Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Mainframe Cybersecurity and Compliance Demands Continuous Vigilance

Building Customer Trust With Cybersecurity Continuous Monitoring, and More From Broadcom

By Stephen Catanzano, Senior Analyst; Scott Sinclair, Practice Director; and Keir Walker, Senior Market Research Analyst
Enterprise Strategy Group

July 2024

Contents

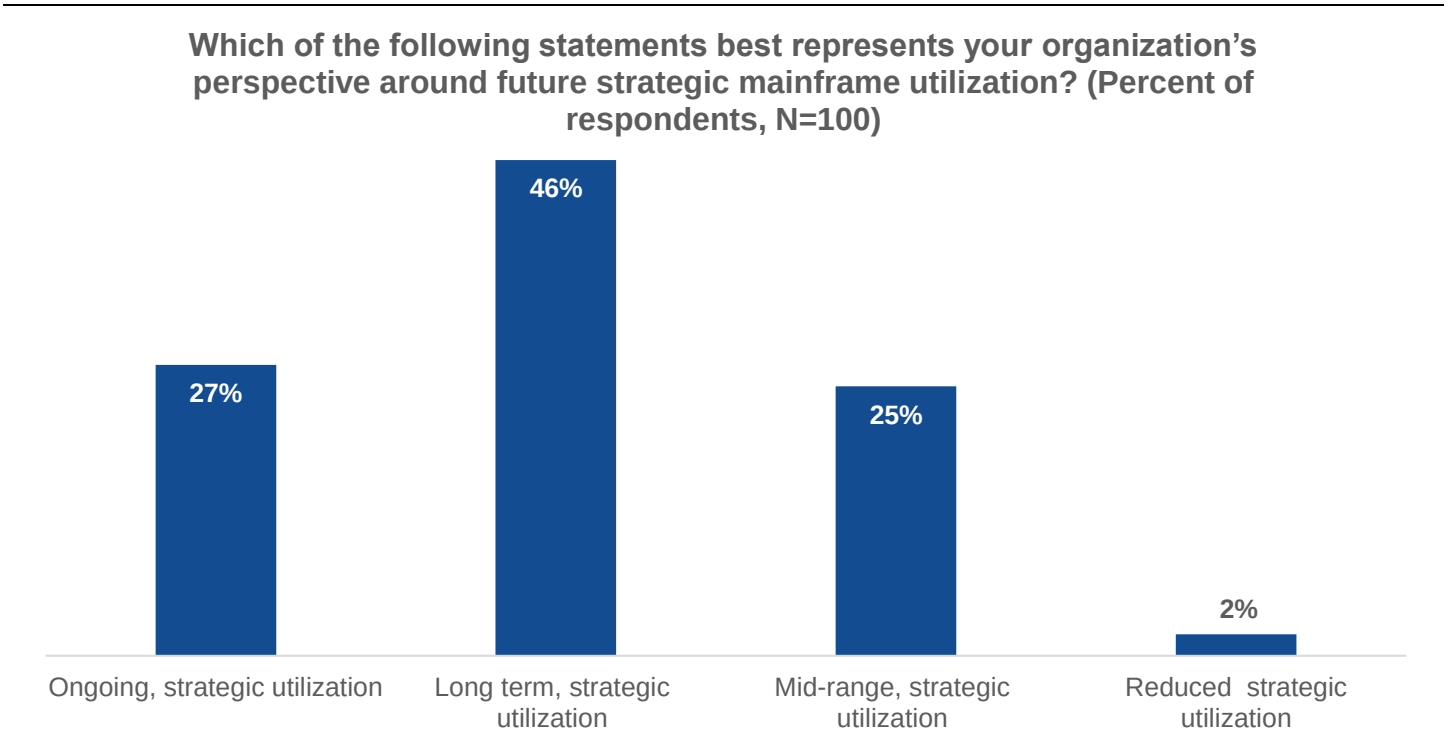
Abstract

While renowned for their inherent robust capabilities, in today's environment, mainframes require organizations to be vigilant about cybersecurity and compliance practices to protect this vital asset along with its data and applications. Comprehensive cybersecurity measures are essential to shield crucial data from evolving threats. Broadcom champions a proactive approach, emphasizing cybersecurity continuous monitoring along with strong identity and access measures as the cornerstone of a robust mainframe cybersecurity posture and unwavering compliance. This paper focuses on the challenges, the changing cybersecurity environments, and the solutions Broadcom offers to help organizations achieve compliance and cybersecurity on mainframe systems, which, when combined with corporate policies and implementations, are the key to success.

