How Does Zero Trust Strengthen Mainframe Security?

Active Threats
Mainframes handle 70% of the world’s production customer transaction workloads. Ninety-two of the top 100 banks use the mainframe to provide banking services to their customers. As with every other part of your IT infrastructure, your mainframe is at risk of a cyberattack.

Implement Zero Trust by assuming every device on the user network is hostile by default.

Harden Against Privileged Credential Abuse

74% of data breaches start with privileged credential abuse.

341 Days
It takes almost 1 year for companies to identify & contain a data breach caused by compromised credentials.

Protect Your Most Critical Data

95% of IT management and decision makers surveyed said the most concerning ramifications of mainframe security is breach of customer data.

A Simplified Path to Zero Trust on the Mainframe

Organizations do not need to overhaul any existing security strategies. Implement Zero Trust with small, incremental steps by using Broadcom’s Protect-Surface approach.

Solve your personnel concerns with a proven Vitality Program. Upcoming mainframe engineers are provided and trained for free for your organization’s mainframe security platform.

Protect your organization against modern mainframe security risks today with Broadcom.

- Implement Zero Trust solutions that map cybersecurity to business objectives.
- Use modern Zero Trust solutions, including privileged access management (PAM), multifactor authentication, zero trust network access solutions to defend your Mainframe Protect Surface.

Broadcom Mainframe Software Division specializes in DevOps, Security, AIOps, and Infrastructure software solutions for vital infrastructure. We enable our clients to embrace open technologies, integrate Mainframe as part of their hybrid cloud, and partner to drive greater value and overall success with the platform.