BROADCOM®
MAINFRAME SOFTWARE

Product Brief

Trusted Access Manager for Z

Key Benefits

- **Control:** Restrict who has access to a privileged state, and timebox the duration of the elevated state.
- **Audit:** Simplify auditing by eliminating privileged credential sharing and maintaing a complete line of sight.
- **Protect:** Stay in complete control when users have privileged access to deliver trusted systems.

Key Features

- **Reduces credential sharing:** Promotes and demotes existing user identities from ACF2, Top Secret, and IBM RACF to manage, monitor, and control access to privileged data.
- **Delivers trust and efficiency:** Integration with your service desk helps to ensure that all access requests have a business need so that you can improve the efficiency of mainframe operations.
- **Aligns with security workflows:** Works directly with ACF2, Top Secret, and IBM RACF, using the same interface, so that it is easy to learn and start leveraging from day one.
- **Offers advanced auditing and forensics:** Integrates with Compliance Event Manager for in-depth auditing and a forensics view of all privileged user activity.
- **Operates 100% on mainframe:** An industry-first solution for privileged access management, operating entirely on the mainframe platform.

At a Glance

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 identities on the mainframe. The solution elevates and demotes existing user identities based on the business need to eliminate privileged credential sharing and persistent elevation. The solution provides comprehensive auditing and forensics for all privileged user activity for complete visibility. The solution also works directly with ACF2™ and Top Secret™ and IBM Resource Access Control Facility (IBM RACF) to align with existing best practices and workflows to restrict access to mission-essential data, and improve efficiency by delivering trusted mainframe services.

Business Challenges

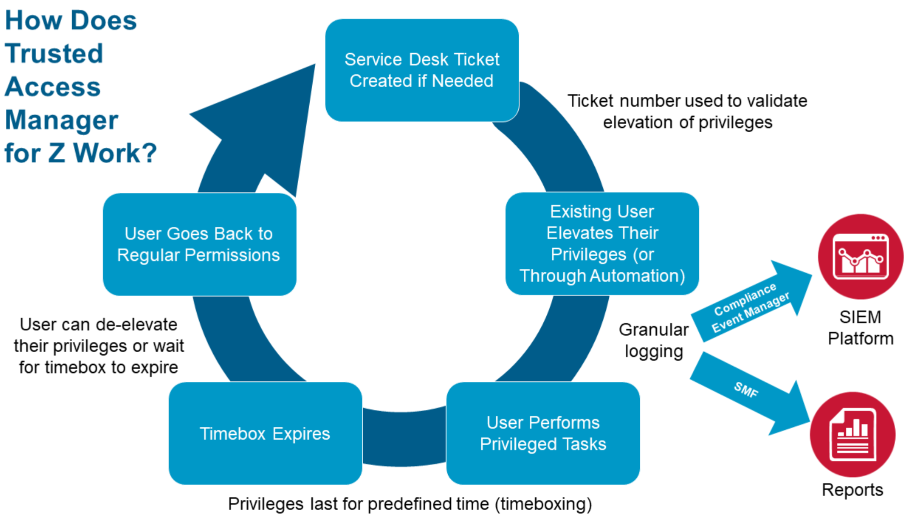
The data breach landscape is evolving, and insider threats now represent most threats. Whether through a malicious breach or an honest mishap, internal actors pose a risk to sensitive resources. Moreover, it is difficult to track the security incidents when security administrators share credentials for privileged identities. Even though internal actors represent the majority of threats, the unauthorized use of privileged identities by external actors can still pose an immense risk as most privileged identities have broad access. For example, many privileged identities have access to data encryption keys or have the ability to issue commands or make configuration changes that potentially allow the privileged identity to circumvent other controls.

On the mainframe, privileged identities have extensive access to the most crucial resources in the business. These privileges are essential to resolving emergencies, general system operations, and maintenance. If these privileges are not managed securely, the business is exposed to a significant risk of data loss. The challenge is that the definition of a privileged user on the mainframe can be broad. In addition, tracking privileged identities on the mainframe requires manual management, which is prone to error. Just one improperly authorized privileged identity can result in a catastrophic breach. You need a unified, automated, and streamlined approach to managing privileged users who have access to mission-essential mainframe resources.

