WHAT IS TEST DATA MANAGEMENT AND WHY DO WE NEED IT?

In Part 1 of a 4-part series, we discuss what TDM is and why it is critical to your enterprise.

Defining a TDM strategy can be challenging—the growing number of systems and environments can even make it seem impossible. This series will address some of the common questions that customers have asked and discuss the delivery and implementation of a cross-platform mainframe and distributed TDM.

This series was written both to help enterprises understand the need for a TDM strategy and to share some tips on how to create a strategy that will obfuscate data in lower environments and minimize the cost associated with unneeded massive volumes of test data.

Posts focus on what TDM is and why it is needed, the stakeholders interested in undertaking a TDM initiative, the challenges of managing test data, solutions that will help you define and implement your strategy, and the benefits of such an implementation.

Part 1: What Is TDM and Why Do We Need It?

What are some compelling reasons for TDM?

Today's Agile DevOps teams need the ability to go faster without sacrificing quality. Developers should not need to spend time on data provisioning tasks – they should spend more time

developing new functionality and managing production problems. A robust TDM solution is a critical part of any enterprise and will ensure the provisioning of the rightsized test data to qualified users in a repeatable and timely manner. The data should contain all required test conditions and be anonymized.

The following factors emphasize the need for a TDM solution:

Legislation. Recent years have brought an increasing trend of local, federal, and international regulations towards the protection of sensitive data. Many of the legislations force businesses and organizations to scrutinize the way proprietary and confidential data is handled across a business enterprise. This legislation comes in the form of Europe's GDPR, California's CCPA, South Africa's POPIA, Canada's CPPA and others.

As a result, many companies are managing internal policy changes that demand the implementation of tighter security measures, strict audit controls, and radical changes to existing business practices. All of this is being done in an effort to meet compliance and demonstrate accountability.

Along with Covid-19, 2020 brought changes in working practices. More and more tech workers are working remotely – in their basement, in their bedroom, hallway, kitchen table, or any space in or outside of their home, maybe public places where wifi is available.

These changes create new challenge for IT leaders. Not only does an organization need to respond to its core business needs, but it also needs to adhere to strict legislative requirements associated with the exposure, theft, or misappropriation of customer, financial, corporate, or personal sensitive information.

Risk mitigation. In order to mitigate against the risk of a data breach from test data files, IT shops are taking different actions to safeguard their data assets. Much effort has been focused around the protection of production data from external threats by means of tighter security access, firewall, network, communications, storage and audit counter measures. However, studies conducted by research firms and industry analysts reveal that the largest percentage of data breaches occur internally, within the enterprise.

While organizations may think that their core data is immune from external Management threats, environments outside of the production perimeter such as testing, development, or quality assurance usually have far less robust security controls. Access to these areas is typically more widely exposed to a larger variety of resources, including in-house staff, consultants, partners, outsourcers, and offshore personnel.

Recent Breaches. As in every year since the turn of the millennium, 2020 has had hundreds of breaches across the globe. A simple search of "data breach 2020 headlines" in your favorite search engine will return headlines of breaches in all business sectors, from financial to healthcare, and from retail to cruise line.

Recent Fines. If you are an enterprise officer you should be afraid, very afraid. Massive fines and settlements have been levied on many household named businesses in the past 2 years. In July 2019 a leading credit agency agreed to pay over $575 million for "failure to take reasonable steps to secure its network." Again, a simple web search of "data breach 2020 fines headlines" will return some of those fines.

Given these legislative requirements, internal and external risks, and recent breaches and fines, the need for and benefits of a TDM solution should be clear. Look for part two in our series for a

discussion of the stakeholders within an organization who have an active interest in the security of test data and how a comprehensive solution benefits each.