

**SOLUTION BRIEF**

CA DATA CONTENT DISCOVERY AND CA COMPLIANCE EVENT MANAGER

# How Can Data-Centric Security Solutions Protect Data Privacy and Simplify Regulatory Compliance?

Data-centric mainframe security and compliance solutions, 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, and therefore the world's most sensitive 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

Data-centric mainframe security and compliance solutions, CA Data Content Discovery and CA Compliance Event Manager find sensitive and regulated data, classify data for compliance, alert to potential risks in real time and inspect threat through advanced reporting and forensics.

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 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. By integrating data security and compliance management on the mainframe, you gain deeper insight into security and compliance issues and an improved risk posture, so you can identify where all your sensitive and regulated mainframe data is located, when it moves and who has access to it.

### Section 1:

## You Can't Protect Your Data If You Don't Know Where It Is

The mainframe is mission-essential and hosts the majority of today's enterprise data—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.

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

But now, the mainframe is increasingly connected with everything else in your business, and while the connected mainframe drives significant business value, the number of risks increase as well. The Internet, Internet of Things (IoT) and millions of mobile devices are now connected through APIs, causing mainframe data to grow, move on and off the platform and become increasingly regulated.

An enterprise-wide data-centric security strategy is critical to managing today's risk.

---

### Section 2:

## A Data-Centric Approach to Mainframe Security and Compliance

In just the past year, there were 3,141 breaches with confirmed data loss, and the average time to discover the breach was 146 days,<sup>1</sup> leaving organizations in a difficult position to guarantee that customer data is secure or prove to auditors that controls are in place to fulfill regulatory compliance. To improve organizations' risk and compliance posture, mainframe security solutions from CA Technologies revolve entirely around data.

**Start with the data.** The first step is knowing where your sensitive data resides on the mainframe. After all, if you can't locate the data, how can you possibly know who is accessing it and how? You must find where your critical data is stored, identify the data type and its sensitivity, understand the risk it faces and manage how it's handled to enhance your data privacy.

**Understand which data is at risk to threat.** After you've identified the location of your data, consider the type of data, its nature and exposure, and the amount of data to determine your organization's risk posture. It's also important to determine how much of the data is critical to regulatory compliance.

**Monitor access to that data.** Once a data set has been identified as sensitive, it's critical to know who is accessing the data, when, and whether their access deviates from their normal activity so the appropriate user controls are in place to avoid misuse.

**Limit access.** Once data has been identified as sensitive, determine who is accessing that data and, critically, who has accessed that data in the past. Ask yourself: Do those users all access the data? Those who rarely access it are prime candidates for revocation, which is an easy start to “least access” principles, leading to more control over your corporate business data.

Our data-centric approach to mainframe security and compliance starts inside out, first by identifying and classifying data on the mainframe, which allows you to examine which users have access to data and reduce that access to only those that have a business case. The second component is the monitoring of user access and alerts in real time of frequent access or movement of the data by the user, so you can act quickly. Enterprises without this confident knowledge of classification of their mainframe data typically have too many users allowed access to sensitive data, which unknowingly leaves the business at high risk of data compromise from credential theft and insider threat, both unintentional and fraudulent.

---

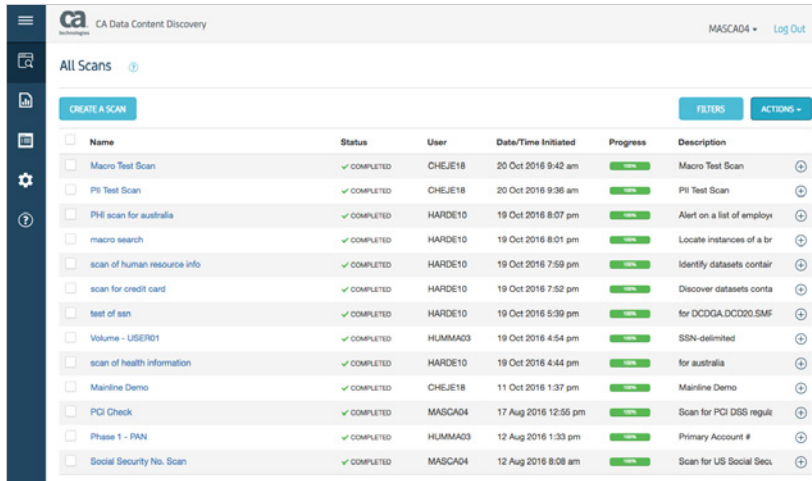
### Section 3:

