BRIEFING DOCUMENT

Data sovereignty in an AI and cloud-centric world: A briefing document for CTOs

Published by

MOBILE WORLD LIVE

In partnership with

AROIT intel

Introduction

As artificial intelligence (AI) reshapes the way CTOs think about technology, it's also raising some new and important questions about data sovereignty. If diverse data sets from different jurisdictions cross borders for inference, how can organisations ensure they meet strict sovereignty requirements? As governments and regulators increasingly start to draw lines in the sand, there's a risk that enterprises will be caught off guard.

In truth, there are still some misconceptions about data sovereignty. Today, it's not just about where data is located (i.e., data residency), but rather, how that data is secured. A data set residing in a home country could still fail the sovereignty test if it's accessible by a foreign-owned entity, for example. But equally, data stored abroad could theoretically still meet sovereignty requirements if it abides by strict confidentiality, availability and portability rules.

In short, AI is creating new governance and sovereignty challenges that many organisations are just waking up to. Its use in cybersecurity infrastructure will raise the stakes further. This matters particularly to telcos, which recently ranked AI-enabled security as a top business priority. With many in the advanced stages of deployment, thoughts must now turn to aligning these plans with sovereignty requirements.

The question is how CTOs navigate these challenges in an era of geopolitical uncertainty and increasingly complex, distributed and business-critical IT environments. To find out more, Arqit and Intel commissioned Mobile World Live to interview over 200 global IT and security leaders.

AI is a priority for network safety

According to our poll, a majority of organisations view AI as a strategic priority to improve network safety and security. Only 8% don't consider it important, while a fifth (20%) rate the task as urgent. (Q1)

They're right to be prioritising the technology. AI offers a range of advantages for network defenders. Organisations are ingesting huge volumes of security data – from the endpoint to the cloud. But the quantities are so great that they need better ways to spot the needle in the haystack that signifies malicious activity. AI can do this far more efficiently than human teams, and work round-the-clock escalating and prioritising important alerts for further investigation. That's more important than ever at a time when industry skills shortages remain acute.

AI is also playing an increasingly important role as a digital assistant, helping human analysts by enabling them to ask questions and receive actionable responses in natural language. This can improve security outcomes and enhance analyst productivity. Even bigger wins could be achieved with agentic systems that work independently on repetitive tasks to detect, respond to and even remediate common threats. According to one analyst, CISOs believe the autonomous SOC may be just a year or two away.

Yet however AI is used, the underlying data needs to be tightly managed according to sovereignty requirements.

Adoption is lagging

Although most organisations see AI as a strategic priority for enhancing network security, the pace of adoption remains relatively sedate. A majority of respondents have either not yet adopted AI for network security (16%) or are only in the testing stage (44%). (Q2) Why the lag?

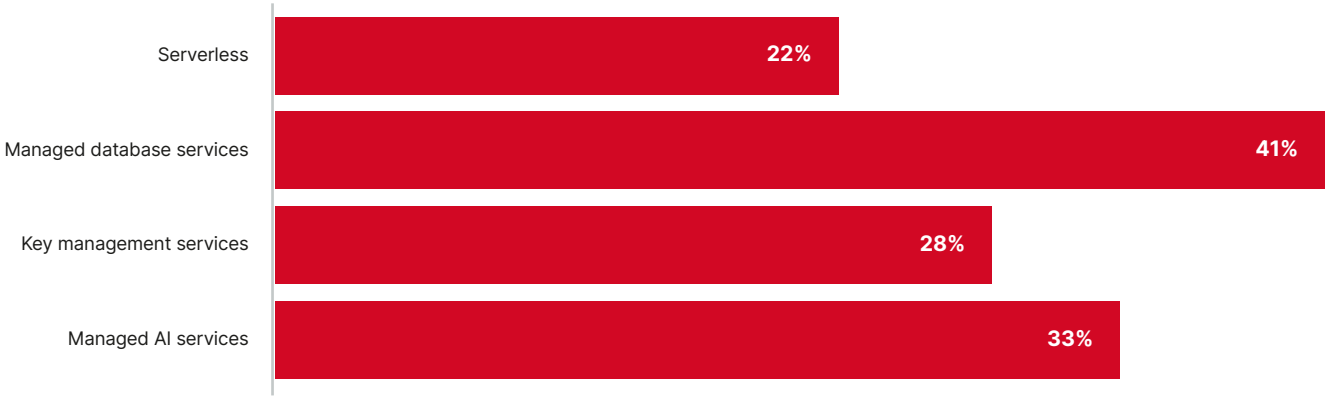
It's certainly not for want of solutions on the market. The security sector is awash with vendors promoting various AI-powered products. The challenge for IT buyers may be filtering out the marketing noise to find the best fit for their company. In what are economically uncertain times, budget might also be a factor, alongside uncertainty over ROI.

Securing data across heterogeneous hybrid cloud environments is no easy task, so organisations may also struggle with product interoperability and skills shortages. The complexity of this work is clearly underlined in the report. When asked which PaaS service would be most impacted if they re-architected AI workflows, respondents pointed to multiple areas, including serverless (22%), managed database services (41%), key management services (28%) and managed AI services (33%). (Q5) (See Figure 1)

What does this tell us? That there are many ways data can be stored, processed and transmitted in, to and from cloud. And there are different risks associated with each. A database typically stores data for a long period of time and may be a more attractive target for adversaries, versus ephemeral serverless functions, for example. The bottom line is: there is no one-size-fits-all data security solution to cover every enterprise use case.

