Hewlett Packard Enterprise

HPE SecureData

End-to-end Data-centric Security for the New Data-driven Economy

Highlights of HPE SecureData Next Generation Capabilities

- 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
- Supports the encryption and pseudonymization guidance in the new GDPR (General Data Protection Regulation) legislation for European Union

[1] Rethinking Personal Data: A New Lens for Strengthening Trust, World Economic Forum. May, 2014.

[2] 2015 Cost of Cyber Crime Study: Global. Ponemon Institute, October 2015.

The Challenge in Data Security

The volume of data, the sophistication of ubiquitous computing and the borderless flow of data are outpacing the ability to understand how personal data is being used. In this data-driven economy, 78 percent of consumers think it is hard to trust companies when it comes to the use of their personal data.[1] Why? The number of cyber attacks against enterprises and governments globally, continues to grow in frequency and severity.

The findings in the Ponemon Institute Cyber Crime Study[2] suggest companies using encryption technologies are more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of $883,000 annually when compared to companies not deploying encryption technologies. These companies deploying encryption technologies also experienced a substantially higher ROI (at 21 percent) than other technology categories.

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. That's the essence of data-centric security.

HPE SecureData includes next generation technologies, Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), HPE Stateless Key Management, and data masking. HPE SecureData "de-identifies" data, rendering it useless to attackers, while maintaining its usability, usefulness, and referential integrity for data processes, applications and services. HPE SecureData neutralizes data breaches by making your protected data absolutely worthless to an attacker, whether it is in production, analytic systems, or test/development systems, such as training and quality assurance.

Key Benefits
Reduce audit scope, costs, system impact and resources. Eliminate sensitive data from production and test systems and enable end-to-end data protection. Satisfies compliance requirements for privacy regulations.

Avoid brand-damaging, costly breaches. Move beyond compliance to easily weave data protection across systems, devices and platforms.

Industry Standard Format-Preserving Technologies—HPE SecureData with Hyper FPE
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 NIST-standard using FF1 AES Encryption, which provides 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:

A Unique Approach to End-to-end Encryption

HPE SecureData is a unique, proven data-centric approach to protection—where the access policy travels with the data itself—by permitting data encryption and tokenization without changes to data format or integrity, and eliminating the cost and complexity of issuing and managing certificates and symmetric keys. As a result, leading companies in financial services, insurance, retail, health care, energy, transportation, telecom and other industries have achieved end-to-end data protection across the extended enterprise with success in as little as 60–90 days, because of the minimum, in most cases zero, impact to applications and database schemas.

Short Time to Success with Data Security

Most applications can operate using protected data without change. For those applications where sensitive data is first captured or live data is needed for controlled business purposes, HPE SecureData can easily be used with virtually any system, ranging from decades-old custom applications to the latest enterprise programs. Powerful, centrally managed, policy-controlled APIs, such as a REST API and command line tools, enable encryption and tokenization to occur on the widest variety of platforms, including HPE Vertica, HPE NonStop, Teradata, IBM mainframe, Linux and other open systems. APIs enable broad deployment into portfolios including ETL, cloud, databases and applications, network appliances, and API brokers such as F5 load balancing, and Hadoop with native on-node cluster-wide datamasking, encryption and decryption. SIEM/SIM systems can take event data from HPE SecureData for data governance reporting, activity monitoring and audit.

HPE SecureData protects information in compliance with PCI DSS, HIPAA, GLBA, state and national data privacy regulation as well as the European Commission's General Data Protection Regulation (applicable in all EU member states). HPE SecureData is also compatible with the more stringent PCI DSS 3.2's new requirements on transport encryption, enabling accelerated compliance ahead of deadlines as recommended by the PCI council. HPE SecureData enables organizations to quickly pass audit and additionally implement full end-to-end data protection to reduce risk impact of data breaches, all without the IT organization having to completely redefine the entire infrastructure and IT processes or policies. On average, HPE SecureData requires less than 0.1 full-time employee (FTE) per data center for ongoing management.

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.

Unicode Latin 1
Hyper FPE Unicode Latin 1 provides format and character set preserving encryption for global enterprises using data in languages such as German, Spanish, French and more.

