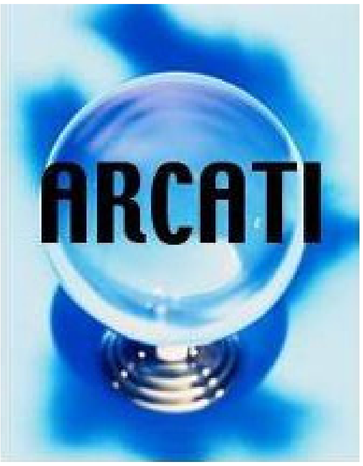
The Arcati Mainframe Yearbook 2023



The independent annual guide for users of IBM mainframe systems

SPONSORED BY:

BROADCOM
Mainframe Software

ACTION SOFTWARE INTERNATIONAL

ASPG
ADVANCED SOFTWARE PRODUCTS GROUP, INC.

VERTALI

Baer Consulting
INCORPORATED

DATAKINETICS
DATA PERFORMANCE & OPTIMIZATION

KRI SECURITY

ESAi
Enterprise Systems Associates, Inc.

PLANET MAINFRAME

Information Technology Company

PUBLISHED BY:

iTech-Ed Limited
iTech-Ed House
16 Brinkworth Close
Chippenham
Wilts SN14 0TL
UK

Phone: +44 (0) 1249 443256
Web: https://itech-ed.com/
Email: arcati@itech-ed.com

iTech-Ed

Contents

SPONSORS

Action Software	36
Advanced Software Products Group Inc (ASPG)	38
Baer Consulting	41, 42
Broadcom Mainframe Software Division	10, 46
DataKinetics	32, 53
Enterprise Systems Associates, Inc (ESAi)	57, 58
Information Technology Company	68, 69
Key Resources Inc	74, 75
Planet Mainframe	13, 89, 90
Vertali	6, 108

Welcome to the Arcati Mainframe Yearbook 2023

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.

2022 was the year when people made the decision whether they wanted to go back to working in an office environment, or whether they preferred to work from home. If your house was big enough to accommodate perhaps two adults working almost fulltime from home, then it was an easy choice. No need to drive through traffic and battle over parking spaces, you could get up, and be going through your emails thirty minutes later. On the other hand, where people didn't really have room to work, or had young children noisily playing around the house, working from home was less ideal. Plus, it's easier to get stuff done when all you have to do is walk over to someone else's desk and ask them. At some organizations, management feared that they would lose control of employees that they couldn't see all day. Other companies trusted their staff to complete tasks at times that suited them. It was just important to get the job done to a suitable high standard. There was also talk of the Great Resignation as many people decided either that the company they were with wasn't right for them, or that still going to work wasn't right for them.

Looking at the word of the year can often help sum up a year. Collins Dictionary's word of the year was 'Permacrisis', which, they said, described the feeling of living through a period of war, inflation, and political instability. Taking a more jovial view, the Cambridge Dictionary's word of the year was 'homer', caused by Wordle players looking up five-letter words, especially those that non-American players were less familiar with.

In the first quarter of the year, IBM announced IBM Wazi as a Service (Wazi aaS), which makes z/OS capabilities available to IBM Cloud. This, they said, reduced the time it takes to access z/OS development and test environments from days to minutes – around six minutes. They also said that IBM Cloud for z/OS development is 15 times faster than using an *x*86 environment. In effect, IBM is offering virtual machines that people can use as mainframe test and development environments with the intention of creating cloud-based virtual production environments. Users get on-demand access to z/OS and can develop and test applications that they are working on.