## Find, Classify and Protect with CA Data Content Discovery

CA Data Content Discovery is the only data security discovery and classification solution that executes solely on and for the mainframe to eliminate the risk of offboarding sensitive data. The solution integrates with leading 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, for both data at rest and in motion. CA Data Content Discovery finds sensitive data that may be lost, hidden or abandoned and classifies the data based on sensitivity level to help facilitate regulatory compliance and protect your most sensitive corporate data—the first steps in a data-centric approach to mainframe security.

“The most valuable feature of CA Data Content Discovery is the ability to recognize, in an intelligent and accessible way, which data sets on the mainframe contain sensitive data that needs to be protected from a governance and regulatory perspective.”

IT Central Station, CA Data Content Discovery review, Dec 6, 2016



The screenshot shows the CA Data Content Discovery web interface. At the top, it displays the CA logo, the product name 'CA Data Content Discovery', the user 'MASCAD4', and a 'Log Out' link. Below the header is a navigation sidebar with icons for home, scans, settings, and help. The main content area is titled 'All Scans' and includes a 'CREATE A SCAN' button, 'FILTERS', and 'ACTIONS' buttons. A table lists various scans with columns for Name, Status, User, Date/Time Initiated, Progress, and Description. All listed scans have a status of 'COMPLETED' and a progress bar at 100%.

| Name                        | Status      | User    | Date/Time Initiated  | Progress | Description               |
|-----------------------------|-------------|---------|----------------------|----------|---------------------------|
| Macro Test Scan             | ✓ COMPLETED | CHEJE18 | 20 Oct 2016 9:42 am  | 100%     | Macro Test Scan           |
| PII Test Scan               | ✓ COMPLETED | CHEJE18 | 20 Oct 2016 9:36 am  | 100%     | PII Test Scan             |
| PII scan for australia      | ✓ COMPLETED | HARDE10 | 19 Oct 2016 8:07 pm  | 100%     | Alert on a list of employ |
| macro search                | ✓ COMPLETED | HARDE10 | 19 Oct 2016 8:01 pm  | 100%     | Locate instances of a br  |
| scan of human resource info | ✓ COMPLETED | HARDE10 | 19 Oct 2016 7:59 pm  | 100%     | Identify datasets contain |
| scan for credit card        | ✓ COMPLETED | HARDE10 | 19 Oct 2016 7:52 pm  | 100%     | Discover datasets contain |
| test of isrn                | ✓ COMPLETED | HARDE10 | 19 Oct 2016 5:39 pm  | 100%     | for DCDGA.DCDD00.SMF      |
| Volume - USER01             | ✓ COMPLETED | HUMMA03 | 19 Oct 2016 4:54 pm  | 100%     | SSN-delimited             |
| scan of health information  | ✓ COMPLETED | HARDE10 | 19 Oct 2016 4:44 pm  | 100%     | for australia             |
| Mainline Demo               | ✓ COMPLETED | CHEJE18 | 11 Oct 2016 1:37 pm  | 100%     | Mainline Demo             |
| PCI Check                   | ✓ COMPLETED | MASCAD4 | 17 Aug 2016 12:55 pm | 100%     | Scan for PCI DSS regulat  |
| Phase 1 - PAN               | ✓ COMPLETED | HUMMA03 | 12 Aug 2016 1:33 pm  | 100%     | Primary Account #         |
| Social Security No. Scan    | ✓ COMPLETED | MASCAD4 | 12 Aug 2016 8:08 am  | 100%     | Scan for US Social Sec.   |

## Find

With the mainframe handling such a large amount of corporate data and able to process over 2.5 billion transactions per day,<sup>2</sup> manually finding sensitive or regulated data on the platform is unrealistic.

That's where CA Data Content Discovery comes in. The solution automatically scans the mainframe data infrastructure to immediately identify the location of sensitive and regulated data. Identifying the location of the data is the key to help mitigate risk associated with the retention of data; once the location is known, business decisions can be made to appropriately secure, encrypt, archive or delete the data identified.

CA Data Content Discovery's supported file types span physical sequential, PDS/PDSE, VSAM, DB2, USS, IMS—SHISAM, Datacom and IDMS—covering all core mainframe applications, and the solution's support for data-in-motion helps prevent costly loss of sensitive data moving on the platform.