Mainframes Remain Strategic As a Foundation for Compliant Businesses

Research from TechTarget's Enterprise Strategy Group, shown in Figure 1, reveals a strong intent by organizations using mainframes to further expand their utilization. Notably, 98% of these organizations continue to use mainframes for strategic, business-critical workloads. Of those, 46% of organizations intend to add significant workloads to their mainframe operations. Another 27% plan to incorporate a wide range of workloads into their mainframes.[1] This data underscores the strategic importance and continued reliance on mainframes in handling diverse and critical business functions.

Figure 1. Strategic Mainframe Utilization



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Custom Research commissioned by Broadcom, *Mainframe Market Pulse Survey*, April 2024. All Enterprise Strategy Group research references and charts in this white paper are from this custom research.

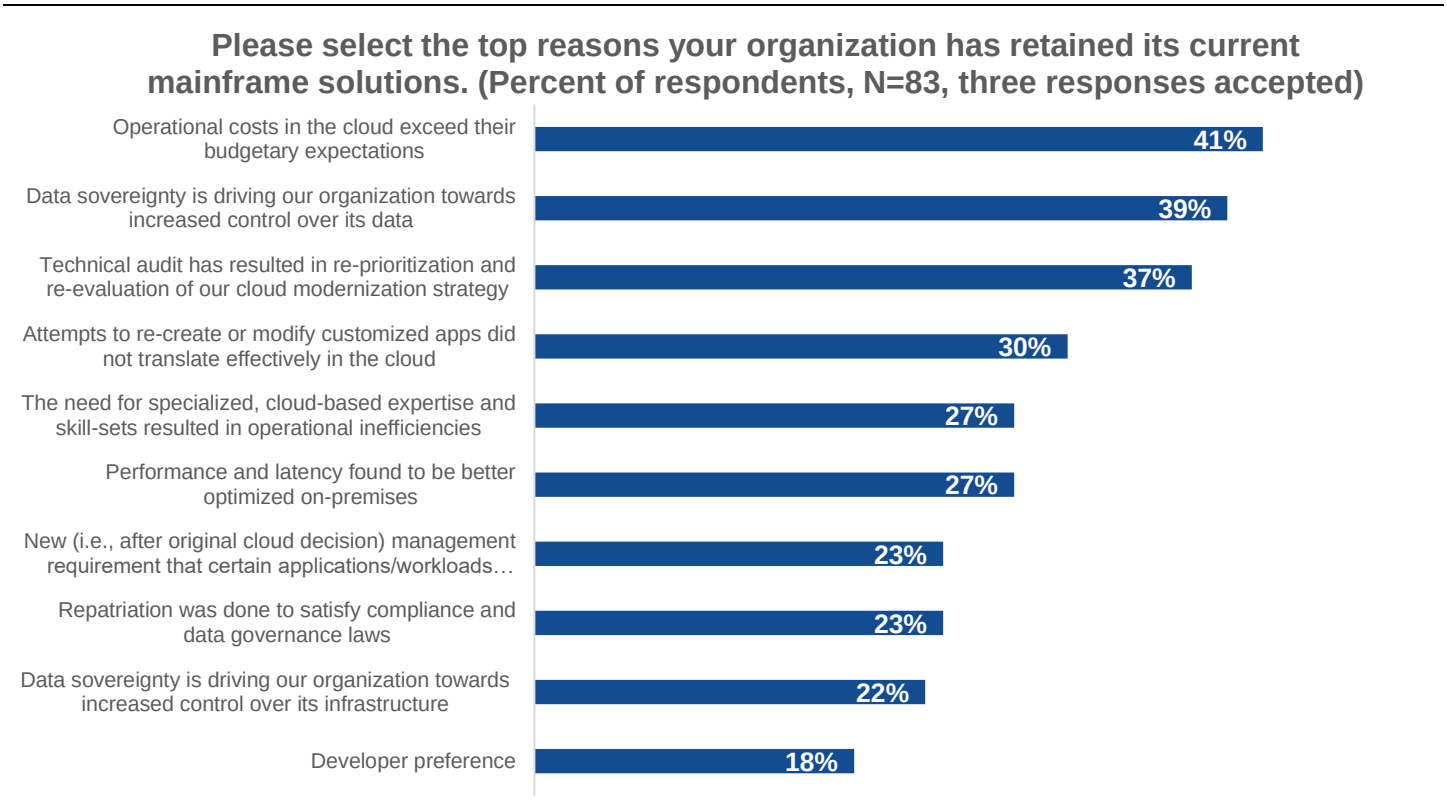
Renowned for their reliability, scalability, and processing capabilities, mainframes have served as the foundation of enterprise IT systems for a long time. The significant number of businesses and percentage of the global economy relying on mainframes for operations underscores their role in ensuring smooth and effective mission-critical business functions.

