Solution Brief

BROADCOM
MAINFRAME SOFTWARE

Mainframe Security

ACF2™ for z/OS and Db2

Mainframe Security solutions enable enterprises to stay ahead of the ever-evolving security threat landscape while modernizing to solve business problems realized through digital transformation. The solutions form the foundation for robust and reliable enterprise security.

Key Benefits

- Continuing investment leading to innovations by Broadcom engineers that meet the needs of today's security and regulatory requirements.
- Integration with enterprise solutions to address the full security lifecycle.
- Same-day support for new operating system releases and subsystem releases.
- z/OS and Db2 centralized security with separation of security and administrative duty.
- Improved efficiency through streamlined administrative and reporting functions.

Key Features

- Modern credentialing and encryption with passphrases and AES encryption, and protection by default for datasets and resources.
- MFA through the Advanced Authentication Mainframe integration in ACF2.
- PAM through the Trusted Access Manager for z integration in ACF2.
- Extensibility and integration with modern enterprise IT MFA solutions, key management solutions, IGA solutions, and more.
- Integrated security for z/OS, Unix Systems Services (USS), Db2, and zLinux on the mainframe for user authentication leveraging the ACF2 logon-id database.
- Built-in administration with robust security administration capabilities provided through panels in TSO and CICS.
- Flexibility to interface with ACF2 through ZOWE.

At a Glance

Broadcom® Mainframe Security solutions provide a foundation that enables the mainframe to connect securely within your enterprise and deliver vital support for digital transformation.

The ACF2™ for z/OS and Db2 (ACF2) solution secures and manages mainframe human and non-human identities, along with the underlying policies and processes that govern how those identities interact with and across the organization's hybrid cloud. Our Mainframe Security solutions enable businesses to comply with relevant regulations and corporate policies, and facilitate the reporting of critical information to demonstrate compliance.

ACF2 provides innovative, comprehensive security for your business transaction environments (including Db2 for z/OS, Linux, UNIX, and z/OS on IBM Z). ACF2 helps you realize the reliability, scalability, and cost effectiveness of the mainframe in a secure, trusted environment through consistent and robust external security.

With ACF2, organizations can further enforce higher, more advanced access controls and visibility with the following products:

- Advanced Authentication Mainframe provides multi-factor authentication (MFA) to help secure mainframe identities to reduce fraud and threat attacks, while also remaining aligned to compliance needs.
- Trusted Access Manager for z provides privileged access management (PAM) auditability, enforcement, and governance to reduce insider threat attack vectors, while also meeting compliance needs.
- Security Insights provides streamlined and automated reporting and auditing to prove compliance and answer key questions about the mainframe security posture of an enterprise.

Key Features (cont.)

- Robust out-of-the-box reporting and auditing, with no additional software to purchase.
- Simulated security testing of changes to ensure that a change will deploy without incurring an outage.
- PDS member-level protection for further restriction of access within partitioned datasets.
- ACF2 supports segregation of data with multilevel security and data classification options.
- Record-level locking in CICS.
- Role-based access controls are available for implementation within ACF2.
- Day 1 support for all new operating system releases and subsystem releases. For example, CICS, Db2, and IMS.
- Apply maintenance without the need to IPL for most PTFs.
- Command-enabled security request tracing through the SecTrace facility.
- Easily determine who has access to data and resources through the ACCESS subcommand.

Related Products

- Cleanup finds and removes obsolete, unused, redundant, and excessive access rights in ACF2, IBM RACF and Top Secret™ for z/OS and Db2.
- Trusted Access Manager for Z monitors and controls privileged users by granting time-bounded just-in-time access to system, critical resources, and regulated data or resources. With the ACF2 license, 1:1 accountability and auditing is included.
- Advanced Authentication for Mainframe provides true multifactor authentication for mainframe users. With the ACF2 license, RSA hard and soft token support, and radius protocol support is included.

Business Challenges

In today's hybrid cloud and hybrid IT environments, mainframes are more connected to enterprise processes than ever before in history. This connectedness changes the security context, opens new threat vectors, and raises the risk level. Access to the mainframe is more open to employees, partners, contractors, and customers. Controlling access to content and resources goes along with identity management for all individuals. Access control must be granular, role-based, and continually updated to ensure that only the correct people have sufficient access.

