opentext™ | Cybersecurity

Position Paper

Secure Sensitive Data with Voltage Structured Data Manager and Voltage SecureData Enterprise

Table of Contents

Meet the Latest Structured Data Management Requirements and Protect Sensitive Data

The next generation of structured data management (SDM) technology has far more to accomplish than its earlier predecessors. Now, with the explosion of data and the regulatory pressures such as the General Data Protection Regulation (GDPR), companies have to enforce solid policies and procedures across the full information lifecycle. While it is critical to effectively manage information in general, the risk is even higher when it comes to managing sensitive information. Data encryption requirements also add complexity, particularly if your existing solution is unable to preserve format and element size when encrypting.

With a comprehensive structured data management solution, you can:

- Automate the process of managing data from old applications
- Reduce cloned and legacy data, which lowers storage, hardware, maintenance, and admin costs
- Enhance operational efficiency by removing inactive data and remaining SLA-compliant
- Cut risk by automating the way you discover and protect sensitive data
- Improve search and eDiscovery with better visibility over previously dark data
- Encrypt data while preserving format and element size

Although performance, storage, and IT resources are a budget mainstay for managing applications, the current landscape brings bigger concerns with regulations, compliance, and data security requirements. Some businesses may not realize how large the risks are when securing, encrypting, and managing sensitive structured data.

Voltage Structured Data Manager (SDM) by OpenText enables organizations to secure data according to the latest compliance and protection requirements, including GDPR. In addition, Voltage SDM integrates with Voltage SecureData Enterprise by OpenText, to encrypt sensitive data in place or in the archive using Format Preserving Encryption (FPE). FPE makes it possible to integrate data-level encryption into legacy business applications. This complete solution allows you to manage high volumes of data with solid processes and analytics to overcome slow performance and meet tightening compliance requirements.

The latest version of Voltage Structured Data Manager V7.5 offers:

- **Integration with Voltage SecureData Enterprise**—Encrypt sensitive data in place, or in the archive, or in your test and development databases.
- **In-place data masking**—Mask or intelligently encrypt database data in place, by acting on production instances. This allows you to manage not only archive databases, but the full relational database management system (RDBMS) lifecycle, to protect all data and adhere to the latest GDPR guidelines.

- **PII discovery**—Use Voltage SDM to discover sensitive data, document it, and act on it, with out-of-the-box industry templates (social security, credit cards, names, addresses, etc.) that let you customize processes to your industry, to meet unique compliance requirements.
- **Compliance documentation & reporting**—Document all steps taken to discover and secure personal data.

New Structured Data Management Challenges

All businesses must meet new regulations that will affect how structured information is processed, particularly for those with sensitive data under management. New regulations are not only requiring encryption of the information—the data must also be managed in ways that were not foreseen when earlier data management applications were first designed and implemented.

Many countries require organizations to be more responsive and clear about how they protect the personal data of users, employees, customers, partners, and suppliers. Using technology that can address these issues comprehensively gives your business an opportunity to finally understand where data resides and then manage it according to pending regulations, such as the General Data Protection Regulation (GDPR).

The Impact of New Challenges

A number of standard and known impacts arise when large volumes of structured data are not effectively managed. For example, decreased application response time, slow performance, increased storage costs, and increased backup times. As the data management landscape changes with the introduction of new regulations, additional effects result when SDM technology is not up to the task, and these effects can spread across the business in areas such as:

- **Data loss:** If data is not categorized correctly, mismanagement of sensitive data can result in potential loss.
- **Regulatory fines:** Regulators now need to know what data you maintain and how you are protecting it. The fines for not meeting regulations vary by data type and have become significant, beyond the cost of protecting the data.
- **Damage to corporate brand and loss of customer confidence:** Breaches of sensitive customer data are regular front page news. The damage to the brand reputation may not be immediately quantifiable, but typically has lasting effects, greater than individual fines.
- **Unprotected data moved into an archive:** Protecting production data may be a number one priority, but if archived data is unprotected and then breached, it can have the same negative consequences.
- **Unencrypted data in an archive:** In the same avenue as protecting archived data, data should also have the same encryption. In place or in the archive, encrypting the data based on its sensitive nature is a must.

Putting Voltage Structured Data Manager to Work in Your Organization

Voltage SDM helps CIOs and CISOs reduce the cost and risk of managing archived data and applications by securing and masking sensitive data in compliance with global privacy and protection regulations such as the GDPR.

