Solution Brief

BROADCOM®
MAINFRAME SOFTWARE

Mainframe Security Suite

Address Risk and Compliance Needs for Your Most Vital Data

Highlights

- Reduce threats with advanced authentication and privileged user management
- Monitor user activity and analyze user behavior to determine insider risk
- 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.

Figure 1: Integrated Hybrid IT and Cloud Environments Add Complexity to Mainframe Infrastructure 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.

Making Security Strategic

Mainframes are often seen as the gold standard for IT security. While the mainframe remains the most secure 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 applicable to mainframe as well. 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.

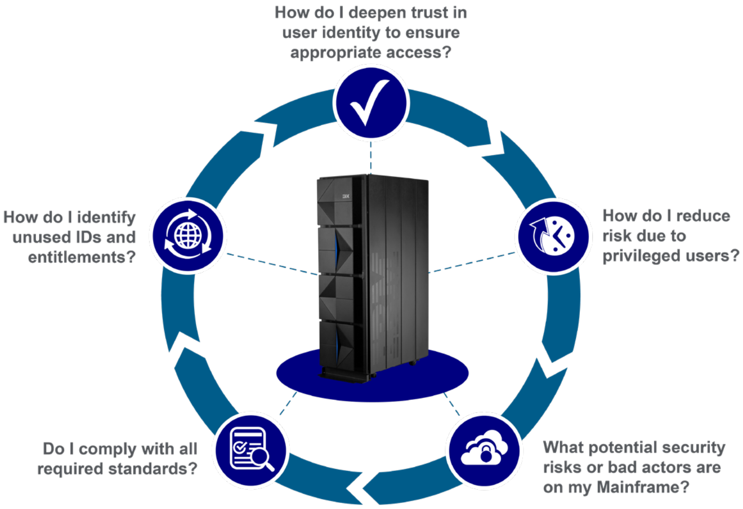
Mainframe apps and data are essential for transformation since they are used by web and mobile applications to deliver critical business operations or functions. Today's hybrid applications depend on the mainframe as much as they do the cloud. With this new connectivity comes new vulnerabilities: insider threats, connectivity through APIs, data transfers, and web access. These new 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.

Figure 2: Re-evaluating Mainframe Security


How do I deepen trust in user identity to ensure appropriate access?
How do I reduce risk due to privileged users?
What potential security risks or bad actors are on my Mainframe?
Do I comply with all required standards?
How do I identify unused IDs and entitlements?

> “We have the ability to modernize because you have multi-factor solutions, privileged user management, and data classification tools which help us work efficiently and keep pace with changing regulations.”
> *– Global Insurance Organization*

Securing the Mainframe

Historically, 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.

We enabled multi-factor authentication support in all three external security managers (ESMs): Top Secret™ and ACF2™ from Broadcom, and Resource Access Control Facility from IBM. Multi-factor authentication deepens the trust in mainframe security and the identity of those accessing the mainframe.

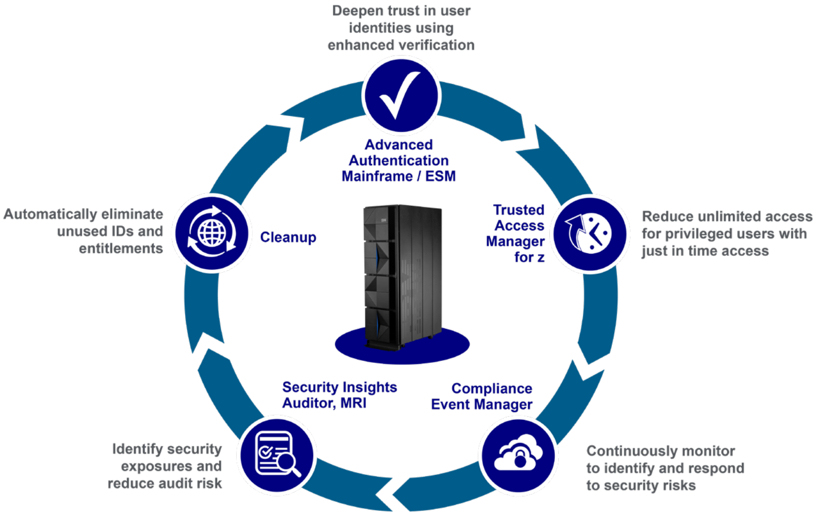
Our focus on access management goes even further, bringing time-boxed privilege elevation to the mainframe, delivering reduced risk while maintaining auditability of privileged user access.

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

We enable integration of mainframe event auditing into the enterprise security view. You can improve compliance, while reducing cost and reserving the time of skilled workers for more complex tasks by first filtering, interpreting, analyzing, and consolidating crucial events and information. Next, send the events and information to Security Information and Event Management (SIEM) tools for inclusion in the enterprise view.

The mainframe security lifecycle, shown in the following figure, presents a security workflow for those responsible for mainframe security. The security portfolio from Broadcom fills the needs of the mainframe security team by integrating solutions that identify, manage, and reduce risk, thus updating and modernizing mainframe security.

Figure 3: The Mainframe Security Lifecycle


Deepen trust in user identities using enhanced verification
Advanced Authentication Mainframe / ESM
Trusted Access Manager for z
Reduce unlimited access for privileged users with just in time access
Automatically eliminate unused IDs and entitlements
Cleanup
Security Insights Auditor, MRI
Compliance Event Manager
Identify security exposures and reduce audit risk
Continuously monitor to identify and respond to security risks

> **“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*

Securing the Mainframe (cont.)

Our expertise in ESMs has brought industry-leading multi-factor authentication, available on all ESMs through Advanced Authentication Mainframe. We have automated the management of privileged users with Trusted Access Manager for Z. Trusted Access Manager for Z also aids you in understanding the underlying risk associated with the access that was granted to users and privileged users alike. You can monitor these users, and z/OS itself for risky activity with Compliance Event Manager, alerting the security operations center’s SIEM to crucial issues. Cleanup automates the process of reducing unused IDs and authorizations. This process reduces risk by former insiders and reduces security staff workload. The Mainframe Security Insights Platform helps identify and reduce risk from threats by analyzing the security posture of your mainframe and suggesting remediation steps.

Conclusion

When it comes to security, it is vitally important to be prepared and to be one step ahead of change. Mainframes secure more than 80% of the world’s mission-critical data (The FutureScape of IT) and are used by nearly three-quarters of the Fortune 100 (Application modernization on the Mainframe). With strategic planning, you can maintain a solid security foundation for your mainframe.

Mainframe Security Suite

The Mainframe Security Suite from Broadcom 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:

- **Advanced Authentication for Mainframe:** Offers enhanced verification to deepen the trust in the identity of users on your system.
- **Auditor:** Identify security risks and automate the z/OS audits and integrity checks.
- **Cleanup:** Automatically eliminate unused IDs and entitlements.
- **Compliance Event Manager:** Collect and monitor real-time security and compliance-related information and events within the mainframe environment with the ability to send data to Splunk or to an enterprise SIEM solution.
- **Mainframe Security Insights Platform:** Collect, aggregate, and analyze security data to understand the mainframe security posture and remediate mainframe security risk.
- **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.

Mainframe Security Suite (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 Security Health Assessment.
- To learn more, go to Broadcom Mainframe Security.

"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® Inc. and IBM, August 2019

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com