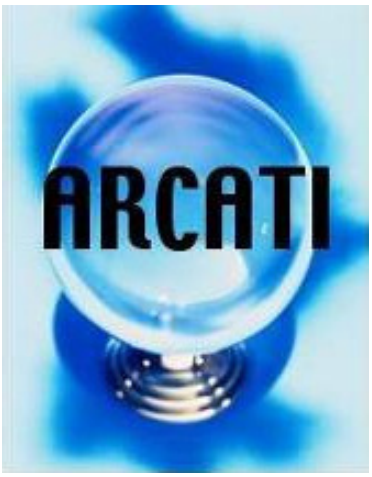
The Arcati Mainframe Yearbook 2019



The independent annual guide for users of IBM mainframe systems

SPONSORED BY:

BROADCOM

ACTION SOFTWARE INTERNATIONAL

ESAI Enterprise Systems Associates, Inc.

bmc

EPV Technologies
IT Cost under Control

DATAKINETICS DATA PERFORMANCE & OPTIMIZATION

TONE SOFTWARE

PUBLISHED BY:

Arcati Limited
19 Ashbourne Way
Thatcham
Berks RG19 3SJ
UK

Phone: +44 (0) 7717 858284
Fax: +44 (0) 1635 881717
Web: http://www.arcati.com/
E-mail: mainframe@arcati.com

iTech-Ed

Contents

SPONSORS

Welcome to the Arcati Mainframe Yearbook 2019

We are very grateful – as always – to all those who have contributed this year by writing articles, taking part in our annual user survey, or updating their company profiles. In particular, I must thank the sponsors and advertisers, without whose support this Yearbook would not be possible.

2018 seems to have continued the trend of 2017, with plenty going on in the mainframe world and mainframe sites willing to, at least, sandbox some more recent trends in mainframe computing, rather than just leaving them on the slides of the latest presentation that they've sat through. It's as if mainframers are getting back their old confidence and wanting to push the envelope of what can be done by their favourite computing platform.

Security is still an important issue, and many companies that got their fingers burned last year with Wannacry and other cyberattacks are well down the road with introducing multifactor authentication for their computers – or is it that the press haven't been told about 2018 attacks? In addition, everyone had to get their heads around GDPR – the EU General Data Protection Regulation that affects anyone who stores information about EU citizens. Customers have to give informed consent for their data to be stored and used, they have the right to access the data, and they have the right to be forgotten. All this comes with hefty fines for companies found to be in breach.

In April IBM announced the IBM z14 Model ZR1 and IBM LinuxONE Rockhopper II. The new systems have a 19-inch industry standard, single-frame design allowing for easy placement into cloud data centres and for private cloud environments. They came with robust security including pervasive encryption, cloud capabilities, and powerful analytics with machine learning. The models are designed to bring industry-leading security for Linux environments with the broad use of IBM Secure Service Container technology. Steps can now be taken to protect data against internal threats at the system level from users with elevated credentials or hackers who obtain a user's credentials, as well as external threats, with no application changes. Applications can be put into a Docker container to be ready for Secure Service Container Deployment, and the application can be managed using Docker and Kubernetes tools. The new design comes with significant increases in capacity, performance, memory, and cache across nearly all aspects of the system in 40 percent less space and is standardized to be deployed in any data centre.

As a quick catch-up, pervasive encryption refers to the ability to encrypt everything everywhere without interfering with the user experience, eg the real-time encryption of all mobile transactions. The Z14 models can "pervasively encrypt data associated with any application, cloud service, or database all the time".

