Mainframe Security in 2025:
Countering New Threats, Using AI, and Getting the Basics Right

Introduction

As we moved into 2025, two trends were front of mind for many of our clients: their continued efforts to achieve a Zero Trust security stance in the face of an evolving threat landscape, and the unstoppable rise of artificial intelligence – countering the risks of AI while seizing the opportunities it presents.

Both trends are linked to the fact that, for many organizations, the mainframe has been seriously overlooked in the past as a cybersecurity risk. And yet vulnerabilities clearly exist, from flaws in code and configuration that can be exploited by criminals, through supply chain and vendor product risks that expose the organization, to insider threats. In short, the threat is real, and growing. IBM's Cost of a Data Breach Report 2024 found that the global average cost of a data breach in 2024 was USD 4.88 million, a ten percent increase on the previous year, and the highest total ever.

Slaying the cyber beast

The cyber threat landscape is continuing to evolve, powered by creative criminals, new tech, and a connected world. It might be likened to the mythical Greek monster, the Hydra: cut off one head and two more cyber threats spring up in its place, presenting new and more complex challenges. At the same time, the mainframe is now mainstream, as much a part of enterprise IT as anything else. And the platform is, of course, hackable. Vertali's mainframe security team has done so many times, as part of formal security assessments and penetration testing, all be it in a safe and secure manner. But once a bad actor gains access, the resulting damage can be catastrophic. Creating backdoors means attacks can escalate even after the initial threat is eliminated.

AI and quantum computing - the latter for complex concurrent computations and so cracking digital encryption faster - add to today's threat complexity, bringing the potential to assist security professionals as well as new opportunities for hackers. Recent technologies bring new back doors and vulnerabilities; today's mobile apps can significantly compromise cybersecurity, with smartphones a target for malware, and therefore another potential route into the mainframe (alongside, in a connected IoT world, things like fridges and exercise bikes, which have even less in the way of security controls). Increasingly, mobile platforms are used to access and process sensitive data: personal and corporate email, messaging services, corporate and financial data, and more.

This all requires robust policies, governance and technology-driven oversight, for both bring-your-own devices and corporate-provided tech: clear policies plus proven mitigating technologies to protect against breaches and data loss, and including logging and monitoring of all devices. And this is just one tiny piece of a hugely complicated jigsaw.

The double-edged sword of AI

It's everywhere and it's growing, across all areas of business and increasingly the public sector. In January 2025, for example, the UK government launched the AI Opportunities Action Plan to improve efficiency and have an impact on areas ranging from healthcare and education to improving roads and supporting small businesses.

Generative AI brings new risks and challenges as well as opportunities. In our world, on the plus side, we're already seeing rapid developments in areas such as Enhanced Threat Detection and Prevention, Automated Security Responses, Enhanced Encryption and Data Privacy, and Vulnerability Management.

On the debit side, AI is already used by criminals to identify vulnerabilities, develop more sophisticated phishing attacks, and automate the exploitation of security flaws. Mainframe security strategies have to evolve fast to counter these threats, but integrating AI technologies and tools into mainframe environments can be a complex ask, and can require significant investment in time, people and resources. We must also be wary that over-reliance on AI and automation does not lead to complacency, with human oversight overlooked.

So, what can we expect from AI?

In enhanced threat detection and prevention, we can look to AI-powered security analytics: analyzing vast amounts of data, identifying patterns, and detecting anomalies that may show a security breach. That can lead to more proactive and adaptive security measures, Generative AI can also automate intelligent security incident responses, and reduce the time lag between detection and targeted action - isolating affected systems and automatically applying patches and updates. AI can be used to dynamically adjust access controls based on real-time assessments of user risk, ensuring only authorized and verified users can access critical mainframe resources. In vulnerability management and predictive maintenance, generative AI can be used to analyze system behaviors, code and configurations to anticipate and predict vulnerabilities before they can be exploited. And so on.