In April, IBM unveiled its much-trailed new mainframe, the z16, its next-generation system with an integrated on-chip AI accelerator, which delivers latency-optimized inferencing. The accelerator is designed to enable clients to analyse real-time transactions, at scale. So, it is ideal for mission-critical workloads such as credit

The Arcati Mainframe Yearbook 2023

Publisher: Trevor Eddolls
Editorial Director: Trevor Eddolls
Contributors: Broadcom Mainframe Software Division, Vertali

card, healthcare, and financial transactions. The z16 is also specifically designed to help protect against near-future threats that might be used to crack today's encryption technologies. The z16, with its pre-announced 7nm Telum processor provides the much needed on-chip AI inferencing, and the rest of the mainframe (like earlier models) provides highly secured and reliable high-volume transaction processing. Banks are now able to analyse for fraud during transactions on a massive scale. IBM asserts that the z16 can process 300 billion inference requests per day with just one millisecond of latency. Users of the z16 will be able to reduce the time and energy required to handle fraudulent transactions on their credit card. For both merchants and card issuers, this could mean a reduction in revenue loss because consumers could avoid the frustration associated with false declines where they might turn to other cards for future transactions.

The IBM z16 is underpinned by lattice-based cryptography, an approach for constructing security primitives that helps protect data and systems against current and future threats. With IBM z16 quantum-safe cryptography, businesses can future-ready their applications and data today. With secure boot (meaning that bad actors cannot inject malware into the boot process to take over the system during start-up), IBM z16 clients can strengthen their cyber resiliency posture and retain control of their system. The secure boot and quantum-safe cryptography (mentioned above) can help clients address future quantum-computing-related threats including harvest now, decrypt later attacks, which can lead to extortion, loss of intellectual property, and disclosure of other sensitive data.

There's been a nagging worry about quantum computing for a little while now. Quantum computing is fast – a whole quantum leap faster than today's technology. Rather than using 0s and 1s, quantum computers work at the quantum level (hence their name!), ie at the atomic or subatomic level, and information can be encoded in more than one place. And that's what makes them so fast. The worry is that large organizations and nation states will use the speed of a quantum computer to break the algorithms used to encode data and then be able to access the previously-encoded information. The z16 supports the Crypto Express8S adapter, which is designed to deliver quantum-safe APIs, letting enterprises start developing quantum-safe cryptography along with classical cryptography and to modernize existing applications and build new applications. In September, IBM added the four National Institute of Standards and Technology (NIST) algorithms that were chosen in August to create a post-quantum cryptography (PQC) standard built on encryption algorithms that can protect against future quantum processor-based attacks. The NIST algorithms are designed for two of the main tasks for which public-key cryptography is typically used: public key encapsulation, which is used for public-key encryption and key establishment; and digital signatures, which are used for identity authentication and non-repudiation. The algorithms used are: CRYSTALS-Kyber for the key encapsulation mechanism (KEM) for public-key encryption and key-establishment; CRYSTALS-Dilithium, which is the primary algorithm in the signature category; FALCON; and SPHINCS+. CRYSTALS-Kyber and CRYSTALS-Dilithium form the basis of its key encapsulation and digital signature capabilities.

Security is an on-going issue for every IT platform. IBM's Cost of a Data Breach Report 2022 found that the current average cost of a data breach is $4.35 million. The average time to identify and contain a data breach is 277 days – 207 days to identify the breach and 70 days to contain the breach. In term of ransomware: for organizations that didn't pay the ransom the average cost of the breach was US$5.12 million; and for organizations that did pay the ransom, the cost of the breach was US$4.49 million plus the cost of the ransom. The biggest problems were phishing attacks, stolen credentials, cloud misconfiguration, and compromised business partners. And those are people problems not software or hardware. And that doesn't include problems associated with disgruntled staff or ex-staff.

IBM Security X-Force, IBM's in-house team of cybersecurity experts and remediators, report found that manufacturing outpaced finance and insurance in the number of cyberattacks levied against these industries, extending global supply chain woes. The report said that manufacturers have a low tolerance for downtime, and ransomware actors are capitalizing on operational stressors exacerbated by the pandemic. About 1 in 4 attacks on this sector were from ransomware. In terms of statistics, 47% of attacks were vulnerability exploitation, 40% phishing, 7% removable media, and brute force and stolen credentials were both at 3%. The report goes on to suggest that as defences grow stronger, malware gets more innovative. Attackers are increasingly using cloud-based messaging and storage services to blend into legitimate traffic. And some groups are experimenting with new techniques in encryption and code obfuscation to go unnoticed.

