

## Product Brief

### Key Benefits

- **Trust:** Deepen trust in the identity of individuals accessing the mainframe.
- **Protect:** Stay in complete control when users have privileged access to deliver trusted systems.
- **Compliance:** Address regulatory requirements and increase identity assurance for users.
- **Consistency:** Leverage the same authentication mechanism as enterprise systems.
- **Zero trust model:** Provide a perimeter check for users entering the mainframe requiring multi-factor authentication.
- **Audit:** Simplify auditing by eliminating shared at rest credentials and maintain a complete line of sight.

### Key Features

- **Flexible for some or all:** Implement permissions for specific users or applications as required by business needs with the ability to fallback to mainframe credentials during service downtime.
- **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.
- **RSA SecurID support:** Using RSA SecurID's authentication APIs, Advanced Authentication Mainframe secures privileged or normal users by requiring them to logon using RSA SecurID's soft-token or hard-token.

# Advanced Authentication Mainframe

## At a Glance

Broadcom<sup>®</sup> mainframe solutions enable enterprises to use mainframe IT to solve business problems, take advantage of the opportunities that mainframe offers for digital transformation, and ensure a trusted environment for customers. Our solutions provide a foundation that enables the mainframe to connect with your network and hybrid cloud—across your enterprise. You can use this connection to securely deliver vital support for digital transformation.

The multi-factor authentication solution from Broadcom, Advanced Authentication Mainframe, features a consistent multi-factor authentication approach to prevent data breaches and address customer compliance requirements. By supporting a wide variety of authentication services, Advanced Authentication Mainframe helps meet government regulations and industry guidelines for stronger authentication.

## Business Challenges

Mainframe systems store 80 percent of corporate data in industries such as financial services, healthcare, transportation, and telecommunications (*The FutureScape of IT*). Not only is this data critical to operations, but it can also be sensitive and regulated for privacy—its disclosure can cause significant financial ramifications and reputational damage. With the interconnectedness of mainframe in the application economy, securing access to mainframe applications with only a password is no longer secure enough.

Increasingly vulnerable to attack, this crucial, high-speed, and completely reliable transaction processing backbone is pervasively interconnected with other servers in the infrastructure and the external Internet. This connectivity means today's modern data center demands additional layers of security to protect your corporate mission and mission-critical data. Insider threats, social engineering, retiring mainframe experts, and skill gaps combine to create the perfect storm where unintentional errors and negligence can leave critical data and resources exposed. In addition, insufficient access controls for privileged users are consistently the top cause of major security breaches.

Advanced Authentication Mainframe provides the additional layers of defense in depth that are now a must across mainframe and enterprise systems. It updates security controls to needed levels of durability and mitigates the risk of data breaches—all while addressing compliance mandates to provide you with unified, multi-factor enterprise security, and peace of mind.

## Key Features (cont.)

- **RADIUS support:** Advanced Authentication Mainframe 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:** Integrates with Symantec® Privileged Access Manager to extend support for smart cards.
- **Audit and Forensics:** 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.

## Related Products

The mainframe security portfolio from Broadcom is designed to work together across the security lifecycle. Each offering delivers individual value, and the combination of data from across the products has even greater value through analytics and insights into previously unknown risks. The complete solution is available within the Mainframe Security Suite and contains the following products:

- **Advanced Authentication for Mainframe:** True multi-factor authentication for mainframe users. It supports RSA hard and soft tokens and radius protocol.
- **Auditor:** Identify security risks and automate the z/OS audits and integrity checks.
- **Cleanup:** Find and remove obsolete, unused, redundant, and excessive access rights in ACF2, Top Secret, and IBM RACF.

## Solution Overview

Advanced Authentication Mainframe 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, Advanced Authentication Mainframe features deliver multi-factor authentication to strictly control who has access to critical business resources.

Advanced Authentication Mainframe is designed to help you address compliance mandates and leverage the same authentication mechanisms as enterprise systems, while remaining implicitly mainframe ESM-centric.

Advanced Authentication Mainframe features address National Institute of Standards and Technology requirements and support hard and soft tokens for two-factor authentication to the mainframe, providing the extra layer of security needed to protect against the rising tide of social engineering attacks.

Advanced Authentication Mainframe 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.

## Crucial Differentiators

Consider the following Advanced Authentication Mainframe 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.
- Broadcom included the entitlement for Advanced Authentication Mainframe along with licensure for ACF2 and Top Secret. If you license either ACF2 or Top Secret, the entitlement also allows the use of Advanced Authentication Mainframe in your IBM RACF environments.
- Integrations with Symantec VIP and Symantec Privileged Access Management to support and deliver stronger authentication for the Mainframe.
- Integrations with popular Session Managers such as, TPX® Session Management to provide a perfect balance of multi-factor authentication with user experience in enabling single sign-on experience without degrading productivity.

## Related Products (cont.)

- **Compliance Event Manager:** A single source for collecting and monitoring real-time security and compliance-related information and events within the mainframe environment. It has the ability to send data to Splunk or an enterprise SIEM solution.
- **Data Content Discovery:** Discover, classify and protect regulated and sensitive business data to reduce risk and simplify regulatory compliance.
- **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.

## Additional Items for Consideration

Broadcom continues to innovate mainframe security capabilities. We also support the growing mainframe security ecosystem by delivering innovations in the following areas:

- **Education:** Online education enables your staff to receive training for new features and functionality on demand. Modularized training allows for flexible learning.
- **Mainframe Vitality Residency Program:** We will train your staff, or we will partner with you to find candidates if you are having trouble finding talent. We train new skills through our Vitality Residency Program and your candidates will become *security experts*. Once the candidate is fully trained with experience in your environment, they are available to transition and become one of your employees. They are fully certified in Broadcom Mainframe Security solutions—all at little to no cost to you.
- **Security Health Checks:** No-cost reviews of key security settings and paid engagements for more in-depth reviews of your mainframe security configurations are available.
- **MRI Security Essentials:** Compare key access control configurations and settings against industry best practices. Executive overviews and dashboards enable simpler reporting.
- **Communities:** Learn, connect, and share with other users as well as Broadcom product experts that promote peer-to-peer engagement.
- **Roadmap Sessions:** Periodic sessions with the product team to view a showcase of future features and functionality. Your organization can prepare to take advantage of upcoming innovations.

For more information, please visit [mainframe.broadcom.com/security](https://mainframe.broadcom.com/security).