OpenText Voltage SecureData Sentry

Simplifies and accelerates the adoption of strong data-centric security in cloud-based services and on-premises applications

Benefits

- 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 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

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

Easy deployment

OpenText™ Voltage™ SecureData Sentry accelerates implementation of data security on premises and in the cloud. This addition to the OpenText Voltage SecureData portfolio by is a data protection and privacy broker, which deploys easily into existing infrastructure. It 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.

The solution uses proxy interception and API technologies to support a broad variety of SaaS applications, such as Salesforce, ServiceNow, OpenText Software Delivery Management, and Microsoft Dynamics 365. 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.

Key functionality

SaaS applications

- Data privacy broker functionality for transparent data protection in externally hosted cloud applications such as Salesforce, Microsoft Dynamics and OpenText Software Delivery Management.

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.

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, Sentry preserves cloud application functionality that is affected 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.

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, unlike most SaaS and cloud CASB security models. 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, 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

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

The OpenText portfolio's data security development of the NIST FF1 AES encryption standard has enabled OpenText Voltage SecureData Enteprise to be the only FPE product to be Common Criteria certified, and FIPS 140-2 validated. OpenText's data security's support for NIST, ANSI, IEEE, and IETF standards—and public peer review from independent security assessment specialists—helps ensure the highest security assurance level certifications for its products. The trust organizations place in OpenText 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's GDPR recommends anonymization and pseudonymization as methods to protect personal data Sentry enables a non-disruptive approach to address privacy compliance using OpenText 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.

OpenText's Format-Preserving Hash (FPH) 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. 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

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. 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. Sentry enables interoperability of encrypted data between multiple SaaS applications, secure outsourcing, and similar use cases, independent of company size or geography.

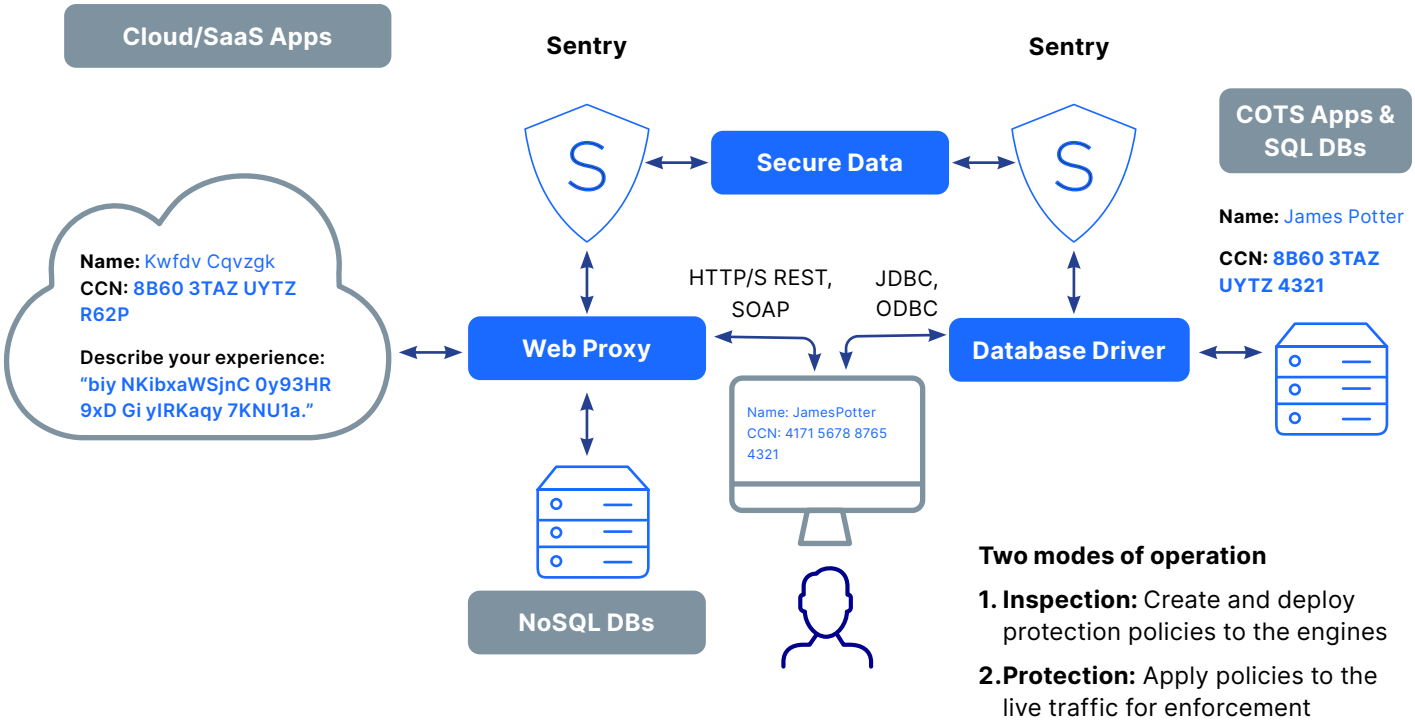

Figure 1. Sentry's consistent and transparent data protection, on premises and in the cloud.

Sentry components	Description
Sentry Management Console	Role0based administration interface to manage Sentry, fully audit-enabled. Policy creation based on application and document types, and/or regulatory requirements.
Sentry Engine	Content discovery and data protection and access, scalable with HA and load-balancing options. High performance; supports forward and reverse proxies, and database drivers.
Sentry Privacy Services for Databases	Services to protect data in databases, supporting ODBC and JDBC, as well as REST for NoSQL databases.
Sentry Protection Mechanisms	Methods that support OpenText FPE, SST, FPH, and stateless key management, with all different content formats

Sentry architecture

Organizations can deploy Sentry on premises and/or in the cloud. It communicates with ICAP (Internet Content Adaptation Protocol) capable network infrastructure, such as HTTP proxies and load balancers, to apply security policies to data traveling to and from the cloud, and it intercepts JDBC (Java Database Connectivity) and ODBC (Open Database Connectivity) API calls to apply security policies to data traveling to and from the database. Wherever it is deployed, the enterprise retains complete control over the infrastructure, without the need to share encryption keys or token vaults with any other party, and Sentry's inspection mode ensures that security policies can be targeted at the specific data fields and file attachments that contain sensitive information.

Sentry uses the Voltage SecureData Enterprise 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 Voltage SecureData ›

opentext™