As the market matures, we'd expect organisations to start thinking in a more detailed and nuanced way about the solutions most appropriate to their key use cases. And the implications for data sovereignty.

Figure 1: Which of the PaaS services would be most impacted if you re-architect your AI workflows?



Sovereignty and security risks slow progress

However, even if organisations want to progress AI security initiatives, there are several other barriers in the way for CTOs and their peers committed to the public cloud. Most are interrelated. Respondents cite IP leakage/theft (42%), secure data sharing (54%) and data privacy compliance (45%) as slowing AI projects (Q3). But the most common blocker is data sovereignty and privacy risk (62%) (See Figure 2).

At its most basic, data sovereignty is the principle by which digital information must be governed by the laws of the country in which it is collected or stored. But in a modern era characterised by distributed computing environments and dominated by US cloud providers, it's more complicated than it sounds. Even data stored in the same country in which it is collected may be subject to laws outside of this jurisdiction, if it's housed in a data centre run by a foreign company, for example.

Regulations add another layer of risk. Although it doesn't mention data sovereignty by name, the GDPR mandates that wherever data is stored, it must be governed in line with the regulation's own high standards. The continuously shifting legal sands around adequacy decisions and transfers to third countries add even more uncertainty for organisations.

Figure 2: When using public cloud, which factors slow down AI security projects?

The case for confidential computing

Against this backdrop, it's tempting to believe some cloud service providers (CSPs) when they claim to offer turnkey data sovereignty tools that solve these problems. In fact, 26% of respondents tell us they believe they have access to facilities with guaranteed data sovereignty. (Q7) The truth is somewhat more complicated.

This is the reality that confidential computing was built for. The technology protects data in use – whatever infrastructure it's running on, whatever the CSP and wherever in the world that data is located. It does this by isolating it within a hardware-based Trusted Execution Environment (TEE).

There are various ways to do this, but Intel delivers confidential computing by providing a hardware root of trust for data protection at the application (Intel SGX) and VM-level (Intel TDX).

There are three tests for true data sovereignty that organisations can use to assess vendor claims:

1) Confidentiality: Is data kept secret from every party it needs to be protected from, including the CSPs themselves?
2) Availability: Can I always access my data? (There is precedent for European citizens being denied access by US CSPs).
3) Portability: Can I easily move my data and workloads elsewhere, as much as I want or need to? Some CSPs may make it difficult to do so.

Credentials and privilege are only available to the data/workload owner. It's faster and less computationally demanding than alternatives like homomorphic encryption, making it ideal for AI use cases. And Intel's broad industry reach across cloud vendors makes solutions built using the technology less likely to suffer from vendor lock in. That's good for portability and, ultimately, sovereignty.

In fact, the vast majority (80%) of technology and security leaders we interviewed say they expect to use confidential computing to achieve data sovereignty in the public cloud, in edge locations or both in the next year. (Q6) Remote edge environments are particularly exposed to the risk of physical tampering, so it's good to see respondents recognising the need for trusted hardware-based enclaves there.

Starting the journey today

Risk and security teams may be delaying much-needed AI projects over data security and sovereignty worries. But the good news is that technology exists today to allay many of these concerns. And we expect to see regulators take a more flexible approach to data sovereignty in the future. There are signs that they will start to allow organisations more freedom in how they use and process data, as long as they deploy controls like confidential computing.

The bottom line is that data sovereignty is emerging as a key consideration when deploying and securing AI, especially in the cloud and at the edge. Regulations loom large over CTO strategy, taking us beyond the traditional view of sovereignty as a data residency issue. In practice, organisations need to think more broadly – exerting more control over not just where data is, but who can access it.

Despite the risks, data sovereignty needn't hold organisations back from deploying their most sensitive data and sophisticated technology, even in the public cloud. Tools such as confidential computing exist to help CTOs exert greater control over the confidentiality, availability and portability of their data.

Ultimately, they must balance their concerns with the risk of delaying projects. Our respondents warn that competitive advantage, operational efficiency, customer experience and brand reputation all hang in the balance. If data sovereignty and security is the destination, it's up to IT leaders to get there as quickly and safely as possible.

What Arqit and Intel are doing

Arqit and Intel are uniquely placed to address these concerns and help organisations benefit from AI-assisted network safety, without costly and disruptive system overhauls.

By bringing together the complementary strengths of Arqit, Intel and leading telcos, we're well positioned to deliver genuine, end-to-end sovereignty for enterprise customers.

Contact us today if you are concerned about the implications of data sovereignty on your business, and want complete control over your data, wherever it is.

Intel is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better.

Find out more at www.intel.com

Arqit secures the world's most critical data with quantum-safe encryption software. Simple, scalable, and compliant, its products integrate with existing infrastructure, requiring no hardware changes.

Arqit provides a complete "Detect, Protect, Comply" solution for governments and enterprises that detects and inventories cryptographic assets, protects data, ensures compliance, and safeguards transition to the post-quantum era.

Arqit's primary product offerings are Encryption Intelligence and NetworkSecure™. Encryption Intelligence detects cryptographic exposure, identifies vulnerabilities, and maps dependencies. NetworkSecure™ protects data in transit with provably secure post-quantum cryptography.

Arqit is an IDC Innovator for Post-Quantum Cryptography (2024) and a multi-award-winner in quantum-safe security.

For more information, visit www.arqitgroup.com

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com