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.

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 back-up 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 corporate 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.

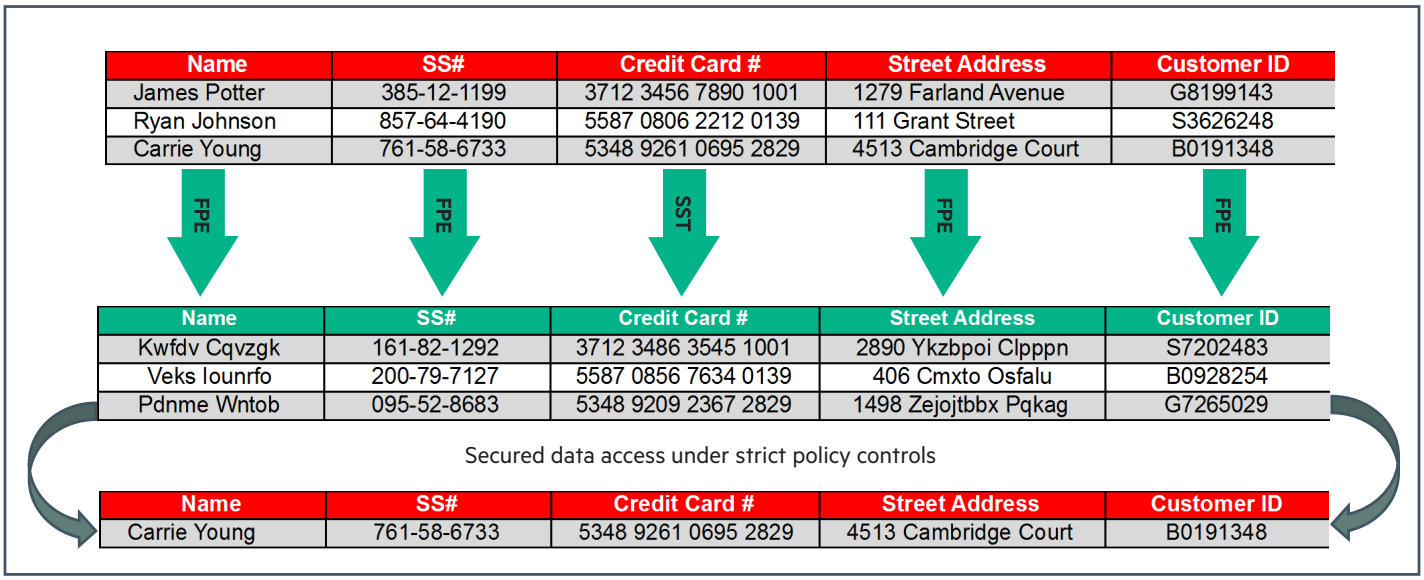

Figure 2: Data Protection with Hyper FPE and Hyper SST

"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.

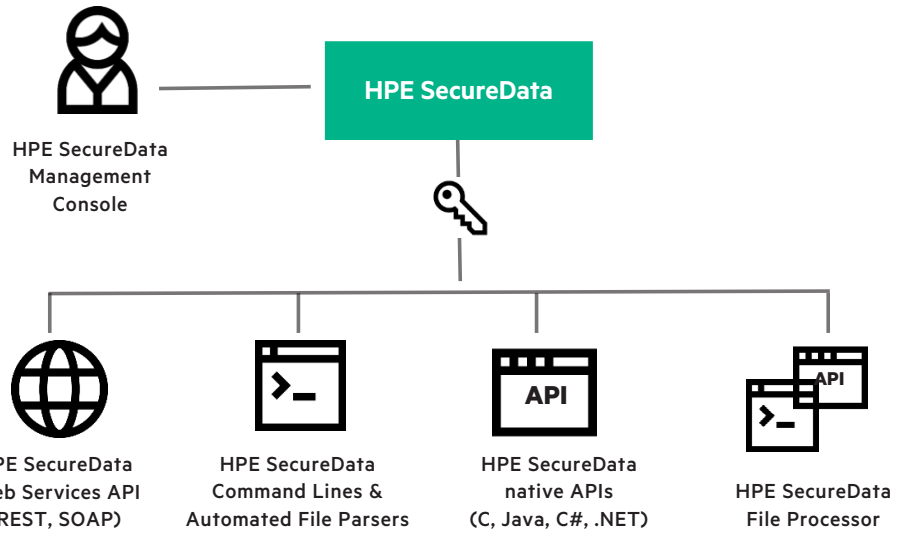

Figure 3: HPE SecureData Architecture with virtual servers and administration tools