In a relatively quiet year, IBM has acquired Neudesic, a cloud services consultancy specializing primarily in the Microsoft Azure platform. It also acquired Databand, a provider of data observability software, and Dialexa, which offers digital product engineering services.

When it comes to looking forward to 2023, it's always interesting to see what Gartner's Top Strategic Technology Trends for the year are. This time they include:

1 Digital Immune System – "By 2025, organizations that invest in building digital immunity will increase customer satisfaction by decreasing downtime by 80%".

2 Applied Observability – "By 2026, 70% of organizations that successfully applied observability will achieve shorter latency for decision making, enabling competitive advantage for target business or IT processes".

3 AI Trust, Risk and Security Management (AI TRiSM) – "By 2026, organizations that operationalize AI transparency, trust, and security will see their AI models achieve a 50% result improvement in terms of adoption, business goals, and user acceptance".

4 Industry Cloud Platforms – "By 2027, more than 50% of enterprises will use industry cloud platforms to accelerate their business initiatives".

5 Platform Engineering – "By 2026, 80% of software engineering organizations will establish platform teams as internal providers of reusable services, components, and tools for application delivery".

6 Wireless-Value Realization – "By 2025, 50% of enterprise wireless endpoints will use networking services that deliver additional capabilities beyond communication, up from less than 15%".

7 Superapps – "By 2027, more than 50% of the global population will be daily active users of multiple superapps. A superapp is an app that provides end users (eg customers, partners, or employees) with a set of core features, along with access to independently created miniapps."

8 Adaptive AI – "By 2026, enterprises that have adopted AI engineering practices to build and manage adaptive AI systems will outperform their peers in the operationalizing AI models by at least 25%".

9 Metaverse – "By 2027, over 40% of large organizations worldwide will be using a combination of Web3, spatial computing, and digital twins in metaverse-based projects aimed at increasing revenue. Metaverse is a combinatorial innovation made up of multiple technology themes and trends."

10 Sustainable Technology – "By 2025, 50% of CIOs will have performance metrics tied to the sustainability of the IT organization. Sustainable technology is a framework of solutions that increases the energy and material efficiency of IT services; enables enterprise sustainability through technologies like traceability, analytics, renewable energy and others; and helps customers become more sustainable through apps, software, marketplaces, and more.

So, it looks like the mainframe industry is an exciting place to work. And, I can confidently predict that 2023 will be an interesting year, and that the mainframe will continue to offer outstanding security, performance, and reliability, and be at the heart of the world's business-critical applications.

.

The NeverEnding Story: Optimizing and Securing the Modern Mainframe

The task list for mainframers is never ending, whether that means prioritizing cyber resilience, implementing data loss prevention, or optimizing project work and BAU activity. There's clearly a continuing demand for specialist skills and expertise.

2022 began with pandemic restrictions still in place and ended with a controversial World Cup. War came to Eastern Europe, precipitating an energy crisis. The UK had three different Prime Ministers in 50 days. A global recession may be imminent. And the mainframe has continued to do what it does: a strategic platform for the ages, the single answer to multiple questions, as relevant in the digital world as the analogue. Mainframes have traditionally accounted for up to two-thirds of the world's IT production workloads but well below 10% of IT spend. However, the mainframe is being modernized, upgraded, optimized and outsourced. And people want help to do that.

We launched Vertali in 2022 as a consulting and services business to help mainframe organizations to navigate change, mitigate risks, and achieve their technology, business and security objectives. There's clearly an appetite within organizations to achieve more, faster. Given our pedigree in IBM Z skills and resources, we saw a gap that our consultants could fill.

Talking to clients and partners has raised a myriad of issues: the continuing changes required by digital transformation, the role of the modern mainframe, and of course cyber security. Let's take a quick look at two topics we're asked about regularly. The first is reasonably specific: Data Loss Prevention (DLP). The second is wider ranging: how to build cyber resilience for mainframe infrastructure, data and processes.

