IBM Case Study

IBM Information Management software

Financial services companies protect data privacy by de-identifying confidential data in non-production environments

Overview

Challenges

- *Reduce risk of privacy breaches in the application development and testing environments. Overcome test data management challenges related to data privacy and cloning large production databases. Implement data privacy policies that leverage the FDIC definitions for protecting personally identifiable financial information.*

Why IBM?

- *IBM® Optim™ helped companies satisfy both the technical and business requirements for improving test data management and protecting privacy in non-production environments.*

Solutions

- *IBM® Optim™ Test Data Management Solution*

  IBM® Optim™ Data Privacy Solution

Benefits

- *Protected privacy by using a variety of masking techniques to de-identify test data across non-production environments. Streamlined application testing by using subsetting to create manageable development and testing environments. Aligned privacy policies with FDIC definitions for protecting consumer financial information.*

Privacy initiatives lead to success

Managing confidential data is part of doing business in every industry. Companies from insurance and financial services to healthcare and telecommunications collect information to support daily business activities, provide superior customer service and generate revenue. However, while most companies use this data for legitimate purposes, the recent rise in security breaches and well-publicized privacy violations suggests that some organizations are not doing enough to protect confidential customer information.

To improve corporate governance, many organizations are proactively looking for effective solutions to manage private data more securely. Specifically, in the financial services industry, companies are implementing sophisticated measures to protect production application environments. However, protecting data privacy in the development and testing environments is often overlooked. Effective application testing requires realistic test data, which means that developers and testers need more access to data, not less. Yet, these environments are often more vulnerable to privacy breaches. So how can you provide access and still protect privacy?

The following stories describe how three forward-thinking financial services companies implemented the IBM Optim Data Privacy Solution to improve application testing processes and, most importantly, to protect data privacy. In the spirit of privacy, these companies are not seeking recognition for their diligent efforts to secure sensitive information and have asked to remain anonymous.

Financial services giant addresses privacy risk

A large US financial services company relies on a myriad of applications to manage every aspect of its retail and business banking operations, as well as venture capital and investment management, and international trade activities. The company's broad client base includes individual, small business and commercial accounts that take advantage of bill pay and checking, payroll and risk management and many other services. The IT infrastructure that supports these diversified applications includes IBM DB2®, IBM IMS™, Oracle® and Microsoft® SQL Server® databases.

Customer information is managed using the Hogan CIS application in an IMS environment and a custom CIS application in a DB2 environment. Additional customer information, bill payment and credit card issuance applications are Oracle-based. Each of these applications is critical to supporting business activities. It was a routine regulatory audit that revealed areas of vulnerability in the application development and testing environments that placed confidential customer information at risk for privacy breaches. As a result, the regulatory agency mandated that the IT organization implement more effective internal controls to protect privacy.

Comprehensive application testing is scheduled for major code releases four times each year. Ensuring reliability among interrelated applications requires integrated system testing and enterprise testing. Because the next test runs were scheduled for early November, the IT group agreed on a self-imposed deadline for implementing a data privacy solution by that year's end.

The CIO and the IT group wanted a comprehensive solution for de-identifying personal information that would also preserve the data integrity for testing purposes. They also wanted a consistent methodology, rather than disparate processes and technologies, and a solution that could be implemented across development and testing operating environments. Because of high costs and the tight deadline, developing an in-house solution was out of the question. Instead, they researched a number of solutions, which included Optim.

Unique among vendor solutions, Optim offers data masking and transformation capabilities for both mainframe and open systems application data. With Optim's capabilities for protecting privacy across applications, databases, operating systems and hardware platforms, the choice was clear. However, some complexities in the application architecture revealed the need to develop site-specific routines for data masking. Because Optim includes the capability to tailor privacy functionality, the Optim team worked with a systems integration partner to meet these site-specific requirements.

Within a week of the purchase decision, the company started working to implement Optim in a staged rollout. The implementation was completed 4 months later, just in time for the next round of application releases. Optim provided a standardized approach, using a single, consistent methodology for de-identifying confidential customer information across development and testing environments. The company was better prepared for any future audits by eliminating the possibility of privacy breaches that could have jeopardized its business.

Financial management providers targets data privacy

This leading financial management organization, a unit of a major multinational banking corporation, specializes in asset management, debt elimination, income protection and education savings programs. Literally hundreds of packaged and in-house applications support these business activities, and for the company to remain competitive, these applications must be updated periodically to provide new functionality and support new products. However, because of the time, expense and resource commitment required, application testing was limited to only two or three times per year.

