

Datasheet: Voltage SecureData™

Encrypting Content Wherever It Goes

Voltage SecureData supports multiple encryption options and automates key management to easily secure data within large data stores and legacy enterprise applications.

HIGHLIGHTS

- ▶ Requires few if any changes to underlying data schemas and applications
- ▶ Centralized, automated key management
- ▶ Flexible options to integrate encryption into your environment

The Hardest To Protect: Back-Office Data

Security experts agree that strong encryption offers the most effective protection against data breaches and privacy policy infractions. When it comes to large databases and enterprise applications, however, conventional options such as encryption proxies, column encryption or lookaside databases can be expensive, cumbersome and often times impractical to implement. Moreover, none of these approaches deliver all the features and functions—strong, persistent encryption; protected backup; online and offline capabilities—required in high-performance enterprise applications.

Bringing Legacy Systems and Operations Into Compliance

Voltage SecureData provides a highly cost-effective, low-impact method for securing sensitive information within even the largest data stores and enterprise applications. A major advance over existing encryption options, Voltage SecureData makes it possible to provision data privacy as a service across the enterprise. With a selection of encryption options and automated key management, the system is able to persistently secure sensitive data irrespective of location, and enable controlled access to data according to authorization policies and with full compliance auditability. As such, large organizations can now achieve policy compliance in their core enterprise operations by integrating transaction security into legacy business application frameworks that were previously impossible to address.

Encryption Where It's Needed

The problem with information security measures that focus on infrastructure (containers) or network resources (pipes) is that today's customer- and partner-centric work processes demand that sensitive, regulated information must be made available to systems that often lack the security and protection of core enterprise IT infrastructure. Voltage SecureData addresses this problem because it is designed specifically to protect content no matter where it goes. In fact, Voltage SecureData is the first information security offering to take advantage of Format-Preserving Encryption™ (FPE), an innovative new technology that secures data while at the same time preserving its original format. With FPE, it becomes possible to mask data in existing data stores, reports and files—one-way or reversibly. The advantage of this approach is that organizations can protect enterprise data within test environments, during batch processing or when sharing information with outside marketing services providers, ensuring policy compliance every step of the way.

Voltage SecureData In Action Life Insurance Processing Service

Hoping to bring its life insurance processing and payment application into compliance with the PCI privacy regulations, a leading financial services provider to credit unions and their members tried to implement a file-based encryption solution. Since this solution encrypted entire database files, however, the company encountered major problems with degraded application performance.

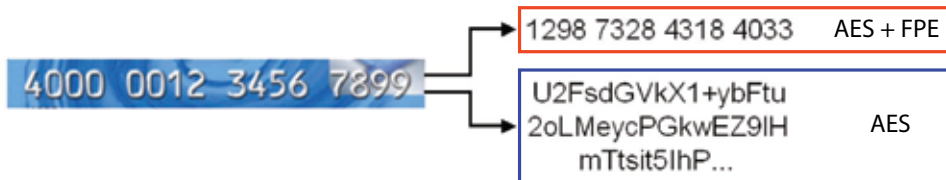
Turning to Voltage SecureData, the company was able to meet its PCI compliance objectives. Initially encrypting credit card data within the processors' SQL database, Voltage SecureData ensures that sensitive personal information is secured no matter where it travels downstream, even when exported to the company's third-party batch processor. With Voltage SecureData, the company can now:

- Enable policyholders to provide credit card numbers for billing purposes.
- Ensure data security without restructuring existing business processes or applications.
- Maintain PCI compliance without incurring large upfront costs or ongoing management requirements.

Global Financial Services Provider

During an internal audit, one of the world's largest insurance and financial services companies discovered that it had potential data leaks in its test environments. With more than 1,000 databases containing PII across the firm's global infrastructure, the implications were serious because the firm frequently moved sensitive information from these stores to the test environments for development projects. Plus, as an international firm, the company is subject to multiple U.S. and overseas privacy regulations. The challenge was to mask data flowing into test environments in order to prevent breaches yet preserve data formats necessary for application functionality. Implementing Voltage SecureData, the firm was able to do exactly that, and:

- Meet compliance goals with PCI, HIPAA, SB 1386 and European and Japanese privacy regulations.
- Protect production data using bulk encryption and ongoing application-level encryption.
- Leverage Voltage's stateless key management technology; eliminate the need for storage servers.



Where older encryption technologies radically alter the structure of data, Voltage SecureData maintains data format integrity, significantly minimizing changes to existing applications.

The Voltage SecureData includes:

Voltage Management Console

Centralized policy management and reporting across the entire Voltage SecureData solution

Voltage Key Management Server

Centralized Voltage IBE, FPE, and symmetric key management

Format-Preserving Encryption Preserving Critical Business Functions By Maintaining Data Format

Format Preserving Encryption (FPE) from Voltage is a fundamentally new process that makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. Unlike traditional algorithms that expand data into binary fields, FPE enables encrypted data to retain its original format, on a character-by-character basis, so that encrypted data "fits" in existing fields, eliminating the need for database schema changes. For example, a 16-digit credit card number can be encrypted, with the output guaranteed to also have 16 digits; the credit card checksum can even be maintained. FPE also preserves referential integrity, which enables encryption of foreign and indexed keys and ensures internal consistency in masked data. Through the use of FPE, Voltage SecureData provides highly efficient, robust data encryption and data masking that can typically be implemented with a fraction of the effort of competing systems.