Data Loss Prevention (DLP)

Mainframe data loss is fundamentally a business problem. Prevention is better than cure, which means focusing on the risk of exfiltration. DLP, or data leakage mitigation, is about detecting, identifying and preventing potentially damaging data breaches, data exfiltration, and the unwanted destruction of sensitive data. Effective DLP means securing and protecting your data, complying with the necessary legislation and regulatory requirements. Gartner estimated that by 2021, 90% of organizations would have implemented at least one form of integrated DLP. But analysts also say the market has reached maturity, with competitive solutions difficult to distinguish from each other, with innovation in functionality stalling.

We should be doing everything in our power to prevent the unauthorized and illicit removal and transfer of data outside organizational boundaries, so avoiding the customer, financial and reputational damage that can result. Data loss may come through a ransomware attack or data exfiltration via malware, and can be the result of outside attacks or insider threats. There are many ways to get data off a mainframe: FTP, SMTP, NJE (Network Job Entry), IND$FILE for mainframe to PC file transfers, commercial products like XCOM and Connect Direct, and what about HTTP and HTTPS in a connected world? And who believes READ access to data is a good idea, as a rule? If I can READ something then I can copy it.

We need to reframe DLP as a strategy, a journey, rather than a product-led approach. We should not look to DLP as a magic bullet to protect sensitive information. It requires a more informed approach. This often starts with a pen test or security assessment. And a DLP strategy has to extend in different ways across different domains: network, cloud, endpoints, and storage, ideally as part of a managed approach to security (and cyber resilience – see below). It means properly understanding our networks, and who or what is connecting to our mainframes, monitoring network activity in real-time. We can make much better use of tools already out there, using solutions that feed into a comprehensive DLP strategy.

You can start by asking a few searching questions:

- What do we define as sensitive information? (The types of data classified as sensitive need to be revisited frequently.)
- How do we currently track (and understand) data access, movement, and usage?
- In what ways do we restrict access to our data?

We also need to be able to automatically detect and respond to threats: connecting the mainframe to an Extended Detection and Response (XDR) approach. It's a very good idea to integrate the mainframe with third-party solutions such as tools for IP Filtering, Intrusion Detection Services, z/OS Encrypted Connection Monitoring (zERT), and Network Management APIs (NMIs) in IBM z/OS Communications Server.

Why risk being caught out? Vulnerabilities almost certainly exist, and you may be at risk of data loss. It could only be a matter of time before a bad actor gets in. Of course, there's much more you can do…

Cyber Resilience: anticipate, recover, adapt

It's been said that resilience ultimately comes from recovery. We live in a complex, ever- evolving world in which the very best cyber defense is not a guarantee against a successful attack.

Cyber resilience is about adapting fast and recovering fast as you respond to a disruptive event. Business continuity today is impossible without a strong cyber resilience plan. It's part-and-parcel of continuously protecting the business and maintaining a hardened security stance. How can you ensure this resilience, securing mainframe systems and data from attack and other threats and, crucially, resume operations quickly and effectively if a successful attack breaches your defenses?

The US National Institute of Standards and Technology (NIST) defines cyber resilience as "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Noting that cyber resilience extends beyond deliberate attack, IBM describes says it "brings business continuity, information systems security and organizational resilience together… the ability to continue delivering intended outcomes despite experiencing challenging cyber events, such as cyberattacks, natural disasters or economic slumps."

The European Union is also proposing an EU Cyber Resilience Act (CRA), "the first horizontal regulation to introduce security requirements for connected devices and related services… Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion [in] 2021."

We are indeed seeing increasing demand from mainframe organizations who want to prepare, protect, detect, respond and recover from cyber threats, internal and external, intended or accidental. We recommend a two-pronged approach: developing a tailored Cyber Resilience Strategy then building, executing and regularly updating a robust Cyber Resilience Plan based on that strategy.