Application Managers can effectively handle application retirement or upgrades, to minimize disruption to services during retirement. By having access to archived data, managers can get to data stored in applications with no suitable upgrade or migration path, to keep inactive but sensitive data (that must be maintained for regulatory and business continuity reasons) in a secure, accessible, and usable manner.

Line of Business Managers can maintain control over data they own and create as it is shared across the organization, while protecting intellectual property from competitive leaks.

Performing Data Discovery in Voltage Structured Data Manager

Voltage SDM Version 7.5 introduces the ability to discover sensitive data, including Personally Identifiable Information (PII) data stored in databases in many formats. Voltage SDM has pre-configured templates to discover sensitive data such as credit card numbers, social security numbers, and names and addresses.

If your organization has industry-specific data that you want to locate; for instance, a trade ID in the financial sector, Voltage SDM can handle your unique requirements. Several out-of-the-box grammars are provided to automate cumbersome processes and significantly improve efficiency and effectiveness as as you address key compliance requirements for finding specific sensitive data.

How to Locate and Protect Sensitive Data

Voltage SDM can assign data a specific field type, or certain data can be placed in a Variable Character field (that is not specified for sensitive data). For example, if someone inputs a credit card number into a Notes field instead of a Credit Card field, the Data Owner may not have the same process to protect this field. Voltage SDM can take action based on the field type to help you locate and protect sensitive data in place, or in the archive.

The Voltage SDM Discovery module is project based, and each Discovery Project in Voltage SDM has a dashboard showing To Do items, Risk Areas, Sensitivity by Classes, and Progress. There is a set of grammars included out of the box. A grammar shows the set of rules that determine the sensitive data. These grammars provide you with templates that let you find data such as bank account numbers, credit card info, and addresses. Grammars are broken down into information classes, including Personal, Contact, Financial, Health, and Other.

> **“[Voltage] Structured Data Manager takes a unique approach to storing, managing and extracting value from structured data that is based on a robust selection of pre-built integrations to cloud storage, comprehensive information management systems and high performance analytics platform. … solution provides excellent flexibility and quick return-on-investments for enterprises of all sizes.”**
>
> **Sara Radicati**
> The Radicati Group

Grammars are also extensible and configurable to allow you to add custom templates for your industry.

Analyzing Uncovered Data

As data is found, you can use Voltage SDM to review columns individually or in bulk. Each column can be scanned for sensitivity as well as the type of sensitivity. Reviews can be indicated with a conclusion and notes for future reference in the dashboard. The review can indicate the number rows scanned, empty rows, and other information such as patterns and aliases.

Fulfilling the GDPR and Data Privacy Requirement

As more regulations are signed, one in particular, GDPR, becomes enforceable in May of 2018. The reach of this regulation extends to businesses in the European Union (EU) that process personal EU citizen data. The regulation also impacts businesses *outside of the EU* that process personal EU citizen data. The cost for non-compliance has severe penalties of up to 4% of worldwide turnover.

