

SOLUTION BRIEF

CA DATA CONTENT DISCOVERY AND CA COMPLIANCE EVENT MANAGER

How Can Real-Time Data Security and Compliance Solutions Secure My Business and Improve My Compliance Posture?

CA Data Content Discovery and CA Compliance

Event Manager identify sensitive data at rest and in motion to help lower the risk of damaging data breaches and reduce the ongoing cost of regulatory compliance.

Executive Summary

Challenge

The mainframe is mission essential in the application economy and hosts the majority of the world's corporate data. However, with the immense amount of data residing on the platform, locating sensitive and regulated data, performing manual audits and responding to potential security threats can be more than time-consuming—it can seem impossible.

Opportunity

Comprehensive data security and compliance solutions, CA Data Content Discovery and CA Compliance Event Manager find and classify sensitive data, and monitor users to generate alerts of potential risks in real time.

This powerful solution combination can help you proactively address malicious attacks and impacts of accidents, secure sensitive information across all aspects of the data lifecycle and facilitate regulatory compliance.

Benefits

CA Technologies provides the only data discovery solutions that run 100 percent on the mainframe to reduce the risk of exposing sensitive data. By bringing the integration of data security and compliance management to the mainframe, users gain deeper insight into security and compliance issues and an improved risk posture, so stakeholders can identify where data is located, when it moves and who has access to it.

Section 1:

You Can't Protect Your Mission-Essential Data If You Don't Know Where It Is

The mainframe is mission essential in the application economy and hosts the majority of today's corporate data—and therefore the majority of the world's most sensitive data. These huge aggregations and collections of regulated data can get lost, abandoned, orphaned or even maliciously hidden by internal fraudsters, subjecting enterprises to unknown degrees of risk.

Security and compliance continue to be top of mind for companies as they strive to protect their sensitive business assets, while ensuring fast and efficient operations. As data continues to grow and becomes increasingly regulated, a focus on data security is essential to managing the risks faced by today's businesses.

With the vast amount of data residing on your mainframe, locating sensitive and regulated data to stay in control and easily facilitate regulatory compliance can be more than time-consuming—it can seem impossible. You must know where your sensitive data is, who has access to it and be able to act fast, before it accidentally or maliciously exits the mainframe due to a data breach.

Section 2:

Find, Classify and Protect With CA Data Content Discovery

CA Data Content Discovery is the only data security discovery and classification offering that executes solely on and for the mainframe to completely eliminate any risky offloading of data. The software integrates with leading enterprise security management and access control products—such as CA ACF2™, IBM® RACF® and CA Top Secret®—revealing not just which data is exposed but who has access to it. Moreover, the solution does this without necessarily imposing burdens on general CPU capacity, because it's implemented in Java™ and its workloads are fully IBM z Systems® Integrated Information Processor (zIIP) specialty-engine compliant.

The mainframe processes more than 2.5B transactions daily.

Find it

With the mainframe handling such a huge amount of corporate data, and able to process over 2.5B transactions per day,¹ manually finding sensitive or regulated data on the platform is unrealistic. That's where CA Data Content Discovery comes in. The software automatically scans the mainframe data infrastructure to immediately identify the location of sensitive and regulated data, which is the first step to help mitigate risk associated with retaining data.

Classify it

CA Data Content Discovery categorizes and classifies the discovered data based on sensitivity level. Once you know the location of mainframe data, you can make business decisions to appropriately secure, encrypt, archive or delete it, and prove to auditors that controls are in place, which makes regulatory compliance faster and easier.

Protect it

CA Data Content Discovery helps key business stakeholders stay in control of their mainframe data, gain quick and critical insights about the potential and magnitude of data exposure on the mainframe, act quickly and reduce risk—all while reducing costs associated with data protection processes. By identifying data exposure risks, classifying the data to determine sensitivity level and providing comprehensive reporting on the scan results, you can protect data, address compliance requirements and mitigate exposure risks.

Section 3:

Alert, Inspect and Protect With CA Compliance Event Manager

CA Compliance Event Manager provides key stakeholders with real-time notifications of potential security breaches on the mainframe, enabling faster and simpler mediation. With multiple components designed to process information about enterprise security manager events and seamlessly monitor systems for changes to critical resources, CA Compliance Event Manager can mitigate the risk associated with negative security events while helping to reduce the cost, complexity and effort required to monitor and report on mainframe security and compliance.

Only 10% of customers are actively addressing their mainframe compliance costs.

Alert

Through more detailed and real-time alerting, CA Compliance Event Manager helps mitigate negative security events. The solution monitors entire systems of security records, security configuration points, system data sets and IBM z/OS® configuration controls, and provides immediate notifications of pertinent violations, plus access and change activities to critical security systems and resources. Stakeholders can act quickly and proactively, thanks to real-time alerts of potential threats.

Inspect

Once data exposure threats are identified, CA Compliance Event Manager generates advanced audit and compliance information that is not available in standard security reports. Through its sophisticated security monitoring, comprehensive auditing and security data logging support, the software enables users to create real-time security alerts, supports forensic analysis of security situations with raw security data recording and provides the ability to search, filter, archive and analyze recorded historical data. Users receive real-time alerts, combined with deeper insights into critical security and compliance issues—all of which lead to an improved risk posture.

Protect

A global survey by CA Technologies shows that only 10 percent of customers are actively addressing their mainframe compliance costs.² And research shows that around 70 percent of organizations believe they'll need to increase their budgets to comply with specific requirements of the EU General Data Protection Regulation (GDPR).³

CA Compliance Event Manager is designed to make regulatory compliance faster and easier by helping you mitigate negative security events, address and reduce the total cost of compliance to keep your mission-essential data secure and avoid risk. The solution provides deeper insight for data security and compliance, and helps organizations locate data when it moves and determine who has access to it.

Section 5:

Real-Time Data Security and Compliance

CA brings the integration of data security and compliance management to the mainframe.

CA Technologies augments traditional user access management with data-centric compliance into a synergistic combination to provide the only sensitive data discovery solution that runs 100 percent on the mainframe.

When integrated together, CA Data Content Discovery and CA Compliance Event Manager provide deeper, real-time insight into security and compliance issues. So you can identify sensitive data at rest and in motion, reduce the risk of costly data breaches and secure data across all aspects of the data lifecycle. From finding and classifying to alerting and inspecting, these CA solutions provide unified enterprise security and help you increase your compliance posture across all platforms that power your success in the application economy.

To learn more about securing your mission-essential data, visit ca.com/mainframe-security.



Connect with CA Technologies at ca.com



CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

¹ IBM press release, "[IBM Launches z13 Mainframe—Most Powerful and Secure System Ever Built](#)," Jan 13, 2015,

² TechValidate, [Survey of 157 users of CA Mainframe Security Solutions](#), Aug 16, 2016, TVID F38-414-77A

³ Kevin Blasko, Baker & McKenzie, "[Data Privacy Survey: GDPR Costs and Complexity](#)," May 4, 2016

Copyright © 2016 CA. All rights reserved. IBM, RACF, z/OS and z Systems are trademarks of International Business Machines Corporation in the United States, other countries, or both. Java and all Java-based trademarks and logos are trademarks of Oracle Corporation in the United States, other countries, or both. All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

Some information in this publication is based upon CA and customer experiences with the referenced software product in a variety of development and customer environments. Past performance of the software product in such development and customer environments is not indicative of the future performance of such software product in identical, similar or different environments. CA does not warrant that the software product will operate as specifically set forth in this publication. CA will support the referenced product only in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.