Mainframe Security in a Hybrid/Mobile World

A BMC Compuware Guide to new best practices for the new threat matrix
Compuware joins BMC to empower the next generation of developers to mainstream the mainframe. With unparalleled mainframe operations management and agile application development and delivery, BMC Compuware provides a mainframe-inclusive DevOps toolchain that increases volume and velocity.

Bring apps that run on the mainframe to market faster with increased quality throughout the process of analyzing, building, testing, deploying, monitoring, and tuning apps and services. Our combined offering accelerates each client’s evolution to an Autonomous Digital Enterprise.
As digital demands on enterprises grow, so does their cybersecurity exposure. More code running on more infrastructure moving more data across more connections means a larger threat surface—and greater risk to the business.

Large enterprises face the further challenge of optimizing cybersecurity across multiple platforms—including mainframe, distributed, cloud, and diverse endpoint devices. Cybersecurity technologies and best practices for the latter three are widely discussed and well understood. The mainframe is another story.

78% of CIOs say that their organization’s mainframe is more secure than other systems.*
While the mainframe is by far the enterprise's most inherently secure platform, it has been neglected when it comes to cybersecurity. This is for two reasons. First, the mainframe's inherent security has led to complacency. Second, because other platforms have proven to be so painfully non-secure, they have kept infosec teams operating in a near-continuous state of crisis—consuming virtually all of their time, attention, and budgets.

Infosec leaders, however, can no longer afford to neglect mainframe security. Four trends in particular require adjustments in mainframe security practices: cross-platform credentialing for cross-platform apps, the high stakes associated with insider malfeasance, intensifying DevOps activity, and outsourcing.

Enterprises that up their mainframe security game to meet these new challenges will continue to reap the benefits of the mainframe's superior security, reliability, scalability, and performance economics for decades to come. Those that don't will put themselves and their customers at risk. And it won't be because there's anything inherently problematic about the mainframe platform itself.

Enterprise infosec leaders must augment their mainframe security practices to address the new threats posed to increasing interconnection with far less secure platforms.
Leaving the Glass House
Most mainframe environments originated as self-contained platforms for core enterprise systems of record and large-scale transaction processing engines. Over the years, that role has evolved considerably. These days, mainframe applications and databases increasingly serve as back-end resources for cross-platform/multi-tier digital services that employees, customers, suppliers, and partners engage with via distributed desktops and web/mobile front-ends.

Cross-platform/multi-tier services have proven to be a superlative way to leverage the power of the mainframe platform, the irreplaceable IP of mainframe application business logic, and the wealth of mainframe-resident data. But hybrid/mobile services also create new mainframe security challenges:

### Challenges

1. **Vulnerability by Association**
   
   While the mainframe is inherently secure, the distributed environments with which mainframes now increasingly interface are just the opposite. Chronic OS vulnerabilities, malware exploits, spear-phishing, and other cyberattacks make it virtually impossible to fully secure end-user devices, email systems, and other common points of entry for attackers. Once compromised, these non-mainframe environments allow attackers to hijack user identities and their associated credentials to gain potential entry into core mainframe systems. Enterprise infosec leaders must therefore not just protect the mainframe from direct attack—but also from cybersecurity exposures resulting from the compromises that so often occur on other platforms.

2. **The Privilege Problem**
   
   As the mainframe’s role in the enterprise continues to expand, so does the potential adverse impact of any misuse of privileged mainframe accounts—whether that misuse is the result of a malicious insider taking inappropriate advantage of legitimate privileges or a malicious outsider who has managed to hijack someone else’s admin-level privileges.

   The mainframe privilege problem has been exacerbated in recent years by the downsizing of mainframe staffs. That downsizing tends to result in a smaller number of mainframe operators having a wider range of privileges. In fact, at many enterprises, highly privileged admins even wind up being responsible for oversight of mainframe access audits—an egregious violation of the separation-of-duties principle.