- Supports data of any format, including numeric and alphanumeric.
- Allows format definition on a character-by-character basis.
- No database schema changes required—data "fits" in existing fields.
- Allows administrators to manage which applications get access to which elements of data.
- Guarantees against collisions through reversible encryption: 1-to-1 mapping between inputs and outputs.
- Deterministic encryption eliminates the need to keep track of data across disparate databases.
- Non-reversible encryption option makes original data unrecoverable, ideal for marketing purposes.

Voltage SOA Encryption Server

Centralized web services encryption option for SOA environments

Voltage Encryption Toolkit

High performance integration option for offline environments or build-in requirements

Voltage Command Line

Scriptable tool for bulk encryption operations

Stateless Key Management

Perhaps the largest barriers keeping organizations from implementing encryption to protect enterprise data are the upfront infrastructure costs and ongoing management requirements imposed by traditional public and symmetric key management systems. Long prevailing systems used randomly generated keys, which had to be backed up, replicated and distributed to ensure security and recoverability in case of a disaster. Voltage eliminates the expense and management requirements associated with legacy systems through its highly innovative “stateless” key management technology. With Voltage SecureData, encryption keys can be mathematically generated and re-generated on demand, obviating the need for complex backup and replication procedures. Voltage also incorporates an advanced, flexible authentication architecture that enables authentication and authorization to leverage nearly any existing mechanism. The result is an automated key management system that provides centralized control and auditing, while requiring little ongoing attention from IT security administrators.

Flexible Integration Options

The second biggest barrier to data store security has been integration: how exactly do you build encryption into very large, very advanced enterprise applications that can’t be recoded, or into critical transactional mainframes that can’t be taken offline? Voltage SecureData solves these problems by offering three distinct methods of incorporating encryption into your critical systems.

Voltage Command Line

The Voltage SecureData command line interface for encryption and/or decryption of files and data can be called via script or by any process capable of external execution. The command line option is the simplest method for integrating encryption into existing operations, and requires no coding. It is ideal for:

- Applications that require encryption but can’t be recoded
- Batch operations performing bulk encryption or decryption of files prior to processing
- Integration via existing IT resources rather than through expensive new research and development efforts

Voltage Encryption Toolkit

In situations where encryption must be added directly into native application code, the Voltage Encryption Toolkit provides a full set of APIs and software tools for the job. Typically, the Toolkit is used for applications that require extremely high performance or that are fully or occasionally offline, and where administrators need to maintain full control over data formats.

Platforms:

- Windows
- Linux
- Solaris
- Mac OSX
- Forthcoming: z/OS, AIX, HP/UX

Voltage SOA Encryption Server

As more and more organizations turn to service-oriented architectures (SOA) to increase operational agility and shorten development curves, the ability to deploy encryption as a service will become more attractive, and even essential for reaching and maintaining policy compliance goals. The Voltage SOA Encryption Server is designed for just such scenarios, providing simplified APIs for enterprise application developers that free them to focus on business processes, not cryptography. The result is a faster learning curve, reduced time to market and fewer chances for security mistakes or weaknesses. The server's SOAP/JMS interfaces easily mesh with a variety of applications and platforms, and allow developers to shift away from monolithic cryptography libraries as their only integration option. By providing a way to achieve zero-footprint encryption, the Voltage SOA Encryption Server is ideal for:

- Transaction-oriented applications that need to quickly apply robust policies to data
- Development processes that require high-level APIs
- Services-oriented architectures

Faster. Less Expensive. More Effective.

Voltage SecureData offers nothing less than a dramatic leap forward in enterprise data protection. Even the largest global organizations now have a way to secure regulated content such as Social Security Numbers (SSNs), credit card numbers and personal health information stored in large databases, without exorbitant cost or performance-degrading changes to existing systems. VoltageFormat-Preserving Encryption technology drastically reduces the need for application re-engineering, and eliminates altogether the database schema and format changes imposed by less advanced encryption offerings. In addition, with Voltage's automated key management and flexible integration options, bringing encryption to existing applications or developing secure new applications has never been quicker or easier. The result for companies facing a highly regulated, privacy-minded business landscape is the fastest remediation for PCI and other privacy regulations: up to five times quicker to compliance reduction at one-fifth of the cost associated with less advanced approaches.

About Voltage Security

Voltage Security, Inc., an enterprise security company, is the global leader in information encryption. Based on next generation cryptography, Voltage solutions provide encryption that just works for protecting sensitive information persistently and based on policy. Voltage delivers the lowest total cost of ownership in the industry through the use of award-winning Voltage Identity-Based Encryption (IBE) and Format-Preserving Encryption (FPE). Offerings include Voltage SecureMail™, Voltage SecureFile™, Voltage SecureData and the Voltage Security Network™ (VSN), a Security as a Service (SaaS) solution for the extended business network. For more information visit <http://www.voltage.com>.