Additionally, data security is critical to achieving business efficiency and growth, superior customer service, and information privacy. Db2 environments remain the storehouse for most systems of record (employee, customer, transactional data, and more), but native Db2 security is no longer enough to keep threats out when hackers are continually trying to get in. To mitigate data breach risks in Db2 environments, organizations must strengthen security, streamline administration, and provide enhanced auditing and compliance capabilities.

Effective security requires consistent content controls across systems and the organization. Organizations need to keep pace with available security solutions that address modern threats. Inconsistent policies increase risk and invite disaster. Companies cannot afford a lapse in security or compliance standards. The average cost of a data breach in 2024 was $4.44 million (Cost of a Data Breach Report 2025). Unanticipated fines, fees and brand damage can be detrimental, if not fatal, to business operations.

Solution Overview

Security is one of the most crucial components of an IT environment today. Although security efforts have been around for four decades, Broadcom continues to evolve ACF2 security to address modern threats and compliance requirements. ACF2 is developed using the continuous delivery model. The solution is ready to solve today's and tomorrow's business challenges as the security landscape changes from a threat vector and a platform support perspective.

ACF2 is the foundation of enterprise security, with modern alignment to the hybrid cloud IT stack, and integration with enterprise Identity and Access Management (IAM), Identity Governance and Administration (IGA), secrets management, and more. Examples of these tools include, but not limited to SailPoint, CyberArk, and Microsoft Active Directory.

Critical Differentiators

- MFA and PAM capabilities are included for advanced, more secure authentication and compliance requirement controls.
- Reporting capabilities are included for flexible audit and compliance report generation needs.
- No need for expensive third-party mainframe administrative or reporting front ends to perform tasks. Easy to use interfaces for your staff are part of our solution.
- Proven integrations with the enterprise IT technology stack (IAM, IGA, secrets management, and more) to enable modernization across the hybrid cloud.
- ACF2 is integrated with cross-platform solutions such as Identity Suite, Privileged Access Manager, and SiteMinder™ for the full security lifecycle.
- Enforced separation of duty when managing Db2 environments to ensure that security is centralized, while enforcing consistent MFA and PAM.

Related Products (cont.)

- Compliance Event Manager provides a single source for the collection and monitoring of real-time, compliance-related information and events occurring within the mainframe environment. It has the ability to send this information to Splunk or an enterprise SIEM solution.
- Security Insights provides powerful reporting for auditing and visibility, allowing for automated report generation and export to understand the security posture within the enterprise.
- Auditor for z/OS (formerly CA Examine Auditing) delivers in-depth auditing, integrity checks, and verification for z/OS.
- Data Content Discovery finds and classifies regulated and sensitive data to ensure that proper security and privacy controls are in place for the data.
- Compliance Information Analysis (CIA) replicates compliance security information from the mainframe security database into a CIA relational data repository for compliance and ad-hoc SQL reporting.
- LDAP Server for z/OS provides a full-function LDAP-compliant directory server.
- PAM Client for Linux for System z is a flexible, open-source architecture for user authentication on Linux systems. Pluggable authentication module client support enables ACF2 to act as an authentication server for one or more Linux systems, eliminating the need for redundant security administration on a system-by-system basis.
- Distributed Security Integration (DSI) is a standalone daemon that runs in the z/OS UNIX environment independent of the LDAP server. In addition, DSI allows applications on a Windows platform to issue calls to ACF2.

- Protection by default. ACF2 can protect both defined and undefined datasets and resources.
- Integrated security for z/OS, USS, and zLinux for user authentication against the ACF2 source of record.
- Granular control over USS superusers.
- Full security control over USS files and directories with true external security. Security staff no longer needs to learn and manage native USS security.
- Simulate authorization to ensure that changes work before deployment to avoid incurring an outage.
- PDS member-level protection for further restriction of access with partitioned datasets, particularly those that may contain application configuration.
- Transmit security information to LDAP compliant directory managed servers through LDAP directory services.
- ACF2 implements ongoing innovations with Broadcom engineering staff and does not rely on third-party engineering.

