



Voltage SecureData Sentry

Voltage SecureData Sentry simplifies and accelerates the adoption of strong data-centric security in cloud-based services and on-premises applications. Voltage SecureData Sentry swiftly enables new value creation and privacy policy compliance while avoiding application code changes.

Product Highlights

Opportunity and Challenge in Hybrid IT Adoption

Today's data-driven enterprises face dissolving organizational boundaries. The adoption of cloud applications ensures data is constantly flowing to and from on-premises systems and cloud services. This includes SaaS applications, commercial off-the-shelf (COTS)

Key Benefits of Voltage SecureData Sentry

- Simplifies data protection for a wide range of applications without modification
- Accelerates time-to-value with flexible deployment of data security across hybrid IT
- Maintains centralized enterprise control over encryption keys and data in cloud services
- Promotes a non-disruptive approach to privacy compliance and the secure use of data
- Provides flexibility to choose from Voltage Format-Preserving Encryption, Secure Stateless Tokenization, and Format-Preserving Hash protection methods at a field level
- Enables interoperability of encrypted data between multiple SaaS applications, independent of company size or geography

of applications and databases. The solution supports different content formats and protocols with a mix of protection mechanisms.

Sentry uses proxy interception and API technologies to support a broad variety of SaaS applications, such as Salesforce, ServiceNow, ALM Octane, Microsoft Dynamics 365, and others. The solution accesses and protects sensitive data flowing through the network, ensuring organizations remain in control of data used in cloud applications. The same technology can be used to secure COTS and in-house applications, providing an alternative to API integration that avoids the need for programming. Voltage SecureData Sentry's inspection mode identifies the data fields in your target applications, allowing easy configuration of field-level protection.

Accelerate Data Protection Time-to-Value Organizations adopt cloud-computing strategies to gain market advantage and realize economic savings, such as reduced operating expenditures. But for sensitive corporate intellectual property and personal data, such as financial and medical records, adopting new cloud services imposes business and compliance risks. Protecting such personally identifiable data at the field level minimizes potential exposure of sensitive information, and can reduce audit scope and compliance costs. Moreover, through additional innovations, such as secure local indices supporting partial and wildcard search terms, and secure email address formatting for SMTP relaying, Voltage SecureData Sentry preserves cloud application functionality that is impacted by competing solutions. Persistent protection of high value data unleashes new benefits for organizations to more safely take advantage of elastic computation models and third-party analytic options that better serve the business.

Unlike most SaaS and cloud CASB security models, because Sentry enables organizations to retain authority over their own cryptographic keys and token tables, and simplifies security deployment to a wide

range of use cases and applications, it allows enterprises to maintain control over their business data, end-to-end, throughout its lifecycle. The consistent protection and referential integrity that results permits the portability of the protected data between multiple services and environments. By reducing the effort required to protect data in applications, and reducing risk of data exposure, Voltage SecureData Sentry not only speeds an organization's time-to-value and return on investment in data-centric security, but also in hybrid IT by removing blockers to adoption.

Rather than replacing CASB solutions, Sentry coexists with brokers that specialize in the provision of complementary technologies, such as shadow IT visibility, DLP, and malware detection, and augments data security by taking care of the cryptographic heavy lifting to add strong data-centric protection mechanisms that can be applied across SaaS and other cloud services as well as to commercial and self-developed applications in internal networks.

Reduce Risk of Data Exposure

Voltage SecureData Sentry simplifies deployment and extends the reach of Voltage by OpenText's market-leading data protection technologies, including Format-Preserving Encryption (FPE), Secure Stateless Tokenization (SST), Stateless Key Management, and Format-Preserving Hash (FPH). Voltage SecureData Enterprise by OpenText de-identifies data, rendering it useless to attackers, while maintaining its

detection (A)14 (SB solution)Tj T*simplurity bNIST onT FF1 AES

Voltage by OpenText de-identifies data, rendering it useless to attackers, while maintaining its integrity and availability. This is achieved through a combination of techniques, including Format-Preserving Encryption (FPE), Secure Stateless Tokenization (SST), Stateless Key Management, and Format-Preserving Hash (FPH). Voltage SecureData Enterprise by OpenText de-identifies data, rendering it useless to attackers, while maintaining its integrity and availability. This is achieved through a combination of techniques, including Format-Preserving Encryption (FPE), Secure Stateless Tokenization (SST), Stateless Key Management, and Format-Preserving Hash (FPH).

