SOLUTION BRIEF • CA TRUSTED ACCESS MANAGER FOR Z

How Can You Deliver Trusted Services and Improve Business Efficiency Through Privileged Access Management on the Mainframe?

CA Trusted Access Manager for Z helps deliver trusted systems and improve business efficiency by providing comprehensive privileged access management for your mainframe. The solution eliminates the need for shared privileged credentials, works directly with your mainframe security best practices, and produces forensics on all privileged user activity so you can stay in complete control over mission-essential mainframe data.

Executive Summary

Challenge

Privileged identities on the mainframe have extensive access to the most sensitive resources in the entire data center. These identities are essential for business emergencies, but often privileged identities with shared credentials are created, which violates many policies and causes failed audits. Today's approach requires manual management, which is prone to error, but when privileged identities aren't managed securely, the business is exposed to a significant risk of insider threats—some of which can take months and even years to discover.

Opportunity

Digital trust is the cornerstone of the application economy. Without it, all business processes grind to a halt. CA Trusted Access Manager for Z helps organizations build trust and improve business efficiency by providing streamlined and secure management of privileged user identities on the mainframe, helping to make sure that only the right users have the right access at the right time.

Benefits

CA Trusted Access Manager for Z runs 100 percent on the mainframe, tightly integrated into external security manager (ESM) solutions CA ACF2™ and CA Top Secret®, to enable security teams to more easily administer privileged identities using existing processes and best practices. The solution can both promote and demote permissions and rules for existing users to greatly reduce the threat surface of sharing privileged credentials.

SECTION – 1

Trust Is the Cornerstone of the Application Economy

Digital trust is the cornerstone of the application economy. Without it, all business processes come to a halt. Trust flows throughout your entire enterprise, people, data and systems—but what happens when the largest risks you face come from inside the enterprise itself? A recent global study found that more than 77 percent of data breaches derive from internal sources, and among those breaches, nearly 70 percent took months or even years to discover.[1] As data continues to grow exponentially, the importance of staying in complete control to reduce your organization's risk becomes paramount.

The security landscape on the mainframe is changing drastically. While the platform is increasingly connected to the rest of the data center (and the outside world), exposing more of its sensitive PII data, the insider threat landscape is evolving: Internal breaches are becoming the majority, and the financial incentives of selling sensitive information on the dark Web are high.

The answer to reducing the insider threat surface on the mainframe is a simple one: tighter access controls for sensitive data, which begins by following the principles of least access. These principles revolve around the ideology of only providing employees with the level of access necessary to perform their job function, removing unnecessary privileges as needed, and then monitoring user behavior to prevent any suspicious activity. This stronger management of access is needed especially for privileged users on the mainframe, who have extensive access to business-critical resources.

When privileged users on the mainframe aren't managed securely, or managed at all, the business is exposed to a significant risk of security threat. And as the threat landscape shifts to predominantly insider-based attacks, the secure management of privileged users across on the mainframe is vital to both business efficiency and developing trust, both inside and outside the organization.

77 percent of data breaches derive from internal sources

SECTION – 2

Privileged Access Management for Mission-Essential Data

Data breaches continue to cause massive damage to today's organizations, both financially and to reputations, so protecting yourself against security threats is job number one. A recent study found that most of today's breaches come from internal actors and that the cost of a single breach to an average U.S. financial services organization is approximately $11 million in direct costs.[2] But more important, 31 percent of consumers surveyed said they would discontinue their relationship with the brand that had the breach.[3] Simply put, digital businesses that fail to develop trust fail to succeed.

This strong prevalence of insider threat calls for tighter management of access controls across the business, especially for users with privileged access rights. Organizations need to securely manage which user identities have which privileges, record what the users are doing in their privileged state to simplify auditing and be prepared to revoke privileged rights when necessary to reduce risk. Starting with the principles of least access, organizations must determine:

Who has access. The first stage of a privileged governance strategy is to identify which user identities have privileged access and to which resources, so you can revoke rights and eliminate orphaned accounts.

Whether users need access. Once you eliminate orphaned accounts and revoke access from identities that no longer need elevated access, you must determine under which circumstances users need privileges. Do users need access all the time to every resource, or just temporary access to specific datasets?

