opentext™ | Cybersecurity

Flyer

# Voltage Fusion for DORA Compliance and Data Security Posture Management

## Organizations that are leveraging a Data Security Posture Management (DSPM) solution are better equipped to comply with DORA and other privacy regulations.

### Safeguarding Data Confidentiality and Integrity

Risk and compliance concerns can create significant headwinds for organizations in today's evolving digital and regulatory environment. Improving data security and privacy postures and creating greater resiliency around processes, systems, and data are critical to building greater business stamina and responsiveness.

The dire consequences of data breaches underscore the need for a multi-faceted approach. The fusion of Data Security Posture Management (DSPM) and its core technologies, including data discovery, data protection, and database activity monitoring, ensures that information and communication technologies (ICT) that contain financial data remain managed and protected, and maintain their integrity throughout their lifecycle. Format-preserving data protection techniques like tokenization, encryption, and anonymization ensure secure data sharing and ethical use. At the same time, database activity monitoring provides real-time insights into data use and potential threats, safeguarding sensitive financial information and building greater resiliency in data security practices.

### The Digital Operational Resilience Act

As of November 2022, financial institutions operating in the EU under the requirements of the European Commission (EC) must comply with the Digital Operational Resilience Act (DORA) guiding data-driven digital transformation, and must become more consumer-centric, and resilient to withstand disruptions across their information and communication technologies (ICT). DORA helps align business strategy with ICT risk management and builds ongoing monitoring and prevention techniques to prevent and detect anomalous activities and minimize damage and disruption to business and financial operations.

### Resiliency and Monitoring Risk

Database monitoring can be beneficial to DORA compliance in several ways. DORA explicitly refers to ICT risk and sets rules on ICT risk management, incident reporting, operational resilience testing, and ICT third-party risk monitoring. By monitoring databases, financial institutions can detect and respond to potential security threats in real-time, helping to prevent data breaches

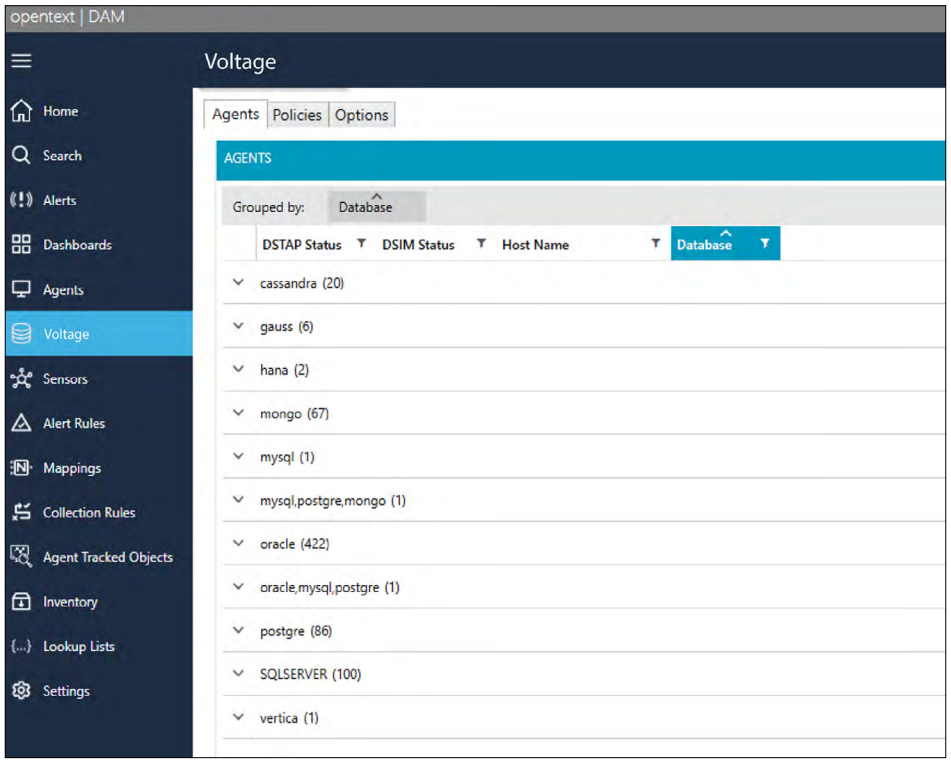



**Figure 1.** Voltage Database Activity Monitoring

and other security incidents with Voltage Database Activity Monitoring (VDAM) by OpenText. Voltage DAM can help improve overall operational resilience and ensure compliance with DORA's requirements for ICT risk management.

## Risk Mitigation and Prevention

Voltage DAM can assist with DORA requirements for ICT risk management. Voltage DAM can help organizations meet this requirement by monitoring and analyzing database activity in real-time, detecting and alerting anomalous activities, and providing detailed audit trails for compliance reporting. These capabilities can help organizations identify and mitigate risks to their information systems and networks and improve their overall ICT and operational resilience.

## Establishing Data Trust

DSPM technologies can help financial institutions identify and classify sensitive data for risk assessment and protect data at rest, in use, and in motion. In addition, DSPM can help maintain high standards of availability, authenticity, integrity, and confidentiality of data, as required by DORA. Financial institutions can demonstrate their commitment to protecting their customers' data and maintaining their trust by complying with DORA's data security standards through sensitive data tokenization and encryption, and database monitoring.

