Solution Brief

Comprehensive Privileged Access Management on the Mainframe

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 operations and emergencies. Often, privileged identities with shared credentials are created, which violates many control policies and causes failed audits. These identities are also targets for those seeking illegitimate access to systems and data.

Today's approach requires manual management, which is prone to error, but when privileged identities are not managed securely, the business is exposed to a significant risk of 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. 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. It helps to make sure that only the right users, have the right access, at the right time.

Benefits

Trusted Access Manager for Z runs 100% on the mainframe, tightly integrated into external security manager solutions ACF2™, Top Secret™, and IBM RACF to enable security teams to more easily administer privileged identities using existing processes and best practices. The solution provides just in time access to a privileged state, greatly reducing the window of privileged access. The solution allows for self-service access provided prior authorization has been granted to obtain privileged status, and optionally business justification for privileged access is validated.

Privileged access management helps deliver confidentiality, integrity, and availability to your systems. It improves business efficiency by reducing the risk related to threats targeting mission-critical infrastructure, applications, and regulated business data. Implementing a comprehensive privileged access management solution reduces the risk associated with privileged access by adding trust in the identity of privileged users, delivering just in time access to privileged resources, following the principle of least privilege, and producing forensics on all privileged user activity.

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. Now consider the mainframe, which continues to execute 80% of business workloads (Application Modernization on the Mainframe). The mainframe is a mission-critical system for business operations. By necessity, privileged identities on the mainframe have extensive access to the most sensitive resources in the data center. These identities are critical for handling *system outages* and other business emergencies outside of normal day-to-day operations, but unless they are managed securely, the business is exposed to a significant risk of catastrophic data loss or system outages.

The security landscape on the mainframe is changing drastically. The platform is increasingly connected to the rest of the data center and the outside world, thus having more exposure. Bad actors target systems and data for various motives, including geopolitical. The human element is involved with 82% of breaches, with phishing dominating as the socially engineered method to extract credentials leading to a breach (Verizon Data Breach Investigation Report 2022). Incentives for selling privileged datasets on the dark web are high. The average cost per stolen record is $161 (USD), and approximately 47% of breaches involve a malicious or criminal attack (IBM Security Cost of a Data Breach 2021). With the sheer volume of sensitive corporate data on mainframes, the financial incentives for stealing and selling that data are attractive. But not all acts are malicious. Another 25% of data breaches are due to negligent employees or contractors, so mistakes can happen too (IBM Security Cost of a Data Breach 2021). The key is to have tighter access controls around critical infrastructure such as the mainframe and its data to prevent incidents before they occur.

Privileged access puts the entire organization at risk, whether it is a malicious attack or an inadvertent mistake. It is imperative to control, restrict, and monitor privileged access.

Trust is the Cornerstone of the Application Economy (cont.)

The answer to reducing privileged access threat exposure on the mainframe is simple.

Deeper Validation of the Identity of the User Accessing the System

Advanced authentication is necessary to add trust in the identity of users accessing mainframe applications. Validation of credentials beyond a simple or complex password is needed to establish identity. Advanced authentication includes the use of multiple authentication factors, a policy detailing which factors should be applied and when, and risk modeling to thwart anomalous behaviors.

Tighter Access Controls and Application of the Principle of Least Privilege

The principle revolves around the ideology of only providing employees with the level of access necessary to perform their job function for the time required to perform such function, removing unnecessary privileges as needed, and then monitoring user behavior to prevent any suspicious activity. This stronger access management is needed especially for privileged users on the mainframe. These users have extensive access to business-critical resources.

Continuous Monitoring

Continuous monitoring of privileged identities, regulated data, and mission-critical infrastructure is required by many regulatory requirements. Continuous monitoring ensures that you have real-time notification of all activity and an audit trail for forensics should it be needed.

Assessing Access Risks

Risk modeling can enable focus on the most significant access risks. Aggregate data to give insights into security risks and focus on mitigating the highest risks.

Build Trust in the Application Economy

Organizations must maintain complete control over their systems and corporate data to win customer loyalty, boost employee productivity, build trust, and succeed in the digital economy. This control starts by securing the most mission-critical systems and sensitive data in the business, and controlling the users with the highest access levels—the privileged identities on the mainframe.

Advanced Authentication Mainframe

Advanced authentication for mainframe systems enables deeper trust in the identity of the users authenticating to mainframes—at the application level.

- Deepens the trust in the identity of users by requiring multi-factor authentication.
- Implementation can be user or application-specific.

Cleanup

Continuously monitor the use of user IDs and entitlements so that they can be removed from the security database when no longer in use.

- Remove user IDs no longer in use.
- Remove entitlements that are no longer in use.
- Streamline re-certification efforts by exclusively focusing on IDs and entitlements in use.
- Command creation to cleanup and restore (if needed).

