Security in the age of AI and the cloud

Across all the regulatory and technological challenges that banks must address, there are core themes that cannot be ignored – cybersecurity, the move to cloud-based services and the role of artificial intelligence. **Peter Hainz**, head of cloud and security strategies for SmartStream, tells *Future Banking* about how banks can stay compliant and competitive while embracing innovation.

The position of chief information security officer (CISO) is becoming ever more important in banks, as it plays a crucial role in managing existential risks faced by an industry that relies so heavily on sophisticated technology. Today, CISOs must manage risks on many fronts – and their list of concerns is growing.

Top of that list are cloud security, and the potential risks that arise with the use of artificial intelligence (AI) and machine learning (ML). Banks are increasingly moving data and applications to the cloud, so must ensure that their infrastructure is configured securely to prevent breaches.

Banks are also collecting unprecedented amounts of data, so are using AI and ML to analyse it, as manual processes could never hope to reach the speed and accuracy needed. The security of these systems is becoming increasingly important, moreover, as attackers could profit greatly by manipulating the results of data analysis.

Peter Hainz, head of cloud and security strategies

“Banks need AI to be at the forefront of technology,” stresses Peter Hainz, head of cloud and security strategies for SmartStream. “In the dynamic realm of financial markets, the front office faces the crucial task of predicting market movements. With the prevalence of algorithms in FX trading leading to

a reduction in the number of traders, the reliance on vast datasets has become paramount. To effectively handle the scale and complexity of these datasets, cloud infrastructure has become indispensable, as scaling on-premise proves impractical. This shift underscores the necessity for agile and scalable back office reconciliation solutions.

"Banks can either use the public cloud, with services providers like AWS, build their own data centre or use private cloud infrastructure," he adds. "They often have hybrid solutions, and the choice depends on how sensitive the information is."

AI and the cloud: perfect partners

According to Gartner, by 2028 AI-driven machines will account for 20% of the global workforce and 40% of all economic activity. Banks are increasingly looking to replace intensive manual work with AI, but they equally realise that they must be very specific in how it is used – and what it can actually do.

"We see a cautious implementation of AI," says Hainz. "We reconcile data using AI, but banks and regulators need to know how that is done. Data reconciled using AI comes with an explanation, and clients can accept or reject the suggestions made by AI. There is no black box AI."

Without the cloud, AI would be relegated to data centres, which would greatly limit the ability to scale and develop solutions. For example, SmartStream's development of its Artificial Intelligence Reconciliations solution would have been impossible without the highly elastic microservices environment the cloud provides. The company's AI-powered Affinity solution, which observes how back office users work, and thus learns the bank's reconciliation workflow, also derives significant benefits from the cloud.

"Banks moving legacy infrastructure to the cloud means they also need our managed services," Hainz argues. "The IT industry is currently facing intense competition for talent, with banks finding it challenging to attract skilled professionals, particularly in areas like microservices, such as Kubernetes. While banks were traditionally considered attractive employers, IT experts now have a multitude of opportunities with institutions offering more competitive compensation and stronger reputations. This heightened competition poses a difficulty for banks in securing the right talent in crucial domains like microservices architecture.

"Banks need to outsource those things via the cloud, so there is a big change in mindset," Hainz adds. "They find comfort in entrusting their data to managed service and cloud providers, like SmartStream and AWS. The extensive security expertise of these providers, honed through collaborations with numerous banks, allows bank's IT and security teams to outsource responsibilities and focus on their core competencies.

Creating a data stronghold

Among many competing concerns – from disaster recovery to data encryption – banks are wrestling with one challenge above all others: the security and integrity of their data. That data is the currency that allows them to operate and compete in the financial services market, so it must be protected at all costs.

Increasingly, banks are requesting that vendors are Payment Card Industry (PCI) and Data Security Standard (DSS) certified, which requires meeting several industry standard practices, such as firewalls, encryption and anti-virus software. SmartStream has had to demonstrate high levels of security across its entire organisation to achieve the PCI-DSS version 3.2.1, Level 1 certification.

However, the company is always looking to go beyond any box-ticking compliance exercise.

"As part of my role overseeing cloud security, I implement a strategy known as Zero Trust," says Hainz. "This approach assumes the presence of potential intruders and prioritises the highest level of security. We ensure that microservices communicate exclusively through authorised, secure and compliant channels."

Pushing the envelope of innovation is a must, in short, but it cannot be at the cost of security – and this is clearly well understood at SmartStream. ●