From cyber resilience strategy to practical plan

A viable Cyber Resilience Strategy depends on the smooth collaboration of several preventative, detective, and responsive approaches, understanding the interrelationships between these elements and how each one complements the functions of the others. Creating your tailored strategy will therefore draw on existing operational disciplines such as Business Continuity (BC), Disaster Recovery (DR), Incident Response (IR), and Cybersecurity Planning. These elements already exist in most organizations but are siloed. We need to bring them together.

Your strategy defines how and what you will develop, and the priorities of your Cyber Resilience Plan. Developing plans, which are clearly documented, updated and regularly tested, is achieved through a balanced program of activities. These include cybersecurity planning, business continuity and disaster recovery (BCDR) plans, incident response plans, periodic Business Impact Analysis (BIA) and Risk Analysis, regular testing, and stakeholder engagement. An important part of the process is educating and updating the senior leadership team on the threat landscape, based on the assumption that a breach will take place. We need to explain the risks and impacts of not having a strong strategy and plan, quantifying benefits wherever possible in monetary terms. Cyber resilience can help to significantly reduce financial loss and reputational damage.

You can also explore and deploy tools to support cyber resilience that work for you. These might include IBM z Cyber Vault ("reduce time to recovery from days to minutes"), Dell's Data Protector for z Systems (zDP) which has been described as a "mainframe data recovery game changer", as well as tools from Maintegrity, Action Software, New Era, Vanguard, BMC, and others.

When it comes to effective cyber resilience, a flexible approach is required, one that may include: identifying and documenting the most critical elements to your business; input from diverse stakeholders; performing a risk analysis and risk rating of systems, applications and data (pen tests and security assessments may be part of this); ensuring your strategy and plan align with wider cyber related requirements e.g. GDPR, NIS Directive; and documenting, testing, refining and updating – and continuing to do so.

What's next on your task list?

When it comes to cyber security and optimizing mainframe operations in general, simply because the task is like painting the Forth Bridge – said to be never ending – doesn't mean we shouldn't be constantly scrubbing away the old, reinforcing and repairing, and providing new layers of protection. With the continuing role of the mainframe, at the heart of so many organizations and activities, these aren't really technical issues or security problems anymore: they are business issues that go to the heart of successful operations, great customer service, and commercial resilience. ■

A global thought leader and international speaker in mainframe security and technology, and passionate advocate of all things Z, Mark Wilson is Vertali's Technical Director. He has more than 40 years' experience across numerous industries and diverse mainframe environments. Mark is also Region Manager for Guide Share Europe (GSE) UK. For more information email: info@vertali.com

Mainframe automation with Ansible

The basic concepts behind Ansible involve a control node or the machine from which you run the Ansible code, which could be a laptop, shared desktop, or server. This can then control databases, the back end, and the front end, using Python modules over a secure connection. There's no need to install Ansible on the target nodes.

The Ansible inventory identifies the nodes that are managed and categorizes them into different groups. Both nodes and groups can be assigned variables for use later during automation. The inventory can be static (using files) or can be provided dynamically.

The Ansible for IBM Z collection contains a powerful set of playbooks and modules that allow users to automate common z/OS tasks. There are also dedicated collections and samples for different IBM products such as IMS and CICS. These are available on Ansible Galaxy. The collections cover basic z/OS tasks and those needed for Db2, CICS and IMS.

Mainframe sites use Ansible to build and provision middleware, roll out fix packs to thousands of servers and for self-service provisioning of portals. Ansible can be used to configure middleware, networks and security.

Bigger Together: How to Maximize Mainframe's Value

Greg Lotko, SVP and General Manager, Mainframe Software Division, Broadcom Inc

The further we evolve as a digital society, the more proof we see of a basic truth: Mainframe systems play a central role in many of the most fundamental aspects of our lives and work. The platform underpins today's society.

The Mainframe is a modern marvel with state-of-the-art hardware and software that drive successful businesses on a global scale. Enterprises trust it and consumers transact on it every day with complete confidence. It's a true workhorse, found in nearly every industry—and for good reason. It has unmatched capability and value.

