Hewlett Packard Enterprise

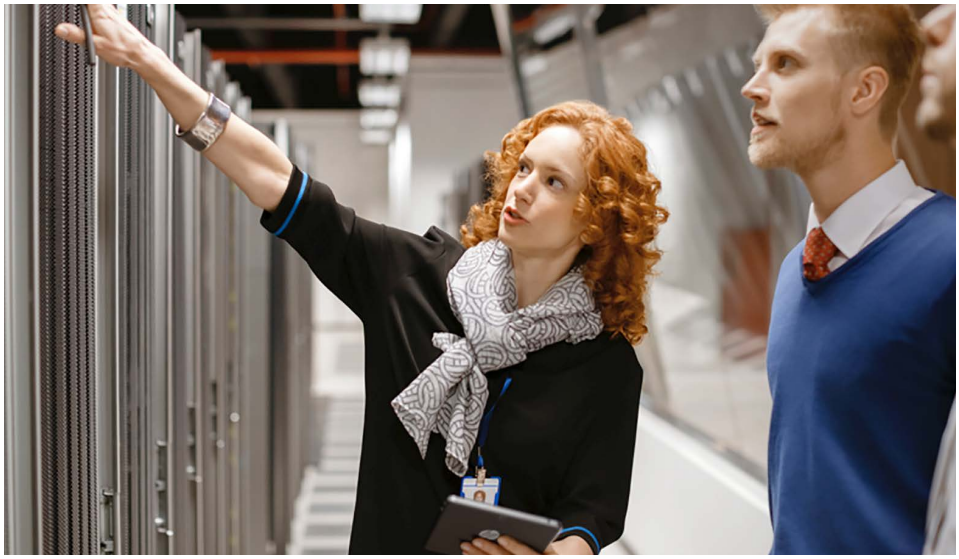
Data De-Identification

Neutralize Breaches: Protect your Data and your Brand

Neutralize data breaches: a new breed of cyber attacks-advanced malware, exploitation networks, and motivated insiders are stealing sensitive data from vulnerable ecosystems. But companies can neutralize data breaches by rendering the data valueless, de-identifying data through encryption, tokenization, and data masking.

Use Cases

- High performance, frequent data masking from production to test/dev
- Hadoop or large data sets for secure analytics and external sharing
- Mainframe data masking, native to z/OS–for DB2, Files, IMS
- Masking in existing workflow; e.g. ETL or data sub-setting tools
- Secure reversibility; e.g. z/OS to Teradata to Hadoop and back again



New Challenges

Today, companies have implemented every type of deterrent, policy, training, intrusion prevention, and firewall, but it is not enough. New challenges exist because businesses are increasingly driving initiatives that push sensitive data into more business areas; at the same time, they need to protect their customers personal information. The only way for organizations to truly protect sensitive data is to make it worthless to an attacker by de-identifying the data while at rest, in use, or in transit.

Traditionally, data masking has been viewed as a technique for solving a test data problem. Now, the scope of data masking has broadened to include data de-identification in production, non-production, and analytic use cases. The December 2015 Gartner Magic Quadrant Report on Data Masking Technology[1] reports the growing importance and trend of data masking for security and privacy of sensitive data. A robust Data De-identification Solution should not complicate workflows or compromise applications' ability to utilize masked data. The challenge is to do this while retaining the business value in the information for consumption and use. HPE SecureData has made that vision a reality.

HPE SecureData for Data De-Identification

HPE SecureData provides a comprehensive data-centric approach to enterprise data protection. It includes:

- HPE Format-Preserving Encryption (FPE) is NIST SP-800-38 G standard
- HPE Hyper Secure Stateless Tokenization (SST) technology, and
- HPE Stateless Key Management for on-demand key generation and re-generation without an ever-growing key store

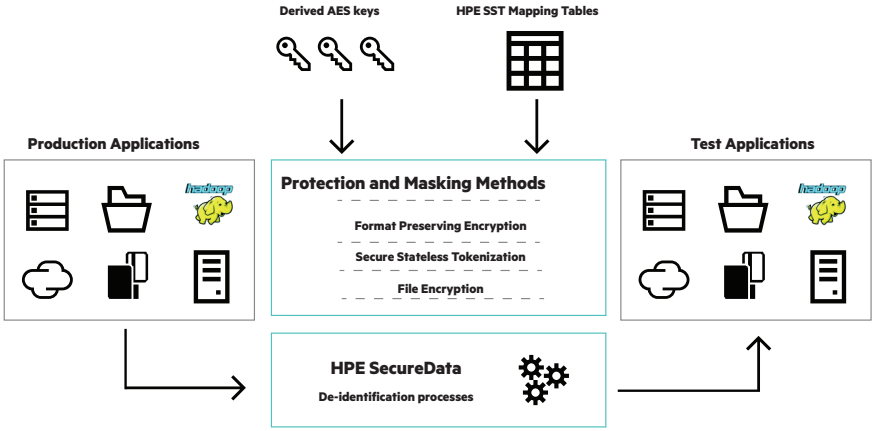
[1] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

HPE SecureData with Hyper FPE uses 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 FPE 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, and using proven methods to protect against a data breach.

HPE SecureData is NIST-standard using FF1 AES Encryption—the most flexible and powerful FPE available—to encrypt virtually unlimited data types.

With the innovative and proven techniques delivered by HPE FPE and SST, data formats are preserved and policy controlled, thus maintaining the analytic value of data. Preserving date ranges, the first 6 and last 4 digits of PAN data, and other critical data characteristics, means protected data can be used by the business without compensating controls or causing significant IT changes.



Key Capabilities

Considerations	HPE SecureData Solution
How are you managing data masking in test environments? Is it the same solution for production data and analytics?	**Delivers single platform** with production, analytic, test, and development protection and masking all in one technology/ platform and enables database integrity across geographically distributed and large data systems
Does the solution require additional servers or databases or increase management cost and complexity? What is the cost to implement and maintain?	**Because of its stateless solution, HPE SecureData eliminates the need for mapping tables or databases** so it is well-suited for projects requiring high scalability and requires less than .1 FTE per data center
Can you easily incorporate data de-identification into existing workflows such as ETL or data sub-setting tools? Does the solution support a heterogeneous data management environment?	**Builds data masking into existing workflows** and data management frameworks using a set of APIs and processing tools that are compatible with extraction, transformation and loading (ETL) and data management solutions across Linux, Unix, Windows, IBM z/OS mainframe, HPE Nonstop, Stratus, Teradata, Amazon Web Services, Windows Azure, Hadoop; technology integration with Informatica
Can you reverse the data masking? How is that done, and can it be done securely and without risk?	**Securely reverses masked data** through centralized key management to its original state, or make it irreversible using one-time, 256-bit FPE keys
How are you masking data for secure analytics in Big Data platforms such as Hadoop?	**Supports Big Data initiatives**—available for Hadoop and certified for Cloudera, MapR, IBM Big Insights, and Hortonworks
How does the solution support access rules from Active Directory, LDAP or other systems?	**Enables on-the-fly masking** that dynamically applies access rules based on input from Active Directory, LDAP or custom identity and access management (IAM) systems
Is the solution built on proven security standards? Will it provide Safe Harbor in the event of data breach?	**Proven Security Leadership track record**—NIST, ANSI, IEEE, IETF—Standards Bodies where HPE SecureData data protection technology breakthroughs are published. Is NIST AES FFX Format Preserving Encryption mode standard

Sign up for updates

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

4AA5-9774ENW, June 2016, Rev. 2

Hewlett Packard Enterprise