The Arcati Mainframe Yearbook 2019

Publisher: Mark Lillycrop
Editorial Director: Trevor Eddolls
Contributors: Broadcom, Mark Wilson

However, IBM's third quarter figures were disappointing. Its revenue dropped by 2.1 percent to $18.75 billion, below the anticipated $19.1 billion. However, it reported adjusted earnings of $3.42, which was better than estimates of $3.39. Nevertheless, its stock tumbled almost 8.1 percent to $133.43, bringing losses so far this year to 12 percent. Cloud revenue grew by 10 percent in the period to $4.5 billion. The figure had seen 20 percent expansion in the second quarter. IBM's Systems business had $1.7 billion in revenue, up 1 percent, but below the $1.79 billion estimate. Systems had reported robust growth in the first half of the year with strong demand for all three offerings, including IBM Z, Power, and Storage. Although revenue growth slowed down in the third quarter, Z system revenues continued to impress, but software revenues were down. Technology Services and Cloud Platforms, hit $8.3 billion (it was expected to be $8.43) in revenue, which was down 2 percent year on year. The Cognitive Solutions business segment produced $4.1 (it was expected to be $4.3) billion in revenue, down 6 percent. And Global Business Services delivered revenue of $4.1 (expected to be $4.06) billion, up 1 percent.

In 2018 IBM acquired only three companies. Firstly in May it acquired Armanta for its aggregation/ analytics software for financial services firms. In June it was the turn of Oniqua Holdings Pty Ltd for its intelligent maintenance repair and operations (MRO) solutions. And thirdly, it was the much-publicized Red Hat, a provider of open source software and solutions. The deal cost IBM $34 billion and is thought to be the biggest software merger ever. Most people assume that IBM is hoping to leverage Red Hat's experience in the cloud computing market to bolster its own efforts. Or, it could be Red Hat's expertise with OpenShift and Kubernetes, as well as Linux (which makes up about three quarters of its revenue).

And talking of mergers and acquisitions, I guess the biggest surprise in 2018 was Broadcom's acquisition of CA Technologies in July. Broadcom, best known for its chip business, paid $18.9bn. When the deal was announced, Broadcom said the acquisition was part of its strategy to buy "established mission-critical technology businesses". Of course, for years, CA was known for acquiring other companies.

IBM has continued its love of DevOps and is creating major releases of products like CICS and IMS every three months. We're currently at CICS Transaction Server for z/OS V5.5.

As well as pervasive encryption, other words or acronyms people in 2018 were starting to use in connection with mainframes include: DevSecOps, Digital reinvention, Nabla container, Solution Consumption License Charges, z/OSMF, and Zowe.

It's interesting to see what Gartner highlights as the top 10 strategic technology trends for 2019. They are:

- **Autonomous things**, such as robots, drones and autonomous vehicles, use AI to automate functions previously performed by humans.
- **Augmented analytics** focuses on a specific area of augmented intelligence, using machine learning (ML) to transform how analytics content is developed, consumed, and shared.
- **AI-driven development** so that, by 2022, at least 40 percent of new application development projects will have AI co-developers on their team.
- **Digital twins**, ie there will be a digital representation of a real-world entity or system.
- **Empowered edge** means edge computing, which is usually associated with IoT devices, will grow using specialized AI chips and greater processing power.
- **Immersive experience** will extend the way people interact with the digital world. Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) will change the way in which people perceive the digital world.

- **Blockchain**, a type of distributed ledger, promises to reshape industries by enabling trust, providing transparency, and reducing friction across business ecosystems potentially lowering costs, reducing transaction settlement times and improving cash flow.
- **Smart spaces** are a physical or digital environments in which humans and technology-enabled systems interact in increasingly open, connected, coordinated, and intelligent ecosystems.
- **Digital ethics and privacy** is a growing concern for individuals, organizations, and governments. People are increasingly concerned about how their personal information is being used by organizations in both the public and private sector, and the backlash will only increase for organizations that are not proactively addressing these concerns.
- **Quantum computing** (QC) is a type of computing that operates on the quantum state of subatomic particles that represent information as elements denoted as quantum bits (qubits). The parallel execution and exponential scalability of quantum computers means they excel with problems too complex for a traditional approach or where traditional algorithms would take too long to find a solution.

It's interesting to see how many of those will use a mainframe in order to work effectively.

So it looks like the mainframe industry is an exciting place to work. And with that in mind, I can confidently predict that 2019 will be an interesting year, and that the mainframe will continue to offer outstanding performance and reliability, and be at the heart of the world's business-critical applications.