Solution Overview

Trusted Access Manager for Z is the first solution on the market that restricts and monitors all activity performed by privileged accounts, and operates 100% on the mainframe. The solution works directly with the top three external security managers (ESMs): ACF2, Top Secret, and IBM RACF. Trusted Access Manager for Z provides just-in-time promote and just-in-time demote for existing user identities after validating the business need through your organization's service desk. This validation of the business need justifies the use of a privileged state by the user.

Privileged User Management with TAMz


How Does Trusted Access Manager for Z Work?
Service Desk Ticket Created if Needed
Ticket number used to validate elevation of privileges
Existing User Elevates Their Privileges (or Through Automation)
Granular logging
Compliance Event Manager
SIEM Platform
SMF
Reports
User Performs Privileged Tasks
Privileges last for predefined time (timeboxing)
Timebox Expires
User can de-elevate their privileges or wait for timebox to expire
User Goes Back to Regular Permissions

Solution Overview (cont.)

The solution also generates auditing and forensics on all activity performed by identities in their privileged state to provide a comprehensive view designed to simplify auditing. Trusted Access Manager for Z aligns with your security team's best practices and workflows. Your security team has the flexibility to issue access to address emergencies quickly. The security team also has a full line of sight into privileged identities on the mainframe, so you can improve efficiency and deliver trusted systems. The solution helps to eliminate the risk of privileged credential sharing, eliminates users in a perpetually defined privileged state, and deters usage outside the need for the privileged state by auditing all activity.

Critical Differentiators

Trusted Access Manager for Z is the only privileged access management solution on the market that operates 100% on the mainframe, supports all three ESMs, and uses the elevation model. Trusted Access Manager for Z leverages the leadership provided by Broadcom in the mainframe security market. The solution builds on the top three ESMs for mainframes to provide just-in-time promotion and demotion of existing user identities to a privileged status for business emergencies or routine system operations. The solution simplifies privileged access management on the mainframe by using the same solutions already in your organization, helping to streamline auditing by reducing privileged credential sharing and providing in-depth reports of user activity, and enabling the business to protect against insider threats to improve efficiency and deliver trust.

Related Products

The mainframe security portfolio from Broadcom works together across the security lifecycle. While each offering delivers value individually, combining data across offerings delivers greater value, yielding insights into hidden risks. The complete solution is available within the Mainframe Security Suite and contains the following products:

- **Advanced Authentication for Mainframe:** Offers enhanced verification to deepen the trust in the identity of users on your system.
- **Auditor:** Identify security risks and automate the z/OS audits and integrity checks.
- **Cleanup:** Automatically eliminate unused IDs and entitlements.
- **Compliance Event Manager:** Collect and monitor real-time security information, compliance-related information, and events within the mainframe environment with the ability to send data to Splunk or an enterprise SIEM solution.
- **Mainframe Security Insights Platform:** Collect, aggregate, and analyze security data to understand the mainframe security posture and remediate mainframe security risk.
- **Trusted Access Manager for Z:** Monitor and control privileged users by granting time-bounded just-in-time access to the system, critical resources and regulated data, or resources with 1:1 accountability and auditing.

The Mainframe Security Suite provides the components you need to completely modernize mainframe security and align the mainframe platform with your enterprise security control mandates. As a package, it enables adoption of components as security needs allow. You have the comfort of knowing that a world expert in mainframe security is available to help you from planning, to install, and with ongoing best practices.

Reduce business risk and improve compliance with a comprehensive modern mainframe strategy. This strategy is a best practices-based process that advances mainframe protection and moves security from firefighting to strategic value.

For more information, please visit www.broadcom.com/products/mainframe/identity-access/trusted-access-manager-for-z.

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

200-319137-0123 January 19, 2023