

# Voltage SecureData Sentry

SecureData Sentry simplifies and accelerates Voltage data-centric security deployment in cloud, commercial, and in-house applications without critical application changes or integration required. SecureData Sentry brokers data privacy to enable new value creation and policy compliance on protected data.

## 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) applications, and in-house proprietary applications. But strict privacy regulations, such as General

Data Protection Regulation (GDPR), PCI DSS, and HIPAA, along with limited trust in hosted environments, make the protection of personal data imperative, anywhere such data may exist.

### Data Security Ease of Deployment

Voltage SecureData Sentry accelerates implementation of data security on-premises and in the cloud. This addition to the SecureData portfolio is a data privacy broker that deploys easily into existing infrastructure. It transparently

## 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, transparent approach to privacy compliance and the secure use of data
- Provides flexibility to choose from Voltage Hyper Format-Preserving Encryption, Hyper 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



protects data fields and files flowing to or from the cloud, and in and out of applications and databases. The solution supports different content formats and protocols with a mix of protection mechanisms.

Sentry leverages 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. 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. 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 SecureData Sentry centralizes management on-premises, enabling organizations to retain authority over their own cryptographic keys and token tables, and simplifying 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, 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.

### **Reduce Risk of Data Exposure**

SecureData Sentry simplifies deployment and extends the reach of Voltage market-leading data protection technologies, including Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), Stateless Key Management, and Format-Preserving Hash (FPH). Voltage SecureData de-identifies data, rendering it useless to attackers, while maintaining its value for business processes, applications, and services. SecureData neutralizes the impact of a data breach by making protected data worthless to an attacker, whether it is in production, analytic systems, or test/development systems.

Leveraging the NIST FF1 AES encryption standard, Voltage SecureData is unique in being the only FPE product to be Common Criteria certified, and FIPS 140-2 validated. Micro Focus Data Security's support for NIST, ANSI, IEEE, and IETF standards—and transparent peer review from independent security assessment specialists—helps ensure the highest security assurance level certifications for its products. The trust organizations place in Micro Focus data security is backed by independent world-class analysis.

### **Enable Data Privacy Compliance with Ease**

Efforts to strengthen regulations for personal privacy protection are underway in many countries and regions, and time pressure to swiftly address compliance mandates is increasing. For example, the EU has introduced the GDPR

to strengthen data protection for all residents. The GDPR recommends anonymization and pseudonymization as methods to protect personal data. SecureData Sentry enables a non-disruptive approach to address privacy compliance by leveraging Voltage encryption and tokenization—two industry-leading methods of pseudonymization, a form of data de-identification in which the protected information can still be used in business processes, and be able to be securely re-identified.

Format-Preserving Hash (FPH), the newest innovation in Voltage data protection methods, provides non-reversible de-identification, supporting the GDPR's Article 17, the right to erasure—often referred to as "the right to be forgotten"—which calls for anonymization. Voltage FPH offers one-way transformation with the strength and use case versatility of FPE, working with existing database schemas and applications without change and without disabling the use of data analytics.

### **Sensitive Data Detection and Interoperability**

SecureData Sentry protects or accesses sensitive data according to policy, with centralized, on-premises, enterprise control and end-user transparency. It supports a variety of content formats, including JSON, XML, HTML, docx, xlsx, csv, and more. SecureData Sentry accesses data streamed over key communication protocols, including HTTPS and SMTP, and through popular APIs, including REST, SOAP, JDBC, and ODBC.

The ability to support JDBC and ODBC protocols with consistent protection, and stateless key management for high scalability on premises and into the cloud, is unique in the market today for enabling enterprise-class performance. SecureData Sentry enables interoperability of encrypted data between multiple SaaS applications, secure outsourcing, and similar use cases, independent of company size or geography.

# SecureData Sentry Conceptual Architecture

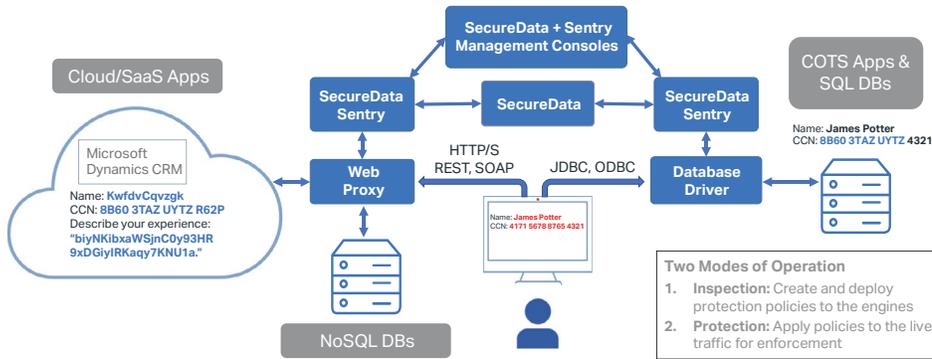


Figure 1. SecureData Sentry consistent and transparent data protection, on premises and in the cloud.

Contact us at:  
[www.microfocus.com](http://www.microfocus.com)

## Key Functionality

### SaaS applications

- Data privacy broker functionality for transparent data protection in externally hosted cloud applications such as Salesforce, Microsoft Dynamics and ALM Octane.

### COTS and in-house applications

- Data privacy broker functionality for transparent data protection of commercial off-the-shelf (COTS) applications and in-house enterprise applications.

### Data Intercept

- Data intercept over key communication protocols, including ICAP/S, HTTP/S, and SMTP, and through popular APIs, including REST, SOAP, JDBC, and ODBC.

SecureData Sentry Components	Description
SecureData Sentry Management Console	Role based administration interface to manage Sentry, fully audit enabled. Policy creation based on application and document types, and/or regulatory requirements.
SecureData Sentry Server	Content discovery, and data protection and access, scalable with HA and load-balancing options. High performance; supports forward and reverse proxies, and database drivers.
SecureData Sentry Privacy Services for Databases	Services to protect data in databases, supporting ODBC and JDBC, as well as REST for NoSQL databases.
SecureData Sentry Protection Mechanisms	Methods that support Voltage Hyper FPE, SST, FPH, static and dynamic data masking, and stateless key management, with all different content formats.

## SecureData Sentry Architecture

SecureData Sentry uses the Voltage Secure-Data platform common infrastructure. This enables enterprises to choose an appropriate combination of encryption techniques for data de-identification to address their use cases

across diverse environments, while avoiding the costs and complexities of deploying and managing multiple products.

Learn More At  
[software.microfocus.com/products](http://software.microfocus.com/products)