BROADCOM
MAINFRAME SOFTWARE

Solution Brief

Mainframe Security Suite

Address Risk and Compliance Needs to Protect Your Financial and Reputational Integrity

Highlights

- Manage the digital identities of users, devices and applications, and the policies and processes that govern how those entities interact with the organization.
- Enable businesses to comply with relevant regulations and corporate policies, and facilitate the reporting of crucial information to demonstrate compliance.
- Reduce threats with advanced authentication and privileged user management.
- Monitor user activity and respond to real-time alerts for cybersecurity threats.
- Quickly interpret and assess the security posture of your mainframe, and see suggested remediation steps.
- Simplify audits with automated reports that are aligned to security standards and regulations.
- Manage 24x7 privileged user access with ease.
- Integrate the Mainframe Security Suite with your security operations center using popular SIEM tools.

Overview

Today's mainframe security team faces an incredibly challenging environment. Business transformation and digital transformation require a more complex, integrated hybrid IT and cloud environment that places more pressure on the security of the infrastructure. Simultaneously, the regulatory, audit, and compliance environment has never been more complex (or costly). Threats are more significant. Bad actors and incursions are increasingly sophisticated, with insider threats growing as the value of data increases. To complicate the situation further, security skills are in high demand and short supply.

These demands cannot be met using the same approaches we have used in the past. Today's environment requires a re-evaluation of security. With a strong focus on automation and remediation driven by an integrated enterprise security plan, we can resolve the challenges brought by transformation, decrease risk, and improve our compliance posture.

Making Security Strategic

Mainframes are often reported to be the gold standard for IT security. While the mainframe remains the most securable platform available, it is only as good as the security solutions and practices that you use to secure it.

Security failures and lessons learned on distributed platforms and clouds over the last two decades have advanced security practices on those platforms. The same lessons are also applicable to mainframes. For example, it is common for distributed assets to be accessed only with multi-factor authentication, but it is less frequent on the mainframe even though mainframe assets are typically the most vital.

Mainframe apps and data are essential for transformation since they are used by web and mobile applications to deliver critical business operations or functions. This connectivity delivers new vulnerabilities: insider threats, connectivity through APIs, data transfers, and web access. These threats intensify the need for modernized mainframe security.

Day-to-day firefighting of enterprise security issues can shift focus away from the mainframe, which is often the most strategic platform in the enterprise. The truth is that technology continues to evolve at increasing speeds. As threats evolve and environments shift, you cannot be strategic if you are buried in the day-to-day chaos of putting out fires. How do you make the shift and advance security for today's modern mainframe to get ahead of the next firefight and prevent it?

That is where enterprise security planning and solutions built around a data security lifecycle can help. At Broadcom, we have used these advanced mainframe security practices and innovations to update the mainframe security workflow, completely modernizing mainframe security.

We provide an extensive enterprise solution portfolio that addresses that workflow to manage and maintain modern mainframe security.

Breaches often occur from stolen credentials, misconfiguration and errors. Mitigation is possible with new tools and processes as we shift from security firefighting to making security strategic, and incorporate security analytics.

Figure 1: The Broadcom Mainframe Security Suite

Securing the Mainframe

Mainframe teams created the early standards for securing IT. Over time, teams working on distributed platforms evolved security tools and practices further to mitigate risks posed by the Internet, such as breaches, hacks, and denial-of-service attacks. The modern mainframe faces similar connectivity-based exposure and requires modern security capabilities to prevent similar attacks as seen on distributed platforms.

In recognizing the impact of hybrid applications on security, Broadcom is leading efforts in applying lessons learned from the distributed environment to mainframe security. This goal of modernizing mainframe security drives our solutions around advanced security tools and best practices that cover the entire security lifecycle.

While Mainframe Security Suite includes the Top Secret™ and ACF2™ external security managers (ESMs), the remainder of the solutions in the suite support all three ESMs: Top Secret, ACF2, and RACF. The Advanced Authentication Mainframe solution provides multi-factor authentication to deepen the trust in mainframe security and the identity of those accessing the mainframe.