The growing interest in extending the use of mainframes to handle workloads (46%) and a broad array of tasks (27%) indicates that companies acknowledge the mainframe's capacity to manage a wide range of responsibilities. This shift suggests an increasing trust in the mainframe's adaptability and potential to support new technologies and modern applications.

Workloads Are Moving Back to Mainframe Environments

One factor in the continued expansion of mainframe usage is that organizations using mainframes today are moving workloads back from the cloud. According to Enterprise Strategy Group research, 94% of respondents indicated that they moved numerous workloads back on premises in the last 12 months. The reasons for keeping mainframe solutions in place are shown in Figure 4 and include operational costs as the top consideration (41%), followed by data sovereignty (39%), technical audits (37%), compliance and governance (23%), and more.

Figure 2. Repatriation of Workloads



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

This shift highlights a strategic reevaluation of cloud versus on-premises infrastructure for some workloads, where the predictable and often lower operational costs of mainframes become increasingly attractive. Data sovereignty concerns further emphasize the importance of maintaining control over sensitive information, a capability that mainframes inherently provide. Additionally, the need to comply with technical audits and stringent regulatory requirements makes mainframes a preferred choice due to their robust security and compliance features.

Compliance Considerations

When we look broadly at cybersecurity challenges for mainframes, an organization must address data privacy and cybersecurity, regulatory demands, access controls and identity management, change management, and logging requirements. Some of the key compliance challenges include:

Data Privacy and Security

- **Data breaches.** Ensure that data stored and processed on mainframes is protected against breaches and unauthorized access.
- **Encryption.** Ensure strong encryption mechanisms are implemented for data at rest and in transit.

Regulatory Requirements

- **Industry-specific regulations and standards.** Adhere to industry-specific regulations such as DORA, PCI DSS, CMMC, NIST, GDPR, and HIPAA, among others.

Audits and Reporting

- **Regularly scheduled audits.** Audits and reports demonstrating compliance with various laws and regulations should be shared with executives and other stakeholders. Ensure 24/7/365 security continuous monitoring over critical system and cybersecurity controls, providing real-time alerting of changes within those critical areas.

Access Control and Identity Management

- **User authentication.** Implementing robust authentication mechanisms such as multifactor authentication (MFA) to ensure that only authorized personnel have access to the mainframe, only to the applications and data they are supposed to access, and only during the period of time when this access is necessary, with tools for privileged user management.
- **Role-based access control (RBAC).** Ensure that access rights are appropriately assigned based on user roles and responsibilities.

Vulnerability and Change Management

- **Identify.** Use software that helps identify both assets and their vulnerabilities on the mainframe.
- **Remediate.** Manage updates, patches, and configurations to address identified urgent vulnerability concerns following the recommendations of your software provider.