## Classify

Once CA Data Content Discovery finds the location of sensitive and regulated data, the software classifies the discovered data based on sensitivity level so organizations can place the appropriate safeguards around the data.

With the growing urgency to comply with industry regulations such as the European Union General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX), the need to quickly communicate your compliance posture to auditors is more critical than ever. CA Data Content Discovery enables you to prove to your auditors that controls are in place and are checked by data type and content by showing how and where the data is being accessed on the mainframe.

## Protect

CA Data Content Discovery helps key stakeholders stay in control of their corporate data, gain quick and critical insights about the potential and magnitude of data exposure from 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.

CA Data Content Discovery “helps us understand the relationship of data to PHI, PII and PCI information.”

IT Central Station, CA Data Content Discovery review, Dec 1, 2016

#### Section 4:

## Alert, Inspect and Protect with CA Compliance Event Manager

Running 100 percent on the mainframe, CA Compliance Event Manager helps mitigate data breaches and insider threats through real-time alerting and advanced reporting. The software provides immediate insights about the magnitude of data exposure on the mainframe, comprehensive auditing and forensics support to inspect compliance issues and deeper insights to protect mission-essential assets, eliminate risk and reduce the cost of data protection processes.

The screenshot displays the CA Compliance Event Manager web interface. The page title is "Create z/OS Monitor Policy Statement". The interface includes a sidebar with navigation icons and a main content area with the following sections:

- Statement Description:** A text input field labeled "Description\*" with the placeholder text "Enter Policy Description...".
- Test Conditions:** A section for building test conditions. It includes a "Date" dropdown menu, an equals sign "=" dropdown, and a text input field containing "MM/DD/YYYY". An "Add" button is located to the right of the input field.
- Test Conditions Review:** A section for reviewing the test conditions.
- z/OS Definitions:** A section for selecting z/OS definitions. It includes a "Definitions" section with a list of items: System Datasets, System Environment, SMF, Authorized TSO, EXITS, and System Programs. Each item has a radio button next to it.

### Alert

CA Compliance Event Manager helps mitigate negative security events by alerting to potential risks in real time. 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.

Alerts to potential risk as they occur enable you to gain immediate and critical insight about the potential and magnitude of data exposure on the mainframe so you can act proactively in its remediation and improve your data privacy.



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

### Inspect

Once data exposure threats are identified, CA Compliance Event Manager generates audit and compliance information that is not available in standard security reports through comprehensive auditing and forensics 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.

Additionally, CA Compliance Event Manager provides enterprise-wide insights through an export of mainframe security incidents to Splunk, including a CA Compliance Event Manager Splunk application, for a single-pane-of-glass view of risks that enables security and audit professionals to better manage security end to end in an enterprise.

### Protect

A global survey by CA Technologies shows that only 10 percent of customers are actively addressing their mainframe compliance costs<sup>3</sup> in the interest of reducing them. 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 GDPR.<sup>4</sup>

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 lower 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.

| Description  | From                     | To                       | Subject                         | Priority | Modified by | Modify Date         |
|--|--------------------------|--------------------------|---------------------------------|----------|-------------|---------------------|
| Email - VPA* verification  | aflo35@ca.com            | aflo35@ca.com            | test                            | Normal   | PODM02      | 2016-05-19 12:11:55 |
| Email - Show that ACT2 Security bill was added   | zml15@ca.com             | rcwm02@ca.com            | SECURITY added to LID           | High     | PODM02      | 2016-05-19 12:19:05 |
| Email - PDS change detected  | rcwm02@ca.com            | rcwm02@ca.com            | DDN changed                     | Normal   | PODM02      | 2016-05-19 12:39:45 |
| Email Action - An AFF Library Changed named %DDNN%                                     | ChangeMon@omg.qewrty.com | groupflow@omg.qewrty.com | AFF Library Changed             | Normal   | PODM02      | 2016-05-19 12:39:11 |
| Email Action - Either the APP or LPA or LNK List Changed: %DDNN%                       | ChangeMon@omg.qewrty.com | user@omg.qewrty.com      | APP/PALAN/ Lnk Changed          | Normal   | PODM02      | 2016-05-19 12:38:58 |
| Email Action - A Signon Violation because of a bad password for %USERDN% was detected. | Aler@omg.qewrty.com      | %USERDN%@omg.qewrty.com  | Signon Violation - Bad Password | Normal   | PODM02      | 2016-05-19 12:38:08 |
| Email Action - The user of %USERDN% had a signon violation for a bad password          | Aler@omg.qewrty.com      | %USERDN%@omg.qewrty.com  | Signon Violation - Bad Password | Normal   | PODM02      | 2016-05-19 12:37:57 |
| Email Action - A Security Modify Command was entered by %USERDN%                       | Aler@omg.qewrty.com      | user@omg.qewrty.com      | Security Modify Command         | Normal   | PODM02      | 2016-05-19 12:37:45 |
| Email Action - A Security Stop Command was Entered by %USERDN%                         | Aler@omg.qewrty.com      | user@omg.qewrty.com      | Security Stop Command Entered   | Normal   | PODM02      | 2016-05-19 12:37:29 |
| Email Action - A Security Start Command was entered by %USERDN%                        | Aler@omg.qewrty.com      | user@omg.qewrty.com      | Security Start Command Entered  | Normal   | PODM02      | 2016-05-19 12:36:58 |