3. **Agile Dev/Test Exposure**
   
   Increased digital agility also puts new pressures on mainframe security. Agile development and testing of new applications requires more frequent sampling of data from the mainframe, even if the code being worked on is running elsewhere. The more mainframe data is shipped to various dev/test servers outside the mainframe environment, the more exposed it is to risk.

   Also, to keep pace with relentlessly evolving market demands, enterprises are attempting to update and modify mainframe code at a much faster pace than the historical norm. Without a corresponding adjustment in mainframe DevOps processes and tools, this faster pace of work can potentially result in application flaws that could compromise system integrity.
Challenges

4. Outsourcing

C-level executives at many enterprises thought it wise at some point to outsource some or all of their mainframe operations and development for economic reasons. While the merits of such a decision are arguable, the cybersecurity implications are clear: Outsourcers with strong financial incentives to skimp on infosec investment now hold the keys to the mainframe kingdom. Outsourcers also often suffer from high employee turnover, further compromising mainframe security. Infosec leaders at enterprises engaged in mainframe outsourcing may not even have adequate mechanisms in place for keeping their outsourcers fully accountable when it comes to cybersecurity practices.

5. Feeding the SIEM

SIEMs play an increasingly important role in enterprise security. As enterprise environments become larger and more complex, it becomes more important to gather all the log and event data relevant to both prevention and rapid response in a single repository—where it can be subject to analytics capable of revealing otherwise clandestine activity.

Unfortunately, enterprise SIEMs are almost invariably starved of mainframe-related data. A full 84% of IT managers surveyed said they don’t have ready access to accurate, timely, and complete data about user activity—including data access—on the mainframe. Without that data, their SIEMs and SIEM analytics can’t sufficiently protect the business.

84% of CIOs agree that understanding what and how mainframe data is used is a blind spot.*

Simply put, it’s not the mainframe itself that exposes the enterprise to risk. It’s outdated mainframe infosec practices. Every enterprise must therefore re-examine and revise those practices.
New Best Practices
For the New Threat Matrix
Enterprises can meet the new cybersecurity challenges posed by the expanding mission-critical role of the mainframe in a hybrid world by adopting several straightforward, non-disruptive measures. These include:

- **Capture more complete and granular data on mainframe user behavior**
  Enterprises routinely capture user activity across their distributed and cloud/SaaS environments in order to proactively detect anomalous activity and, when necessary, perform security forensics. Unfortunately, capture of mainframe session activity tends to be far less robust. This deficit can easily be remedied with new tools that capture mainframe activity.

- **Integrate mainframe user behavior activity into the enterprise SIEM**
  Because mainframe breaches are almost universally the result of compromises elsewhere in the enterprise environment, problematic activity is best detected by correlating user behaviors across platforms. Mainframe activity data should therefore be fed into an enterprise SIEM—where appropriate analytic intelligence can be applied to the enterprise as a whole.

- **Reduce dependency on excessively privileged users**
  As noted earlier, enterprises often become highly dependent on a relatively small number of mainframe super users. This is in part due to reduced mainframe staff headcount—but it’s also a result of continued reliance on outdated tools with ancient, nongraphical interfaces that are only useful to those with highly specialized knowledge of cryptic codes and commands. By investing in modern, intuitive tools, enterprises can democratize mainframe tasks and more closely restrict special privileges.

- **Separate mainframe ops privileges from mainframe audit privileges**
  This seems like a no-brainer—but is commonly neglected. With sufficiently intuitive mainframe audit tools, however, enterprises can easily shift mainframe audit responsibilities away from privileged users and put them in the hands of more appropriate infosec and/or IT governance staff.

- **Improve and enforce mainframe test data privatization**
  Many enterprises still perform masking and obfuscation of mainframe test data on a largely ad hoc basis, depending on individuals to mask data inconsistently. A much better approach is to deploy a single, feature-rich data privatization solution as a “gateway” between all mainframe databases and all teams that need test data—and use that gateway to consistently enforce appropriate data protection policies as a prerequisite for any and all dev/test tasks.