How to monitor access. After identifying which users need privileged user rights and eliminating those that do not, you'll then need to monitor privileged identities to ensure that their activity in the privileged state is in accordance to their job roles and responsibilities.

Now consider the mainframe, which continues to transact the majority of today's enterprise data. Privileged identities on the mainframe have extensive access to the most sensitive resources in the data center. These identities are critical for handling "system down" situations and other business emergencies outside of normal day-to-day operations, but unless they're managed securely, the business is exposed to a significant risk of catastrophic data loss.

The incentives of selling privileged datasets on the dark Web are high. The average cost per stolen record is $141,[3] and approximately 47 percent of breaches[3] involve a malicious or criminal attack. And with the sheer volume of sensitive corporate data residing on mainframes, the financial incentives for stealing and selling that data are attractive. But not all employees are malicious, and another 25 percent of data breaches are due to negligent employees or contractors,[3] so mistakes can happen too. The key is to have tighter access controls around the data to prevent the risks before breaches occur.

However, tracking privileged identities on the mainframe requires manual management, and many privileged credentials are shared among employees, which causes significant credential control issues and huge obstacles for auditing. What is needed is a unified, automated and streamlined approach to managing access across all users with access to mission-essential mainframe resources.

The average cost per stolen record is $141

SECTION – 3

Build Trust in the Application Economy

CA Trusted Access Manager for Z is the only solution on the market that restricts and monitors all activity performed by privileged accounts on the mainframe

Organizations must maintain complete control over their corporate data to win customer loyalty, boost employee productivity, build trust and succeed in digital business. This starts by securing the most sensitive data in the business and controlling the users that have the highest levels of access to it: privileged identities on the mainframe. CA Trusted Access Manager for Z is the **first and only solution on the market** that restricts and monitors all activity performed by privileged accounts, operating 100 percent on the mainframe. Working in conjunction with CA ACF2 and CA Top Secret, CA Trusted Access Manager for Z promotes and demotes your existing user identities to reduce the risk of credential sharing and operates in line with your security team's processes and work flows, while providing in-depth reporting and forensics into all privileged user activity.

Reducing the Risk of Credential Sharing

As insider threats are taking over the data breach landscape, ensuring that employees only have the necessary levels of user access is increasingly essential. Whether it's a malicious attack or an inadvertent mistake, once an employee infiltrates the data, the entire organization is at risk. The challenge today is that organizations have a variety of expert users who are qualified to use privileged identities. However, only a small number of privileged identities are created, and these identities are shared among these expert users—and until now, that has meant sharing the credentials for privileged identities, which creates a massive audit failure waiting to happen. How can you build trust with your stakeholders if you don't have full insight into exactly who is accessing your data and when?

CA Trusted Access Manager for Z greatly reduces the risk of credential sharing and the insider threat surface by elevating and demoting existing user identities on demand. With this solution, security administrators of CA ACF2 and CA Top Secret can validate requests to elevate the permissions of existing users by checking that the request is initiated by a ticket from their organization's service desk. CA Trusted Access Manager for Z then gives security managers the option to approve or deny the employee's access request, and, if it is approved, the option to timebox how long the access should be given for. The solution then audits all access requests, so security leaders have full insight into which identities submitted access requests and when.

Comprehensive Auditing and Reporting

A picture is worth a thousand words. CA Trusted Access Manager for Z not only provides auditing reports on access requests but also generates auditing and forensics on all activity performed by identities in their privileged state—from the activity in the datasets to the demotion of the user identity—providing a holistic, full-picture view for security managers. The auditing and forensics is done natively and via integration with CA Compliance Event Manager, which monitors mainframe data for abnormal activity, alerts to risks in real time, inspects the source of incident through advanced forensics and provides in-depth reporting on the security issue, bringing the solutions together to protect against security threats.

With CA Trusted Access Manager for Z's comprehensive auditing and reporting, security leaders have full insight into all privileged activity and can then follow the principles of least access. Security teams can review exactly which identities have privileged access, evaluate whether access is needed, monitor that access, revoke access when suspicious activity is suspected and reduce risk through staying in full control.

