Voltage security

DATA SHEET
Voltage SecureData z/Protect

Simple Standards-based Encryption for z/OS Mainframe Data

AN EASILY INTEGRATED, COMPREHENSIVE, NATIVE SYSTEM Z SOLUTION FOR CICS AND OTHER Z/OS ENVIRONMENTS (BATCH, DB2, IMS, IMS, ET AL.). IT'S NOT JUST A NEW WAY TO PROTECT MISSION-CRITICAL ENTERPRISE DATA END-TO-END, BUT A NEW WAY TO PROCESS PROTECTED DATA.

Reduces Audit/Compliance Scope and Risk of Data Theft

Voltage SecureData z/Protect™ minimizes application changes, since Voltage Format-Preserving Encryption™ (FPE) means that data size and character set do not change when data is encrypted. Most applications can thus operate on the encrypted data without decrypting anything, reducing the number of applications in scope for compliance auditing.

Voltage SecureData z/Protect also provides role-based data access, which is impossible with traditional all-or-nothing full database encryption. With Voltage SecureData z/Protect, key access is controlled using native z/OS security methodologies (RACF, ACF2, Top Secret). This avoids the need for applications to store credentials, further reducing the exposure of sensitive information for hackers to steal. Because the business environment now has a reduced number of applications accessing sensitive data in its live form, audit and compliance scope are reduced where there is no ability to decrypt the data. Additionally, in the event of a breach, the hacker only possesses useless encrypted data, thus greatly reducing the risk of data theft.

Preserve and Extend Mainframe Security

As secure as the mainframe is and always has been, it needs new ways to protect data as the boundary blurs between its traditional cocooned data center and today's highly connected but more risk-prone online transactional world. Enterprise security requires protecting personally identifiable information (PII), wherever used, via a scalable approach that works across business applications, rather than securing individual applications with piecemeal solutions. And the approach should also minimize having live (unencrypted) data on production systems.

The traditional approach of encrypting full databases or data sets is cumbersome, inefficient, and counter-productive: it imposes significant overhead on every data access, increases DASD required, imposes data format changes, and can leave upper application layers vulnerable. Voltage SecureData z/Protect makes it easy to implement and manage data protection on z/OS—natively and with full interoperability with other Voltage SecureData™ components.

Reduce Implementation Cost, With No Disruption to Existing Processes

Enterprise encryption has always entailed significant application and database redesign, due to data format changes. With Voltage SecureData z/Protect, encrypted fields are the same length and format as their original data. Database schemas and file layouts are unchanged. Indexes and JOINs still work, since a given value encrypts to the same ciphertext in all databases. This all means that only a small fraction of the applications that use the data need to be updated. Most applications can operate on the encrypted values: only the few trusted applications that actually need the live data need changes.

Highlights

- Adds native encryption with minimal or no program or data structure changes
- Reduces audit scope by eliminating application specified credentials
- Builds on existing z/OS security (RACF, ACF2, Top Secret) granular controls
- Isolates via built-in z/OS and System z hardware facilities, cannot be subverted by flawed or malicious application programs
- Works with a wide range of technology requirements
- Minimizes application changes and controls live data access
- Enables role-based data access

Another significant cost of implementing encryption has been training application programmers. The traditional approach to encrypting data has required knowledge of key management and cipher choices; this complexity makes it easy for application groups to introduce subtle errors, leading to integrity and consistency problems, or even data loss. With Voltage SecureData z/Protect, all encryption control is centralized in the z/Protect configuration. Training applications programmers is simple, and opportunities for error are greatly reduced.

Features

Centralized Control and Management

The centralized design of Voltage SecureData z/Protect not only means better control, but also enables faster auditing. Every encryption operation can be accounted for, on a per-user or per-application basis. As encryption usage grows throughout the enterprise, this allows verification of whether applications are using encryption as mandated, and also allows charge-back to business units for resources used. Standard z/OS SMF data can be generated, fitting into enterprise performance tuning and capacity planning processes.

Satisfies Multiple Technology Requirements

A significant z/OS security shortcoming is the lack of encryption developer abstraction for Customer Information Control System (CICS), used by 80% of z/OS customers. Voltage SecureData z/Protect provides fully compatible encryption services across all z/OS environments. This allows the Voltage SecureData platform to provide comprehensive cross-application and cross-platform compatibility, speeding application implementation and security retrofitting, and minimizing training requirements.

> *Voltage has helped us approach security beyond simply maintaining compliance. We now protect data persistently and transparently across the sophisticated data flows within BJ's Wholesale, without the disruption and complexity of traditional approaches. With Voltage SecureData z/Protect, we can add encryption to applications seamlessly.*
>
> *– Cherri Heart*
> *CISO, BJ's Wholesale Club*

Voltage SecureData z/Protect isolates critical processing from application programs: CICS transactions call a minimal application programming interface (API), which transfers the request to a started task that performs the operation and returns the results. This universal z/OS API allows new application groups to quickly exploit Voltage SecureData z/Protect as more data is brought under its protection.

Voltage SecureData z/Protect introduces "Cryptids", defined in the started task configuration and combining data format and identity into a single named entity. With their up to 64-character customer-defined names, Cryptids are much easier to use and manage—and are less error-prone—than ciphers, key names, options, etc. Centralized administration ensures that applications use correct encryption, and provides granular controls, such as limiting which users can encrypt/decrypt. In addition, application programs don't need security credentials because the job owner or CICS userid provides authentication. The started task architecture also facilitates auditing operations (answering, "How much does application XYZ use encryption?") and chargeback (billing for each operation, if desired).

Rich Function Set

Besides Format-Preserving Encryption, z/Protect Cryptids can perform a rich set of other cryptographic operations: Advanced Encryption Standard (AES), Voltage Secure Stateless Tokenization™ (SST), Base 64 encoding/decoding, and a variety of digest functions. These all use the same API, further simplifying use by application programmers.

Interoperates with Voltage SecureData Platform

Because it is built on the same technology as the rest of the Voltage SecureData family, data encrypted with Voltage SecureData z/Protect can be decrypted using other Voltage SecureData Enterprise components, and vice versa. This includes crossing the ASCII–EBCDIC chasm: Format-Preserving Encryption means that just as a given plaintext value such as "abcdef" can be translated between ASCII and EBCDIC, so can its encrypted equivalent. When decrypted, the results are identical, in the local character set.

About Voltage Security

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.
For more information, please visit **www.voltage.com**.

v02-22-2013