Data sheet

HPE SecureData

An end-to-end data-centric approach to securing the business of government

Highlights of HPE SecureData next generation capabilities

- FIPS 140-2 validated solution for Format-Preserving Encryption Solution
- Hyper FPE, a next generation high performance format-preserving encryption for virtually unlimited data types
- Sensitive data is protected with NIST-Standard FF1 AES encryption, pioneered by Hewlett Packard Enterprise
- Designed for compute intensive demands and the explosion of data and formats that need protection across a broad array of use cases
- REST API—web services interface for easier integration and adaptability
- Hyper SST—next generation high performance tokenization
- More flexible encryption for global markets with Unicode language support

The growing threat to data

Our world runs on data. From consumer information (health files, banking and financial data, education records, and more) to research findings and classified national security information, we generate an ever-increasing volume of critical, sensitive data. Criminals target much of this information, and cyber attacks against enterprises and governments globally continue to grow in frequency and severity. A U.S. federal government agency data breach announced in June 2015 involved the greatest theft of sensitive government data in the history of the United States. Data targeted in the breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses. Worse, the hack went deeper than initially realized, and likely involved the theft of detailed security clearance-related background information. The estimated number of stolen records is 21.5 million, with an estimated cost of more than $1 billion.[1]

How did it happen? The agency maintained an unsecured and unencrypted database for security clearances. A 2006 agency report states that this "Data Repository" is premised on a "shared-disk (shared-data) model," and that "all of the disks containing databases are accessible by all of the systems." An official at the Department of Homeland Security (DHS) testified that the attackers most likely gained valid user credentials to the systems by a phishing attack through social engineering. The breach also consisted of a malware package that installed itself within the agency's network and established a backdoor. From there, attackers escalated their privileges to gain access to a wide range of the agency's systems.

[1] **fcw.com/articles/2015/09/10/opm-breach-cost.aspx**

Key benefits

- 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 legislations such as Cybersecurity Act of 2015, DFARS CUI, GDPR or HIPAA.
- Protect foreign citizen data with unicode latin 1 support.
- FIPS validated solution and NIST standardized technology.

The damage is not limited to the agency. Whatever entity successfully breached the agency system potentially gained pass-through access to other extraordinarily sensitive national security data. Whether perpetrated by lone operators or state-sponsored actors, data theft is a constant, and protecting data is of the utmost importance. It's not a question of if you will be hacked; it's a question of when. And it's vital to be prepared.

The government challenges

Government customers have some of the same challenges faced by private sector corporations, including:

- The exponential growth of high-value and personally identifiable information from citizens, employees, and anyone with any business with the government.
- The difficulty of adding security to legacy applications and platforms with limited native data security options.
- Gaps in data protection from the over-reliance on data-at-rest, network and endpoint security.
- The need to leverage rich data for analytics and share data between agencies and with contractors.
- Compliance with privacy and data protection legislation such as GDPR, HIPAA.
- The need to adopt innovations such as cloud and IoT.

HPE SecureData provides an end-to-end data-centric approach to enterprise data protection. It is the only comprehensive data protection platform 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 includes next generation technologies, Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), HPE Stateless Key Management, and data masking.

A comprehensive approach to end-to-end encryption

HPE SecureData with Hyper FPE has the ability to "de-identify" virtually unlimited data types, from sensitive personally identifiable information (PII), to IDs, health information or classified 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. It also provides accelerated encryption speeds that enables government agencies to adopt new technologies such as the cloud or Hadoop or invest in innovations such as IoT, all while lowering the risk of disclosing sensitive personal data or compromising high value data.

A major challenge faced by federal agencies, including those attacked by nation state adversaries, is the dependency on legacy applications and platforms with limited native data security options. HPE SecureData helps build data security into both new and decades-old legacy applications, de-identifying high-value data classes; for example, protecting classified information, or eliminating reliance on using Social Security Numbers for business processes. Security assurance is increased, while unleashing utility of data for secure adoption of big data analytics, Hadoop and other new applications and solutions.