One of the biggest problems facing mainframe sites is their ageing population of experts. Many mainframe geeks, gurus, and mavens are starting to think about their pensions and their retirement. One solution to the problem of an ageing and retiring staff is to automate as much as possible, but that doesn't solve the problem of how to create new applications or update existing applications to work in new ways, such as cloud, mobile working, or incorporating public APIs to create some completely new app. The big question for organizations is how do they ensure that they can digitally transform so that they can still operate successfully in the fast-evolving digital world? The answer is to come up with a way of making everything on Z available to people who are used to working in other ways on other platforms. And that, in a nutshell, is where Zowe comes in.

Zowe is the first Open Source framework for Z. Zowe provides solutions for development and operations teams to securely manage, control, script, and develop on the mainframe like any other cloud platform. These new developers do not need to have previous mainframe experience! By using Zowe, non-mainframer developers can use the open-source industry-standard tools they are already familiar with to access mainframe resources and services.

Zowe has four components. These are: Zowe APIs, Zowe API Mediation Layer, Zowe Web UI, and Zowe Command Line Interface (CLI).

IBM contributed the extensible z/OS framework that provides REST-based services or APIs allowing users to use new technology, tools, languages, and modern workflows with z/OS. It's also contributing z/OS Explorer Core, which gives developers a set of discoverable foundational services or building blocks that can be used across all aspects of Zowe. Rocket Software is providing a Web user interface, and CA Technologies will provide a Command Line Interface.

As an aside, apparently, the name Zowe was used because it sounded exciting and new. Retrofitting it into an acronym, we get Z for IBM Z, O for open source, and WE because it is inclusive of everyone.

I expect that we will hear a lot more about Zowe in the future.

Increasing The Power Of Hybrid IT Through Open Source

Hybrid IT is all about harnessing the power of the digital age to deliver, analyze, adapt and innovate your enterprise's critical functions—regardless of technology or platform. The mainframe is key to your hybrid IT strategy containing a rich repository of data and applications delivered through unmatched scalability and security. Mainframe organizations however, are challenged with making the mainframe more readily consumable across all platforms and by the next-generation workforce—limiting the ability to deliver value to the business.

Overcoming Productivity Challenges on Mainframe

Broadcom is a founding contributor of the Open Mainframe Project's Zowe initiative, unveiled CA Brightside solution and the API Mediation code base open source through Eclipse Public License 2.0, which encourages collaboration and innovation opportunities for the IBM® z/OS® platform. Brightside, designed to make it easy to integrate the mainframe into enterprise DevOps workflows, allows development teams to control, script and build for the mainframe like any other cloud platform, using familiar open source tools, such as Jenkins, Gradle and IntelliJ, thru a command line interface. Releasing the code via public domain enables a broader community to contribute new innovations and improvements, while further strengthening the mainframe platform and ecosystem.

Introducing Zowe

To help businesses meet this challenge, mainframe industry leaders Broadcom, IBM and Rocket Software joined forces to create a new open-source mainframe software framework. In collaboration with the Linux Foundation's Open Mainframe Project, we created Zowe—a modern interface for z/OS that brings open source to the mainframe. Zowe enables application development and operations teams to securely manage, control, script, develop and interact with the mainframe like any other cloud platform. In this way, Zowe is key to building an integrated and agile mainframe.