Monitoring and Logging

- **Activity monitoring.** Continuously monitor system activities to detect and respond to suspicious or noncompliant behavior.
- **Log management.** Maintain comprehensive logs of all system activities and access attempts for audit and forensic purposes.

Threat-led Penetration Testing

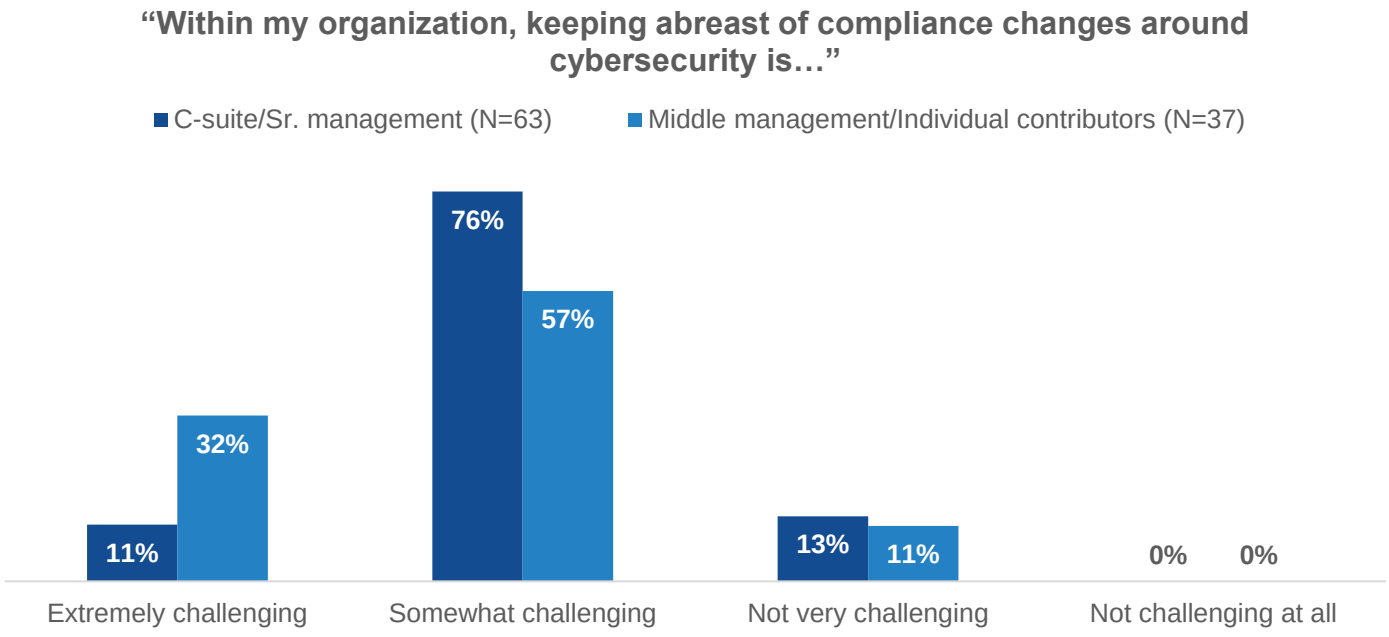
- Train employees on threat-led penetration testing (TLPT). Following recommendations from DORA and other frameworks such as NIST, ensure that staff are adequately trained to conduct TLPT effectively. Conduct TLPT at least every three years. Adhering to guidelines from DORA and aligning with best practices recommended by frameworks like ISO/IEC 27001, perform these tests regularly to identify and mitigate potential vulnerabilities.

Addressing these compliance challenges requires a combination of robust security measures, regular audits, thorough documentation, and continuous monitoring to ensure that mainframe environments remain secure and compliant with applicable regulations.

Staying Ahead: Mainframe Cybersecurity Compliance Challenges

Organizations are constantly faced with many cybersecurity-related challenges, including data privacy, financial regulations, and privacy and security guidance. In recent research from TechTarget's Enterprise Strategy Group, shown in Figure 1, organizations were asked how challenging it is to keep abreast of compliance requirements around cybersecurity. 87% of C-suite and senior managers find it somewhat (76%) to extremely (11%) challenging, and among middle managers, 89% found it somewhat (57%) to extremely (32%) challenging.

