BROADCOM® | Mainframe Software

Modernize Mainframe Security at the Enterprise Level

Broadcom's security solution suite helps secure the mainframe with comprehensive and simplified protection

For decades, mainframe security has set the bar for IT security. But as more organizations adopt hybrid IT architecture, mainframes have moved from being isolated systems to integral, connected parts of distributed networks. Despite this, mainframe security has often remained separate from the rest of the enterprise, frequently dependent on a diminishing pool of experts. Because of these changes, maintaining mainframe security in the modern era has become more difficult.

Broadcom solves this by offering the only security solution suite that integrates with all three mainframe security managers (ESMs) — IBM RACF®, ACF2™, and Top Secret® — at the enterprise level. This allows organizations to use in-house tools like SIEMs to gain a comprehensive, simplified view of mainframe security alongside all other hybrid infrastructure security, while also making it easier to address potential threats and vulnerabilities. The results are greater visibility, more control, and improved security.

Business Challenges and Opportunities

The way organizations use mainframes has changed. Once seen as isolated systems, they now communicate with distributed on-premise and off-premise networks, interact with applications in the cloud, and share data across a range of different systems. As a result, more people than ever before have access to the mainframe. This has raised the risk profile of mainframes and made them vulnerable to a greater variety of threats — especially given that mainframes often host the most crucial enterprise data and applications.

But while mainframes have become an integral part of complex hybrid environments, their security has largely been left separate from the rest of the enterprise. There are many reasons for this. For instance, mainframes hold vast amounts of data, which can make locating threats and mitigating them a resource-intensive process. Mainframe security also requires specialized knowledge and years of experience, making it more difficult to assess risk postures properly.

Organizations can no longer afford to keep the security of their mainframes isolated from the rest of their enterprise. The average cost of a data breach has grown to $3.86 million and insider threats have increased, making a comprehensive view of enterprise security vital. Simultaneously, growing compliance and regulatory requirements have made security more complex and led to an increased demand for qualified mainframe and security practitioners. In turn, this has made it difficult for many companies to find and hire experts who can meet their needs.

DEFINITIONS

» **Top Secret:** This is a mainframe security system developed by Broadcom and first introduced in 1985.

» **SIEM**: Short for Security Information and Event Management, this type of software application monitors and manages all security issues across an enterprise.

MAINFRAME SECURITY CHALLENGES

Mainframe security is often isolated from the rest of the enterprise. This has led to the following challenges:

- Lack of a comprehensive view of enterprise security
- Difficult to properly assess mainframe security posture
- Aggregating mainframe security data can be slow and manual
- Inability to meet growing compliance and regulatory needs
- Mainframe is often misunderstood by senior leadership, assumed to be secure, and omitted from enterprise security strategies
- Fewer security experts who can interpret, assess, and remediate mainframe security risks

SOLUTION

Broadcom enables organizations to modernize their mainframe security by making it easy to fully integrate with SIEM systems, as well as identify and reduce risks throughout the security lifecycle. Broadcom offers the only solution that works with all three mainframe security managers (IBM RACF®, ACF2™, and Top Secret®), ensuring organizations can address mainframe security exposure through a single security lens.

Here's how it works:

1. **Broadcom Mainframe Security Solution**
   Broadcom Security Solution makes it simple to both connect mainframe security with the rest of the enterprise, and to identify and reduce risk from threats. By acting as a foundation between the mainframe and other parts of the hybrid IT environment, as well as integrating with SIEMs, it gives organizations a quick and easy way to assess their mainframe security needs alongside the rest of their enterprise.

Once connected, Broadcom Security Solution helps strengthen mainframe security by interpreting and assessing data, identifying threats, and making recommendations to reduce risks. For example, using point-in-time data, Broadcom Security Solution can help determine access rights, assess data encryption, and look at system critical resources. It can also automate manual, time-consuming security tasks like data collection.

Key benefits:

- **Interpretation, Assessment, and Remediation:** Quickly identify and understand threats to reduce mainframe security risks.
- **Simplicity:** No programming skills or specialized mainframe security knowledge is required to use and benefit from the Broadcom Security Solution.
- **Multi-System Support:** By using and making data available through APIs, the Broadcom Security Solution enables organizations to assess mainframe security through other in-house tools.

2. Security Lifecycle Tools

Because mainframes are crucial parts of complex hybrid environments, more employees, customers, contractors, and people now require access. As a result, the greatest security risks often come from the inside. Whether a malicious breach or an honest mishap, these threats require constant vigilance and fast mitigation.

Broadcom offers several tools for securing the mainframe across the broader security lifecycle:

» **Trusted Access Manager for Z:** When not properly managed, privileged identities on the mainframe can leave organizations exposed to extensive risk. Trusted Access Manager for Z is the first solution that allows businesses to restrict and monitor all activity performed by privileged accounts. This simplifies auditing and lets security teams address emergencies more quickly so that they can mitigate risk before extensive damage occurs.

» **Compliance Event Manager:** Making sure data and processes remain compliant can be time-consuming, yet non-compliance can be even more costly. Compliance Event Manager monitors users, security settings, and system files to help organizations stay on top of any suspicious activity. All critical security events, forwarded to SIEM systems and analyzed alongside other enterprise activities, give organizations a more comprehensive view of their security posture.