Trusted Access Manager for Z

Trusted Access Manager for Z reduces the risk of insider threats that could lead to data loss and system outages by streamlining the management of privileged access on the mainframe. Trusted Access Manager for Z provides the only mainframe elevation-based (just in time) privileged access management solution.

- Elevate to privileged state when the business requires the user have it.
- Define granular elevation points to adhere to Principles of Least Privilege.
- Full audit trail of activity while in privileged state.
- Simplifies auditing by providing advanced forensics on all privileged user activity through integration with Compliance Event Manager.
- Reduces the risk of credential sharing by promoting and demoting existing identities to privileged access.
- Runs 100% on the mainframe.
- Supports all three external security managers.

Compliance Event Manager

Continuously monitor the mainframe user IDs, data, and resources critical to business operations.

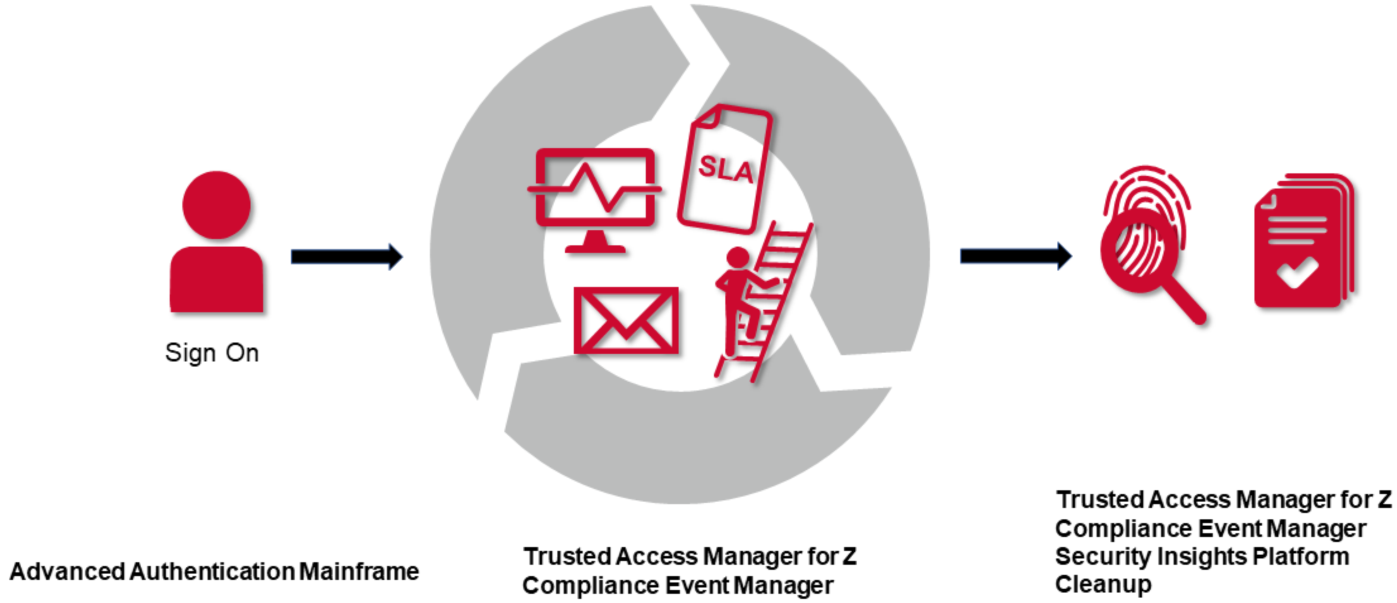
- Real-time monitoring of security events, security configuration, operating system security configuration, and partitioned data set member content.
- Receive real-time alerting or audit trail for forensics.
- Real-time alerting when a user elevates to a privileged state.
- Filterable events to hone in on audit records needed.
- Integrate with SIEM for inclusion in enterprise reporting.

Security Insights

Risk modeling with correlated data sources can pinpoint risk relative to system critical resources and access to data.

- Self-service reporting to identify the risk of system critical resources or data owned by the business.
- Interpreted output to understand risk and remediation efforts by data owners and technical staff of all skill levels.

Privileged User from Sign On to Forensics


Sign On
SLA
Advanced Authentication Mainframe
Trusted Access Manager for Z
Compliance Event Manager
Trusted Access Manager for Z
Compliance Event Manager
Security Insights Platform
Cleanup

Conclusion

Trust has a direct correlation to business outcomes. Delivering trusted mainframe services and improving business efficiency revolves around simple, streamlined, and effective security.

Organizations can build trust by securing the most mission-critical systems and sensitive data in the business, and controlling the users with the highest access levels—privileged identities on the mainframe.

When privileged users on the mainframe are not managed securely or managed at all, the business is exposed to a significant security threat risk. Implement the Broadcom® Privileged Access Management solution to reduce the risk associated with privileged access by controlling, restricting, and monitoring these high-powered IDs.

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

200-319139-0622 August 10, 2022