Informatica

White Paper

Mitigating Risk in Master Data

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Table of Contents

Executive Summary

To create a trusted, authoritative view of the customer, product, and other business-critical enterprise information, organizations invest in Master Data Management (MDM) initiatives. MDM combines elements of customer, product, and other essential data across the enterprise into consolidated records to create trusted data to be shared with the people and applications that need it. This has tremendous value for any business that wants to become customer-centric; improve customer service and loyalty programs; create efficiencies in product management and offerings; and so on.

Trusted data becomes the crown jewels of the organization's customer and product initiatives and provides clear competitive advantage. However, this consolidation of sensitive data also provides an attractive target for outside attacks and breaches and is subject to privacy regulations, such as the General Data Protection Regulation (GDPR).

Natural questions arise for data protection and compliance for these environments:

- Where is all the data?
- What is feeding the repository and who is accessing data with what applications?
- Does current access and use adhere to regulations and data use policies?
- Are data protections appropriate, and is data risk remaining at acceptable levels or are there conditions creating more risk that should be remediated?

The results of the discovery and classification of sensitive customer data become the foundation for decision support regarding the risk, security, and compliance of MDM data.

This white paper provides a framework of considerations and strategies for mitigating risk with a data-centric solution that:

- Applies analytics, automation, and AI to identify and protect sensitive MDM data
- Complies with evolving data governance and security regulations
- Provides audit readiness
- Alerts key stakeholders when anomalous user behavior occurs

Introduction

According to research firm IDC, the world is predicted to create 180 zettabytes of data in 2025, up from less than 10 zettabytes in 2015.[1] Organizations across all industries rely on the accuracy, availability, and security of their data to generate revenue, serve customers, increase productivity, and conduct other mission-critical business processes.

The continued exponential growth in data volume and usage also includes sensitive master data across multiple silos, both on-premises and in the cloud, and in a variety of data formats. These conditions have rendered traditional data security methods obsolete,[2] requiring a new approach to master data security across an organization.

[1] IDC webcast, "2016 IoT Mid-Year Review – The Report Card for Everyone," August 4, 2016.
[2] Gartner, "Market Guide for Data-Centric Audit and Protection," March 21, 2017.

However, most companies cannot accurately identify where all their sensitive master data is located, especially if it is in unstructured formats. This lack of knowledge increases an organization's risk, and for these reasons, a data breach is the top IT security risk.[3]

With data breaches on the rise in tandem with the proliferation of sensitive master data, organizations must develop a risk mitigation strategy that includes a data-centric security product with these key features:

- Visibility into all data sources to locate and classify sensitive master data from across the organization
- Ability to implement protection mechanisms for sensitive master data to mitigate breaches
- Compliance with current data security and privacy regulations, including the use of automation and AI to monitor user behavior and report anomalies in near real time
- Rich analytic visualization tools for sensitive data management
- Transparent and robust reporting capabilities for audit readiness

Gartner predicts that by 2020, data-centric audit and protection products will replace disparate siloed data security tools in 40 percent of large enterprises, up from less than five percent today.[4] These data-centric protection solutions provide a centralized, SaaS view of at-risk data, so that all key stakeholders across an organization can track sensitive data movement and apply protection mechanisms as required by governance policies and regulations.

A Four-Point Strategy for Mitigating Sensitive Data Risk

Sensitive data risk is the impact of losing sensitive data, and the most common cause of this loss is a data breach. A common misperception is that simply locating sensitive master data is enough to remediate risk. However, locating and classifying this data is only the first step in a comprehensive risk remediation strategy.

The next steps involve assessing your organization's risk based on the results of the location and classification analysis. You need to determine a strategy for reducing the risk—with automated controls that enforce data governance policies and involve all key stakeholders—not just IT. Your strategy should also include procuring and implementing a robust, data-centric security product that provides capabilities for regulatory compliance; rich analytic visualizations of sensitive data for dashboards and audit reporting; and protection for all sensitive MDM data types across the organization.

1. Discovery and Classification

A common approach to discovery is to review existing sources and send questionnaires. However, this highly manual approach is inadequate because it consumes valuable time and resources, and it is often inaccurate and out of date, with reliance on self-reporting rather than actual monitoring of user behavior.