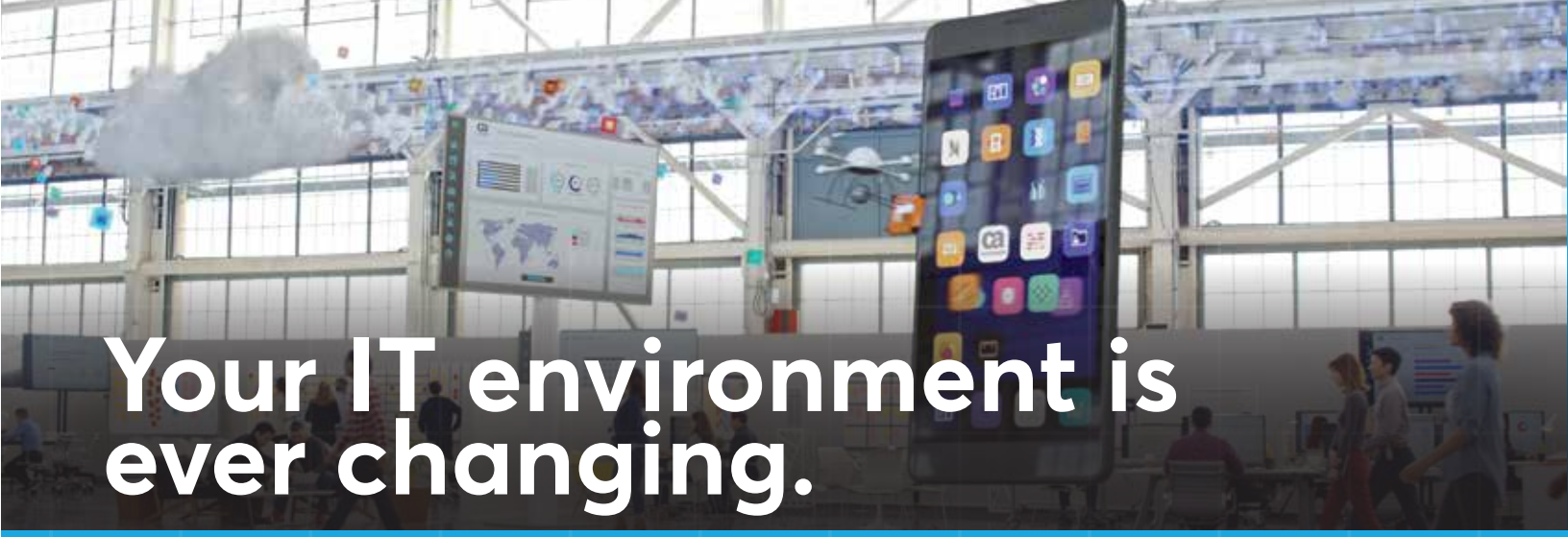
The Case for Open Source

How will Zowe benefit the mainframe platform, ecosystem and our industry?

- **Ensure long-term mainframe innovation**. Participate in the initiative and collaborate with other enterprises in further developing the mainframe and preparing it for the future of business. As an open-source project, you'll leverage the latest innovations from the community to help extend the viability of the platform.
- **Adopt new technologies and capabilities.** Community collaboration around the Zowe framework and standards allows for more integration opportunities and choices with respect to technology—providing the agility you need to effectively respond to market changes using the latest innovations.
- **Address the mainframe skills gap.** Zowe provides simplified and familiar infrastructure services for the mainframe. Programmers can interact with the mainframe using familiar tools and frameworks—increasing productivity and ensuring business continuity.

It's Your Move

As an industry, we encourage all vendors and clients to support the Zowe initiative through community participation. We all know the power and value the mainframe brings to business. The key is tapping into community knowledge and global innovation to drive even greater value. Making that shift towards a more community-driven innovation approach is up to you.



Your IT environment is ever changing.

It's time for the integrated and agile Mainframe

It's where mobile-to-mainframe agility, automation, insights and security come together to help your business compete in the rapidly changing application economy.

It's what you build with end-to-end tools and guidance from Broadcom.

It's how you continuously deliver better apps, faster and at scale—to meet ever-growing consumer demand.

To learn more visit broadcom.com/mainframe

BROADCOM®

Participation in the Zowe community also gives you the opportunity to influence the direction of the entire platform. You can literally shape the future of the mainframe through your inclusion and contribution to the open-source project.

How to Get Started

Zowe is powerful enough to help you support and innovate your business. That much is clear. So, how do you take advantage of Zowe?

Simply go to the site to participate in and contribute to the Zowe developer community. You will join hundreds of developers from enterprises worldwide who are dedicated to opening the mainframe. Take the opportunity to share your ideas, submit fixes and showcase your development skills to further Zowe's goals and modernize the mainframe.

Zowe is a truly powerful, open collaboration initiative helping businesses experience the full benefit of digital transformation through a dynamic hybrid IT architecture inclusive of the mainframe. Engage with Zowe today and increase the power of your business!

Why Broadcom?

Only Broadcom can bring a more simplified user experience that spans the breadth of open DevOps and machine learning-based operational intelligence to make the mainframe an agile, integrated part of an evolving IT architectural landscape.

Broadcom offers customers a leading and differentiated portfolio of best-in-class solutions across a diverse set of technologies that are designed to accelerate modernization and integration initiatives, allowing enterprises to leverage mainframes as strategic enablers of digital transformation. You can get real-world expertise and practical how-to guidance on mainframe, machine learning, DevOps and security by visiting our Mainframe Virtual Summit Series and view all content on-demand.

Broadcom is constantly architecting ways to help you develop, run, and manage mainframe applications—be it in the cloud or on-premise—to provide you with the agility you need to optimize the infrastructure and encourage cross-enterprise collaboration—all of which drive digital transformation and propel your business forward. Learn more. Visit us today: broadcom.com/mainframe.

Broadcom Inc. (NASDAQ: AVGO), a Delaware corporation headquartered in San Jose, CA, is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation.

Don't be confused by the Mainframe cryptocurrency. The Mainframe project came about because the project members thought that today's Web services are built on protocols, services, and other tools that are susceptible to centralized control, surveillance, and manipulation. Their communication network is resistant to censorship, surveillance, and disruption. They incentivize people to use it with their Mainframe cryptocurrency.

Security, skills and the system-of-record: we live in interesting times

Mainframe security (naturally) and planning for the next generation of mainframers provided major themes for the last year, writes Mark Wilson, head of RSM Partners' Technical and Security teams

We all know that saying, "May you live in interesting times". Many people maintain it's actually a curse. Whichever way you look at it, times seldom get more interesting than today. In last year's *Arcati Mainframe Yearbook*, I wrote about how the mainframe was now, properly, mainstream. Its stock was continuing to rise based on its inherent capabilities as "the most future-ready platform in the world ... The mainframe is more in vogue today than has been for more than 20 years, and is becoming even more critical to an organization's business success (and good health). It has become a streamlined super-fast data monster, a transaction eating behemoth, the system-of-record." And so it goes...

Running faster just to keep up

Early in 2018, I was on a working trip to the USA. In the hotel gym one morning, on the running machine, I was musing about how we, and the industry in general, seemed to be running faster just to keep up. In the week or so previously, our office felt more like a travel agency than a mainframe consulting company. The reason being that we were so busy booking travel and accommodation for 12 major security jobs coming up, in locations ranging from New Jersey to North Carolina. Right from the get-go, we were talking to more mainframe customers, visiting more places and working on more projects than ever before. I know, because I checked, looking back at workload in the previous three years when it had seemed we were pretty busy. In 2015, 2016 and 2017 we carried out, on average, 12 mainframe security assessments and pen testing projects globally each year. We had performed 12 such projects in the first three months of 2018 - and that trend continued. My view, as I've said before, is that people had woken up to the reality that the mainframe will be around for another 10, 20 maybe 30 years, and were asking more of it, while at the same time cyber crime was becoming a massive issue and a real threat. So mainframers are thinking, "Hmm, we really need to find out exactly how secure our systems are ..." So, security was a big theme for the year, to which I'll return a little later.

'Mainframers in training'

The last 12 months have also, I think, seen the pace of change speed up in terms of developing the next generation(s) of mainframe professionals. A year ago, I wrote that while we saw this increased recognition and appetite for mainframe systems and services, a potentially massive spanner in the works was the diminishing pool of skills, as expert mainframers retired and organizations so often lacked proper succession plans. But I believe we're making real progress. In the summer, for example, I attended a "University Day" in London organized by the IBM Systems Technical University, for people to meet and network with academics, practitioners and industry professionals from organizations including IBM, Lloyds Banking Group and the University of Wolverhampton. Events like this have an important role to play in "priming the pump" and having a real impact on the future of the industry.