HPE SecureData is the first data protection platform to earn FIPS 140-2 validation of its Format-Preserving Encryption (FPE) technology under the new National Institute of Standards and Technology's (NIST) AES FFX Format-Preserving Encryption (FPE) mode standard. This enables public sector customers, when operating in strict FIPS mode, to take advantage of true FIPS-validated cryptography and build compliance programs for regulations such as the Cybersecurity Act of 2015 data security requirements, DFARS CUI, and General Data Protection Regulations (GDPR).

With the HPE SecureData FIPS validation, government agencies and contractors can now use a standardized data security product with extensive enterprise deployments, neutralizing data breaches while liberating analytics and innovation.

First FIPS 140-2 validated and NIST-standardized Format-Preserving-Encryption solution

HPE Security—Data Security has contributed technology and core specifications for the new **National Institute of Standards and Technology's (NIST) AES FFX Format-Preserving Encryption (FPE) mode standard**.

The NIST standard provides an approved and proven data-centric encryption method for government agencies, and HPE has been involved as a developer through open cooperation with NIST from initial proposals of Format-Preserving Encryption technologies with formal security proofs to independent peer review of the NIST AES modes. The NIST standard is critical in setting the bar to ensure organizations are maintaining regulatory and audit compliance, as well as using proven methods to protect against a data breach.

HPE SecureData is FIPS 140-2 validated, leveraging the NIST FF1 AES encryption standard, providing all the benefits of data-centric security delivered by Hyper FPE—the most flexible and powerful FPE available—with the ability to encrypt virtually unlimited data types.

The work HPE Security—Data Security is doing with NIST, ANSI, IEEE, IETF, and independent security assessment specialists, stands unique in the market. Standards Bodies where HPE SecureData protection technology breakthroughs are published include:

NIST National Institute of Standards and Technology U.S. Department of Commerce

IEEE

ANSI American National Standards Institute

IETF

Hyper FPE: encryption and masking—how we do it

Traditional encryption approaches, such as AES CBC have enormous impact on data structures, schemas, and applications as shown in Figure 1. Hyper FPE is NIST-standard using FF1 mode of the Advanced Encryption Standard (AES) algorithm, which encrypts sensitive data while preserving its original format without sacrificing encryption strength. Structured data, such as Social Security, Tax ID, credit card, account, date of birth, salary fields, or email addresses can be encrypted in place.

Traditional encryption methods significantly alter the original format of data. For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. As a result, database schema changes are required to facilitate this incompatible format. Hyper FPE maintains the format of the data being encrypted so no database schema changes and minimal application changes are required—in many cases only the trusted applications that need to see the clear data need a single line of code. Tools for bulk encryption facilitate rapid de-identification of large amounts of sensitive data in files and databases. Typically, whole systems can be rapidly protected in just days at a significantly reduced cost. In fact, Hyper FPE allows accelerated encryption performance aligning to the high volume needs of next generation Big Data, cloud and Internet of Things, and supports virtually unlimited data types.

Hyper FPE de-identifies production data and creates structurally valid test data so developers or users can perform QA or conduct data analysis—all without exposing sensitive data. The HPE SecureData management console enables easy control of policy and provides audit capabilities across the data life cycle—even across thousands of systems protected by HPE SecureData. Hyper FPE also provides the option to integrate access policy information in the cipher text, providing true data-centric protection where the data policy travels with the data itself.

