The SWIFT Journey to the Cloud

How banks & financial institutions can save time, resources and reduce risks in an increasingly complex digital world

Financial institutions are at a crossroads. With significant regulatory and cybersecurity challenges, increased competition, digital disruption, and a new generation of consumers who expect more from their financial service providers, institutions must develop greater resilience and find more efficient operating models that aren't reliant on complex legacy infrastructures. Whether financial institutions can overcome the challenges at hand and transform their operations will largely depend on the utilization of cloud technology in key business areas. inancial institutions can overcome the challenges at hand and transform their operations will largely depend on the utilization of cloud technology in key business areas.

A challenging financial landscape

Today's financial landscape is evolving rapidly and increasing with complexity. Advances in technology have changed customer expectations and enabled a new generation of digital banks, without the burden of legacy infrastructures, to introduce innovative financial service offerings faster than ever before.

While a growing number of solution providers crowd the market, financial institutions are also having to combat an unprecedented rise in cyberattacks and fraud. If that weren't enough, an increase in the number and complexity of regulations across different jurisdictions has also made it much more challenging for institutions to stay on top of the latest standards resulting in increased compliance costs and risks.

Competition

A host of new competitors have moved into financial services over the last two decades, squeezing bank's profit margins and offering more convenient, customer-centric financial services, especially in payments. From large multinational tech companies like Microsoft, Apple, Amazon, Google, and Facebook to innovative new start-ups, competition has never been greater, and adoption is growing. McKinsey research found approximately 40% of US consumers leverage a fintech platform for daily financial activities[1] . These numbers are considerably higher in many parts of Asia.

Cybersecurity

Financial institutions have to deal with a broad array of complex and interconnected cybersecurity threats that will become even more complicated with the introduction of open banking. Today, recurring breaches, cyber-attacks, and fraud have become the norm, with nearly 70% of financial companies experiencing a cybersecurity incident[2]. In 2016, Bangladesh's Central Bank was subjected to unidentified hackers making payments via SWIFT and attempted to carry out one of the biggest-ever cyber heists of nearly $1 billion.

The bad news is cybercriminals are getting more sophisticated, leading institutions to spend more and more on cybersecurity with no let-up in sight. According to an Accenture and Ponemon Institute study, banks, capital market firms, and insurers have a per-firm average of $18.5 million annually to combat cybercrime[3] .

[1] https://www.mckinsey.com/industries/financial-services/our-insights/how-us-customers-attitudes-to-fintech-are-shifting-during-the-pandemic

[2] https://www.prnewswire.com/news-releases/nearly-70-of-financial-services-companies-globally-have-experienced-a-cyberattack-301057261.html

[3] Accenture & Ponemon Institute, LLC, Financial Services Cost of Cyber Crime Study.

Regulatory compliance

Regulators worldwide are stepping up efforts to ensure financial institutions implement strong security measures to protect customer data and fight back against money laundering and a rising tide of fraud. More stringent regulations with greater levels of complexity are seeping into new and unchartered areas, drastically testing the capabilities of risk and compliance departments within financial institutions and driving up costs.

Regulations such as PSD2 and GDPR have set the stage for more stringent data privacy rules and forced financial institutions to put in place robust additional security measures. According to Deloitte, operating costs spent on compliance have increased by over 60% for retail and corporate banks compared to pre-financial crisis spending levels [4].

Why cloud has become the new default

Financial institutions have traditionally built their business models around costly legacy infrastructure, on-premises installations, and proprietary capabilities. In today's digital environment institutions are feeling the pressure to transform how they operate and prepare for a future that looks very different. They face rising consumer expectations, increasing competition, and growing cyber threats. Furthermore, systems are being updated frequently due to the increasing tide of regulation. Machine learning adoption is increasing in order to detect sophisticated financial crime, with models requiring calibrating and monitoring.

Due to the fast-changing environment of capital markets coupled with the rise in financial crime, there has been a notable shift to the cloud being accelerated in recent years as more institutions see the value cloud computing can bring to their organizations and recognize the maturation of the technology. The proliferation of quality cloud solution providers, many of which hold security as a core competence, has also played a significant role in increasing adoption.

Cloud computing is viewed as a cheaper, faster, and more flexible alternative to on-premises data storage. There is a growing understanding among CEOs, CIOs, and Chief Compliance Officers within financial institutions of the ability of the cloud to optimize systems, reduce risks, build resilience, provide scalability, and develop innovative new services.

92% of banks are already making significant use of the cloud [5]

54% of banks have a cloud adoption strategy ready to implement within the next 12 – 24 months [6]

[4] Deloitte, The Future of Regulatory Productivity, powered by RegTech Position Paper.

[5] ACI Worldwide, Culture of Innovation Index.

[6] Finastra, Cloud Banking - Innovation without limits Report

Key benefits of cloud computing

Scalability

The cloud allows financial institutions to grow as demand requires and be scaled back when unneeded, eliminating the need to invest in unused capacity. By providing a way to quickly scale up and down processing capabilities without any additional investment, institutions can respond to changing market conditions at reduced costs, helping them to remain robust in today's highly competitive and dynamic landscape. During periods of market volatility, such as the early stages of the COVID-19 pandemic, financial institutions with a cloud computing solution in place had greater flexibility to meet significant spikes in payment volumes and processing requirements.

