Velotix

EBOOK

Managing Secure Data Access for Enterprises

How CDOs can strike the right balance between data accessibility and data security by optimizing data access management.

00

Managing Secure Data Access for Enterprises

By 2025, 30% of Gartner clients will protect their data using a "need to share" approach rather than the traditional "need to know" approach.

As you're the key data stakeholder at your company, ensuring data security and access is your top priority.

And yet, many CDOs struggle to achieve efficient data access management due to data fragmentation in silos, the complexity of diverse data ecosystems, compliance demands, resource limitations, and organizational resistance to change. To overcome these challenges, you'll need a robust strategy that incorporates advanced software, fosters collaboration, and leads a data-centric culture to manage secure data access across your enterprise.

You'll find that effectively managing data has many benefits, including:

- Enhanced security by safeguarding sensitive information
- Improved compliance adherence
- Streamlined workflows through faster and more targeted data retrieval
- Optimized decision-making backed by data
- Smoother operational efficiency
- And better collaboration

When you have effective data management, you ensure the right people access the data they need leading to improved performance and reduced risk.

On average, data-driven enterprises generate more than 30 percent growth per year.*

Accenture ↗

01 Optimizing Data Access Management

Optimizing data access management consists of a few parts: Data security, data access, and policy compliance. While some data teams may implement overly strict security measures preventing any data access at all, there is a way to allow data access without compromising compliance regulations. But first, here are a few reasons why data access may be hindred at enterprises:

1. **Security Concerns**

   Enterprises often handle sensitive and confidential data. To protect sensitive and confidential data from falling into the wrong hands, they implement strict security measures, such as firewalls, encryption, access controls, and authentication protocols. While crucial for safeguarding data, they can lock up data from the very people who need to access it.

2. **Data Silos**

   When data is stored in separate locations or formats, authorized users may have difficulty accessing the information needed or may require permissions that take a long time to receive.

3. **Complicated Systems**

   When an enterprise relies on complex IT infrastructure or outdated legacy systems, integrating the data from these systems can be challenging, delaying access to the data required.

Not to mention the unspoken red tape. Enterprises may have a bureaucratic process that slows down data access, which may mean you not only need optimized software but an organizational shift to help provide your company with smooth and secure data access.

The Cost of Non-Compliance & Dark Data

On the other hand, locking up your data doesn't solve the issue either. Although you reduce your security risk, you pay the cost in other ways including hindering productivity, missing opportunities, and potentially reducing revenue generation.

To allow secure data access that upholds the latest security and compliance regulations, data teams should use a data security platform (DSP) with the most cutting-edge AI technology to manage data, allow secure data access, and automate policy compliance.

Once you establish secure and accessible data your enterprise will gain:

- Agility and responsivness
- Improved productivity
- Better collaboration
- Data-backed decision-making
- And compliance confidence

By working with a DSP, data departments can strike the perfect balance between security and data utilization. By staying on top of the latest technology and striving to become cutting-edge, enterprises maintain a competitive advantage, quickly adapt to change, enhance efficiency, and remain policy compliant.

02 The Problem with Dark Data

What Is Dark Data?

Dark data refers to the vast amount of unstructured or semi-structured data that organizations collect, process, and store but don't actively use or analyze for decision-making or business insights. This type of data remains largely untapped and underutilized, residing in storage systems without being leveraged for any strategic or operational purposes.

1. **Unstructured Data**

   Dark data often exists in various formats such as text files, images, videos, emails, social media posts, sensor data, etc., making it challenging to organize and analyze effectively.

2. **Storage and Accumulation**

   Enterprises gather dark data as a byproduct of regular business activities, from various sources, applications, and systems. This data is often kept in storage without being classified, analyzed, or utilized.

3. **Potential Value**

   Despite being overlooked or underutilized, dark data holds the potential to provide valuable insights, uncover trends, identify patterns, or reveal opportunities that could benefit the organization.

How Does It Happen?

Dark data happens when enterprises start to accumulate overwhelming amounts of unstructured data, data silos, underutilized data, and limited resources for analysis. Without a proper data governance practice or data management strategy, dark data can become evermore prevalent. As a result, enterprises miss out on valuable insights to help make game-changing business decisions.

How Dark Data Prevents Compliance

Not only does dark data prevent business insights, but it poses compliance challenges by introducing risks related to unmonitored, unclassified, and unsecured information. The presence of unanalyzed data increases the probability of inadvertently storing sensitive or regulated data without proper safeguards or control measures. Without being able to identify and manage this data effectively, enterprises might fail to meet regulatory requirements regarding data retention, protection, and privacy.

The Cost of Non-Compliance

On top of that, non-compliance could cost a company's brand reputation and rack up nearly $15 million in business disruptions, productivity loss, revenue loss, and other fines and penalties. While dark data is estimated to cost businesses worldwide €2 billion each month in storage capacity.

03 Ensuring Smooth and Secure Data Access

Centralizing Data (Integrating Data Sources)

The first big step towards effective data management is to centralize your data. By integrating all your data in one place, you'll gain better visibility over the entire landscape, use fine-grained access control to determine who should have access, and monitor requests. You'll also gain an efficient auditing process and recovery strategy, improved data governance, better collaboration, and reduced of data redundancy. Overall, centralized data allows your data team to implement compliance rules, and efficiently manage data across the entire enterprise for secure and smooth data access.