	Tax ID 934-72-2356	**First Name:** Gunther **Last Name:** Robertson SSN: 934-72-2356 **DOB:** 08-07-1966
FPE AES-FF1 Mode	**253-67-**2356	**First Name:** Uywjlqo **Last Name:** Muwruwwbp SSN: **253-67-**2356 **DOB:** 01-02-1972
Regular AES-CBC Mode	8juYE%Uks&dDFa2345^WFLERG	Ija&3k24kQotugDF2390^32 0OWioNu2(*872weW Oiuqwriuweuwr%oIUOw1@

Figure 1. Format-Preserving Encryption (FPE) versus regular AES Encryption

HPE Stateless Key Management: transparent, dynamic

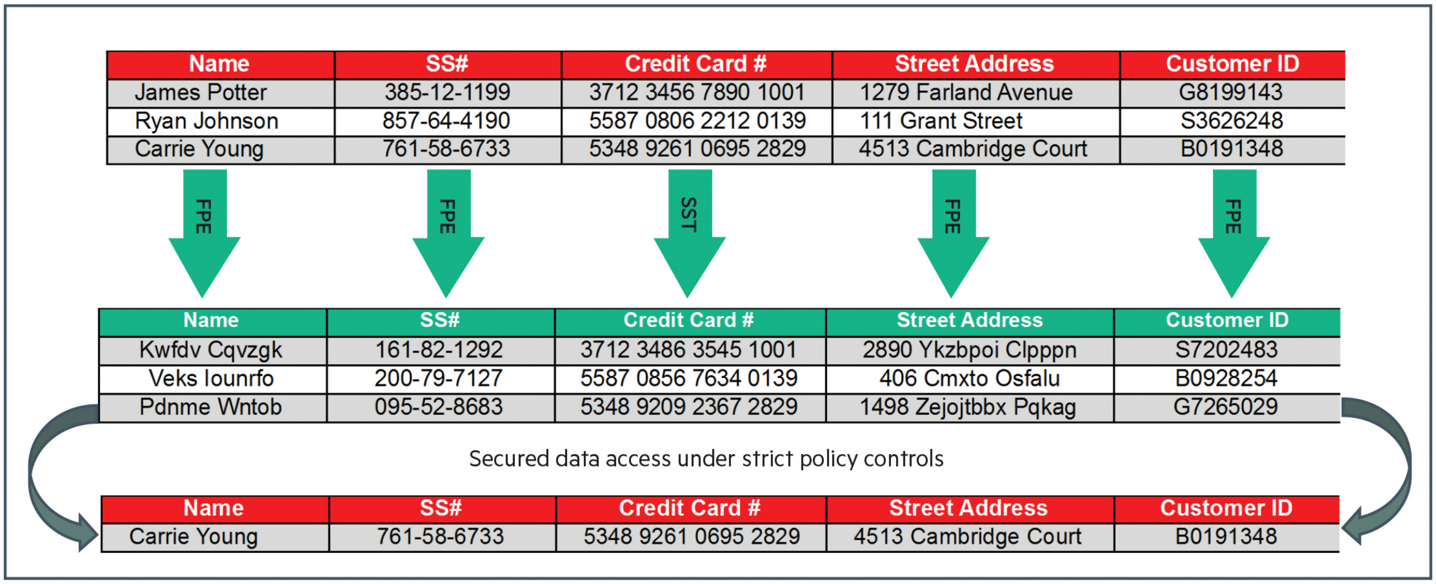
HPE Stateless Key Management securely derives keys on the fly as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. Advanced policy controlled caching maximizes performance. HPE Stateless Key Management reduces IT costs and eases the administrative burden by:

- Eliminating the need for a key database, as well as the corresponding hardware, software and IT processes required to protect the database continuously or the need to replicate or backup keys from site to site.
- Easily recovering archived data because keys can always be recovered.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and via web services.
- Maximizing the re-use of access policy infrastructure by integrating easily with identity and access management frameworks and dynamically enforcing data-level access to data fields or partial fields, by policy, as roles change.

Hyper SST (Secure Stateless Tokenization)

Hyper SST is an advanced, patented, data security solution that provides enterprises, merchants, and payment processors with a new approach to help assure protection for payment card data. Hyper SST is offered as part of the HPE SecureData platform that unites market-leading encryption, tokenization, data masking, and key management to protect sensitive information in a single comprehensive solution.

