirement is not specifically applicable to HPE SecureData, however, the HPE SecureData infrastructure is easily tested at any time for correct operation, backup, restore, failover, and other business continuity functions, per this requirement.
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security	Use of HPE SecureData for comprehensive data protection of cardholder data allows written policies to be enforced at the data level. This data-centric approach to PCI compliance brings security policy-based control and, more importantly, allows the organization to easily prove compliance to auditors through compliance attestation reports on a direct basis.

Conclusion

PCI DSS compliance can be a complex, time-consuming, and disruptive process and can introduce ongoing costs to the business with invasive audits and continuous compliance assessments. End-to-end data protection—using HPE SecureData's data-centric approach—significantly reduces the complexity and costs associated with meeting and maintaining PCI DSS compliance. With a full suite of data-centric encryption solutions, which protects data so it can move between applications and devices without changes to existing process or disrupting the user experience, HPE SecureData dramatically simplifies the complexity and reduces the costs of PCI DSS compliance for companies in virtually any business sector. The following table summarizes how HPE Security—Data Security products add compliance value.

	HPE SecureData Enterprise	HPE SecureData Payments	HPE SecureData Web	HPE SecureFile	HPE SecureMail
Meet PCI DSS requirements	√	√	√	√	√
Reduce PCI DSS scope	√	√			
Secure sensitive data enterprise-wide	√			√	√
Secure merchant POS transactions		√			
Secure e-merchants web-based transactions			√		

About HPE Security—Data Security

HPE Security—Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise we protect the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use and in motion. Our solutions provide advanced encryption, tokenization and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission critical transactions, storage and big data platforms. HPE Security—Data Security solves one of the industry's biggest challenges: how to simplify the protection of sensitive data in even the most complex use cases.

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise