Solution Brief

BROADCOM

Mainframe Security

Address Risk and Compliance Needs for Your Most Vital Data

Highlights

- Analyze your system and compare insights to best practices to address potential risks and security gaps.
- Reduce threats with advanced authentication and privileged user management.
- Identify hidden risks in your data, from the perspective of governance and regulatory compliance.
- Monitor user activity and analyze user behavior to determine insider risk.
- Address skills shortages by automating routine tasks and shifting experienced staff to higher-value work.

Overview

Today's mainframe security teams face 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 complexity of security and compliance environments is increasing. The regulatory, audit, and compliance environment has never been more complex (or costly) and 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, skills are in high demand and short supply. And there is a need to continue to replace high-performing talent that is aging out of the workforce.

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

Figure 1: Today's mainframe security teams face an incredibly challenging environment.

Breaches often occur because of misconfiguration and errors. Mitigation is possible with new tools and processes as you shift from security firefighting to making security strategic.

Making Security Strategic

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

Security failures, and lessons learned on distributed platforms and cloud platforms over the last two decades, have advanced security practices on those platforms. And those practices apply to mainframes, as well. For example, it is common to require that distributed assets be accessed only with multi-factor authentication; but it is less frequent on the mainframe, even though mainframe assets are typically the most vital.

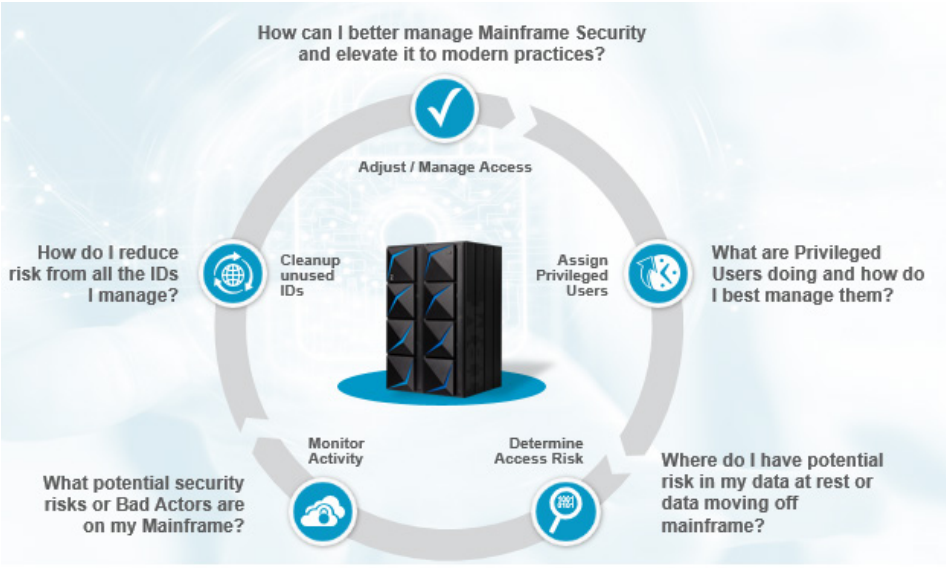
Mainframe apps and data are essential for transformation. Used by web and mobile applications to deliver better CX, they depend on the mainframe as much as they do the cloud. With this new connectivity come new vulnerabilities: insider threats, connectivity through APIs, data transfers, and web access. 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 the modern mainframe in order 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 CA, A Broadcom Company, we have used these advanced mainframe security practices and innovations to update the mainframe security workflow. We provide an extensive enterprise solution portfolio that addresses that workflow, to manage and maintain modern mainframe security.

Figure 2: Re-evaluating Mainframe Security



Securing the Mainframe

Securing the world's most securable platform involves more than managing IDs and passwords. It is no longer an acceptable practice to maintain full-time privileged users with on-demand access or time-boxed access elevation.

Instead, you can determine risk at the data level, and then monitor that data to see the accounts that access it.

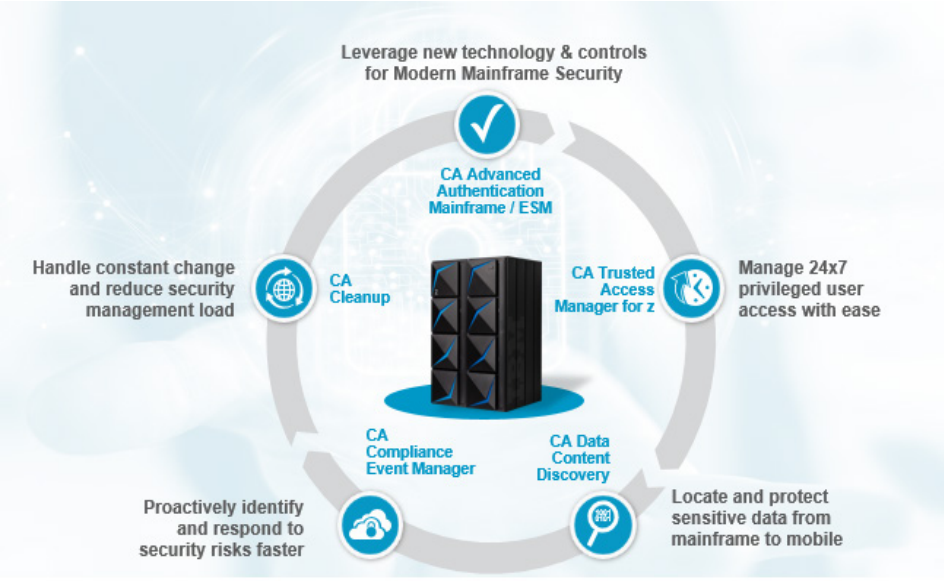
Reducing risk from insider threats without overwhelming the security team is now possible by automatically identifying and removing unused and retired accounts. You can locate, in an intelligent, simple way, the data sets that contain sensitive and PII data that requires extra protection from a governance and regulatory perspective. This not only simplifies your audit but also boosts customer trust.

Historically, mainframe teams defined security and created the early standards for securing IT. Over time, teams working on distributed platforms evolved security tools and practices to the exposure that the internet poses. Breaches, hacks, DDoS, many people never envisioned these on the mainframe. Now, however, the modern mainframe is facing similar connectivity-based exposure and attacks and requires new security capabilities.

CA is a leader in modernizing mainframe security: addressing vital security issues facing the mainframe and enabling customers to apply lessons from 20 years of distributed IT security knowledge to the mainframe.

We offer advanced security tools and best practices that cover the entire security lifecycle.

Figure 3: The Mainframe Security Lifecycle



"One of the easiest ways to lose customers is to expose them to a security breach."

- Peter Rutten, Matthew Marden; *The Business Value of the Transformative Mainframe, An IDC White Paper*

Securing the Mainframe (cont.)

We enabled multi-factor authentication support in all three external security managers (ESMs): Top Secret and Access Control Facility (ACF2) by Broadcom, plus Resource Access Control Facility (RACF) by IBM. Multi-factor authentication addresses a key gap in mainframe access management and improves your security posture.

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.

We delivered the first and only data classification solution that runs on the mainframe, helping companies around the world to locate and protect sensitive data and to address data privacy regulations. And, we addressed a key gap in enterprise security, integrating mainframe into the enterprise security view. By filtering and consolidating crucial events then sending them to security Information and event management (SIEM) tools, you can improve compliance, while reducing cost and reserving the time of skilled workers for more complex tasks.

The mainframe security lifecycle, shown in Figure 3, presents a security workflow for those responsible for mainframe security. The security portfolio from CA fills the needs of the mainframe security team by integrating solutions that identify, manage, and reduce risk, thus updating and modernizing mainframe security.

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 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 CA Compliance Event Manager, alerting the Security Operations Center's SIEM to crucial issues.

And finally, with CA Cleanup, we automated the process of reducing unused IDs, thereby reducing risk by former insiders and reducing security staff workload.

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 70% of the world's mission-critical data and are used by nearly three-quarters of the Fortune 100. With strategic planning, you can maintain a solid security foundation for your mainframe.

"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

Conclusion (cont.)

The mainframe security portfolio from Broadcom is designed to work together across the security lifecycle. Each offering delivers individual value and the combination of data from across the tools deliver even greater value through analytics and insights into previously unknown risks.

Related Products and Solutions

- **CA Advanced Authentication for Mainframe**
  Increase information security through consistent password policies and requiring users to successfully authenticate with two factors before logging in to mainframe applications.
- **CA Trusted Access Manager for Z**
  Increase business efficiency by delivering trusted mainframe services through privileged access management.
- **CA Data Content Discovery**
  Find, classify and secure essential business data to reduce risk and simplify regulatory compliance.
- **CA Compliance Event Manager**
  Alert, inspect and protect to simplify regulatory compliance and streamline audits
- **CA Cleanup**
  Easily automate continuous and unattended security file cleanup.

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, visit: mainframe.broadcom.com/trymri-securityessentials.

For more product information, please visit our site at mainframe.broadcom.com/security.

BROADCOM®
connecting everything®

For more product information: broadcom.com

MF-Security-SB101 June 10, 2020