Beyond the Mainframe's impressive technological credentials, it's really the people—the community of developers, engineers, data scientists, and system programmers—who leverage it to power progress. Working together, the community's expertise, dedication, passion, and ingenuity are what bring this technology to life for businesses around the world.

A Business-Forward Mindset

Competitive forces are fiercer than ever. The ability to achieve and maintain leadership requires continuous transformation. Transformation of business models, processes, and services—and of the right technology stack to support it all. You'd better be transforming because you can bet everyone around you is. It's more than a choice. It's a necessity. And it's how you move forward. You have to be anticipating the future and thinking about what's next. That awareness is crucial.

The implications of transformation are different for every organization. This doesn't mean throwing away the technology investments you've made, but rather improving and building on them. Sometimes the key to moving forward is with new technologies. Sometimes it's with a tried-and-true platform. Most often the right answer is a combination of both.

Opening the Mainframe to Growing Possibilities

As we surge toward the future, the need for increasing scale and speed will continue to drive change across all industries. Look at the finance, travel, and retail industries as examples. Customers demand faster, more connected experiences. The Mainframe is an essential part of that customer experience. Consider the Mainframe's role in processing nearly 90% of all credit card transactions, not to mention doing much of the heavy lifting for airline reservations, banking, healthcare and supply chain systems.

As Mainframe expands its integration with Hybrid Cloud, the value of the platform expands as well. An open and connected Mainframe allows developers and IT of all generations to use common tools and strategies that allow visionary work in fields ranging from AI and machine learning to cyberthreat defense, data management, and much more. All while leveraging Mainframe's inherent strengths.

It's the People that Make It Possible

When most people think of the Mainframe, they concentrate on what's inside. But, the inherent strengths of the Mainframe include way more than the technology.

Yes, the Mainframe delivers unparalleled performance, scalability, efficiency, security, and reliability. More importantly, it's the people—those who develop the hardware, write the code for middleware, and develop the applications—who fuel business value.

This community brings forth their know-how, experience, and commitment to continuously strengthen and evolve the IT backbone of our society. And these same people are sharing their knowledge, passing it forward to train the next generation of talent for tomorrow. These are Mainframers.

Being a Mainframer is more than working with the platform. It's knowing that the platform is bigger on the outside. That it's the hardware, software, and even more so the people—together—working to drive greater business value and meaningful impact on the world around us.

We're Bigger Together

Our full potential is realized when we work together towards a common business goal. It's being able to link the known with the new, so that we can build upon today's IT investments to create even greater value tomorrow. It's this kind of bigger, collaborative thinking that empowers businesses into the future.

Let's go BIGGER!

Mainframes, Git, and application development

Git can be used to develop new applications. Visual Studio Code (VS Code) is a popular application development environment. Programmers working collaboratively on source code use Git, and every Git-managed directory is a full-functioning repository (often called a repo). A repository contains all the files needed to compile and link an application. For mainframe applications, this could include source programs, copybooks, JCL or Rexx execs. It also usually includes a README file containing project instructions, documentation and any other useful information.

All Git instances or clones are equal. Developers use *pull* operations to integrate code from another developer into their repository and working directory. A *push* operation sends their code to a remote repository. Developers can also branch, switch branches, stash work, and perform other operations.

VS Code is probably the most popular editor these days, and it has built-in Git capabilities. Broadcom's free Code4z extension pack makes VS Code and similar tools usable by mainframe developers,

Git can be installed on a mainframe. IBM recommends Rocket Software's port of the Git client, which is usually installed in z/OS USS. It includes code page translation, which means that mainframe source code (in EBCDIC) can be stored and retrieved from Git (in ASCII). This allows developers to work on repositories stored on mainframes while working on a laptop. The .gitattributes file tells Git which files should be translated from ASCII to EBCDIC when working on z/OS.

Z
IBM
Big Iron Thrives
Contribute to its growth today!
PLANET MAINFRAME
Join the conversation at
planetmainframe.com/arcati