Cost of ownership

Cloud reduces the total cost of ownership of infrastructure by minimizing hardware equipment costs, the need for expertise, and eliminating IT expenditures such as the overheads involved in developing and maintaining servers. By utilizing the cloud, financial institutions can also access various software and application updates without requiring further investment, enabling them to respond to changing trends and unpredictable external events.

Agility and innovation

Cloud enables financial institutions to innovate at speed and create custom solutions that can be launched rapidly and updated in real-time. Instead of focusing time on running and maintaining costly IT infrastructures, institutions can better deliver market-relevant products to their customers in a timely manner.

Security & resilience

Cloud provides financial institutions with a more secure and robust infrastructure to meet strict compliance standards and combat cybercrime. By using the cloud, financial institutions can take advantage of cutting-edge security technologies and processes that are often more superior to the tailored on-premises, locally hosted setups used by most institutions.

Taking SWIFT connectivity to the cloud

The SWIFT network is an invaluable and trusted resource for banks and financial institutions worldwide, providing connectivity to more than 10,000 financial institutions in over 200 countries.

Implementing direct SWIFT connectivity requires SWIFT and internal technical expertise, which is an increasingly scarce resource globally. The investments in hardware, software, and ongoing upgrades are substantial, and implementation can be technically challenging. Regular technology updates and on-site expertise are required to ensure seamless, continuous access to the SWIFT Network. Eastnets' SWIFT Hosting is a fully accredited SWIFT service bureau used by more than 300 leading corporations and financial institutions. It offers a unique, highly cost-effective solution for SWIFT connectivity, delivering a fully outsourced, cloud-based alternative to the traditional SWIFT infrastructure. Our dedicated Service Bureau provides a way for SWIFT users to outsource their internal IT operations to a trusted SWIFT certified partner without compromising their operational efficiency, data security, and business availability at a much lower cost of ownership. Eastnets' analytics, dashboards, and message relationships to support investigations provide an added value service offering.

SWIFT Hosting as a Service

Outsource your SWIFT messaging interface and connectivity through Eastnets certified Shared Alliance Access service. With Eastnets SWIFT Hosting, you can create view and exchange messages (FIN, FileAct, InterAct, RMA) with counterparts manually or by integrating automatically with the back office without the need to purchase, install or maintain any SWIFT products on premise. In addition to our secure and reliable service, we can assist you in compliance towards the Customer Security Programme (CSP) security controls via our CSP independent assessment service.

Cloud base Sanctions Screening

SafeWatch Screening uses advanced technologies to provide fuzzy matching watchlist screening solution for real-time transactions, customer information batch mode capabilities, and other ad-hoc screening. SafeWatch Screening provides flexibility to connect to watch list data sources via blockchain technology to alleviate vulnerabilities by streamlining the multi-step process for keeping watch lists of sanctioned individuals and entities current. This reduces information lag times and the risk of manipulation and mistakes by personnel.

SafeWatch Screening provides continuous monitoring of customer information and financial messaging. It provides the central check point for all financial and non-financial traffic of the institution, whatever the format or transportation of the data, allowing compliance officers to have a single interface where all alerts from all sources are consolidated.

SafeWatch Screening includes several techniques for reducing false positives such as matching scores, good guys, violation/business rules, and a decision re-application feature based on algorithms for suppressing repetitive matches.

Other than screening capabilities, SafeWatch Screening can detect transaction compliance with FATF recommendations 16, handle cover-match and message pairing, wire-stripping, advanced integration, and advanced workflows.

Eastnets Anti-Fraud as a Service

A robust, real-time and multi-channel fraud prevention solution that dynamically detects and stops fraudulent payments by analysing against a wealth of past data. Eastnets PaymentGuard uses machine learning to reference a historical database of customer data – including transactions, device information, and geolocations to intelligently model existing and emerging patterns.

These patterns predict trends as they occur and generate instant alerts that can be processed using a sophisticated-yet-simple case manager. PaymentGuard has seamless integration with the SWIFT environment and helps banks to comply with the transaction control requirements in the SWIFT CSP.

About Eastnets

Eastnets ensures peace of mind by securing a safer future for everyone. A global provider of compliance and payment solutions for the financial services sector, our experience and expertise help ensure trust at 750 financial institutions across the world, including 11 of the top 50 banks. For more than 35 years, we have worked to keep the world safe and secure from financial crime. We do it by helping our partners manage risk through sanction screening, transactions monitoring, analysis, and reporting, plus state-of-the-art consultancy, and customer support.

eastnets

About

Eastnets ™ ensures peace of mind by securing a safer future for everyone.

A global provider of compliance and payment solutions for the financial services sector, our experience and expertise help ensure trust at 750 financial institutions across the world, including 11 of the top 50 banks. For more than 35 years, we've worked to keep the world safe and secure from financial crime. We do it by helping our partners manage risk through Sanction Screening, Transactions Monitoring, analysis, and reporting, plus state-of-the-art consultancy, and customer support.

Learn more at www.Eastnets.com

Belgium | Egypt | Hong Kong | Jordan | Luxembourg | Pakistan | Qatar | UAE | United Kingdom | USA