**Hewlett Packard
Enterprise**

HPE SecureData and HPE Atalla HSM Integration

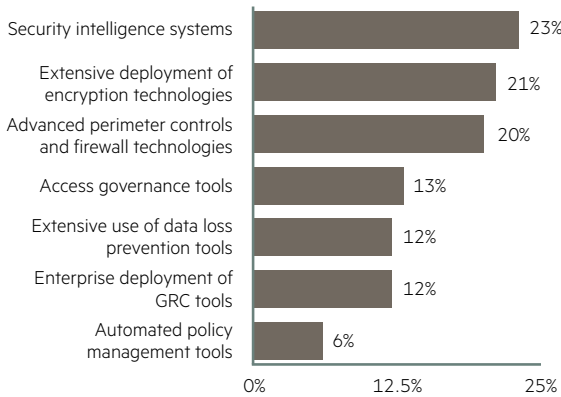HPE SecureData and HPE Atalla HSM streamline data protection and reduce management complexity
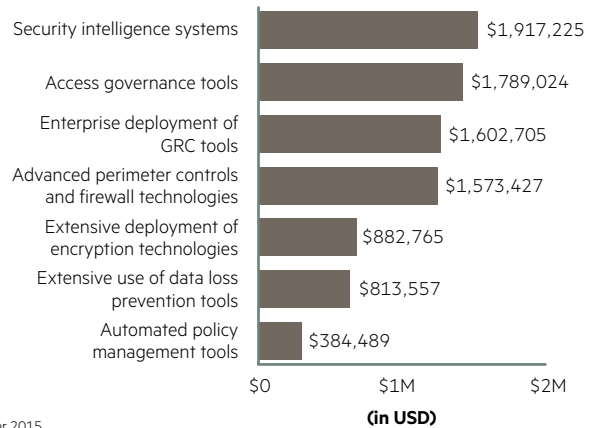
Challenge

The volume of data, the sophistication of abundant computing, and the borderless flow of data are outpacing the ability to understand how personal data is being used in enterprises. In this data-driven economy, the number of cyber attacks continues to grow in frequency and severity. Heightened regulatory requirements and increasing risk of cardholder data breaches create a feeling of uncertainty for companies, merchants, payment processors, and acquirers who need to protect payment data anywhere it moves, anywhere it resides, and anywhere it's used. Companies of all types are being targeted—anyone with valuable data for attackers.

Companies deploying encryption extensively achieved 21 percent ROI[1]

Security intelligence systems	23%
Extensive deployment of encryption technologies	21%
Advanced perimeter controls and firewall technologies	20%
Access governance tools	13%
Extensive use of data loss prevention tools	12%
Enterprise deployment of GRC tools	12%
Automated policy management tools	6%

0%   12.5%   25%

Companies deploying encryption extensively saved $883,000 USD annually[2]

Security intelligence systems	$1,917,225
Access governance tools	$1,789,024
Enterprise deployment of GRC tools	$1,602,705
Advanced perimeter controls and firewall technologies	$1,573,427
Extensive deployment of encryption technologies	$882,765
Extensive use of data loss prevention tools	$813,557
Automated policy management tools	$384,489

$0 $1M $2M

(in USD)

1, 2 "2015 Cost of Cyber Crime Study: Global," HP (now Hewlett Packard Enterprise)-commissioned study, Ponemon Institute, October 2015

Figure 1. The value of deploying encryption

Unique approach

End-to-end data protection

HPE Security — Data Security provides a comprehensive data-centric approach to data protection that addresses the security and privacy needs for data-at-rest, in-motion, and in-use through the combined, integrated solutions of HPE SecureData and HPE Atalla Hardware Security Module (HSM). By joining data-centric data protection with a tamper-reactive hardware security module, companies are able to neutralize data breaches by protecting data rendering it useless to attackers.

HPE SecureData provides an end-to-end data-centric approach that enables you to protect data over its entire lifecycle—from the point at which it's captured, throughout its movement across your extended enterprise, all without exposing live information to high-risk, high-threat environments. HPE SecureData enables companies to neutralize breaches and render data useless using breakthrough, proven encryption, tokenization, and stateless key management solutions—protecting sensitive data such as personally identifiable information (PII), protected health information (PHI), and credit card and social security numbers. HPE SecureData leverages HPE Format-Preserving Encryption (FPE) and Secure Stateless Tokenization (SST) to enable companies to securely protect data

while maintaining its usability and referential integrity for data processes, applications, and services preventing costly database schema changes. HPE SecureData has a unique key derivation and management infrastructure called HPE Stateless Key Management that dynamically derives keys on demand after authorization as needed for data protection. HPE Stateless Key Management eliminates the need to store or manage keys and seamlessly integrates with existing identity management and authorization systems to provide policy-based access to data.

