

Mitigating Risk with Voltage Data Discovery and Data Protection

High-value and sensitive data are what drive your business, but they increase your risk as well. Organizations need a holistic view of risk across both unstructured and structured data repositories to address how best to protect their “crown jewels.”

Voltage Data Discovery

Solution at a Glance:

Voltage Data Discovery helps organizations quickly find, protect and secure sensitive and high-value data.

Detect

Leverage AI-driven analytics to identify sensitive data, powered by IDOL

Protect

Highly sensitive data, consumer trust and corporate reputation

Evolve

To meet the growing data discovery workloads and drive operational excellence

Discovering and Protecting Sensitive Data

Data privacy has become a social movement and has grown beyond regulations and guidelines organizations need to follow to protect their data. As a result, the expectations of personal data privacy for your customers, employees, and others your business interacts with are now the norm. Customer data, intellectual property, and other corporate data need to be protected—in transit, in use, and at rest. Content analysis and data discovery can drive key business decisions, while improved insight helps protect critical business data, reducing risk while enabling secure information sharing—building a foundation for better risk management and privacy practices that build trust with customers.

Understanding Data

Connect to Data Repositories

To protect data, you must first understand where your risky data resides. Unstructured data repositories have long been a culprit for redundant, out-of-date, and trivial data—taking up space and the IT resources to manage the sprawl. Cloud-based file and object stores have become the modern-day equivalents as many organizations are simply moving the problem to the cloud. Without the appropriate level of controls and protection, structured applications and databases can grow and add further risk, if left unsupervised. Connecting to disparate

data repositories to evaluate the underlying risk across your ecosystem on-premises and in the cloud is a crucial step towards protecting data.

PII Detection—Understanding Context

Detecting personally identifiable information (PII) and personal information (PI) is at the core of protecting sensitive data. With over 80% of data being unstructured, the challenge shifts from simply detecting sensitive data to accuracy, confidence, and reducing false positives. Simple pattern matching will not be adequate in tackling today's data discovery workloads. You will need to understand, not only that a pattern match exists, but that the context of that pattern along with the contents of the document or file indicates that it is a “true” positive and should be protected. Context is critical to identifying sensitive data.

Analyzing Unstructured Rich Media

In many organizations, risky and sensitive data is not just present in emails, documents, and the rows and columns of business applications, but exists in rich media files like audio recordings, images, and videos. Our work environments have been forced to support remote work and improve productivity. As a result, video conferencing, especially in industries like healthcare, education, and telecommunications, have seen a huge spike in growth of rich media formats.

Protecting privacy and being able to identify where sensitive data is present inside rich media files is increasingly important. The ability to detect and appropriately mask personal data (e.g., credit card information captured during a call center recording, a passport photo scanned by an airline, or CCTV footage outside public space) used by the business, protects the business from fines and reputation loss, as well as the customer data from possible personal data leaks.

Voltage Data Discovery Solutions Help Understand Your Data, Mitigate Risk

Privacy and protection are becoming a competitive advantage for businesses with the right approach. If organizations can demonstrate that they have developed a risk management and privacy practice built on protecting customer data and establishing trust, it can become a very compelling differentiator to harness for the business.

Voltage Data Discovery helps establish the foundation of these practices by understanding risk in the most common unstructured repositories on-premises and in the cloud including:

- NT file shares
- SharePoint
- Microsoft Exchange
- Micro Focus Content Manager
- Documentum
- Filenet
- Office 365
- SharePoint Online
- OneDrive
- Google Drive
- Azure files
- Amazon S3
- Additional connectors and custom ingest REST API

For structured applications and databases Voltage supports:

- SQL
- NoSQL
- Oracle
- Oracle eBusiness Suite
- PeopleSoft
- SAP
- JDEdwards
- Any JDBC compliant data source

Voltage Data Discovery supports PII detection across unstructured and structured data along with rich media analysis of images, audio, and video files. Our context-sensitive and aware grammars support over 39 languages and economic region entity-types in support of identifying data in support of data privacy (GDPR, CCPA, PIPEDA, POPI, KVKK), as well as PCI and PHI.

Protecting Your Data

Remediating Access to Data

Ensuring data has appropriate permissions applied and is secured can be challenging due to several factors, especially the growth of data. During data discovery activities finding data that is misplaced, or over-exposed is commonplace. Users have never really been reliable for filing data into the appropriate folder, location, or content management system—and, as a result, data containing sensitive, or personal data can sit over-exposed out on the network or public cloud. The ability to pinpoint where sensitive data is, report on permissions, and remediate data security controls is a powerful tool to protecting and governing access for data in use.

Protecting Data in Use

Protecting data-in-use can be complex. Data must be shared for the business to function. Team members need to collaborate, combine data sets and work on sensitive data together, securely. As a business, your organization needs to define and manage these interactions through data protection

policies. Data protection policies help ensure secure sharing and collaboration. Data must be protected based on role and business purpose (to access it), and activities such as print, attach to email, cut and paste, etc., should be blocked where necessary to reduce the proliferation of sensitive data.

Shifting towards Test Data Management

The proliferation of sensitive data can also be caused by application testing, quality assurance, and training. Real-world data has long been used to ensure the correct behavior of business applications before it is pushed into production. With increased privacy regulations, many organizations are shifting away from using real-world data to reduce risk. Recently the market has shifted towards test data management.