Hyper SST is “stateless” because it eliminates the token database, which is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. Hyper SST uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual “appliances”—commodity servers—and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with Hyper SST, thus improving the speed, scalability, security, and manageability of the tokenization process. In fact, Hyper SST effectively surpasses the existing “high-octane” SST tokenization performance.



Name	SS#	Credit Card #	Street Address	Customer ID
James Potter	385-12-1199	3712 3456 7890 1001	1279 Farland Avenue	G8199143
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348

Name	SS#	Credit Card #	Street Address	Customer ID
Kwfdv Cqvzgk	161-82-1292	3712 3486 3545 1001	2890 Ykzbpoi Clpppn	S7202483
Veks Iounrfo	200-79-7127	5587 0856 7634 0139	406 Cmxto Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 9209 2367 2829	1498 Zejojtbbx Pqkag	G7265029

Secured data access under strict policy controls

Name	SS#	Credit Card #	Street Address	Customer ID
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348

Figure 2. Data protection with Hyper FPE and Hyper SST

GDPR—new national data protection law
European Commission is modernizing data protection legislation by replacing the EU Data Protection Directive 95/46 EC with the General Data Protection Regulation (GDPR), which will be directly applicable in all European Union (EU) member states. GDPR pushes the EU into a new era of data privacy, compliance, and enforcement in 2018.

Any enterprise in the EU needs to revisit the meaning of personal data due to GDPR's expanded definition of personal data. New expanded data includes name, location data, online ID, genetic factors, etc. When an enterprise collects sensitive data, personally identifiable information (PII), payment card industry (PCI), or protected health information (PHI), it must secure and protect that data. Enterprises face significant financial penalties for non-compliance.

HPE SecureData de-identification and privacy protection of sensitive data, production and non-production, including PII, PHI, and PCI, throughout the enterprise, provides end-to-end data-centric security. Hyper FPE delivers strong and flexible encryption to protect EU citizen's personal data and to follow pseudonymization guidance in the new GDPR.

> "We needed fast deployment in an environment that is reluctant to change, but we were able to move through very quickly. We were able to get PCI compliant, which is a very big win for us, and improve our security and the additional controls around the data as it's being moved, and we have very few support calls."
>
> – Tim Masey, Director of Enterprise Information Security, AAA—The Auto Club Group

HPE SecureData Architecture

HPE SecureData solutions share a common infrastructure, including the same centralized servers and administration tools. This enables HPE SecureData customers to choose an appropriate combination of techniques to address their use cases, across diverse environments, while avoiding the costs and complexities of deploying and managing multiple products.

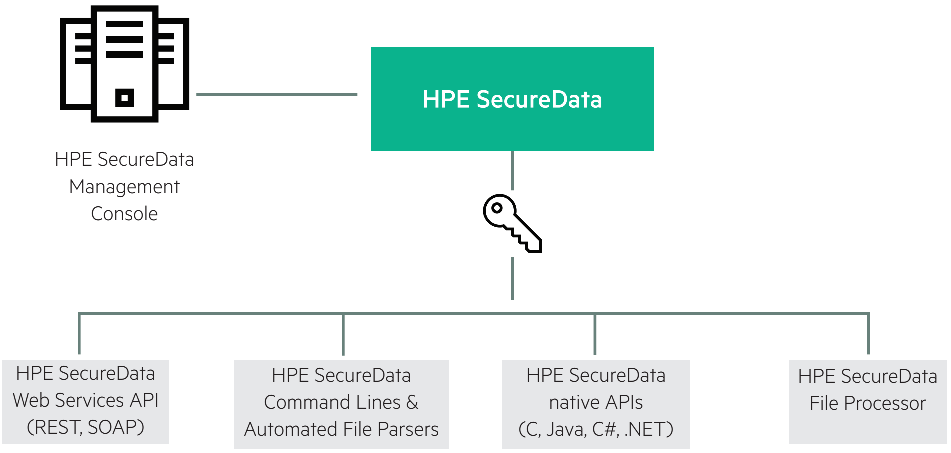

HPE SecureData Management Console
HPE SecureData
HPE SecureData Web Services API (REST, SOAP)
HPE SecureData Command Lines & Automated File Parsers
HPE SecureData native APIs (C, Java, C#, .NET)
HPE SecureData File Processor

