BROADCOM®
MAINFRAME SOFTWARE

Solution Brief

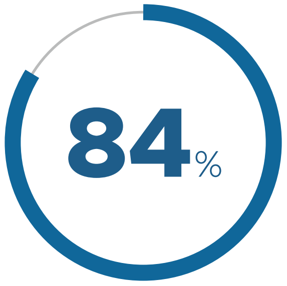
Bridging The Hidden Gap in Your Cyber Resiliency Strategy

Modernize mainframe security to prevent threats in a highly interconnected ecosystem, ensuring the resiliency of your most critical operations.

In the face of constantly evolving cyber threats and regulatory requirements, cyber resiliency — the ability to withstand, adapt, and recover from disruptions — is paramount. The term often sparks conversations around backups and recovery from outages, but these come into play after a disruption has occurred. A true resiliency-centric approach is much more proactive, prioritizing prevention and protection alongside incident response.

While many factors contribute to downtime, the number one cause is security incidents. This means we can only achieve true resiliency through comprehensive cybersecurity — at every level.

True Resiliency is Dependent on the Depth and Breadth of Your Cybersecurity Strategy



84% of corporations cite security incidents as the leading cause of downtime.[1]

Mainframe Availability: The Cornerstone of Cyber Resiliency

Hybrid ecosystems have become the norm, but we're seeing the industry shift once more. Many organizations in highly regulated industries, such as finance, healthcare, and government, are strategically returning their most critical workloads and data to the long-trusted mainframe. These systems have a decades-long track record of high availability and built-in redundancies, but the notion that they are inherently secure is a dangerous misconception in today's interconnected world.

[1] ITIC 2023 Global Server HW, Server OS Reliability Report

The mainframe may still be considered "on prem," but in the modern hybrid ecosystem it also interfaces with web-based applications and exchanges data with private and public cloud storage. This dynamic and distributed model has significantly increased accessibility, collaboration, and scalability — but it also demands a more modern approach to security.

So how do you secure your mainframe and ensure cyber resiliency without hindering your team's innovation and agility?

Safeguarding Your Mainframe With Modern Defenses

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 designed with both the mainframe and your wider cybersecurity strategy in mind. Built to run on the mainframe, they often eliminate the need to interface with an off-platform tool that would introduce added risk. Additionally, these products support all three ESMs and integrate seamlessly into your SIEM for comprehensive protection and visibility.

Multi-Factor Authentication – Advanced Authentication Mainframe (AAM MFA)	Trusted Access Manager for Z (TAMz)
Combat the Risk of Compromised Credentials Implement an extra layer of user verification, significantly boosting confidence in user identities and system security, while meeting compliance requirements.	**Enable Granular Access Control Without Hindering Productivity** Significantly reduce the risk inherent in shared credentials and "superuser accounts" by bestowing higher-level permissions only when needed and only as long as necessary.
Cleanup for z/OS	**Compliance Event Manager (CEM)**
Declutter Your Security Database Automatically remove the obsolete user IDs and access rights that have been accumulating over decades, establishing a clean, streamlined security database and simplifying compliance.	**Improve Threat Detection, Auditing, and Forensics for Mainframe** Monitor and secure your systems with real-time file monitoring and intrusion detection, simplifying compliance management and enabling proactive threat response.

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.

DORA: Establishing a Blueprint for Holistic Cyber Resilience

The EU's Digital Operational Resilience Act (DORA) marks a pivotal shift in regulatory thinking, recognizing that cyber resilience, security, and compliance are highly interconnected and interdependent. DORA enhances cybersecurity and strengthens resilience for the financial sector by mandating a comprehensive approach integrating these functions.

This framework offers valuable insights for other regions and highly regulated industries, illustrating how a unified strategy can bolster resilience, streamline compliance, and proactively safeguard critical operations against evolving cyber threats.

OPTIMIZATION

Expert Guidance for Mainframe Modernization

Take advantage of Expert Guided Planning, white-glove 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 cybersecurity and compliance workshops and software rationalization services, ensuring high ROI.

Security, Resiliency, and Growth Go Hand in Hand

Cyber resilience is crucial for serving your customers. Don't go at it alone. Broadcom is here to help with solutions, workshops, experience, and more. Access Broadcom cyber resilience resources.

Access Broadcom Cyber Resilience Resources

For more product information: broadcom.com

BROADCOM®
MAINFRAME SOFTWARE