Our focus on access management goes even further with Trusted Access Manager for Z, bringing time-boxed privilege elevation to the mainframe, and delivering reduced risk while maintaining the auditability of privileged user access.

Reducing risk from insider threats without overwhelming the security team is now possible with Cleanup by automatically identifying and removing unused and retired accounts and entitlements.

Security Insights enables quick response to impromptu audit requirements and provides self-service reporting to line of business. It can save hours of custom report writing or data gathering by the mainframe security team. We enable integration of mainframe event auditing into the enterprise security view with Compliance Event Manager. You can improve compliance, while reducing cost and reserving the time of skilled workers for more complex tasks by filtering, interpreting, analyzing, and consolidating crucial events and information, then sending the events and information to Security Information and Event Management (SIEM) tools for inclusion in the enterprise view.

“Broadcom mainframe security solutions provide us with insights and control for our ever changing environment. We are able to detect, respond and support security events and needs at a level that brings greater benefit to the organization.”

– IT administrator, Global 500 insurance company

Conclusion

When it comes to security, it is vitally important to be prepared and to be one step ahead of change. Mainframes secure 68% of global production IT workloads and 90% of all credit card transactions (Ushering in a new era of mainframe modernization) and are used by nearly three-quarters of the Fortune 100 (Application modernization on the mainframe). The Mainframe Security Suite integrates solutions that identify, manage, and reduce risk, thus updating and modernizing mainframe security. With strategic planning, you can maintain a solid security foundation for your mainframe.

Mainframe Security Suite

The Mainframe Security Suite works together across the security lifecycle. While each product offering delivers value individually, combining data across offerings delivers greater value, yielding insights into hidden risks. The complete solution is available within the Mainframe Security Suite and contains the following products:

- **ACF2 and Top Secret for z/OS:** Provides innovative, enterprise-grade, comprehensive security for your business transaction environments. They enable a secure, trusted environment to help you realize the reliability, scalability, and cost-effectiveness of the mainframe.
- **ACF2 Option for Db2 and Top Secret Option for Db2:** Provides the ability to externalize security for IBM Db2 without the need for an exit.
- **Advanced Authentication Mainframe:** Offers enhanced MFA verification to deepen the trust in the identity of users on your system.
- **Auditor:** Identifies security risks and automates the z/OS audits and integrity checks.
- **Cleanup:** Automatically eliminates unused IDs and entitlements.
- **Compliance Event Manager:** Monitors for real-time violations of critical security systems and resources, and incorporates file integrity monitoring of critical system files to identify cybersecurity indicators of compromise. It integrates the enterprise SOC through Splunk or any enterprise SIEM solution.
- **Security Insights:** Modern reporting platform that eases the burden of meeting your audit and compliance needs without requiring large manual efforts. It helps you solve your most challenging problems by creating simple, custom compliance reports with ease.
- **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.

“The customer experience has become the central tenet of business today… this is the battlefront where organizations win or lose. One of the easiest ways to lose… customers, is to expose them to a security breach; personal information, credit card information, social security numbers, bank account data, browsing activity, and shopping behavior—with everything becoming digital, everything becomes vulnerable to attack. The potential revenue loss from an attack can be in the tens or even hundreds of millions of dollars, but the loss of trust among customers is nearly irrecoverable.”

– Peter Rutten, Matthew Marden; The Business Value of the Transformative Mainframe, An IDC white paper, sponsored by Broadcom and IBM

Conclusion (cont.)

The Mainframe Security Suite provides the components you need to completely modernize mainframe security and align the mainframe platform with your enterprise security control mandates. As a package, it enables adoption of components as security needs allow, with the comfort of knowing that a world expert in mainframe security is available to help you, from planning, to install, to ongoing best practices.

Reduce business risk and improve compliance with a comprehensive modern mainframe strategy, a best practices-based process that advances mainframe protection and moves security from firefighting to strategic value.

Next steps:

- To get started today, go to Mainframe Resource Intelligence or explore a mainframe cybersecurity workshop.
- To learn more, go to Broadcom Cybersecurity and Compliance Management.

BROADCOM®

For more information, visit our website at: www.broadcom.com

MF-Security-SB106 June 3, 2026