Later, in October, I attended the similarly excellent five-day IBM Systems Technical University in the USA, which included a new "z/OS for Rookies" track for early-career programmers and engineers, along with a "Professional Development and Leadership Training" stream. Alongside formal training and academia, knowledge sharing and mentoring are proving critical. On our part, RSM is continuing to develop the successful Mainframer in Training (MIT) program, which provides three years of hands-on structured training followed by

two years of bespoke specialist training. Crucially, the trainees start doing real-life work on the support desk, shadowing more senior mainframers, after just three months. Later still, at November's GSE UK Conference, this remained a central theme: how to attract and develop the brightest new talent, and in particular the role of women in IT. It was extremely encouraging to see so many students attending GSE, with many organizations interested in the fact that we already work with so many young people, and how many are women. All very encouraging – especially when you consider the major challenge of our age: security.

Is the mainframe the Cinderella of security?

In the last yearbook, I wrote about the coming of Pervasive Encryption; what was then talk and planning has since become action for many organizations. And while a new era of 'Crypto as a Service' hasn't quite emerged yet, security developments have continued. Indeed, ongoing issues around security, vulnerability - and the increasing attractiveness of our lovely mainframes to cyber criminals - go hand-in-hand with the reality that around 80% of the world's system-of-record data resides on mainframe systems, and more commercial transactions are processed on mainframes than on any other platform. They are high-value targets yet their security is so often taken for granted, with an old-fashioned security posture that "everyone had read access to everything". Simply because a mainframe is hidden away deep within a network, behind three firewalls, and at the back of a data center, doesn't mean that it's secure. To the bad actors, the mainframe is "just another server" to be attacked. Bad actors are looking at mainframe technology across the globe, right now, and working hard to identify vulnerabilities to exploit.

I've spent quite a bit of time raising the spectre of mainframe hacking. I had the feeling that, in some quarters, people were uncomfortable discussing the subject. But that won't make the problem go away, and could actually make things worse. The elephant in the room is that it doesn't actually require any specialist mainframe knowledge to breach a mainframe and steal data: it's true. I know the real-life case of a non-mainframe pen tester who exfiltrated all the production DB2 data from a mainframe. Using standard Linux/Unix tools like ssh and grep, plus ODBC and a little ingenuity, somebody with no mainframe experience drained the system of all its sensitive client data. It really is a trivial matter for a competent hacker or penetration tester – which means it should be a very serious matter for all of us, right up to board level.

Raising our game in security

The thing is, mainframe security isn't really a mainframe security issue at all, it is an enterprise security issue. Which means we need to educate C-level executives about the real possibility of a mainframe breach. (And, of course, these enterprise security challenges also tie-in to the skills gap and the need for next-generation mainframe experts). Arguably the greatest threats are insider threats: the bad actors won't be looking to target a system or application, they are more likely to target individuals and steal system logins and credentials. This is why I've been talking recently about "the problem with passwords" and evangelizing how multifactor authentication (MFA) can help counter the security threat. If organizations are still authenticating users via passwords alone, a move to MFA is long overdue.

The mainframe often has the weakest password policies and algorithms in an entire enterprise. Are we making it difficult enough for potential hackers to get in? In effect, passwords represent a single point-of-failure. With mainframes, the maximum password length is eight characters. Up to 100-character passphrases are available but few sites use them. While there have been efforts to tighten up password security, the problem is, if passwords then are too complex and tricky to remember, it drives behaviors in user communities where, say, passwords are 'stored' on sticky notes and written to text files, or even on whiteboards. Some people use password vaults

but not everyone. Passwords, in general, are easily shared, easily stolen, and easily guessed. One of the biggest threats is password reuse; combine this with other problems described here and you end up with some convenient attack points. At the same time, multiple risks are associated with any breach, no matter how it's perpetrated: for example, fines imposed by regulatory bodies relating to GDPR or PCI. If there is a data breach, the organization will also likely face compensation payments and the costs for identity theft insurance for all affected users for 12-24 months in addition to the media coverage and reputational damage. Other impacts may be even more damaging: from a denial of service attack that disables all mainframe systems, to a Ransomware attack where all data is encrypted and a ransom demanded.