Figure 3. Staying Abreast of Cybersecurity Challenges Is a Challenge



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

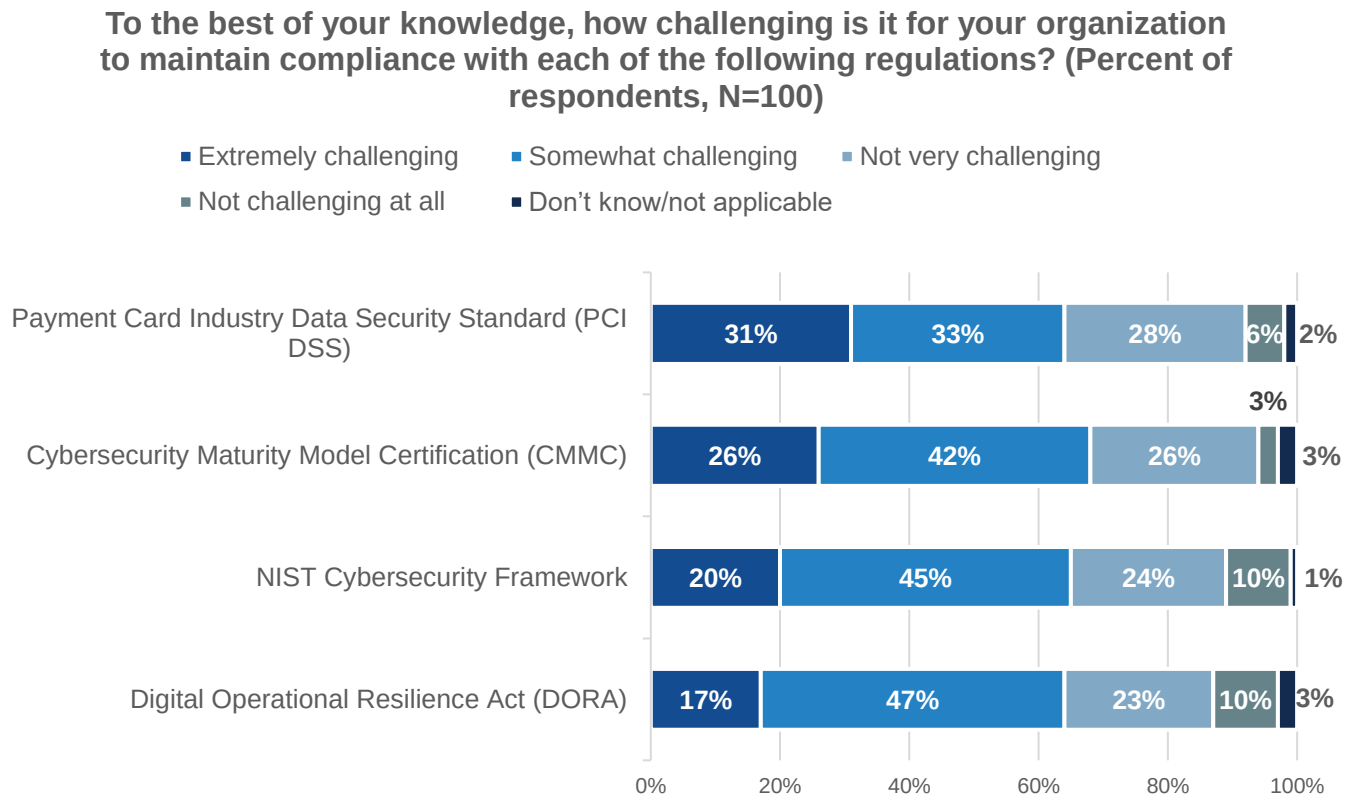
Based on the research, it is evident that compliance with cybersecurity requirements poses significant challenges across all levels of management. The high percentage of senior managers (87%) and middle managers (89%) struggling with these issues underscores a pervasive concern within organizations. This challenge is not only widespread but also intensifies as we move down the managerial hierarchy, indicating a potential gap in resources, knowledge, or support systems. Addressing these challenges is crucial for organizations to ensure customer and employee trust in an increasingly complex regulatory environment. These findings highlight the urgent need for comprehensive strategies and tools to alleviate the compliance burden and enhance cybersecurity resilience across all organizational levels.