Test data management enables data privacy and protection in non-production and production environments by anonymizing the application data during testing. This is a process of rendering completely new data sets that look and act like real-world data but ensures no real customer or sensitive data is present. This is very appealing for applications that capture and store personal and sensitive data such as credit card information, health information numbers, names, addresses, and phone numbers. This approach also streamlines the pipeline between development, test and production, driving greater efficiency inside your IT organization.

Secure Data Analytics and Anonymization

Among the massive volumes of data captured and consumed by organizations is sensitive data that, if stolen, or breached, can result in regulatory fines, sanctions, reputation loss, and other significant consequences to the business. Combine this with the use of big data, and the rise of analytics in the cloud, the inherent risk exposure is exponentially more dangerous.

With enterprises capturing personal information, intellectual property, health information, and more new classes of sensitive data than ever before, information in a data lake can form toxic combinations that present significant risk to the organization.

Organizations need to minimize the risk associated with secure data analytics while ensuring analysts can still safely and securely run queries and reports on trends and business patterns. At the same time, they need to ensure the approach will also help comply with data privacy regulations and risk mitigation around a data breach.

Voltage Data Discovery Solutions Help Protect Your Data, Manage Risk

Voltage Data Discovery solutions support risk management and data privacy practices that build trust around how data is accessed, used, and protected. By enabling rights permissions reporting and remediation, along with transparent file encryption Voltage helps protect your data from unauthorized use and ensures secure information sharing.

For structured data, Voltage Data Discovery supports application retirement and archiving, in place data masking, test data creation, Format Preserving Encryption (FPE) supporting data privacy readiness, test data management, and secure data analytics. These capabilities not only help protect the data inside the applications that run your organization, but they also ensure that when the data is being used to support and grow the business, it is done with privacy and risk management practices built-in.

Voltage Data Privacy and Protection

Voltage Data Discovery solutions help organizations find, secure and protect their data. Our portfolio includes:

Voltage File Analysis Suite (FAS)—Data Discovery

Voltage File Analysis Suite data discovery solution enables organizations to quickly find, secure, and protect sensitive and high-value data. FAS Data Discovery provides complete visibility and insight across unstructured data silos, 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.) personal and sensitive data types (e.g., PI/PII, PCI, PHI, etc.). Voltage FAS supports transparent file encryption policies for data protection along with litigation hold and long-term retention management to meet data preservation requirements.

Voltage Structured Data Manager (SDM)

Voltage Structured Data Manager (SDM) enables the complete management of structured data across its lifecycle. SDM can discover sensitive data in on-premises, cloud or hybrid systems and classify in-scope data for disposition. SDM enables policy-based disposition of data, defining archival, protection, deletion or any other disposition based on pre-set company policy. SDM performs all that through a user-friendly interface that allows structured data to be managed throughout the enterprise from a single pane of glass. For test data management (TDM), SDM can generate contextual “fake” data to be used for testing, training, and quality assurance where they do not need privileges to see the real data. SDM supports multiple mechanisms to protect data for these use cases including:

- Format-Preserving Encryption (FPE)
- Format-Preserving Hash (FPH)
- Random Generation of Meaningful Values (RGMV)
- Random Generation of Meaningful Unique Values (RGMUV)

- Random Mapped Generation of Meaningful Values (RMGMV); and,
- Random Mapped Generation of Meaningful Unique Values (RMGMUV) which masks sensitive data contained in text, comments and notes, or any custom transformation.

Voltage SecureData

Micro Focus Voltage SecureData provides an end-to-end data-centric approach for enterprise data protection. By leveraging Voltage Format Preserving Encryption (FPE), Format-Preserving Hash (FPH), Secure Stateless Tokenization, 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, without gaps in security. SecureData “de-identifies” data, rendering it useless to attackers, while maintaining its usability and referential integrity for data processes, applications, and services. SecureData enables the adoption of a continuous data protection model wherever data flows, in analytic platforms and applications in hybrid multi-cloud environments and native cloud-services.

Voltage SmartCipher

Voltage SmartCipher simplifies unstructured data security, delivering control over the use and proliferation of sensitive files for secure collaboration and improved privacy compliance. It provides persistent file encryption, and complete control and visibility, over file usage and disposition across platforms. By combining critical technology features into a single solution for endpoint privacy and security, SmartCipher simplifies compliance and risk control with a single endpoint solution that transparently works with any datatype, on-premises or cloud solution, including transparent file encryption, usage controls, content inspection, and activity monitoring.

“Data Discovery allowed us to effectively find and understand our data risk. The insights we found from the analysis were invaluable in taking effective actions to protect our data and monitor it going forward.”

Kadir Yildiz
CISO
Turkish Airlines

Contact us at [CyberRes.com](https://www.cyberres.com)
Like what you read? Share it.



Voltage SecureMail

Voltage SecureMail is an essential part of any privacy compliance program or transition to Office 365 cloud. SecureMail is the best of breed end-to-end encrypted email solution available for desktop, cloud, and mobile that is scalable to millions of users while

keeping Personally Identifiable Information (PII) and Personal Health Information (PHI) secure and private. SecureMail adds end-to-end encryption to Office 365, with flexible deployment options, additional compliance and collaboration features, ease of use, and privacy in the cloud.