Figure 3. HPE SecureData Architecture with virtual servers and administration tools

HPE SecureData platform modules	Description
HPE SecureData Management Console	Enforces data access and key management policies, and eliminates the need to configure each application, because flexible policies are centrally defined and reach all affected applications. Manages data format policies, business rules enforcement over data access, integration with enterprise authorization and authentication systems and connectivity to enterprise audit and security event monitoring systems. It also manages data security policies such as the choice of Hyper FPE, file encryption and data masking.
HPE Key Management Server	High-scale, on-demand, stateless key management eliminates the need for traditional complex storage-based key management, because keys are dynamically derived; seamlessly integrates with existing Identity Management and Authorization Systems and Key Management using FIPS 140-2 Hardware Security Modules.
HPE SecureData Web Services Server	Centralized web services encryption and tokenization option for Service Oriented Architecture environments, enterprise applications, and middleware. Supports SOAP and REST API web services, and Unicode Latin 1 for native languages.
HPE SecureData Simple API	Maximizes efficiency on a broad range of application servers through native encryption on HP-UX, HPE NonStop, Microsoft® Azure, Amazon Web Services (AWS), Solaris, Stratus VOS, Linux (Red Hat®, SUSE, CentOS), AIX, and Windows®. Additional APIs are available for embedded platforms such as payment terminal devices. Supports hardware accelerated encryption processes where available, e.g., Intel® AES-NI.
HPE SecureData Command Lines	Scriptable tools easily integrate bulk encryption, tokenization, and file encryption into existing batch operations and applications.
HPE SecureData File Processor	Aggregates support for both tokenization and encryption of sensitive data elements. It provides a unique value to the customer as a single client converging both web services and native API interfaces. The converged clients expand the support for new file types by decoupling input file processing from the underlying encryption and tokenization operations. Delivers high performance data de-identification, with parallel multi-threaded processing of sensitive data elements simultaneously protecting data fields across columns.
HPE SecureData Mobile	Includes simple data security libraries to easily incorporate into native mobile applications. This enables the mobile application to secure captured data end-to-end to the trusted host using a one-time cryptographic key. Supports iOS and Android.
HPE SecureData also supports mainframe, Big Data, and payment security ecosystems	• HPE SecureData z/Protect: Maximizes CPU performance on mainframe systems through native z/OS support for encryption and tokenization. • HPE SecureData z/FPE: Mainframe data processing tool to fast track integration into complex record management systems such as VSAM, QSAM, DB2, and custom formats. De-identify sensitive data for production as well as test use. • HPE SecureData for Hadoop Developer Templates: Provides templates to enable customers to integrate HPE FPE and HPE SST technologies into their Hadoop instances. Templates come with pre-built integrations for Sqoop, MapReduce, and Hive, and can be quickly expanded to integrate into other technologies in the Hadoop stack such as Flume. • HPE SecureStorage: Data-at-rest encryption for Linux with HPE Stateless Key Management. • HPE SecureData Web and Optional Add-ons: Secures data end-to-end from browser applications and forms to secure back-end applications, extending end-to-end security beyond transport encryption such as SSL and TLS. • HPE SecureData Terminal SDK and Host SDK: Provide market-leading P2PE payments security.
HPE Professional Services	Available to help clients scope projects, combat advanced threats, reduce compliance burden and quickly solve difficult data privacy challenges.