Key Cybersecurity Specific Challenges

Compliance challenges around mainframes are multifaceted, often stemming from the complexity of the systems' environment, as well as criticality and the stringent regulatory requirements they must meet. In recent Enterprise Strategy Group research, shown in Figure 2, organizations were asked how challenging it is to maintain compliance with some key security-related regulations. In these top four compliance areas, we find that a majority of organizations find it challenging, with a high percentage finding it extremely challenging:

- **Digital Operational Resilience Act (DORA) compliance:** 64% find it challenging (17% extremely).
- **PCI DSS compliance:** 64% find it challenging (31% extremely).
- **Cybersecurity Maturity Model Certification (CMMC) compliance:** 68% find it challenging (26% extremely).
- **NIST Cybersecurity Framework compliance:** 65% find it challenging (20% extremely).

Figure 4. Specific Security Regulatory Compliance



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

These areas highlight the pressing need for more effective compliance strategies and solutions. Mainframes are critical in handling sensitive data and operations, so any compliance lapse could have severe implications. Organizations must invest in robust compliance management tools, continuous monitoring, identity and access, regular audits, and ongoing training to navigate these complexities effectively. The high percentage of organizations finding compliance extremely challenging signals a critical area for improvement and innovation in compliance management practices.

Security Continuous Monitoring Is Crucial for Compliance

Traditional security reviews are extremely limited, and organizations need to move beyond merely "passing audits" to embrace continuous monitoring. Broadcom's Security Suite, utilizing tools such as Compliance Event Manager (CEM) Multi-factor Authentication – Advanced Authentication Mainframe (AAM), and Trusted Access Manager for Z (TAMz), enforces best-practice policies in real time, helping organizations stay ahead of evolving threats. The trend of moving workloads back to mainframes is evidence of the "hybrid app" approach, where the mainframe drives enterprise applications. However, this shift also introduces connectivity and access vulnerabilities that were not

present when the applications were entirely contained within the mainframe. Consequently, mainframe security must adapt and improve.

Security continuous monitoring extends beyond event detection. Our research shows that many organizations may fail to see the distinction between monitoring event detection on a continual basis versus monitoring every event on the system on an ongoing basis. This gap can present a real danger. In today's world of continuous cyberthreats, which may be greatly fueled by AI, cybersecurity continuous monitoring is required for a higher level of protection. This includes the oversight of privileged access management (PAM) IDs, cleaning up all IDs, and enforcing change control. This comprehensive approach to continuous cybersecurity monitoring ensures that organizations maintain robust security postures in an increasingly complex and interconnected IT environment. It involves the surveillance of mainframe components, like z/OS system configurations and External Security Manager (Broadcom Access Control Facility 2, Broadcom Top Secret, IBM Resource Access Control Facility) settings and monitoring critical areas within software and applications in real time for alerts. This process entails providing event notifications to security information and event management (SIEM) solutions and SOC teams. As shown in Figure 5, Broadcom offers a comprehensive solution for mainframe security.

PAM and Identification/MFA are also crucial to the compliance process. Implementing a comprehensive PAM solution enhances organizational compliance by adhering to best practice access controls to secure critical data and infrastructure. This approach mitigates risk by reducing threat landscapes. Additionally, adaptive authentication (such as risk-based MFA) strengthens trust in privileged user identity and enables just-in-time (JIT) access. These measures are crucial for zero-trust initiatives, which aim to minimize threat exposure by limiting unnecessary or malicious access to mainframes integrated with external technologies.

Figure 5. Broadcom Security Lifecycle and Continuous Monitoring

Source: Broadcom, Inc.

