Voltage SecureData™

Database Encryption, Data Masking and Data De-Identification

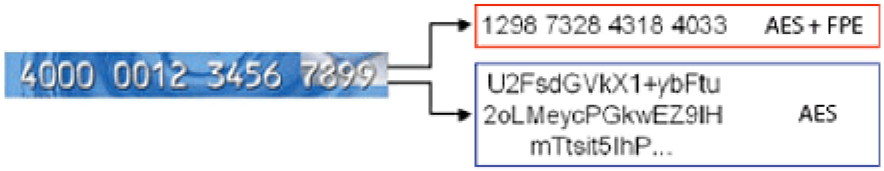
Click here to learn about the latest features of Voltage SecureData

Voltage SecureData delivers a comprehensive solution for data encryption, de-identification, and masking that does not require costly and time-consuming data schema and data format changes in existing systems. Voltage SecureData enables enterprises to ensure sensitive data is protected end-to-end: as it is collected, used, stored, and distributed to less controlled environments (e.g., test and development) regardless of infrastructure or application format requirements.

- **End-to-end encryption at lower cost**
  All data within your organization - whether it arrives from remote locations or flows within your databases and applications can be encrypted with minimal changes to your applications. This results in not only rapid deployment but also dramatically lower costs.
- **Protect your customers from Identity Theft**
  By encrypting identity information such as credit card numbers, bank account numbers, social security numbers with FPE, criminals will be unable to compromise customer identities in the event of a data breach
- **Rapid compliance with PCI, Identity Theft Red Flag and other regulations**
  By using the FPE approach with Voltage SecureData, it is possible to rapidly enable compliance - on average 5 times faster than traditional techniques
- **Reduce risks with outsourced environments**
  By safeguarding your data with FPE and Voltage SecureData, the risks of unintentional exposure of sensitive data is dramatically reduced
- **Enable developer access to production data**
  By masking or de-identifying your production data for use by developers in test and QA environments, you ca continue to get the best results from your developers without compromising the safety of sensitive information

Voltage SecureData™ enables companies to simply and rapidly protect the data itself, without the need for major changes to their applications, databases or business processes. Based on a revolutionary technology called Format-Preserving Encryption™ (FPE), Voltage SecureData encrypts data in databases and applications while retaining the format of the original structured information. FPE is a mode of standard AES, recognized by NIST.

Standard encryption methods alter the original format of data, producing a different output. For example – a 16 digit credit card number encrypted with AES produces a long alphanumeric string, with FPE mode AES- the encrypted credit card number that looks and feels the same as a regular credit card without sacrificing strength, and without any additional data storage. By maintaining the format of the data being encrypted, database schema changes are zero and application changes minimized – in many cases 1-2 line of code total. This means that whole systems can be rapidly protected in just days at significantly reduced cost.



Using Format-Preserving Encryption (FPE),Voltage SecureData maintains data format and eliminates business process changes.

Key Features and Advantages

Maximum Data Security. Employs proven encryption technologies to protect sensitive customer and company information in backups and production databases.

Supports Your Business Needs. Encrypts data in a way that preserves its original format, so it can be used by developers inside and outside your company, without exposing any sensitive information. Also enables different views of the data, based on a person's functional responsibilities, so each employee only sees the amount of information they require to perform their job.

Minimal Implementation Time and Costs. Easily integrates into most popular operating systems and databases, so little or no changes are required to the existing business architecture. On average, 5 times faster to implement than competing solutions.

Easy to Administer. Eliminates the need to store encryption keys.

Voltage SecureData™ - What's New?

Distributed End-to-End Encryption of Sensitive Data

Protection for end-to-end data
Encrypt your sensitive customer data where it is most vulnerable – between the POS terminal, the store's database, and the HQ datacenter. Voltage SecureData provides end-to-end protection of your most sensitive customer data, safeguarding you from data breaches that can cause irreparable damage to your reputation and brand image.

Mainframe z/OS
For IBM mainframe customers using z/OS, Voltage SecureData now operates natively, providing a simple API that can be accessed by COBOL and other Language Environment (LE) programs to protect data, as well as an integration and scripting tool called z/FPE that enables bulk encryption and masking of z/OS data (CICS, DB2, IMS, QSAM, VSAM) – providing full end-to-end data encryption, accessible from within or outside the z/OS system.

HSM integration
Voltage SecureData now integrates with Hardware Security Modules (HSMs) to store cryptographic information in order to meet internal company security requirements. HSMs are widely accepted as an industry best practice for securing encryption keys that protect an organization's most sensitive data.

Direct Oracle database encryption
Encrypt structured data directly within your Oracle database, without creating extracts or building a separate encryption application.

Manage encryption across multiple servers. Voltage SecureData allows administrators to manage several servers from a single point, speeding updates and lowering operational costs.

Secure data in a cross-platform environment. Supports Windows, Linux, AIX, Solaris, HP-UX, z/Linux and z/OS.

Encrypt databases directly. With the Voltage SecureData Command Line, customers can encrypt data directly without building a separate encryption application or creating extracts.

Meet compliance requirements. Includes built-in PCI audit reports, comprehensive logging across infrastructure and integration with third party log management systems.

Integrate encryption in existing applications. Developers can add encryption with just two lines of code; competing products require as many as 100 lines to accomplish the same task.

Extended modes of encryption
Decrypt data, independent of the original identity used for encryption. Voltage SecureData supports

identity-based encryption using AES (IBSE), and includes command line and Web-based tools to enable symmetric key data decryption.

Extended modes of encryption

Decrypt data, independent of the original identity used for encryption. Voltage SecureData supports identity-based encryption using AES (IBSE), and includes command line and Web-based tools to enable symmetric key data decryption.