HPE Security—Data Security offerings for government

Providing full data protection

HPE Security—Data Security is a technology leader in data-centric security and encryption solutions for government. With over 80 patents and 51 years of expertise, we protect government institutions the world over 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 infrastructure, cloud, payment ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security—Data Security solves government challenges of simplifying the protection of sensitive data in even the most complex data security use cases.

Use cases

Compliance and scope reduction
Our solutions enable public sector customers to take advantage of FIPS-validated technology when building compliance programs for regulations such as the Cybersecurity Act of 2015, Department of Defense Federal Acquisition Regulations for Controlled Unclassified Information (DFARS CUI), Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulations (GDPR).

HPE SecureData—Reduce compliance costs with point-to-point encryption (P2PE). Combines HPE Secure Stateless Tokenization (SST) with HPE Page-Integrated Encryption (PIE) for complete data protection. FIPS 140-2 validation of Format-Preserving Encryption (FPE).

HPE Atalla HSMs—Payments applications, EMV, debit, mobile, customizations and compliance in FIPS 140-2, level 3 appliances, and full integration with HPE SecureData.

Data de-identification and privacy
HPE SecureData: HPE SecureData has achieved the industry's first Federal Information Processing Standard (FIPS) 140-2 validation of Format-Preserving Encryption (FPE). HPE SecureData with Hyper FPE "de-identifies" sensitive personally identifiable information (PII) such as social security numbers (SSN), and other high value data, rendering it useless to attackers in the event of a security breach. This allows government agencies to securely leverage the de-identified data for big-data analytics, and collaborate with shared data between other agencies or contractors.

HPE Enterprise Secure Key Manager—A FIPS 140-2 and Common Criteria EAL2+ certified secure server, storage infrastructure and cloud environments with OASIS KMIP interoperability and enterprise key management against losses, mishandling, administrative and operational attacks.

HPE SecureMail—Email security without PKI complexity using HPE Identity-Based Encryption (IBE); protect sensitive PII and PHI throughout the enterprise and cloud.

Cryptography Innovations, Government and Industry Standards
As one of the U.S. government's largest cybersecurity providers, HPE Security products not only support government standards, but also help define them

- HPE IBE—IEEE 1363.3

- National Institute of Standards and Technology Special Publication (NIST SP) 800–38G FPE standard

- HPE Page-Integrated Encryption (HPE PIE)

- HPE Secure Stateless Tokenization (HPE SST)

- IETF 5408, 5409, and 5091

- PCI Security Standards Council

- ANSI X9.119, X9.124

- FIPS 140-2 Compliance

- Common Criteria EAL2+ certified

- HIPAA/HITECH

Combined data security and encryption solutions
- Our combined solutions are built on 51 years of innovation, delivering advanced information protection of sensitive data under a data-centric security vision

- Our solutions provide continuous protection through data classification, data encryption, and key management, offering flexibility, reliability, and manageability

- We solve the challenge of simplifying the protection of sensitive government data in even the most complex data security use cases

Solutions

HPE SecureData Enterprise
Protects sensitive data end-to-end, from moment of capture across information lifecycle

HPE Atalla Hardware Security Module (HSM)
Leading payments security appliance—also known as an Atalla Network Security Processor (NSP)

HPE Enterprise Secure Key Manager, HPE Stateless Key Management
Complete key management support from infrastructure to the application level

HPE SecureData Payments
Provides point-to-point encryption and tokenization for payment data protection from swipe through to the payment processor

HPE SecureData Mobile
Protects data in motion captured on mobile end-points

HPE SecureData Web
Leverages unique HPE Page-Integrated Encryption to secure sensitive browser data

HPE SecureData for Hadoop
Enables protection of sensitive data in use with Hadoop and Big Data technologies

HPE SecureData for Cloud
Protecting data before it enters, as it moves, throughout the cloud

HPE SecureMail
Policy-based enterprise-wide email encryption for employees, customers, and mobile users

Product benefits

HPE SecureData Enterprise
• Layer data-centric security into decades old legacy systems and applications.

• Protect all kinds of structured high value data: personally identifiable information (PII), personal health information (PHI) or Classified data types.

• Expand access to de-identified data, drive big data analytics.

• Enable agencies to share data (data portability), improve citizen services and collaborate with other agencies and contractors.

• Adopt innovations such as cloud, Hadoop and IoT.

• Address specific requirements in legislation such as Cybersecurity Act of 2015, DFARS CUI, GDPR or HIPAA.

• FIPS validated solution and NIST standardized technology.

HPE Atalla Hardware Security Modules
• Meets the highest government and financial industry standards

• Mitigates risk, enforces controls

• Scales easily as customer's data security systems grow

• Provides secure, high-performance financial transaction processing

• Enables superior remote management and key protection

Major industry segments served
- Government
- Healthcare
- Financial services
- Insurance
- Retail
- Transportation
- Teleco

The HPE Security—Data Security difference
- One of the U.S. government's largest cybersecurity providers
- Standards-based: ANSI, NIST, IEEE, KMIP
- Well supported and widely proven
- Widest variety of use cases
- Breadth of platforms

HPE Enterprise Secure Key Manager
- Meets strong security standards—FIPS 140-2 and Common Criteria EAL2+
- Achieves automated policy and audit regulatory controls for safe harbor rules
- Compliant certified for open standards and interoperability for OASIS KMIP
- Ensures auditable security to meet compliance
- Enables robust key management scalability

HPE SecureData Payments
- Protects credit card data-at-rest and in transit within the cardholder data environment
- Reduces PCI scope without impacting business processes and workflows
- Provides complete point-to-point encryption (P2PE) and tokenization for retail payment transactions

HPE SecureData Mobile
- Provides compliance and scope reduction
- Enables PII and PHI compliance
- Protect sensitive data at every level of the omni-channel and unified commerce experience
- Developer friendly—simple, native libraries, easy to incorporate into iOS and Android apps
- Protects data in motion captured on mobile end-points

HPE SecureData Web
- Protects sensitive browser form data at capture using HPE PIE technology
- Protects data, e.g., payment or personal data, end-to-end, through web and cloud systems to trusted host destinations
- Helps merchants reduce Payment Card Industry Data Security Standard (PCI DSS) scope by reducing live data exposure in web applications

HPE SecureData for Hadoop
- Protects data as close to its source as possible
- Supports data encryption, tokenization, and data masking protection techniques
- Ensures data is usable for most applications in its de-identified state
- Re-identifies data securely when required—strictly for authorized users and applications
- Achieves high performance, high scalability appropriate for Hadoop speeds

HPE SecureData Cloud
- Protect data at field level; enabling business process and cross-cloud analytics on protected data
- Control keys independently of cloud to separate physical data location
- Enables simpler compliance to PCI DSS, HITECH, EU Privacy, cross border data exchanges privacy regulations
- Reduces audit-creep due to different cloud tools with incomplete protection data control

HPE SecureMail

- Provides a single solution for desktop, cloud, and mobile

- Enables data-centric protection for email and attachments

- Leverages stateless key management using standards-based HPE Identity-Based Encryption (HPE IBE)

- Allows flexible deployment options on-premise, in the cloud, or hybrid deployments

- Enhances security for Office 365 cloud-based environments

HPE Security—Data Security provides full data protection

PCI/compliance/ scope reduction

Collaboration security for users, cloud apps, and data interactions

Data de-identification and privacy

HPE Security—Data Security is a leader in data-centric security safeguarding data throughout its entire lifecycle—at-rest, in-motion, in-use—across the cloud, on-premise and mobile environments with continuous protection.

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

f y in ✉

Sign up for updates

Hewlett Packard Enterprise