Initially, test data was obtained by cloning production environments, comprising several terabytes of DB2 relational data and non-relational VSAM® and QSAM® files. Cloning was time consuming and expensive. There was no way to automate the process of de-identifying cloned data to protect privacy, and production data was accessible from the development, testing and quality assurance environments. Data privacy compliance required de-identifying customer names, phone numbers, addresses and income information, as well as payment history, loan and deposit balances, credit card transactions and credit report details. Faced with the risk of internal privacy breaches and the challenges of updating and testing mission-critical applications more frequently, maintaining the status quo was not an option.

In searching for a test data management solution, the IT group had several requirements. First, the solution had to provide the capability to subset relational and non-relational data to create "federated" test environments, across the mainframe and open systems platforms. Next, they wanted automated techniques for de-identifying test data that would also retain the referential integrity of the data to be useful for testing purposes. The IT evaluation team identified Optim as the only solution that could meet these requirements.

From a technical perspective, Optim's subsetting capabilities provided repeatable, automated and scalable processes for performing federated extracts across DB2, VSAM and QSAM data stores. It took much less time to create and refresh realistic, "right-sized" development and testing environments. A variety of automated techniques for masking and propagating de-identified data made it possible to isolate the production and non-production environments and protect customer information from unauthorized exposure.

From a business perspective, implementing Optim reduced the risk and costs associated with privacy breaches that could have ruined the company's reputation. Business users and customers now benefit from the timely delivery of more reliable and feature-rich applications because upgrades and testing can be done more often and at a lower cost. More robust financial applications improve customer service and expand revenue opportunities.

Banking technology firm builds privacy competence

This billion-dollar financial technology firm offers products and services that drive account processing, electronic funds transfer, consumer healthcare payments and more. To support its business operations, the company developed an end-to-end electronic payment application to manage daily transaction activities. Serving thousands of clients across industries, this innovative application processes millions of payments each month.

With increasing regulatory pressures, and knowing that the trust and loyalty of its customers depends on protecting sensitive data effectively, senior management adopted a proactive leadership position on data privacy protection. The company developed enterprise policies for classifying consumer information, based on the Federal Deposit Insurance Corporation's (FDIC) definitions of personally identifiable financial information. Specifics included information collected during the application process, information acquired from a financial product or service transaction, or information obtained from a third party in connection with providing a financial product or service.

The IT group considered data classification and retention programs in place and applied encryption techniques to protect data on laptops and BlackBerry devices. Primary security for production data residing on servers was managed using encryption, access controls and the network infrastructure. However, the development and testing environments presented unique challenges. Simply replicating production safeguards for these environments would not be sufficient.

Supporting privacy compliance would require removing, masking or transforming elements that could be used to identify an individual. De-identified data would be acceptable to use in open testing environments, and masking techniques would have to propagate de-identified data accurately, while preserving the referential integrity to support reliable testing.

Research on several competitive alternatives revealed that only Optim provided a variety of proven masking capabilities for de-identifying data. Using substrings, random or sequential numbers, arithmetic expressions, as well as date aging and other techniques, it was possible to substitute customer data with contextually accurate, but fictionalized data to produce accurate test results. Optim was scalable across applications, databases, operating environments and hardware platforms.

Optim's capabilities satisfied requirements to protect customer information in the development and testing environments. The consistent approach for managing test data improved operational efficiencies to lower costs. The ability to secure confidential data helped reduce legal risks that would have resulted in financial penalties. In addition, the company was able to maintain its strategic business advantage by engendering customer trust resulting in increased revenue opportunities.

Best practices for protecting privacy

Worldwide, stringent data privacy laws mandate that organizations protect personal data from misuse. Although most companies have established security measures in the application production environments, the development, testing and training environments are often the most vulnerable. To address this challenge, de-identifying data is a recognized best practice for providing realistic test data that also protects privacy. Optim offers comprehensive and proven test data management capabilities for de-identifying test data to meet these requirements.

About IBM Optim

IBM® Optim™ enterprise data management solutions focus on critical business issues, such as data growth management, data privacy compliance, test data management, e-discovery, application upgrades, migrations and retirements. Optim aligns application data management with business objectives to help optimize performance, mitigate risk and control costs, while delivering capabilities that scale across enterprise applications, databases and platforms. Today, Optim helps companies across industries worldwide capitalize on the business value of their enterprise applications and databases, with the power to manage enterprise application data through every stage of its lifecycle.

For more information

To learn more about IBM Optim enterprise data management solutions, contact your IBM sales representative or visit: www.optimsolution.com.

IBM Software Group
111 Campus Drive
Princeton, NJ
USA, 08540-6400
www.optimsolution.com

Produced in the United States of America
05-08
All Rights Reserved

This case study is an example of how customers use IBM products. There is no guarantee of comparable results.

References in this publication to IBM products, programs or services do not imply that IBM intends to make them available in all countries in which IBM operates or does business.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.