HPE Atalla HSM integrates seamlessly with HPE SecureData to enable enhanced protection of the underpinning cryptographic secrets and key materials needed for key derivation, data encryption, de-identification, and masking. HPE Atalla HSM manages the system-level keys used for key derivation within a hardened FIPS 140-2 Level 3 device, eliminating the risk of exposure or compromise. Cryptographic encryption or decryption and key derivation are performed within the secure boundary of the HPE Atalla HSM inside the tamper-reactive security module environment.

HPE Atalla HSM provides differentiated capabilities for the security market such as a flexible approach to HSM configuration and key management. This is especially important where flexible and compliant solutions are

required to manage HSM configuration in lights-out facilities while meeting Payment Card Industry (PCI) Dual Control Requirements. Additionally, the Atalla HSM offers robust backup and restore capabilities where a policy can be set to specify that M of N cards must be required for restore. This approach provides increased robustness and policy control around recovery of sensitive encryption keys and configuration data.

The integrated solutions of HPE SecureData and HPE Atalla HSM enable organizations to quickly pass audits and additionally implement full end-to-end data protection. The integrated solution helps to reduce risk impact of data breaches, all without the IT organization having to completely redefine the entire infrastructure and IT processes or policies. It protects information in compliance with PCI Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), state and national data privacy regulations, as well as the European Commission's General Data Protection Regulation (GDPR). The integrated solution enables companies to comply with the more stringent PCI DSS v3.2 requirements on transport encryption.

Key benefits

- Enables centralized configuration and enforcement of security policies

  – Reduces deployment and configuration time with single configuration and management console for HPE SecureData and HPE Atalla HSM

  – Derives and distributes encryption keys to the application for secure data protection, end-to-end

  – Safeguards and manages system-level encryption keys associated with data-centric security technology

- Builds trust into your data protection system

  – Protects cryptographic material with industry-leading root of trust

  – Expands the security of mobile and card payment protection to include end-to-end data protection

  – Protects customer personal identification numbers (PINs) and associated cryptographic keys for safeguarding value-based transactions

  – Enables end-to-end data protection to meet Point-to-Point Encryption (P2PE) v2 requirements for merchants and payment processors

  – Enhances comprehensive logical and physical protection for key derivation, distribution, and storage and security policy enforcement

- Assists companies to reduce risk and demonstrate PCI DSS compliance

  – PCI v1 validated HSM

  – Highest level of protection with secure tamper key protection—FIPS 140-2 Level 3 security boundary

  – Reduced cost of compliance and audits

- Achieves single vendor, lowest TCO, simplified ordering, and single vendor contact and support

The benefits of a complete HPE solution

The integrated HPE SecureData and HPE Atalla HSM solution provides a comprehensive data security offering to address the challenges of end-to-end data protection through data-centric security, and ensures the security from an HSM by safeguarding and managing system-level encryption keys. By selecting the integrated HPE Security solution, companies are able to reduce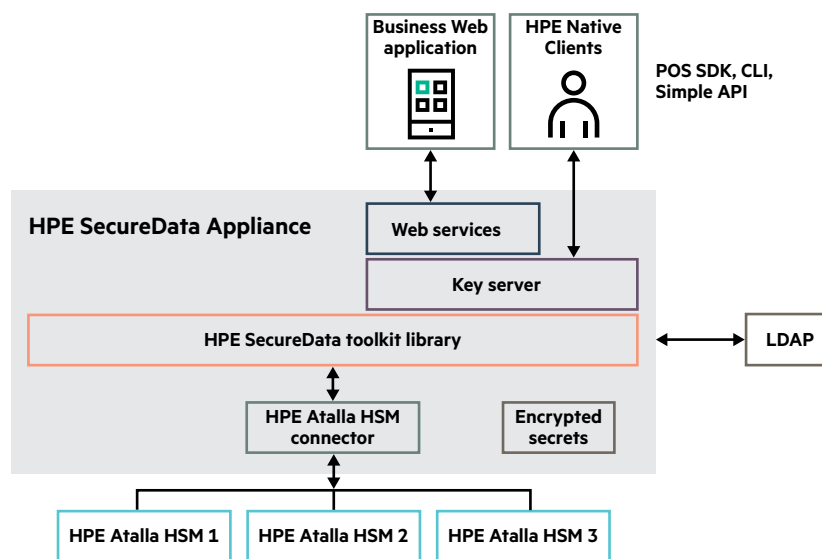 deployment and configuration time by streamlining setup through a centralized management console while reducing risk and demonstrating PCI DSS compliance and PII or PHI data protection with a single vendor solution. Additionally, Hewlett Packard Enterprise has more than 35 years' expertise in data protection, security, and cryptographic performance.

Customers demand data-centric security that is powerful yet simple to deploy and administer. This HPE Security solution offers the power of HPE SecureData plus HPE Atalla HSM in a simple, integrated, easy-to-buy, easy-to-install-and-configure, and easy-to-administer solution.

- Single point of purchase—HPE Security

- Centralized configuration for management of HPE FPE keys

- Industry-leading data-centric security integrated with a secure root of trust to store your most sensitive cryptographic secrets

Figure 2. How it works

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

Hewlett Packard
Enterprise