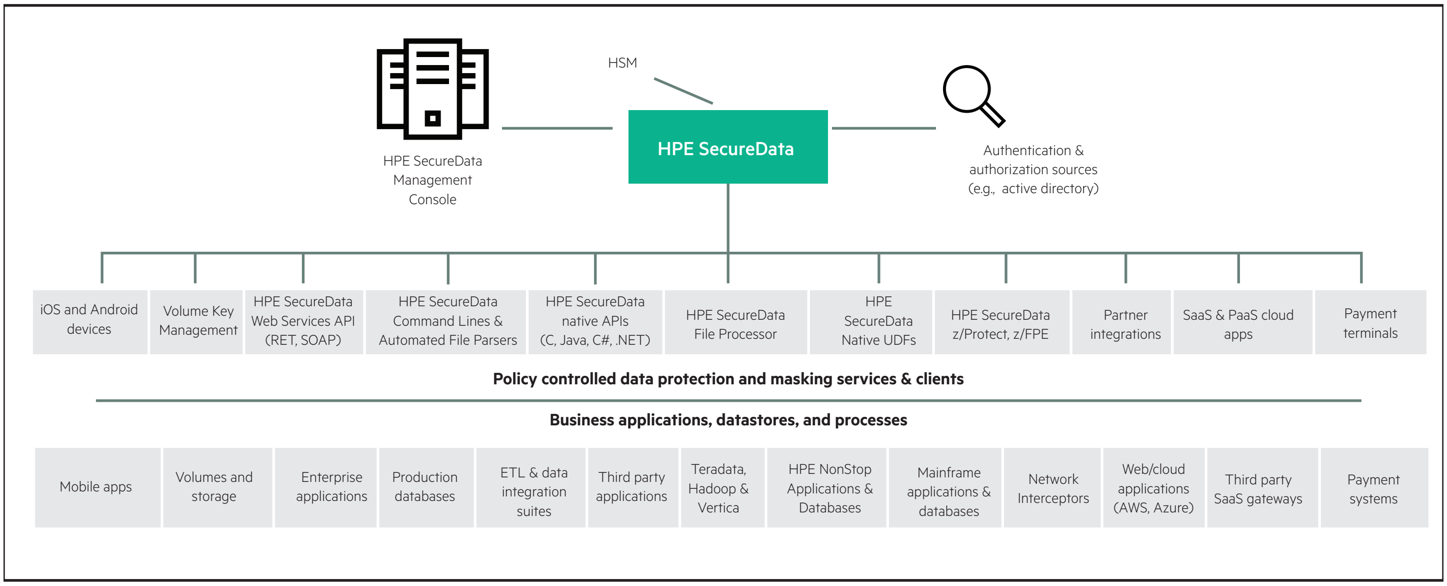

HPE SecureData Management Console
HSM
HPE SecureData
Authentication & authorization sources (e.g., active directory)
iOS and Android devices
Volume Key Management
HPE SecureData Web Services API (RET, SOAP)
HPE SecureData Command Lines & Automated File Parsers
HPE SecureData native APIs (C, Java, C#, .NET)
HPE SecureData File Processor
HPE SecureData Native UDFs
HPE SecureData z/Protect, z/FPE
Partner integrations
SaaS & PaaS cloud apps
Payment terminals
Policy controlled data protection and masking services & clients
Business applications, datastores, and processes
Mobile apps
Volumes and storage
Enterprise applications
Production databases
ETL & data integration suites
Third party applications
Teradata, Hadoop & Vertica
HPE NonStop Applications & Databases
Mainframe applications & databases
Network Interceptors
Web/cloud applications (AWS, Azure)
Third party SaaS gateways
Payment systems

Figure 4. HPE SecureData Architecture addresses use cases for enterprises across diverse environments

“**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.”

HPE Security offers products and services designed to help organizations protect their most-prized digital assets, whether on-premise, on cloud, or in between. We help protect organizations by building security and resiliency into the fabric of their enterprise, proactively detecting and responding to threats, and safeguarding continuity and compliance to mitigate risk effectively.

Learn more at
voltage.com

hpe.com/software/datasecurity

Sign up for updates

Hewlett Packard
Enterprise