### Section 5:

## Enterprise-Wide Data-Centric Security and Compliance

CA Data Content Discovery and CA Compliance Event Manager simplify security management across the enterprise and enable robust, end-to-end protection for data in motion from mobile to mainframe. CA Data Content Discovery and CA Compliance Event Manager are the only data-loss prevention solutions in the market that run 100 percent on and for the mainframe and include all core mainframe applications, with simpler reporting and coverage. And as the IT workforce trends toward a younger, experience-hungry demographic, CA data security solutions provide a simplified yet thorough dashboard that gives IT teams of any skill level the visibility to see and respond to potential vulnerabilities across the enterprise.

As the mainframe continues to transact the majority of enterprise data, plays a critical role as mobile and Internet of Things (IoT) transaction volume and velocity increase, and as new regulations come into play, such as the EU-U.S. Privacy Shield agreement and EU GDPR, these solutions eliminate the need for manual audits by quickly isolating sensitive data, which is the first step in GDPR data privacy compliance.

From finding and classifying to alerting and inspecting, CA Data Content Discovery and CA Compliance Event Manager provide unified enterprise security while helping to increase compliance posture across all platforms.

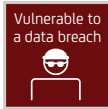


CA brings the **integration of data security and compliance management** to the mainframe.

# Why CA Data Content Discovery?

Fifty years on, the mainframe remains the heart of the data center, managing vast amounts of data. And it's difficult & time-consuming, if not impossible, to locate all the regulated or sensitive data – until now.

## A MAINFRAME WITHOUT CA DATA CONTENT DISCOVERY



- Regulated data open to compromise.
- Data compromise is costly.
- Your company's brand and reputation are at stake.

## A MAINFRAME WITH CA DATA CONTENT DISCOVERY



- Locate and protect regulated data from internal and external risks.
- Reduce risk, complexity, and cost.
- Preserve customer loyalty.

[learn more at ca.com/dcd](http://ca.com/dcd)

To learn more about data-centric security solutions, visit [ca.com/mainframe-security](https://ca.com/mainframe-security).



Connect with CA Technologies at [ca.com](https://ca.com)



CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit [ca.com/customer-success](https://ca.com/customer-success). For more information about CA Technologies go to [ca.com](https://ca.com).

- 1 Verizon, "2016 Verizon Data Breach Investigations Report," 2016, [http://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2016\\_Report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf)
- 2 IBM press release, "IBM Launches z13 Mainframe—Most Powerful and Secure System Ever Built," Jan 13, 2015, <https://www-03.ibm.com/press/us/en/pressrelease/45808.wss>
- 3 TechValidate, Survey of 157 users of CA Mainframe Security Solutions, Aug 16, 2016, TVID F38-414-77A, <https://www.techvalidate.com/product-research/ca-testing-solutions/charts/F38-414-77A>
- 4 Kevin Blasko, Baker & McKenzie, "Data Privacy Survey: GDPR Costs and Complexity," May 4, 2016, <http://www.bakermckenzie.com/en/newsroom/2016/05/data-privacy-survey-gdpr-costs-and-complexity>

Copyright © 2017 CA. All rights reserved. IBM® and RACF® are trademarks of International Business Machines 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.

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.