cm FIRST
Rethink Modernization

// WHITE PAPER

Big Iron Is Vulnerable

How to Protect Mainframe Data at Rest and in Motion

The mainframe is a pillar of our economy. According to IBM, IBM Z[1] alone supports nearly 70 percent of the world's production workloads and more than 30 billion transactions per day—more than the number of Google searches every day.

How important is the mainframe to your business? How long could you survive a mainframe breach or shutdown without losing money?

While z/OS is arguably the most secure computing platform, you must take extra measures to protect sensitive or regulated data residing on the mainframe infrastructure. "Security by obscurity" no longer suffices in a world where cyber attacks are escalating and regulatory requirements are stricter than ever.

What you need are robust, proactive classification and protection processes for data at rest and in motion. Yet finding this data in your mainframe infrastructure is time consuming and difficult, especially with duplicate copies of data in random locations, improper access controls, and the constant motion of data on the mainframe for testing and support.

Here are the reasons why the mainframe environment is at risk and how you can get a handle on your sensitive and regulated data.

Contents

1 https://www-03.ibm.com/press/us/en/pressrelease/52805.wss

Threats to the Mainframe

Security threats and regulatory requirements are hastening the need to reinforce Big Iron. The average annual number of security breaches is up nearly 30 percent, according to the Ponemon Institute's 2017 Cost of Cyber Crime Study[2]. The study also found the global average cost of cyber crime is now $11.7 million, up 22.7 percent from the year before. The most expensive attacks are malicious insiders, denial of service, and Web-based attacks.

Mainframes are vulnerable to these external and internal threats for many reasons.

MALICIOUS INSIDERS

Humans are always the weakest link in security. Making closely held mainframe information available to only a chosen few has historically been a strength, but it can also be a liability. In an article for SHARE.org[3], Reg Harbeck, chief strategist with Mainframe Analytics Ltd., wrote:

> "When only insiders know obscure mainframe configuration and implementation information, but you don't know which insiders for certain, then you become just one more organization that is open to security compromise by insiders—which happens to be the main source of security exposures. And by ex-insiders, who may have any number of reasons and incentives to abuse their knowledge."

PUBLIC INFORMATION ABOUT MAINFRAMES READILY AVAILABLE

The amount of mainframe information publicly available has grown over the years. This includes data such as IP addresses, user IDs, terminal IDs, and detailed error messages. Public email lists can reveal who sent an email, what domain, and even which terminal and/or IP address it came from.

According to Harbeck, this information – whether gathered from public sources or provided by an insider – "…provides the starting point for a well-informed hacker to start drilling into the mainframe, feeding known vulnerabilities and CICS transactions, etc., along with this gleaned information to scripts that then check ports, IDs, passwords, etc., in a sufficiently covert manner not to rouse suspicion while persisting at a large enough volume to have a good chance of finding an opening."

Making matters worse, security researcher Philip Young has found more than 450 mainframes on the Internet[4] that present a login screen to anyone who connects. These mainframes belong to federal and state government sites, airlines, and university health administration systems, among many others.

2 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
3 https://www.share.org/blog/young,-the-mainframe-hacker-public-disclosures
4 https://www.slideshare.net/PhilipYoung14/philip-young-current-state-of-mainframe-hacking-vanguard-101016

MAINFRAME HACKS

With these vulnerabilities, mainframes are not immune to hackings, as Sweden discovered in 2013. A hacker breached the IBM mainframe of Logica[5], a Swedish IT firm that provided tax services to the Swedish government. Not only did he download social security numbers and other confidential information, but also successfully stole funds by hacking into the IBM mainframe of the Swedish Nordea Bank.

Young thinks it's only a matter of time before "a Logica type event[6]" happens in the U.S.:

> "But today's bad actors aren't going to take your mainframe down, at least not on purpose. They're going to inject code in to a CICS transaction to syphon funds, or encrypt all the datasets in your replicated environment to demand a hefty ransom, or steal confidential information to later sell on the darknet. Today's threats are sophisticated and they are aware of the platform [mainframe], they've just been able to target lower hanging fruit."

Indeed, CICS is particularly interesting to Young:

> "Once I realized it's not that different from a web app I started to think about the current lack of research or discussions. When you break it down, it's just screens with data behind it. How can I manipulate the business logic to gain access to areas of the application I shouldn't?"