- **Embrace automated mainframe unit testing**
  Unit testing is a common practice in the Java world. But in the mainframe world, the burdensome time and effort required to create, run, and evaluate such tests means it is often neglected. Fortunately, new automated tools now make it easy for COBOL developers to quickly and iteratively perform unit testing. Enterprises typically adopt these tools to accelerate mainframe DevOps—but they also provide cybersecurity benefits by ensuring that new code doesn’t introduce software vulnerabilities into the environment.

Other common mainframe security practices—such as multi-factor authentication, data encryption, and proper RACF configuration—remain important. These supplemental practices, however, are now also essential for keeping the mainframe, and its data safe in an increasingly perilous digital world.
Superior Outcomes
For Digital Security & Business Performance
While adoption of enhanced practices for mainframe security requires a modest investment of time and money, that investment pays for itself many times over in multiple ways:

**Improved Mitigation Of Risk For All Stakeholders**

The primary benefit of improved mainframe security is improved enterprise security. Breaches of mainframe systems have great potential adverse impact on enterprises—as well as their customers, partners, and other stakeholders. Investment in better mainframe security should thus be part of any enterprise security effort.

**Streamlined, Reliable Compliance**

Regulatory mandates require enterprises to document that they have taken appropriate measures to protect customers, shareholders, and others from the potential adverse consequences of cybercrime. Plus, if and when an incident does occur, regulatory auditors may launch forensic investigations to determine whether negligence was involved. New mainframe security best practices are essential for fulfilling the requirements of both routine and forensic audits.

**Greater Digital Agility**

Many of the same best practices that improve mainframe security—such as unit testing and automated data privatization—also help accelerate delivery of mainframe application updates. These updates can be crucial for differentiating digital customer experiences and achieving other competitive advantages in an increasingly digital marketplace.

**Avoidance of Costly and Counterproductive Re-platforming**

It certainly makes good business sense for enterprises to obtain certain “commodity” business applications such as payroll and purchasing as cloud/SaaS services. But the wholesale re-platforming of core mainframe applications is an enormously expensive and risky undertaking that does nothing to improve services to customers. It is far better to simply modernize certain mainframe practices—and thereby continue to take advantage of the mainframe’s unmatched security, reliability, and performance at scale for transaction processing and other systems of record.
The mainframe remains the primary engine of global commerce. And total MIPS running on the platform will continue to grow over the long term. Wise stewards of that platform will therefore take reasonable steps to better protect the mainframe in light of the new threat matrix spawned by the ascendance of hybrid/cloud computing and the proliferation of mobile/IoT endpoints. To do anything less would be irresponsible.

**BMC Compuware** provides a complete portfolio of mainframe security solutions to help you address your new cybersecurity challenges, including:

- **BMC Compuware Application Audit**
  This innovative cybersecurity and compliance solution fully captures user mainframe application session activity from start to finish—and integrates the resulting data into your SIEM environment for cross-platform analysis of user behaviors.

- **BMC Compuware Test Data Privacy**
  BMC Compuware Test Data Privacy uniquely enables you to efficiently and flexibly select, cleanse, mask, and validate test data for use in both mainframe and distributed DevOps to ensure security and compliance with regulatory mandates such as GDPR.

- **BMC Compuware Topaz for Total Test**
  BMC Compuware Topaz for Total Test brings Java-like unit testing to mainframe application development by automatically creating and executing tests for logical units of COBOL code.

For more information on how BMC Compuware can help you modernize your mainframe security—and your entire mainframe DevOps value chain—visit [bmc.com](http://bmc.com).

*Findings from an April 2017 survey of 400 CIOs at large companies across vertical markets in both Europe and the U.S. commissioned by BMC Compuware and conducted by independent research company Vanson Bourne.*
About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

www.bmc.com