The Broadcom Security Portfolio includes:

- **Trusted Access Manager for Z.** TAMz reduces the risk of insider threats, from malicious attacks to inadvertent threats. It is designed for mainframe environments, helping organizations control and monitor privileged access to mainframe systems. TAMz enforces strict access policies and provides comprehensive auditing and reporting capabilities, ensuring compliance with regulatory requirements and internal security policies by restricting access to critical systems, maintaining detailed audit trails, and implementing robust security policies.
- **Compliance Event Manager.** CEM simplifies regulatory compliance and streamlines audits through advanced compliance management and threat detection. It is a tool used to ensure organizations meet regulatory and internal security standards by monitoring, detecting, and responding to compliance-related events in real time. CEM provides real-time alerts and detailed reports, linking related security events to identify patterns and potential threats, as well as generating comprehensive reports for compliance audits and internal reviews.
- **Multi-Factor Authentication.** To strengthen mainframes in the new world of hybrid applications, customers must address access management improvements, including implementing MFA and PAM. These measures are security mechanisms that enhance resource protection by requiring users to provide two or more verification factors, such as a password (something you know), a mobile phone or security token (something you have), or biometric verification like a fingerprint (something you are). This approach significantly reduces the likelihood of unauthorized access.

Implementing security monitoring on mainframes enables organizations to receive alerts about changes and potential security breaches that could jeopardize the integrity of their mainframe, applications, and data. Without this monitoring in place on a mainframe, it's impossible to be aware of any incidents that occurred two hours ago, leading to a system compromise or unauthorized access, resulting in the theft of customer data.

Here's why security continuous monitoring is a game-changer:

- **Limited scope of audits.** Traditional audits offer a snapshot in time. They miss activities happening outside the audit window, leaving systems vulnerable.
- **Exploiting the gap.** Malicious actors know of and can take advantage of the time between audits, compromise systems, and then revert to a seemingly safe state before the following review.
- **Continuous vigilance.** With CEM, organizations have a guardian on duty 24/7. It continuously monitors mainframes for cybersecurity lapses, insider threats, unauthorized changes, and potential breaches. It further provides real-time alerts, enabling security teams to take immediate action.
- **Upgrade from reactive audits to proactive security.** CEM empowers organizations to:
  - **Proactively detect threats.** Identify suspicious activity as it happens, not weeks or months later.
  - **Strengthen defense.** Enable the monitoring and alerting on best-practice security policies.
  - **Maintain compliance.** Stay ahead of regulations and demonstrate a commitment to robust data security.

Use Cases

How CEM Has Helped Customers Detect Pen Test Attempts

The Broadcom CEM has been instrumental in assisting customers in detecting penetration (pen) testing attempts by offering monitoring and immediate alerting functions. During a penetration test, security experts simulate attacks on the IT infrastructure to pinpoint vulnerabilities. CEM supports this process through features such as:

- **Real-time monitoring.** CEM consistently oversees network and system activities, enabling the identification of unusual patterns or behaviors that might indicate a pen test. This real-time surveillance ensures recognition of any attack endeavor.
- **Event correlation.** By linking events from sources, CEM can identify attack patterns that a pen test could utilize. This correlation aids in distinguishing between activities and suspicious actions linked to penetration testing.
- **Comprehensive logging and auditing.** CEM maintains detailed logs of all operations within the IT environment. These logs help recognize actions undertaken during a pen test, such as unauthorized access attempts, privilege escalation, or vulnerability exploitation.

"The team received an alert in real time as the internal pen test team took their first steps to penetrate the mainframe systems. Continuous monitoring enabled the team to catch the test team 'red handed,' call the specific pen tester, and stop the test before any progress against the mainframe occurred."

—Multinational financial services company

- **Alerting and reporting.** CEM generates instant alerts upon detecting activities resembling those of a pen test. These alerts are relayed to security teams for investigation and response.
- **Policy enforcement.** CEM enacts security protocols that can trigger alerts during a pen test. For example, any efforts to circumvent security measures or access restricted areas will be promptly flagged for attention.