Working With Your Mainframe Security Processes and Workflows

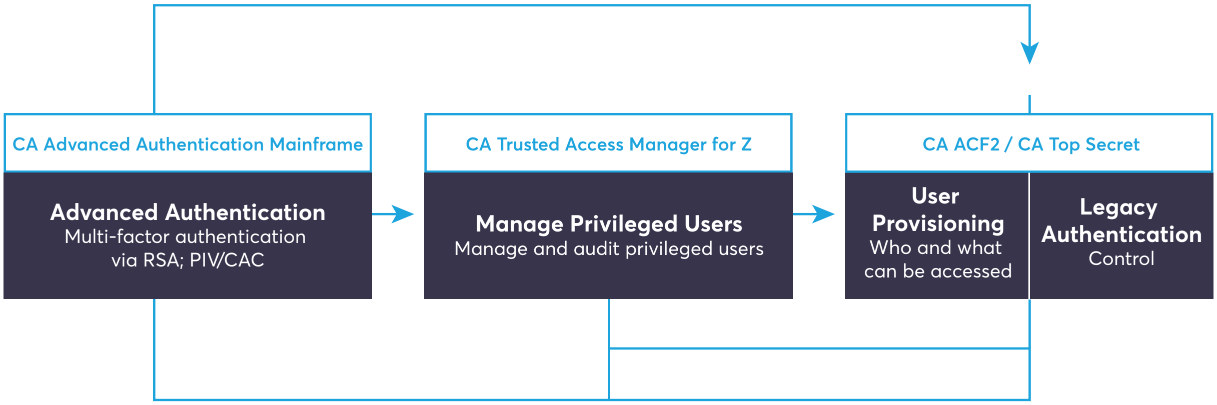
As the mainframe continues to interconnect with the rest of the data center, privileged access management is an essential component of your mainframe security strategy. But security also needs to be streamlined and frictionless so it doesn't slow employees down or impact the customer experience. CA Trusted Access Manager for Z provides you with the flexibility to issue privileged access quickly, so teams can address emergencies before they impact the business, but also securely, so managers have a full line of sight.

By integrating directly into CA ACF2 and CA Top Secret, CA Trusted Access Manager for Z not only reduces the risk of creating more identities and credentials to be managed but also enables teams to operate with their established processes, best practices and workflows. Security teams can add CA Trusted Access Manager for Z on top of their CA ACF2 or CA Top Secret security infrastructure using the same user interfaces, so it's easy to learn and start leveraging from day one. CA Trusted Access Manager for Z adds the additional layer of security needed for today's connected mainframe environments without adding an additional layer of complexity.

Deliver trusted mainframe services with CA Trusted Access Manager for Z

FIGURE A.

The CA Mainframe Identity and Access Management Story


CA Advanced Authentication Mainframe
Advanced Authentication
Multi-factor authentication via RSA; PIV/CAC
CA Trusted Access Manager for Z
Manage Privileged Users
Manage and audit privileged users
CA ACF2 / CA Top Secret
User Provisioning
Who and what can be accessed
Legacy Authentication
Control

SECTION – 4

Conclusion

Trust has a direct correlation to business outcomes, and data breaches are causing a loss of trust and limiting growth in the digital economy. Delivering trusted mainframe services and improving business efficiency revolves around security that is simple to use, streamlined and effective. Organizations can build trust by securing the most sensitive data in the business and controlling the users that have the highest levels of access to it: privileged identities on the mainframe.

CA Trusted Access Manager for Z:

- Reduces the risk of credential sharing by promoting and demoting existing identities from CA ACF2 and CA Top Secret to privileged access for business emergencies.
- Simplifies auditing by providing advanced forensics on all privileged user activity via integration with CA Compliance Event Manager.
- Aligns with mainframe security best practices and workflows, so it’s easy for teams to learn.
- Provides comprehensive management of privileged users with access to the most sensitive data in the business.

Protect against recovery costs, customer loss and fines and succeed as a digital business in the modern software factory by delivering trusted mainframe services with CA Trusted Access Manager for Z.

For more information, please visit **ca.com/TAM**

Connect with CA Technologies

[1] 2016 Verizon Data Breach Report

[2] Ponemon Institute, Data Breach Study, 2016

[3] Ponemon Institute, Reputation Risk Study, May 2017

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.