» **Advanced Authentication Mainframe:** Multi-factor authentication is a quick but effective way to increase security. Advanced Authentication Mainframe lets organizations phase multi-factor authentication in for any users in the system, providing an additional layer of protection.

KEY DIFFERENTIATORS

Broadcom's approach to mainframe security gives organizations a holistic solution to securing their entire enterprise. The following are some key differentiators of this strategy:

- **True Enterprise Integration**: Broadcom offers the only mainframe security suite that integrates with all three mainframe security managers (IBM RACF®, ACF2™, and Top Secret®). Organizations can also view mainframe security data through in-house SIEM tools such as QRadar or Splunk, as well as with secure VPN access tools and Symantec solutions.
- **Modernizes Mainframe Security:** By automating manual and time-consuming tasks like data collecting and auditing, as well as by bringing mainframe security data to the larger enterprise, Broadcom helps make mainframe security more widely accessible beyond just mainframe security experts.
- **Strengthens Security Lifecycle**: Broadcom's mainframe security suite of tools helps organizations gain greater control over privileged identities, take proactive measures against possible compliance issues, and improve security access with multi-factor authentication. The result makes the mainframe, as well as the rest of the enterprise, more secure.

Learn more about Broadcom's approach to Mainframe Security.
https://www.broadcom.com/solutions/mainframe/security

ENABLING IBM IS TEAMS WITH SECURITY SOLUTIONS

Your customers' mainframes have moved from isolated systems to integrated parts of complex hybrid networks, opening them up to a variety of new threats. Through IBM's partnership with Broadcom, you can help your customers modernize their mainframe security so that they are better prepared to locate vulnerabilities and mitigate threats throughout the security lifecycle.

Leverage Broadcom Mainframe Security to help your customers:

» Fully integrate their mainframe security with the rest of the enterprise, allowing them to view all security data in one place.

» Automate manual and time-consuming security tasks, such as data collecting and auditing.

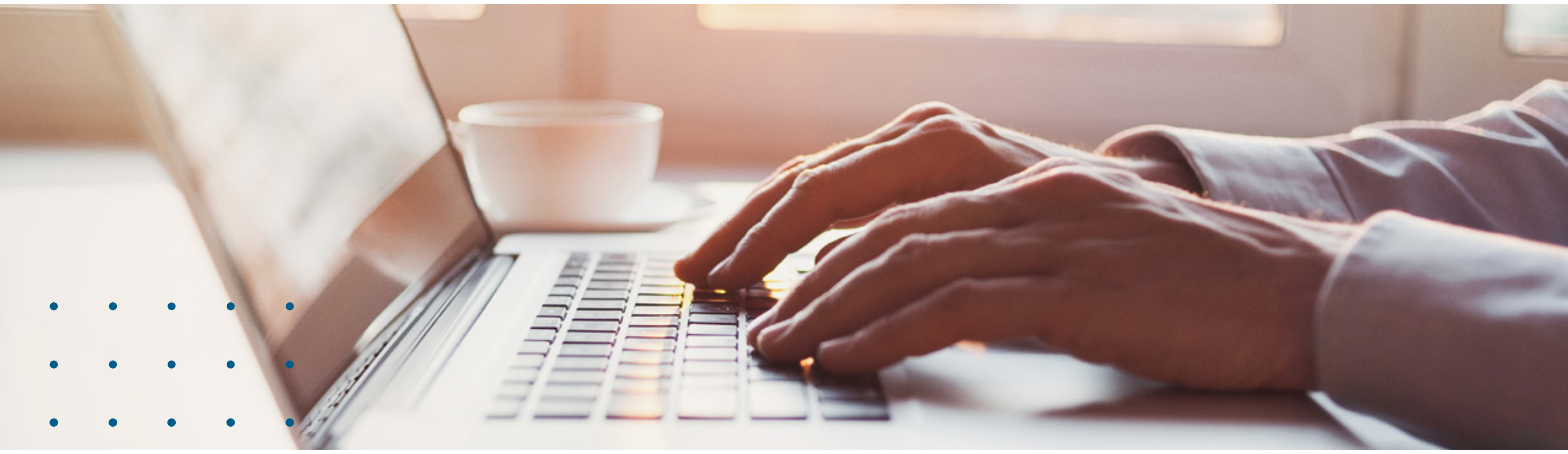
» Make mainframe security management accessible beyond just mainframe security experts.

» Strengthen security lifecycle with tools for controlling privileged identities, managing compliance issues, implementing multi-factor authentication, and more.

The way customers are using their mainframes has changed. The Broadcom-IBM partnership enables IBM Infrastructure Services team to turn today's mainframe security threats into opportunities for building a holistic solution for securing the entire enterprise.

Explore how changing risks are affecting your clients and begin leveraging the power of this partnership by contacting:

Contact
Jim Brace
Mainframe Business Specialist | IBM
Broadcom Mainframe
Software Division
james.brace@broadcom.com



mainframe.broadcom.com

@BroadcomMSD

Broadcom Mainframe Software