With these features, CEM empowers organizations to efficiently identify and respond to pen test endeavors, ensuring the strength of their security measures and swift resolution of any identified vulnerabilities. This proactive approach boosts the organization's security stance, enhancing its resilience against cyberthreats.

Implementing Security Continuous Monitoring From Broadcom for Mainframe Protection

Financial, manufacturing, and many other mission-critical organizations operate a complex IT environment with critical financial data and applications hosted on mainframes. With cyberthreats becoming increasingly sophisticated and driven by AI, organizations need a robust solution to ensure continuous security monitoring and compliance with regulatory requirements.

To resolve these challenges, organizations can implement Security Continuous Monitoring via Broadcom's Security Suite, including CEM, MFA-AAM, and TAMz.

Deploying CEM provides:

- Real-time monitoring, which offers continuous monitoring of all mainframe activities, detecting unusual patterns indicative of potential security breaches that organizations need.
- Event correlation and alerting features, which correlate events across the IT environment, generating real-time alerts for suspicious activities. This allows for quick identification and response to potential threats.
- Detailed logging and reporting, which create comprehensive logs and reports that are facilitated by thorough forensic analysis and which support compliance with industry regulations.

Example

Article 9 of the Digital Operational Resilience Act mandates that financial entities continuously monitor and control the security of their information and communication technology (ICT) systems. This requirement emphasizes the importance of ongoing vigilance and proactive management of security to safeguard against cyberthreats and ensure operational resilience within the financial sector.

Deploying TAMz provides:

- Privileged access control, which enforces strict policies for privileged access to mainframe systems, reducing the risk of unauthorized access.
- Audit and compliance features, which include detailed auditing capabilities, ensuring that all access and actions are tracked and reported and supporting compliance efforts.

Deploying MFA - AAM provides:

- Enhanced security by requiring multiple forms of verification, which significantly reduces the risk of compromised credentials and unauthorized access.
- Increased user trust and compliance by ensuring that only authenticated and verified users can access sensitive systems and data, thereby meeting regulatory requirements.

Implementing CEM, MFA, and TAMz enhances security posture with continuous monitoring to proactively detect and mitigate potential security threats, significantly reducing the risk of data breaches. Detailed logs and real-time monitoring also enhance regulatory compliance, ensuring compliance with regulatory standards, including those mandated by industry regulations. Operational efficiency is also streamlined, providing a unified view of security events and reducing the time and effort required for manual monitoring and compliance reporting.

Sharpen Skillsets: Ethical Mainframe Hacking Course

As cybersecurity disciplines are advancing, it is more clear than ever that simulating adversarial attacks to test defenses is particularly effective. Pentesting is a unique skill, requiring deep knowledge of both the mainframe and strategies used by cyberadversaries. Broadcom offers customers a three-day instructor-led course on ethical mainframe hacking to bridge the skills needed in this particular and important area for cybersecurity teams.

In this course, participants will learn:

- The latest attack vectors, techniques for gaining system access, and how to perform an end-to-end penetration test.
- How to develop techniques to perform appropriate mainframe penetration testing.
- How to use open source tools and libraries for all steps of a penetration test.
- How to write tools for pentesting.

Broadcom customers can find the latest courses by contacting Learning@Broadcom.com.

Conclusion

Mainframes are inherently secure but only when organizations implement the right solutions and best practices to keep them secure. In the ever-changing IT landscape of hybrid mainframe and cloud environments, and given the escalating threat of cyberattacks with the use of AI, organizations need to be more diligent than ever before. This demands continuous vigilance, which is an essential aspect of building customer trust. While these challenges are significant, organizations do not need to face them alone. Broadcom's suite of tools and solutions is designed to provide continuous monitoring and more, ensuring robust cybersecurity and compliance. With Broadcom's support, organizations will have the resources and expertise necessary to meet these demands confidently. For any organization navigating the regulatory landscape and looking to ensure a compliant, secure, and trusted mainframe environment, Enterprise Strategy Group highly recommends a discussion with Broadcom for vigilant and continuous cybersecurity and compliance.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com