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 PLATFORM MODULES	DESCRIPTION
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.

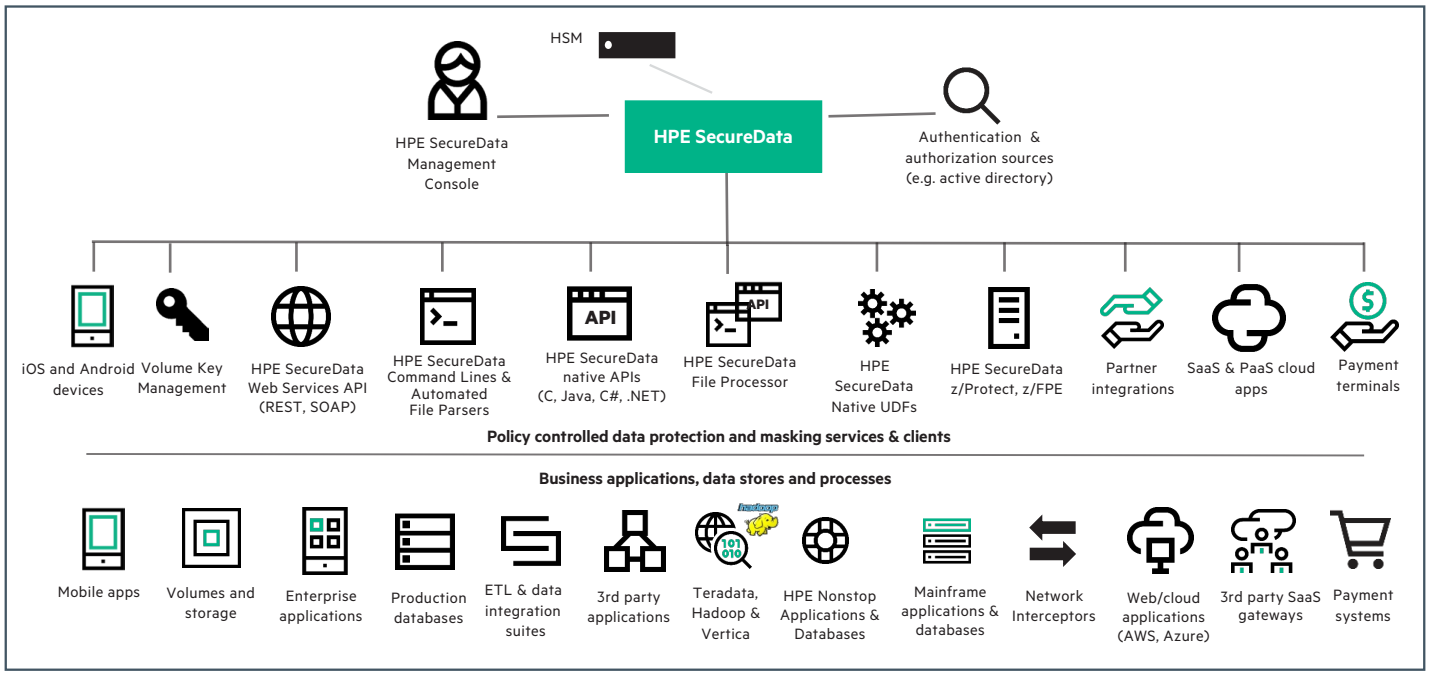

Figure 4: HPE SecureData Architecture addresses use cases for enterprises across diverse environments

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

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

4AA6-0208ENW, May 2016, Rev. 2