However, while a mainframe may not be secure right now, the mainframe is the most securable commercial computing platform available, and all the tools you might need are out there. These can include: security products such as RACF, ACF2 or Top Secret; network segmentation; privileged user management e.g. RSM Partners Breakglass; Real-time Threat Detection; MFA; removing application passwords and using encrypted Passtickets; Client/Server certificates; and incident response. Deploying them should also be part of a planned sequence of actions. First: understand your security posture, carry out a Security Assessment, conduct Pen Testing and remediate issues. Second: implement Role Based Access Control, working to a least privilege model, also implement Real Time Alerts and a 'break glass' solution to manage privileged users and their access. Third: deploy MFA. The fourth but vital step in this initial rollout is to educate all users on the measures now in place and the actions and behaviors expected, bringing home the fact that security is the responsibility of everyone.

Given that some 81% of breaches can be attributed to credential reuse, MFA can be a powerful weapon in your identity and access management armory, creating a high degree of friction for bad actors while presenting minimal delays and disruption to legitimate users. Indeed, investing in MFA can be an extremely smart decision, as mainframes become more open and connected to the wider world, as regulations like GDPR demand stricter compliance (and include bigger fines) for data protection, and with PCI DSS actually requiring MFA to be implemented. MFA works by inspecting multiple identifying elements associated with a particular user account, raising the authentication assurance level that a system requires from a specific user. Various products are available. For example, IBM Multi-Factor Authentication for z/OS is integrated with RACF; RACF has an MFA API set available for other vendors to use. Other options include OTP (one-time password) generators to create a password only valid for a short time, maybe 60 seconds.

In fact, true MFA for the mainframe only arrived with IBM Multi-Factor Authentication for z/OS in late 2017, expanding the options available

to deliver that all-important "layered defense". This integrated approach, designed to support various token types, requires that selected Z users authenticate using multiple factors: something they know - password or security question; something they have - ID badge or cryptographic token device; and something they are - a fingerprint or other biometric. In my view, the best way to unlock the benefits of MFA while also delivering a great user experience is to also use a Session Manager (we use Tubes for z/OS from Macro 4). Indeed, the secure mainframe is best achieved in general by using a range of best-of-breed technologies, expertise and professional services. And if **we** don't make the case for securing the mainframe, and then actually do it, who will?
www.rsmpartners.com

About the author

An award winning global thought leader in mainframe technology and security, Mark Wilson heads RSM Partners' Technical and Security teams. Drawing on more than 30 years' experience in mainframe systems in diverse sectors and environments, in both hands-on technical and strategic roles, his insight and solutions-driven approach mean he is highly valued by RSM Partners clients, IBM and third-party technology partners, and is much in demand as a speaker on the international circuit. Mark is Chair of the Guide Share Europe Large Systems Working Group and Technical Co-Coordinator of the GSE Enterprise Security working group.

Blockchain and mainframes

Blockchain can be thought of as the antithesis of centralized computing. In fact, it uses encrypted ledgers that are distributed across multiple computers in a network. It's a way of recording data using an encrypted ledger of verified events, which is distributed across lots of computers in a network. So, once a transaction is proven to have taken place, it's forged into a block of data that can't be changed. These blocks are then bound together into chains (hence the name blockchain) of events that prove a given sequence of events took place in a particular order at specified times.

It's not just financial information that can make use of blockchains, blockchains can be used simply to record events, for medical records, and other records management activities, identity management, transaction processing, and proving data provenance. And that means it can be used for anything where you want to keep the data completely secure from any kind of alteration. All that can happen is additional blocks can be added to the chain.

The IBM site at https://www.ibm.com/it-infrastructure/z/capabilities/blockchain-transactions talks about blockchain transactions on Z. It says: "Run your distributed ledgers on a server platform tightly integrated to your secure transactional data and applications". It also goes on to say: "Having your blockchain in a mainframe can greatly accelerate interactions with existing business data in CICS, IMS, TPF, Db2, and VSAM databases. With the capability to support 8000 virtual machines with up to 32TB of memory and 170 dedicated processor cores, Z can run the toughest workloads – quickly and securely."