REGULATORY ISSUES

State, federal, and international regulatory requirements present another reason to secure your mainframe environment. Depending on your industry, in the U.S. alone you may be subject to data privacy and security stipulations from federal laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act. Countries such as Russia, Germany, Canada, and France have laws that require personal data about its citizens to stay within each country's borders (or in France's case within EU territories).

One international regulation that presents both a mandate and opportunity to strengthen security is the EU's General Data Protection Regulation[7] (GDPR), effective May 25, 2018. Basically, GDPR requires companies to pinpoint as well as demonstrate how and why personally identifiable information is being

5 https://www.pcworld.com/article/2034733/pirate-bay-cofounder-charged-with-hacking-ibm-mainframes-stealing-money.html
6 https://www.share.org/blog/young-the-mainframe-hacker-ob-sec-urity
7 http://www.eugdpr.org/

used, with the proper measures and control in place. Organizations must know where data is stored and how to mitigate risks.

GDPR applies to any company that offers goods and services within the EU and has customers and employees based there. It gives the EU more power to enforce strict fines and penalties on organizations that don't comply with the law or experience data breaches.

Protecting Regulated and Sensitive Data

The best practices for complying with regulations such as GDPR and securing your mainframe data apply to any organization. These three steps serve as a starting point:

- **Catalog your tech and data assets and determine their use, including:**
  - Which data elements contain privacy information?
  - Where is the data physically stored?
  - Which systems/processes use the information and can create, read, update or delete?
- **Analyze data protections and identify at-risk data:**
  - What controls are applied to technology assets/processes to support secure handling and transport of information?
  - What confidentiality level is required to keep the data safe?
- **Understand data lineage and where and how that data is being used:**
  - What applications process the data and how? How secure are they?
  - Where is the data processed?
  - Is the information transferred cross-border (in the case of GDPR and other regulations)?

Data Lineage and Security

CM evolveIT[8] together with the CA Data Content Discovery[9] product provide a complete data lineage and security analysis solution for mainframe data at rest and in motion. This powerful combination can help you proactively secure sensitive information across all aspects of the data lifecycle and facilitate regulatory compliance, from database to application code.

8 http://cmfirstgroup.com/offerings/products/cm-evolveit/
9 https://www.ca.com/us/products/ca-data-content-discovery.html

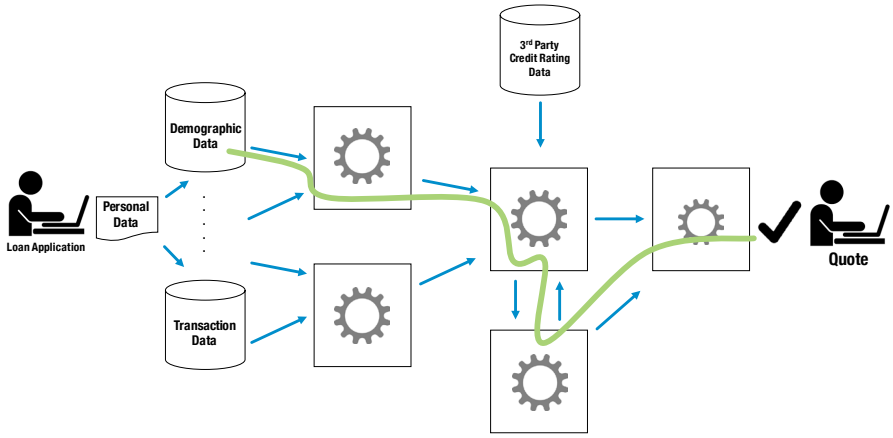

Figure 1. Understanding data origin, where it moves and what happens to it over time is critical for assuring sensitive data security and compliance

CA Data Content Discovery scans the mainframe data infrastructure to find and classify sensitive data. CM evolveIT examines the entire mainframe application portfolio to trace the data lineage, showing where and how sensitive data is processed. Here's how both work.