The changing nature of AI-driven security

As AI becomes more commonplace in mainframe security and operations, we will need to ensure that our usage complies with the necessary regulatory standards and requirements. We will have to ensure transparency and auditability for security-related actions taken with AI involvement. And in terms of the new skills needed, we will see a rising demand for professionals with expertise in both mainframe environments and AI, and ideally security. Continuous training and ongoing professional development will be crucial for our security teams to keep up with, and benefit from, evolving AI technologies and approaches.

Remember the basics: mainframe security 101

In this short paper, we've taken a look at the threat landscape, and at the risks and opportunities presented by AI. It's worth adding this third element to any discussion of strategy. With continuous innovation and new functionality, such as AI and extending to developments such as Pervasive Encryption (PE), multi-factor authentication (MFA) and file integrity monitoring (FIM), it's important that we don't forget the basics, and suffer from what a colleague calls "shiny object syndrome". Buildings are only as strong as the foundations they are built upon, and it's the same in mainframe security. We need be on top of the detail and have those basics in place if we're going to achieve a true Zero Trust stance. We have a blog on this topic, but I can summarize the main points here.

Authentication - logging on or connecting to the mainframe. Accountability can only be assured if you can be sure that whoever or whatever is accessing your system is who or what they say they are. Are your password rules strong enough? How often do you require a password to be changed. Have you implemented the RACF encryption algorithm KDFAES? If you use MFA, how is it used?

Access management - the insider threat allied with phishing and ransomware pose a serious risk; no amount of encryption will prevent someone with valid access to your data from editing, copying, or selling it to the highest bidder. They may even re-encrypt it using their own key. Issues to consider in access management include:

- **Data ownership** – do you know who owns what data on your system?
- **Role-based access control** – role-based security to restrict access to authorized users, implementing mandatory or discretionary access control, is important.
- **Approval process** – all requests should be subject to some level of approval before being actioned, with different levels of access, or access to sensitive functions/data, requiring different approvals.
- **Automated systems** - can complicate issues, requiring other factors to be considered, including issues around Privileged Access, and the principle of Least Privilege.
- **JML** – redundant accounts and access can provide a way to bypass security controls. Rigorous JML processes should reduce the risk, provided they are followed.
- **Recertification** – with high numbers of users and profiles, recertification of mainframe access can be tricky and time consuming. But this is a key control that safeguards your data.
- **Privileged access and accounts** – issues to consider include the number of accounts with privileged access, is this access recertified regularly, are privileged accounts behind a break-glass process, and is the usage of such accounts logged, monitored and alerted on?

Encryption: regulations, standards and best practice increasingly require the use of encryption. Risks that still need to be addressed include key management (where and how are keys generated? How are keys distributed? How often are keys changed/rotated? Are keys backed up?) and ICSF and cryptographic services (are the key datasets protected correctly? Are the datasets backed up and ae the backups protected? Is key usage audited? Who has access to the ICSF Panels?)

Dealing with complexity and ensuring observability

From conversations internally and with clients, we are seeing increasing awareness and interest around complexity and observability. These will continue to come to the fore, and of course are closely linked to wider issues around cyber security, how AI can be used, and why getting the basics right is so important.

So many mainframe deployments now sit at the centre of a highly complex web of applications and services. As we've seen, especially during and since the pandemic, the modern mainframe is now a hub for digital transformation. To help deal with this complexity, we will continue to see AIOps tools and approaches that combine AI and automation to streamline and optimize systems management and operations. Observability is critical, of applications and systems, and today that means extending our horizons further, across different software and servers, for multi-cloud, on-premises mainframe, and hybrid environments. Having that 360° view is more important than ever. Security matters feed into and out of all that, and AI has the potential to be a golden thread running throughout. Let's see what's changed, and what's new, when we gather our thoughts in 12 months and look ahead to 2026.

Leanne Wilson
Senior Technical Delivery Manager / Senior Security Consultant
Vertali Ltd.

With more than 13 years' experience in mainframes, systems engineering and cybersecurity, Leanne Wilson leads Vertali's mainframe technical delivery of security and infrastructure projects. She focuses on helping organizations around the world to secure, protect and optimize their mainframe infrastructure and related applications.