BROADCOM
MAINFRAME SOFTWARE

SOLUTION BRIEF

Unlock the Power of the Mainframe with Modern Cybersecurity and Compliance Solutions

Use mainframe-centric cybersecurity tools and expertise to simplify and streamline compliance initiatives.

The integration of robust mainframe systems and agile cloud infrastructure has ushered in a new era of enterprise Hybrid IT. While this hybrid landscape offers unprecedented versatility and scalability, it has exposed the once-isolated mainframe to network-based threats through APIs, web services, and complex third-party supply chains. Despite this heightened risk, the **lingering misconception of mainframe invulnerability** has led to a concerning lag in mainframe cybersecurity and compliance.

Today's IT leaders are tasked with securing these complex environments without stifling the innovation that drives their organizations forward. The unique capabilities of mainframe systems, coupled with a shrinking pool of mainframe expertise, leave many organizations struggling to navigate this new hybrid IT landscape. As a result, mainframe cybersecurity and compliance are often siloed, with limited visibility, reporting, and funding.

Compliance in the Cloud: Mainframe Meets Modern Risks

Compliance is at the epicenter of this cybersecurity storm as regulators push organizations to secure dispersed ecosystems — even though many auditors lack the mainframe expertise required to facilitate this process. Many IT teams become trapped in an endless cycle of audits, manually poring over mountains of data to demonstrate compliance with complex requirements often communicated as cloud or distributed mandates. This resource-intensive approach hinders more strategic initiatives, causing cybersecurity and compliance to feel like burdens instead of the competitive advantages they could be.

So how do you secure your mainframe and meet regulatory requirements without hindering your team's innovation and agility?

Develop Cyber Resiliency with NIST and DORA

The NIST Security Framework 2.0 (NIST CSF 2.0) provides a comprehensive model for developing resilient systems and offers valuable insights for highly regulated industries, such as banking and financial services, healthcare, and government. This approach demonstrates how unifying cybersecurity, compliance, and cyber resilience can safeguard the organization and facilitate growth.

> The EU's Digital Operational Resilience Act (DORA) marks a significant shift in regulatory thinking, directly addressing the interconnectedness of cyber resilience, security, and compliance in the financial sector. The regulation mandates a more proactive and comprehensive approach to risk management, incident response, resilience testing, and reporting. Further, it specifically states, "Financial entities shall continuously monitor and control the security of ICT systems." The combination of continuous cybersecurity monitoring and the more comprehensive risk management establish a more holistic cybersecurity posture.

Simplify Mainframe Compliance in 3 Steps

Mainframe-specific security solutions designed for today's threat landscape empower you to create a more integrated, secure, and resilient environment across your enterprise — safeguarding your bottom line, fostering growth potential, and strengthening customer trust.

Broadcom's End-to-End Cybersecurity for the Mainframe

Broadcom's cybersecurity solutions are structured with both the mainframe and your wider cybersecurity strategy in mind. Designed to run on the mainframe, they avoid added risk by eliminating the need to interface with unnecessary external security tools. Additionally, these tools support all three external security managers (ESMs) and integrate seamlessly into your security information and event management (SIEM) tool for comprehensive protection and visibility.

Combat the Risk of Compromised Credentials	Enable Granular, Least Privilege Access Control Without Hindering Productivity	Improve Threat Detection, Auditing, and Forensics for Mainframe
Multi-Factor Authentication (MFA) – Advanced Authentication Mainframe Implement an additional layer of user verification, significantly boosting confidence in user identities and system security while addressing compliance requirements.	**Trusted Access Manager for Z (TAMz) and Cleanup** Gain comprehensive privileged access management, access control, and auditing capabilities to enhance the security and governance of your mainframe environment. Further reduce the risk inherent in shared credentials and "superuser accounts" by only bestowing higher-level permissions as needed. Simplify compliance and ensure a clean security database by automatically cleaning up obsolete identities and authorizations.	**Compliance Event Manager (CEM)** Continuously monitor and secure your systems with real-time file monitoring and intrusion detection, enabling proactive threat response and simplifying compliance. This self-service model of reporting ensures traceability of all events, while also allowing different users to easily customize the reports they pull.

Broadcom Empowers Your Team Before, During, and After Implementation

Broadcom provides support at every stage of your mainframe modernization journey. Our Beyond Code programs help organizations innovate without disruption, optimize their mainframe environments, and amplify the value of their mainframe investments to drive growth and innovation.

OPTIMIZATION

Expert Guidance for Mainframe Modernization

Take advantage of Expert Guided Planning, and VIP support from experienced professionals, to navigate complex changes and maximize the value of your mainframe investments.

EDUCATION

Cultivating In-House Capabilities for Long-Term Success

Access Broadcom's comprehensive, no-cost mainframe education program with courses, labs, and virtual training to bridge the skills gap and empower your workforce.

INNOVATION

Collaboration to Fuel Mainframe Innovation

Address unique business challenges through collaborative design workshops and software rationalization services, ensuring high ROI.

Compliance, Security, and Growth Go Hand in Hand

To learn more about streamlining compliance through multidimensional mainframe cybersecurity, talk to a Broadcom rep today or visit:

Access Broadcom Compliance for Mainframe Resources

Immutable Storage and Access Control:
Powerful Protection from Ransomware Across Multiple Security Frameworks

Highly regulated industries are facing increasingly stringent security requirements, especially in the face of rising ransomware threats. Many regulations and standards now emphasize using immutable storage to protect sensitive data at rest. This technology prevents unauthorized modification or deletion, effectively safeguarding against malicious encryption and extortion attempts common in ransomware attacks.

CA 1™ Flexible Storage enables users to back up their mainframe data using immutable volumes that reside on any device or cloud. These cost-effective backups are encrypted before leaving the mainframe, ensuring protection against threats. In the event of a ransomware attack or another data loss incident, the tape backup can be used to restore the mainframe to a pre-attack state, significantly reducing downtime and financial losses.

Implementing **Multi-factor Authentication - Advanced Authentication Mainframe and Trusted Access Manager for Z (TAMz)** in conjunction with **CA 1™ Flexible Storage** ensures complete control over who has access to these encrypted files and the encryption keys needed to unlock them. Broadcom's auditing capabilities also enable you to track user access and quickly pull reports to prove the effectiveness of your security measures.

For more product information: broadcom.com

BROADCOM MAINFRAME SOFTWARE