About CA Data Content Discovery

CA Data Content Discovery is the first of its kind automated tool for finding sensitive and regulated data 100 percent on the mainframe. The solution:

- Finds regulated and sensitive data on z Systems to prevent the risk of data exposures
- Classifies sensitive data and verifies that controls are checked to satisfy compliance regulations. Helps you address potential audit findings and risks
- Protects highly regulated or other non–public, business-critical data and helps you control who has access to it

Figure 2. CA Data Content Discovery finds sensitive data in the mainframe infrastructure so it can be classified and protected appropriately

CA Data Content Discovery identifies data exposure risks by scanning through the mainframe data infrastructure. The product finds and classifies data across common file types, databases, and transfer products and provides comprehensive reporting on the scan results.

Determining the location of the data is the key to help mitigate the risks associated with data retention. Once the location is known, you can make business decisions to appropriately secure, encrypt, archive or delete the data. Working with popular mainframe access control products, user access to sensitive information can be monitored and restricted, as necessary.

About CM evolveIT

CM evolveIT completes the solution by analyzing the mainframe application portfolio to trace the data lineage, showing where and how it is processed in screens, reports, files, and databases through millions of lines of code. With this information, you can make necessary code changes to ensure all instances of data use are known, appropriate, and secure.

CM evolveIT is designed to work at scale across your project portfolio, reducing problems caused by analyzing programs in isolation. The product automates discovery and documentation of business rules and system interactions. You'll quickly discover a thorough, reliable understanding of the business logic embedded in your legacy systems. New teams can master your business-critical applications fast with:

- Auto-documentation that provides a complete, understandable picture of the application, immediately accessible through the metadata repository
- Impact analyses that are generated and delivered through intuitive graphical interfaces and reports
- Visualizations that help analysts find, interpret, describe and model how rules in the application are running the business
- A common language that both business and software analysts can understand
- Scalability to reduce problems caused by analyzing programs in isolation

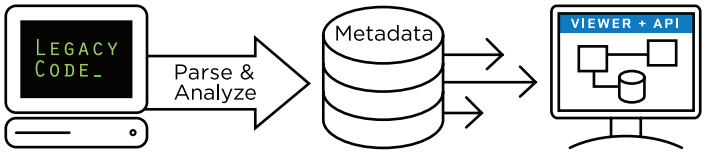

Figure 3. CM evolveIT analyzes mainframe source code to determine how sensitive data is processed

CM evolveIT eliminates the chaos and panic of maintenance and enhancements or modernization. Your business continuity is protected since CM evolveIT's full view of business rules and system interactions lets you find the safest path to migrate or decommission legacy code.

With your business rules abstracted from the restrictions of legacy code, you are future-proofed and can deploy apps on the optimal platform. In addition, a common understanding between your business and software analysts means you're better positioned to ensure your apps deliver the value that's needed.

Benefits of the Data Lineage and Security Solution:

- **Risk Mitigation:** Gain critical insight into the magnitude of potential data exposure on z Systems. Help detect, categorize, and secure highly regulated and sensitive data to facilitate regulatory compliance and prevent data breaches. Prove to auditors that controls exist for identifying and reporting on all sensitive data. Determine whether to encrypt, archive or delete the data to prevent misuse or duplication of data elsewhere.
- **Cost Reduction:** Determine areas of duplication for elimination or consolidation, driving reductions in systems costs, IT time, and maintenance expenses. Lower staffing costs associated with manual detection of regulated or sensitive data on the mainframe and all application references to it.
- **Improved Customer Experience:** Instituting data privacy controls gives you a better understanding of your customer-facing processes and applications as well as their purpose within the organization. This also helps to support privacy by design approaches to technology.

About CM First Offerings

CM First's powerful automation tools, augmented by professional services staff with many decades of software engineering and DevOps experience, ensure successful outcomes for even the most demanding modernization projects. Our products and expertise have helped over 400 customers in the public and private sectors reach their desired future state faster and more cost effectively than by using conventional approaches.

CM First software quickly analyzes, documents and re-platforms legacy code bases with minimal errors and rework, including those that are too large and complex for humans to tackle in any reasonable timeframe. The output is immediately usable by all team members, regardless of experience and knowledge of legacy software languages, accelerating application maintenance and modernization projects.

For more information, visit **cmfirstgroup.com**

Request a Demo Today

Contact us for more information or to schedule a demo. Call 888-866-6179 or email us:
info@cmfirstgroup.com

cm FIRST
Rethink Modernization

CM First Group
888-866-6179
cmfirstgroup.com

7000 North Mopac Expressway
Plaza 7000, 2nd Floor
Austin, Texas 78731