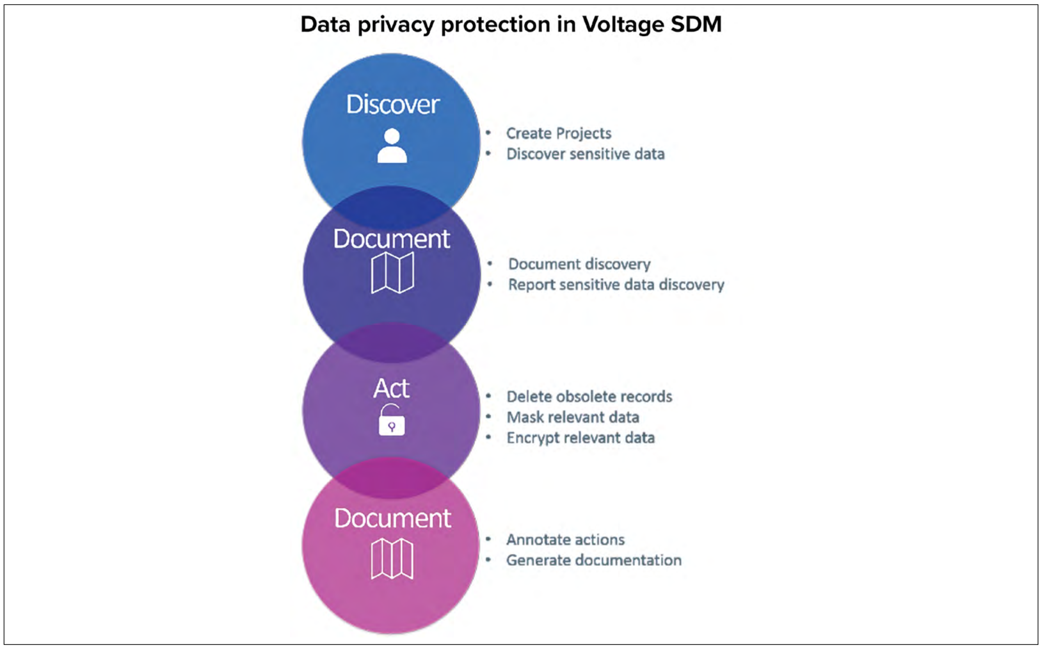

Figure 1. Data privacy protection in Voltage SDM

The immediate need to fulfill GDPR requirements does not only effect the IT department, but also the business as a whole and its holistic approach to managing the full data lifecycle. Considerations must be made for data across all environments. If a customer's personal data is located in a production database, an archive, or a test database, the breach can still affect that person all the same.

Organizations have to make decisions based on the context of different types of data whether it should be deleted in a defensible manner, or masked to protect it. Organizations are wise to consider the following:

- **Do you know if the data meets encryption requirements for compliance?** Regulations such as GDPR specify how encryption must be done, and how data should be encrypted throughout the processing lifecycle.
- **Do you have proof that you protected the data?** With Voltage SDM, you can protect the data, and maintain a record for auditors and regulators to prove that such actions have been taken. The documentation of encryption activities is saved in a report for archiving with the data or for reference.

Voltage Structured Data Manager and Voltage SecureData Enterprise Integration

The ability to encrypt sensitive data in place or in the archive is enabled with Voltage SecureData Enterprise. The Voltage SDM–Voltage SecureData Products Integration integration supports Format Preserving Encryption (FPE), which makes it possible to integrate data-level encryption into legacy business applications. For example, the format of a credit card number with four sets of four digits is maintained when encrypted. The result is a strong encryption scheme that provides encryption with only minimal modifications to the way existing applications work.

By maintaining the usability of data in protected form, Voltage SecureData Enterprise creates end-to-end data-centric protection over the entire data lifecycle—from the point of capture, throughout the movement of the data across the extended enterprise—all without gaps in security. Hyper FPE delivers strong and flexible encryption to protect EU citizen’s personal data and follows pseudonymization guidance in the new GDPR.

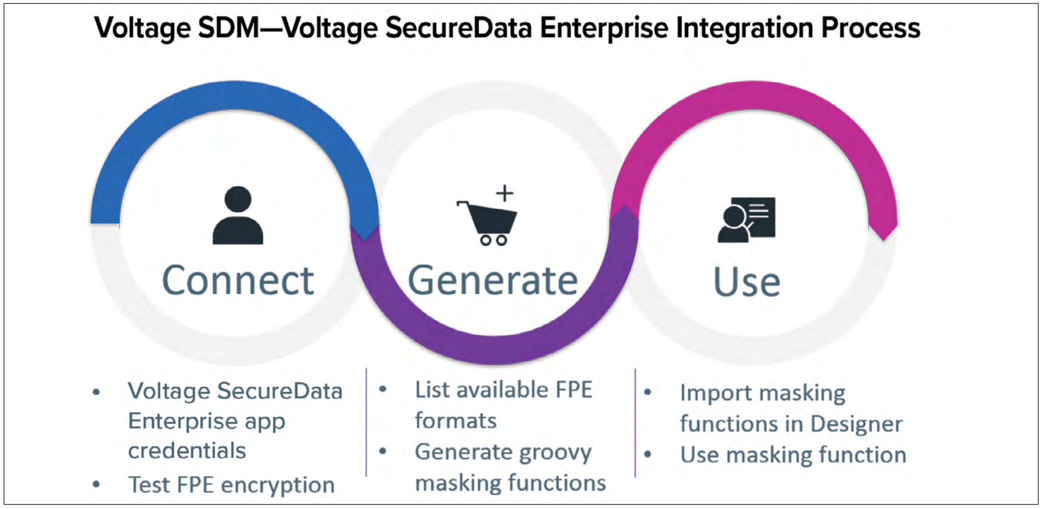
Voltage SDM—Voltage SecureData Enterprise Integration Process
Connect
Generate
Use
Voltage SecureData Enterprise app credentials
Test FPE encryption
List available FPE formats
Generate groovy masking functions
Import masking functions in Designer
Use masking function