[3] Ponemon Institute LLC, "Data Breaches and Sensitive Data Risk," February 2016.
[4] Gartner, "Market Guide for Data-Centric Audit and Protection," March 21, 2017.

Organizations need to ask themselves:

- What data do you store, who has access to it, and for what purposes?
- How do you manage user privileges and data rights?
- How will you protect sensitive MDM data and ensure that the appropriate controls are in place?

Other considerations for discovery and classification compliance include:

- Defining and understanding your data landscape, including databases and unstructured data
- Mapping which systems contain sensitive MDM data
- Procuring a solution that can map the movement of this data across your ecosystem while maintaining a near real-time view with analytics and reporting tools

2. Compliance

Organizations struggle to identify, monitor, and remediate data risks to comply with data privacy and security regulations. Further, they must monitor, analyze, and alert on data access or movement that could jeopardize compliance.

The GDPR, enforceable beginning May 25, 2018, was adopted with the intent to strengthen and unify data protection for all individuals within the EU, thereby simplifying the regulatory environment for international business.

Many businesses have not yet prepared for this regulation and will not be sufficiently compliant, but noncompliance could result in significant fines and reputational damage. On the other hand, compliance can provide the opportunity for competitive advantage as an MDM data privacy and security differentiator, while also driving digital transformation outcomes.

Organizations need to develop intelligent policies that identify data stores that contain GDPR-relevant "data domains." These policies are multifactor, with logic that determines which combinations pose a privacy threat.

3. Protection

In 2016, there were 1,093 data breaches with a total of nearly 36.6 million records exposed.[5] Clearly, despite large investments in security, critical data remains vulnerable. Organizations need to continuously secure high-risk data; identify suspicious behavior and unauthorized use or movement of critical data assets; and automate and orchestrate remediation.

Organizations should identify critical data risks and remediate these risks with data-centric controls (rather than classic cybersecurity tools). For example, these controls include data masking, access controls, and encryption solutions.

In addition to data controls, organizations should monitor end user data access and behavior. Excessive data access or unusual behavior can indicate that users are not adhering to privacy policies or that user credentials have been stolen.

[5] Identity Theft Resource Center, "2016 Data Breach Category Summary," December 31, 2016.

4. Audit Readiness and Response

Companies undergo more audits and assessments of sensitive data than ever before. They struggle to provide proof to auditors that they have visibility and protection of critical data.

Organizations should be able to immediately respond to auditors and provide evidence that they know where data exists, what is its risk, how the data is protected, and how the data is being used. They should consider that auditors will want reports and visualizations that are abstracted for departments or locations, and that provide the ability to drill down on specific data domains.

Conclusion

The power of MDM can help organizations transform their operations and services. The power of this data is clear, but it also represents a tempting target for internal or external actors to misuse. Coupled with the continued onslaught of data breaches and growing compliance requirements, organizations must rethink their processes and tools for identifying, analyzing, and protecting sensitive data.

In the current climate of heightened security risk and regular data breaches, companies now must develop a robust digital strategy to continuously monitor, analyze, and remediate the risk of their sensitive master data. They need to monitor data in near real time for signals of misuse or breach, excessive access, unusual behavior, or cross-border transfers. With this diligence, organizations can leverage MDM and improve their data risk posture to help mitigate the impact of data breaches or internal misuse and meet the stringent requirements of regional and industry regulations.

Recommendations

1. Perform a risk assessment to gain a clear understanding of where your sensitive MDM data is located, how far it propagates through your data ecosystem, and which sets of sensitive data are most vulnerable.
2. Based on the assessment results, prioritize your organization's top 10 sources of the most sensitive MDM data; determine a strategy and product for protecting these; and implement this strategy as a pilot for your new approach to data security.
3. Define, document, and distribute your organization's compliance policies and the key stakeholders that are accountable for GDPR compliance. Build a strategic plan for 2018 and beyond.

Further Research

For more information about sensitive data security risks and protection considerations, refer to the following publications and videos:

Informatica Secure@Source

Informatica Master Data Management

White Paper: "Detect and Protect: A Data-Centric Approach to Security," April 2017.

Video: Detect and Protect

Ponemon Institute LLC, "Data Breaches and Sensitive Data Risk," February 2016.

meeting your organization's security and compliance standards.

Informatica

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871

IN09_1118_03409