Ensuring Mainframe Security in a Dynamic World

Systems of Record have never been so connected and the once siloed mainframe is no more. As organizations are digitally transforming, the need to provide access to mainframe applications and more importantly the data that resides on the mainframe is becoming more crucial. We have seen a trend over the last 10 years for mainframe-based data becoming more available to first web applications and now most recently, mobile applications. This trend has only accelerated over the last couple of years as the COVID-19 pandemic accelerated the pace of digital transformation and increased the adoption of mobile and remote interactions with mainframe data.

Against this backdrop we have also seen a fundamental shift in how mainframe systems are managed and administered. As support and SysProg teams were forced to go remote in March 2020 we saw a seismic shift in the way mainframe systems were managed and more crucially where they were managed from – just another node in a complex hybrid environment. Gone are the days where a support and SysProg team is based in the same location as the physical mainframe datacenter. The new normal is that these teams can be based in different locations, cities, states and even countries altogether.

In addition to these changes, we are seeing an increasingly dynamic geopolitical landscape as well as an increase in sophisticated cyber criminals looking to steal, compromise and disable systems of record through cyber attacks or ransomware threats. The security posture of many enterprises has fundamentally changed over the last couple of years to deal with these increasing pressures.

These three threat vectors place unique challenges on CISOs and the wider security team tasked with ensuring the safety and security of mainframe systems and the data they house. Organization needs to adapt to new paradigms of working which includes changing processes while also improving security postures to deal with the increasing threat levels.

As organizations are adjusting to the new dynamics, they are continuously met with challenges. Now is the time to look at the changing dynamics, identify the challenges and roadblocks that are impacting your organization and consider the technology solutions that can help negate threat vectors and provide robust security to mainframe data and mitigate risks.

Common Mainframe Security Challenges

The role of the mainframe in many large enterprises is growing rapidly. IBM recently stated in its 2021 Annual Report that the z15 generation had seen more MIPS shipped in this hardware generation than any previous mainframe cycle. Also according to the latest BMC sponsored research 92% of organizations see the mainframe as a platform for long-term growth and new workloads. Fundamentally, we need to re-think a better approach of managing the mainframe in this new paradigm.
However, the growth of mainframe workloads has not been without its challenges. These include:

Remote and hybrid work practices. The pandemic changed how we fundamentally work. Whereas employees once used to be in the same location as the mainframe, that is often no longer the case. CISOs and IT teams now have to determine who has access to data, where they are accessing the data from, and for how long. The process has become incredibly complex. Increasing number of privileged users, with the elevated access rights are now working from homes, hotels, and coffee shops.

Increased risk of cybersecurity threats. Cybersecurity is a pervasive issue that impacts everyone in an organization, and in some cases the environment, society, and even supply chains. And while access to the mainframe is typically limited, it is still vulnerable to nefarious threat actors. We've also seen an increase in the Solar Winds style supply chain hack that has changed the landscape for trust around development. These threats coupled with the rising geopolitical tensions, result in a complex system that needs enhanced security at every level, modeled in a new way, analyzed with different parameters, and remediated with increase velocity.

Increasingly complex operation and administration of mainframe systems. Mainframes are generally accessed by a relatively small number of people, in terms of direct users, and few administrators. However, in recent years, there has been increase in the number of people on an operations team including teams outside an organization. Managing the operation and administration is no longer as simple as it once was. The mainframe is now just another node in a complex hybrid environment, managed by a new generation of engineers.

As the mainframe security landscape becomes ever more dynamic and hybrid organizations need to improve on the 'indicators of compromise'. It is no longer sufficient to provide role-based access and control functionality that has been the bedrock of mainframe security for many decades. But rather there is an increased need to enhance security further to ensure the people logging into the system not only have the privileges they need but also that they are logging in from a known location at a time that would be expected. The real threat within an organization then becomes the privileged user, that by nature has security controls in place, but now the model by which we analyze the behavior has changed.

How Iconium and DataLenz Can Help Organizations Reach Their Security Goals

These challenges and evolving needs have led us at Futurum Research to evaluate potential technology solutions and partners in the mainframe security space. Iconium Software, while still relatively new to the mainframe space, brings a leadership team with decades of experience in securing the largest mainframe deployments in the most demanding industries around the world, in the public and private sectors where security is paramount.

We believe the level of functionality and robustness of the DataLenz solution uniquely position it to help organizations improve mainframe security in an ever more dynamic environment. The DataLenz solution enhances the traditional, role-based access and control functionality seen deployed on mainframe systems with tools like RACF, TopSecret and ACF2 and deliver context rich geospatial data allied with time zone-based data that can be exposed to multiple observability platforms both on the mainframe and beyond.

We've also identified that the solution focuses on three major areas that include:

Mitigate Data Loss. A primary focus of the DataLenz tool is to reduce the costly loss, manipulation, compromise and theft of mainframe data. The DataLenz solutions seeks to achieve this by effectively filtering out false positives and responding to incidents quickly.

Audit and Compliance. The DataLenz solution enables customers to improve their audit and compliance posture by providing rich contextual data which ultimately leads to greater data security trust. Modeling user access types, with geolocation and time analytics, allows accurate reporting and forensic anomalies.

Rapid Incident Resolution. Not only does the DataLenz platform provide improved reporting but also allows customers to develop policies to immediately alert them when a data breach has occurred to resolve incidents in as near to real-time as possible via several alerting mechanisms. No longer can we wait a day or days to determine security breaches and remediate them – the DataLenz technology can identify the potential security breach, terminate the transaction and suspend the user's access near real-time.

Improving Mainframe Security in a Dynamic World

Mainframes are just as essential to many organizations as they have been for decades. Many organizations continue to expand the use and exploitation of their mainframe-based systems of record. However, the threat landscape for organizations is getting increasingly complex and dynamic — even more so for organization in heavily regulated industries such as financial or government. The added pressures of our changing geopolitical environment and the shift in how we work has meant that mainframe security has never been more stressed. With new challenges comes new opportunities for innovation, as Iconium Software has delivered.

As organizations look to adopt the Zero Trust Model where no actor, system, network, or service operating outside or within the security perimeter is trusted, the need to verify anything and everything attempting to establish access is paramount. The Zero Trust paradigm shift is from an approch centered on securing infrastructure, networks, and data, and verifying once at the perimeter to continual verification of each user, device, application, and transaction. The DataLenz solution plays a role in a holistic Zero Trust deployment approach.

Against this backdrop, CISOs and security teams are on the lookout for solutions that integrate seamlessly with existing tools and process while bringing enhanced contextual data points that not only improve reporting but can be used to prevent threats in near real-time.

We at Futurum Research fully believe that Iconium Software and its DataLenz solution is worth consideration. The software tool focuses on three key areas that would improve the mainframe security posture in any organization. Furthermore, we believe that mainframe security requires the right technology partner who will work with an organization to help continuously improve security in our dynamic world. Iconium Software and their team of experts with decades of mainframe and security experience does just that.

At a time when mainframe security is tantamount to success, finding the right partner and technology solution is table stakes. Iconium Software delivers on all fronts.