## Voltage Fusion for Data Security Posture Management

Voltage Fusion by OpenText DSPM and compliance solutions help organizations find, secure, and protect their most valuable data. Our portfolio includes:

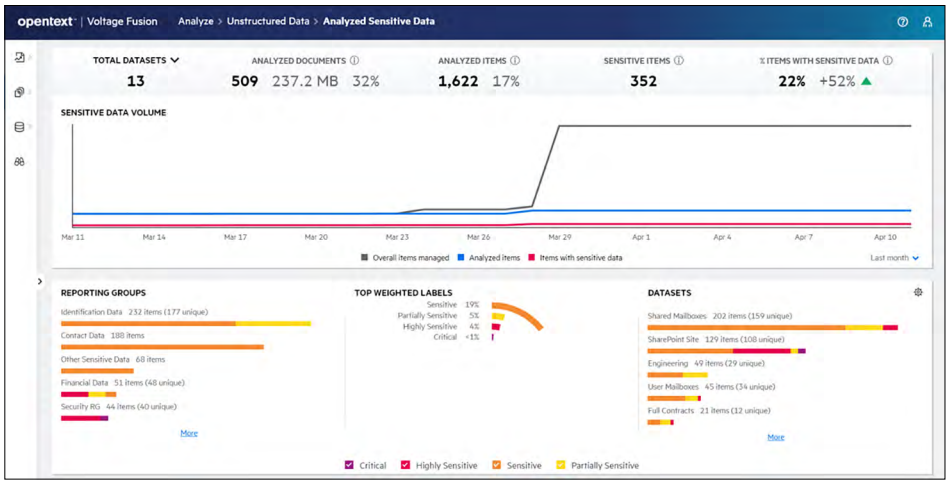



**Figure 2.** Voltage Fusion Analyzed Sensitive Data

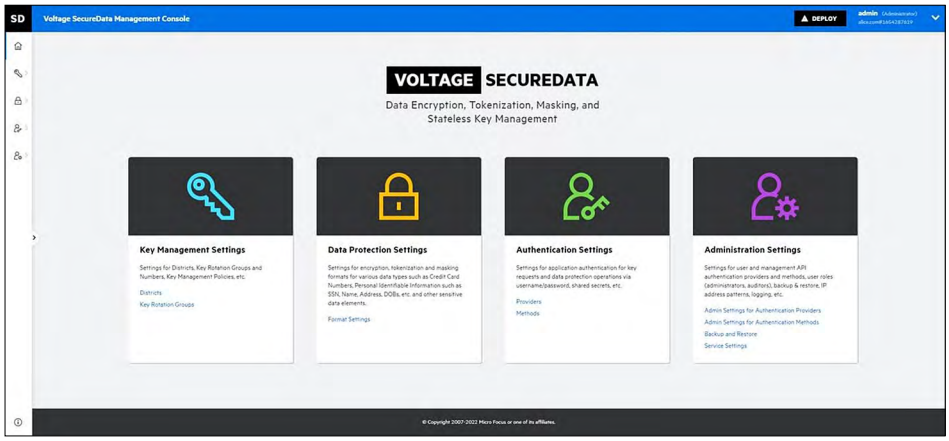
### Voltage Fusion Data Discovery

Voltage Fusion Data Discovery enables organizations to quickly find, classify, and protect sensitive, high-value data. Voltage Fusion provides complete visibility and insight across structured and unstructured data silos and helps contain data management costs while delivering actionable analytics that improve efficiency, data quality, and data privacy compliance. Contextually aware, AI-driven grammars reduce false positives and quickly identify high-value assets (e.g., contracts, intellectual property, patents, etc.) and personal and sensitive data types (e.g., PI/ PII, PCI, PHI, etc.). Voltage Fusion supports data masking/ anonymization, 3rd party tagging, including Microsoft Information Protection (MIP) for data protection, and supports use cases such as litigation hold, and long-term retention management to meet data preservation requirements.

### Voltage Database Activity Monitoring

Voltage Fusion Database Activity Monitoring (VDAM) is a powerful solution that monitors all database activities within an organization. VDAM actively monitors databases in real-time and generates alerts for any policy violations. VDAM works with Oracle DB, Microsoft SQL, IBM DB2, MongoDB, MySQL, and many more. VDAM's monitoring capabilities encompass various activities, including database administrator actions and application transactions such as data manipulation, schema modifications, access control changes, and transaction control. With VDAM, organizations can enable faster IT modernization and contain costs by retiring dormant data, improve their privacy posture through insights into applications interacting with sensitive data, and support green IT and sustainability mandates.

**Connect with Us**
www.opentext.com




**Voltage SecureData Enterprise**
Voltage SecureData Enterprise by OpenText provides an end-to-end data-centric approach for enterprise data protection. By providing privacy-enabling technologies including Voltage Format-Preserving Encryption (FPE), Format-Preserving Hash (FPH), Secure Stateless Tokenization (SST), and Stateless Key Management, SecureData protects sensitive structured data over its entire lifecycle—from the point at which it's captured and throughout its movement across the extended enterprise, eliminating security gaps. Voltage SecureData Enterprise "de-identifies" data, rendering it useless to attackers while maintaining its usability and referential integrity for data processes, applications, and services. Voltage SecureData Enterprise enables adopting a continuous data protection model wherever data flows, in analytic platforms and applications in hybrid multi-cloud environments and native cloud services.

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.