Requirements for securing Db2 resources are just as important as securing data in other applications. As such, ACF2 provides the following functionality:

- Protection by default
- Secondary AUTHIDS reduction
- Controlled data sharing
- Db2 ownership and creator concepts
- Changing ownership
- Securing privileges and authorities
- Authorize resource access in ways that align with your organization's standard security policies with only one ID

Additional Items for Consideration

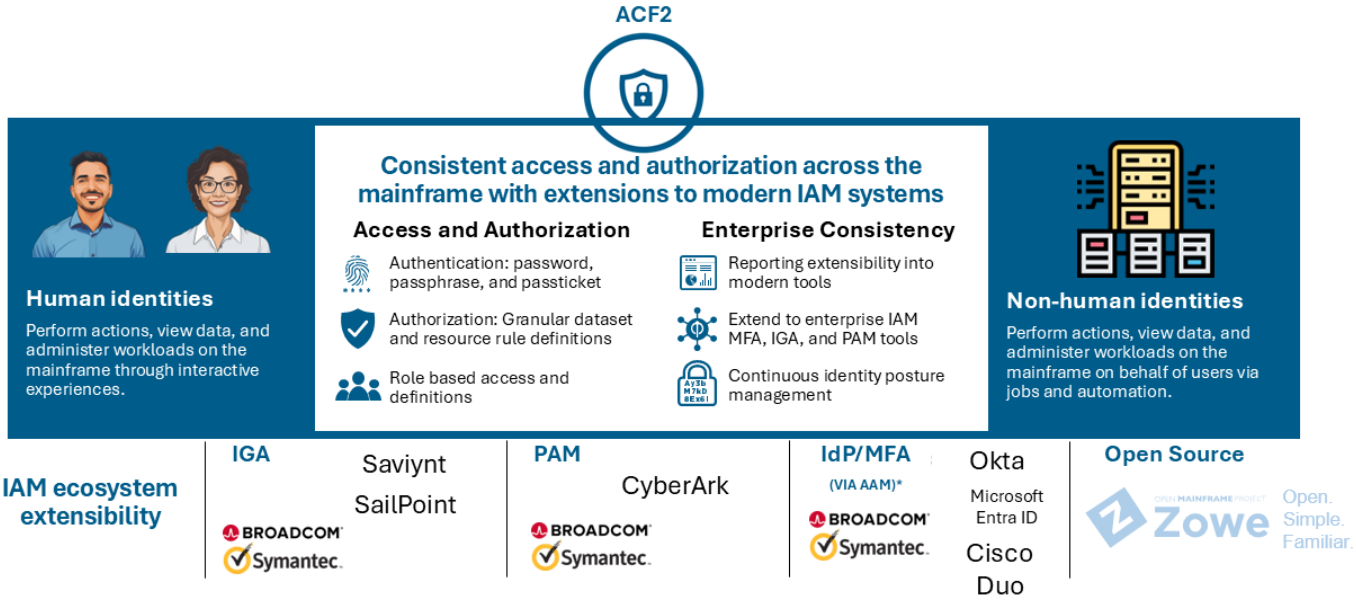
Broadcom not only continues to innovate mainframe security capabilities, but also in other areas to support the growing mainframe security ecosystem:

- STIG – Our mainframe security STIGs are a collection of recommended settings for ACF2. These articles sit somewhere between a hard requirement and a best practice. For each article, we include the following information:
  - A possible security exposure.
  - How to identify if your site is exposed.
  - How to remedy the exposure.

  For each STIG, we include detailed steps. In this case, the steps include ACF2 commands. Users have the information they need in one location to remediate the audit finding.
- Education – Online education enables your staff to train in new features and functionality on demand. Modularized training allows for flexible learning.
- Mainframe Vitality Residency Program – Broadcom will train your staff. If you are having trouble finding talent, we will partner with you to find candidates and train them to become ACF2 experts through our Vitality Residency Program. Once fully trained with experience in your environment, the residents are available to transition and become one of your employees. They are fully certified in our solutions 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.
- Roadmap sessions – Periodic sessions with the product team to highlight future features and functionality. Your organization can prepare to take advantage of upcoming innovations.

The ACF2 for z/OS and Db2 Solution for Mainframe Security



For more information, please visit: www.broadcom.com/products/mainframe/security/acf2

CA-ACF2-zOS-SB102 October 2, 2025