Solution Brief

Industry: Cross-vertical
Solution Components: z/OS APIs, z/OS Diagnostics Analyzer

IBM Z Data Privacy for Diagnostics

Improve your ability to address compliance challenges without compromising on serviceability.

IBM Systems / 5 January 2021 / © 2021 IBM Corporation

Customer data is a key currency in today's information-based economy. As a result of consumer concern, regulators are setting new standards to ensure that not only the collection and storage of sensitive customer data is kept secure, but also the sharing of it.

Data Privacy for Diagnostics is designed to tag and redact sensitive data in diagnostic dumps after they are captured on IBM Z®.

Help improve your ability to maintain control of your data when working with third-party vendors with Data Privacy for Diagnostics.

The challenge

Customer data is a key currency of today's information-based economy. Enterprises collect and store immense amounts of customer data in order to provide valuable services.

Governing how it is collected and shared is a primary concern for today's top enterprise businesses around the world.

The misuse of sensitive customer data has forced some of the largest organizations around the world to face large financial penalties, loss of customer trust, and employee discharges.

One of the ways enterprises solve technical challenges and maintain their compute environments is by sending diagnostic dumps to third parties for root cause analysis.

Although sending dumps is a great method for resolving technical problems, if an error were to occur while sensitive data was in use, the data could end up being included in the resulting diagnostic dump.

This could impose a major data privacy issue if the dumps were to contain sensitive user data and shared with vendors.

Current approaches to securing diagnostic data may significantly increase problem resolution times and give service teams, who may not be on a business need-to-know basis, access to diagnostic dumps that contain sensitive customer data.

Having loose access controls may result in organizations not meeting compliance standards and may be discontinued as regulatory entities strengthen their compliance requirements.

The choice between compliance and serviceability

z/OS® system programmers may find challenges in helping to ensure that sensitive diagnostic data is not being shared with third-party vendors. As a result, organizations are often compelled to make a choice between regulatory compliance and serviceability.

The IBM solution

IBM Z Data Privacy for Diagnostics is a z/OS security function designed to tag and redact sensitive user data from SVC and standalone diagnostic dumps after they are captured on IBM z15™.

There are two ways to tag data in diagnostic dumps:

- z/OS APIs
- z/OS Diagnostics Analyzer

z/OS APIs

z/OS APIs are used by applications and system components to tag pages of diagnostic dumps as sensitive if they contain user data and will tag pages as non-sensitive if they contain metadata.

Sometimes, applications are unable to identify all the locations of sensitive data and some pages are left untagged.

z/OS Diagnostics Analyzer

z/OS Diagnostics Analyzer complements z/OS APIs and tags additional sensitive data in previously untagged pages of memory.

It determines sensitivity based on criteria from a list of built-in identifiers provided and custom identifiers that you can specify to fit your unique environment.

Utilize the z/OS APIs with the z/OS Diagnostic Analyzer to help minimize post-processing time as much as possible.

Sharing with vendors for root cause analysis

The tagged sensitive pages are redacted to create a new dump to be shared with third-party vendors for root cause analysis. You can still access the original dump even after redaction occurs.

System Requirements

Hardware

- IBM z15, IBM z15 T02

Software

- z/OS v2.3 or higher

The solution value

Data Privacy for Diagnostics is designed to help improve your ability to address compliance challenges in the area of diagnostic data without compromising on serviceability.

It gives you the capability to search for and redact sensitive user information from diagnostic dumps quickly with no additional impact to dump capture time.

By redacting sensitive data in diagnostic dumps, you can limit sensitive data exposure to third-party teams who may not be on a need-to-know basis while still allowing them to continue their normal job functions.

Maintain control of your data when working with third-party vendors and help protect sensitive customer data with Data Privacy for Diagnostics.

Why IBM Z?

The IBM Z platform offers an industry-leading level of data privacy, security and resiliency across on premises, public and hybrid cloud environments.

Leveraged by business of all sizes, from large enterprises to next-gen startups, IBM Z represents a sound investment for your security solutions.

Learn more

Learn more about Data Privacy for Diagnostics by visiting the following pages:

IBM Enterprise Security: https://ibm.co/3a9Qgiz

IBM Blog: https://ibm.co/3qVc6w5

IBM Knowledge Center: https://ibm.co/3oTElt0

Produced in the United States of America, January 2021.

IBM, the IBM logo, ibm.com, IBM Z, z15 and z/OS are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml. This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.