Solution Brief

BROADCOM
MAINFRAME SOFTWARE

Advanced Authentication Mainframe and Trusted Access Management for Z Entitlement

Key Benefits

- **Trust:** Deepen the trust in the identity of individuals accessing the mainframe.
- **Protect:** Stay in complete control when users have privileged access to deliver trusted systems.
- **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 maintain a complete line of sight.

Key Features

- **Flexible for some or all:** Implement for particular users or applications as required by business needs.
- **Aligns with security workflows:** Works directly with ACF2, Top Secret, and IBM RACF using the same interface, so it is easy to learn and start using from day one.
- **Reduces credential sharing:** TAMz 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:** TAMz integrates 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.
- **Offers advanced auditing and forensics:** TAMz integrates with Compliance Event Manager for in-depth auditing and a forensics view of all privileged user activity.

Multi-factor authentication and privileged user management entitlements are now included with ACF2™ and Top Secret™.

At a Glance

Management and control of privileged users is a difficult task in any environment. Broadcom is pleased to announce we are making this job easier on the mainframe by including the entitlement for Advanced Authentication Mainframe (AAM) and Trusted Access Manager for Z (TAMz) along with licensure for ACF2™ and Top Secret™. If you license either ACF2 or Top Secret, the entitlement also allows the use of AAM and TAMz in your RACF environments. Additionally, Broadcom has included the entitlement for Symantec® VIP Authentication Hub along with AAM for a modern multi-factor authentication experience on your mainframe. If you license or are entitled to AAM, the entitlement also allows the use of Symantec VIP Authentication Hub with your mainframe environment.

AAM helps reduce the risk that could lead to data loss and ensures more trusted system access by providing multi-factor authentication to users. Advanced Authentication is perfect for privileged users due to the increased risk of access and can be implemented for any user on the system. Implementation is flexible and can be phased into the environment with no application updates required because AAM can be configured to always supply an 8-character logon credential. AAM's risk-based authentication policy provides extra protection for privileged users above and beyond traditional mainframe multi-factor authentication solutions. AAM asks for additional verification for high-risk logons based on criteria such as time of day, location, or logon velocity.

TAMz 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 business need to eliminate privileged credential sharing and persistent elevation. It also provides comprehensive auditing and forensics for all privileged user activity.

Business Challenges

The data breach landscape is evolving, and insider threats now represent the majority of all threats. Internal actors, whether through a malicious breach or an honest mishap, pose a risk to sensitive resources. Moreover, it is difficult to prevent one of the most common types of insider threats because it is hard to track the incidents when shared credentials are used for privileged access.

Key Features (cont.)

- **RADIUS support:** AAM supports the RADIUS protocol which enables configuration against all popular authentication services.
- **Compound in-band support with RADIUS:** Increase identity assurance by requiring users to provide an ESM password or passphrase along with a RADIUS credential.
- **PIV/CAC support:** AAM integrates with Symantec Privileged Access Manager to extend support for smart cards.
- **Audit and Forensics:** AAM Integrates with Compliance Event Manager for real-time alerting and reporting on authentication events in addition to native SMF reporting through the ESMs to track user activity.
- **No application updates required:** AAM integrates with Symantec VIP Authentication Hub to always provide an eight-character credential for logon, eliminating the need for application updates to support multi-factor authentication.
- **Risk-based authentication policy:** AAM integrates with Symantec VIP Authentication Hub to require additional factors for high-risk logons based on logon conditions such as location, time of day, or logon velocity.

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.

Business Challenges (cont.)

On the mainframe, privileged identities have extensive access to the most critical resources in the business. These privileges are essential to resolving emergencies outside of daily operations, but when they are not managed securely, the business is exposed to a significant risk of data loss. The challenge of tracking privileged identities on the mainframe is that it 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

Implementation of a full solution for privileged users reduces the risk surrounding these high-powered identities. The Broadcom® privileged user management solution starts with control and management at sign-on, continues with management and control with each user action, and concludes with the ability to fully audit the session.

AAM can significantly increase the security of application and data access. By requiring additional information beyond a password, applications have greater assurance that its users are who they say they are.

Working with External Security Managers (ESMs), ACF2, Top Secret and IBM RACF, AAM features deliver multi- factor authentication to strictly control who has access to critical business resources.

AAM's risk-based authentication policy provides extra protection above and beyond traditional mainframe multi-factor authentication solutions by asking for additional verification for high-risk logons based on criteria such as time of day, location, or logon velocity.

AAM is perfect for privileged users due to the increased risk of access and can be implemented for any user on the system. Implementation is flexible and can be phased into the environment with no application updates required.

TAMz 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. TAMz 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.

TAMz also generates auditing and forensics on all activity performed by identities in their privileged state to provide a comprehensive view designed to simplify auditing. 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

Related Products (cont.)

- **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.

Crucial Differentiators

Consider the following AAM and TAMz differentiators:

- Listening to customer needs and working together to deliver new solutions within mainframe security to meet new cybersecurity requirements.
- Implementing ongoing innovations with Broadcom engineering staff without relying on third-party engineering.
- An industry-first solution for privileged access management, operating 100% on the mainframe platform.
- Compliance reporting included for flexible audit/compliance reports.
- No need for expensive third-party mainframe administrative or reporting front ends to perform tasks. We provide easy-to-use interfaces for your staff as part of our solution.
- Through integration with Symantec VIP AuthHub AAM provides a modern MFA experience for your mainframe by always providing an eight-character logon credential and risk-based authentication policy.
- TAMz is the only mainframe-based privileged user management solution using an access promotion/demotion model supporting all three mainframe ESMs.

Additional Items for Consideration

Broadcom continues to innovate mainframe security capabilities and innovates in the following areas to support the growing mainframe security ecosystem:

- **Education:** Online education enables your staff to train in new features and functionality on demand. Modularized training enables flexible learning.
- **Mainframe Vitality Residency Program:** Broadcom will train your staff or, if you are having trouble finding talent, we will partner with you to find candidates and train new skills through our Vitality Residency Program to become ACF2 experts. Once fully trained with experience in your environment, they are available to transition and become one of your employees fully certified in our solutions—all at little to no cost to you.
- **Security Health Checks:** Both no-cost reviews of key security settings and paid engagements for a more in-depth review of your mainframe security configurations are available.
- **MRI Security Essentials:** Compare key access control configurations and settings against industry best practices with executive overviews and dashboards.
- **Communities:** Learn, connect, and share with other ACF2 users as well as Broadcom product experts that promote peer-to-peer engagement.

For more information, visit mainframe.broadcom.com/security.

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

Copyright © 2023 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA-AAM-TAMZ-SB103 April 25, 2023