Figure 3. Voltage SDM

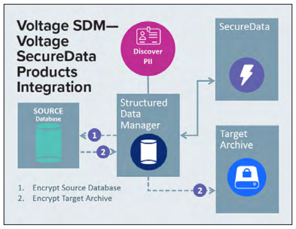
Voltage SDM—Voltage SecureData Products Integration
Discover PII
SecureData
SOURCE Database
Structured Data Manager
Target Archive
1
2
2
1. Encrypt Source Database
2. Encrypt Target Archive

Figure 2. Data protection and usability

Data Protection and Usability

Voltage SecureData Enterprise with Hyper FPE maintains data usability for analytics and business processes, ensuring protection without loss of competitive edge. Voltage SecureData Enterprise encrypts virtually unlimited data types, including IDs, VINs or bank accounts, while preserving their formats, so they can flow through existing databases and applications with minimum impact. Hyper FPE also maintains relationships, context and meaning of data so that analytics can be performed on de-identified data. That, combined with Voltage SecureData Enterprise granular policy control, enables wide access to de-identified data, powering big data, cloud, and IoT initiatives while using policy management control to limit access to highly sensitive data.

Connect, Generate, and Use Data with Voltage SecureData Enterprise

Voltage SecureData Enterprise with Hyper FPE is a National Institute of Standards and Technology (NIST) standard and uses FF1 AES Encryption. The NIST standard provides an approved and proven data-centric encryption method. With this integration, Voltage SDM enables your business to protect only the data that needs protecting, with industry leading encryption technology.

Using the integration starts with a connection to the Voltage SecureData Enterprise appliance. This enables functions such as reversible or non-reversible encryption to be available in Voltage SDM designer so that you have options to protect sensitive data. During archiving, in place or to a target archive or test database, the integration allows the process to encrypt your data selectively, and by transaction. This lets users work while their purchase orders, for example, are encrypted.

Five Things to Do to Assess Your Structured Data Management Preparedness

1. Start by understanding your data management objectives.
   - Check to see if business leaders and IT agree on and know the location of sensitive data.
2. Find out if you can comply with *current* regulations.
3. Find out if you can comply with *future* regulations such as GDPR.
4. Assess whether your current application stack enables your business to meet the previous questions.

If your current technology has gaps, consider consolidating into a broader archiving solution.

Your company's sensitive data is important to many stakeholders, including your employees, your business, and your customers, and this has always been true.

The requirement to protect this data is not simply an internal best practice. The penalties for failing to comply can jeopardize much more than the data—your success in the industry and financial standing could fall into jeopardy. Today's regulators know that businesses cannot hold huge volumes of sensitive data without solid data management solutions in place. For this reason, businesses should assess whether they have the right technology in place to proactively avoid an information breach and also provide secure data management capabilities within the organization and for external customers.

For more information on Voltage Structured Data Manager, visit
www.microfocus.com/en-us/cyberres/data-privacy-protection/structured-data-manager.

For more information on Voltage SecureData Enterprise, visit
www.microfocus.com/en-us/cyberres/data-privacy-protection/securedata-enterprise.

Learn More

Voltage Data Discovery by OpenText solutions can help detect, protect, and evolve as your business transformation journeys unfold.

Data discovery is mission critical and a fundamental part of data minimization, data privacy readiness, data protection, and data preservation—and can act as a catalyst for building greater data resiliency and supporting your broader cyber resiliency programs. Voltage Data Discovery solutions include:

- Voltage File Analysis Suite by OpenText
- Voltage Structured Data Manager by OpenText
- Voltage SecureMail by OpenText
- Voltage SmartCipher by OpenText
- Volatge SecureData
- OpenText™ Content Manager

www.microfocus.com/en-us/cyberres/technology/privacy-compliance

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.