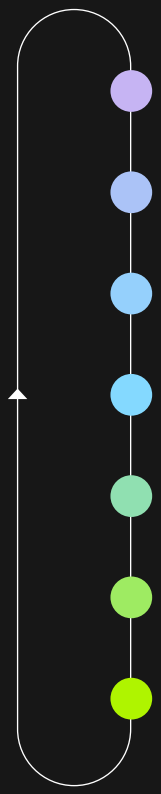
Discovering & Organizing Data with AI

Once you've integrated all your data into one central place, you can use AI to discover and organize data automating classification, deduplication, content recommendation, and predictive analysis. Through the use of AI, you'll streamline data cleansing, improve search capabilities, generate metadata for unstructured data, summarize data, and use natural language processing for text analysis. As a result, you'll empower your enterprise to effectively understand and use data to drive insights and make better decisions.

Using Fine-Grained Access Control

After your data is discovered, organized and classified, you'll want to use fine-grained access controls to precisely determine who should have access and why based on their their roles, responsibilities, and needs. This granular approach ensures that only the right people gain access without delay. Fine-grained access controls supported by AI recommendations based on your policy rulebook will remove the needs for information gatekeepers to sift through irrelevant or sensitive information, speeding up data access, while maintaining security and compliance.

A Secure Data Access Lifecycle



1. A data access request is made
2. One team identifies and verifies the requester
3. The data is located and retrieved
4. The data is reviewed, and unauthorized data is redacted based on policy rules
5. The data is formatted and delivered
6. The request process is documented
7. The policy catalog is updated

As of now, many enterprises require multiple stakeholders to complete this process. But what if you could automate steps 2-7 with the right DSP (data security platform) and the help of AI?

Automating Policy Management

Creating a policy rulebook with the help of AI will allow you to manage the upkeep and remain compliant while allowing fast and secure data access. But don't worry, you don't have to do this alone. You can use a data security platform (DSP) to do this for you.

04 Implementing the Right Data Security Platform

Velotix Data Security Platform Built for Enterprises

Velotix's AI data security platform allows for self-serve data access, faster data verification, automated data redaction based on policy rules, and an efficient process for documenting requests to maintain transparency for future auditing.

How Velotix's simple yet effective data access lifecycle helps data teams optimize data access management:

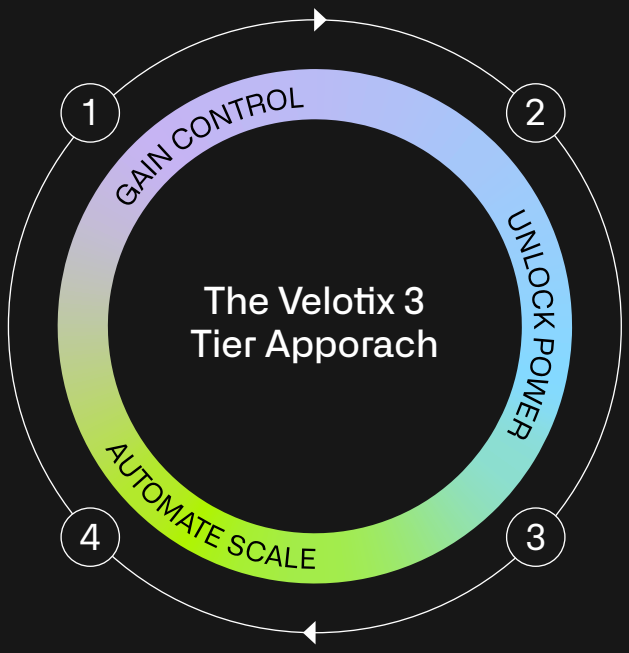
Velotix Data Security Lifecycle

1. DISCOVERY

- Data Discovery
- Classification Discovery
- Catalog Integration

2. MANGAGE POLICY

- Machine Learning
- Automated Policy Management
- Automated Policy Updates



4. MONITOR & GOVERNANCE

- Data Lineage
- Detecting & Cataloging Dark Data
- Inferred Policy

3. REQUEST & SHARE

- Self-Service
- Custom Workflow
- Enforcing Privacy-Enhancing Technologies (PETs)

The Data Access Lifecycle with Velotix

1. Discover Data & Permissions

Integrate your existing database with Velotix to discover, classify and analyze data so you identify sensitive information and protect it.

2. Request Access via Self-Service

Provide your enterprise with one platform where employees can request data and your data department can review requests and make decisions based on AI recommendations.

3. Automate Policy Management

With Velotix, you'll create a single source of truth by automating and enforcing your policy database in one place.

4. Share Authorized Data

Based on policy rules, Velotix will redact unauthorized data, so your data team can grant secure data access in hours not weeks.

5. Monitor Process

Since all data requests are happening in one place, your data department can track the data lifecycle, defeat dark data, and ensure policy compliance all from one easy-to-use dashboard.

"Powered by AI, Velotix provides indispensable technology by monitoring, learning, and predicting how data will be used to provide the right people with the compliant data they need to fuel data democratization and business success."

Noam Biran,
VP Product at Velotix

Secure Data Access at Scale

Velotix, our AI data security platform, was built to help enterprises provide secure data access at scale. Our use of AI is not an afterthought. It's our genesis. We use AI and machine learning to discover and organize your data, then automate policy creation and subsequent access control so you remain secure, compliant, and agile as you grow.

BOOK DEMO TODAY