Moving payments to the public cloud with CGI All Payments

CGI

The promise of the cloud—whether private or public—is tantalizing for banks. The stated benefits are many, including sustainability, resource elasticity, reduced capacity planning, improved resiliency, increased efficiencies, and lower costs.

The arguments for why banks should consider replacing their data centers with the cloud are compelling. In fact, of the 264 banking executives we interviewed face-to-face as part of our 2021 CGI Voice of Our Clients program, 60% are planning to migrate at least 21% of their applications to the cloud over the next 2 years.

However, with data sets that are comprised of almost 100% personally identifiable information (PII) and the negative impacts of any compromise, security is a huge issue for banks. While many banks view the private cloud as less of a security risk, most banks have been reticent to move their core systems—or "crown jewels" as one of our clients calls them—to the public cloud because of its unique security issues.

Protecting core assets is not the only concern of banks in moving to the public cloud. There also are legal security and regulatory requirements to consider. In light of these challenges, it is clear that unleashing the rewards of moving your payments to the public cloud can seem as complex and even overwhelming.

At CGI, we have a long history of helping clients do complex things well—from securely steering satellites, to delivering valuable defense data, to innovatively processing passports, to implementing market-leading payment systems. Our latest payment deployments have involved both the private and the public cloud, and three fundamental capabilities have helped our clients break free of the obstacles holding others back:

Platform

a fit-for-purpose, multi-cloud-native, and cloud-independent payments platform

Experience

extensive infrastructure and application management experience

Security

advanced cloud security coupled with a strong risk management approach

Separately, these fundamentals are not rocket science, but bringing them together requires intense focus and dedication. By combining these three capabilities, our clients have been able to move their payments to the public cloud securely and seamlessly.

The right platform

The challenge of putting any application into the public cloud is ensuring that the application's entire technology stack will enable an efficient and secure deployment. While the technology is available to put a mainframe application into the cloud, nobody really wants to do that because mainframe applications are not cloud native or ready to capture the benefits of the cloud.

When you consider moving your payments infrastructure to the public cloud, the first step is to find the right platform—a fit-for-purpose, multi-cloud-native, and cloud-independent solution that will make the most of the benefits of cloud deployment. Independence is a significant component in reducing cloud risk. While cloud providers have endeavoured to make deployment easier by providing cloud-native tools, the use of these prevents interoperability of the deployed solution, can tie a bank to a specific cloud platform, and generates inherent technology debt (i.e., the implied costs of updating less-than-optimal technology).

Beginning in 2016, we reimagined and engineered our payments platform, CGI All Payments, to meet these requirements precisely. Based on an ISO 20022 data structure, the platform is purpose-built for delivering orchestration, real-time processing, and certified network gateways. It also supports the 24/7 processing of any payment type. Designing CGI All Payments to deliver these future-proof capabilities has enabled us to deliver both public and private cloud deployments ahead of the market and ensure our clients benefit from the resource elasticity, resiliency, high availability, and other cloud benefits they need.

This has become hugely important as payments processing undergoes major change globally. Within the next five years, nearly every bank around the world will need to support ISO 20022-based payments as international infrastructures migrate to ISO 20022. Domestic, regional and international real-time payments running 24/7 are already a reality for some, and banks are recognizing the business need to prepare for this. In addition, and highlighted further by the global pandemic, payments infrastructure needs to be more flexible than mainframes, with secure remote deployment and maintenance a must have.

The right experience

Although finding the right platform to achieve the benefits of public cloud deployment is essential, without the right experience for deploying securely and within a resilient, self-healing cloud environment, your platform will fall short. Proven cloud expertise and processes coupled with effective cloud risk management are just as critical for minimizing risks, costs, and business disruption as choosing the right platform and payment solution.

On the guidance side, before any public cloud deployment, we conduct an in-depth requirements analysis (CGI Cloud Risk Assessment), which identifies the why, what, when and how of the migration. This facilitates proactive issue resolution, drives efficiencies and reduces risk. Success at this stage requires open and clear communication about requirements, issues, opportunities, feasibilities, etc. A trusted relationship based on honesty and close collaboration is a key part of this.

On the process side, we have developed robust cloud processes, along with a significant investment in staff training and certification, to assist banks with process implementation. We train bank teams on how the deployed platform works, how to monitor it proactively, and how to troubleshoot and handle issues. These management processes are rigorously tested and, once operational, highly effective.

In 2019, we became the first Scaled Agile (SAFe) global transformation partner, and this approach to development and delivery has enabled us to reduce time-to-market while improving quality. Our agile teams use multiple environments in developing code (e.g., non-production, testing, pre-production, production), which enables them to deploy less code per release and test more quickly and effectively. Additionally, through automated testing, the teams can ensure required changes have no negative impact on code that is already working.

Applications are deployed into an environment that is truly fit-for-purpose, leveraging public cloud features such as automated patching and Kubernetes' self-healing to ensure 24/7 processing and high availability far beyond that of more traditional deployments. While cloud resiliency makes failover less likely, process automation dramatically reduces geo-location failure recovery time to under 30 minutes.

All of this is pulled together by decades of experience in providing application managed services (AMS) to clients around the world. We deliver services under "least access" protocols by security-cleared staff with transparent service-level agreements, strong but simple governance processes, and highly effective change management. This ensures high efficiency, low cost, and high quality. All of our services also are well documented and auditable, which addresses one of the chief concerns of banking regulators when assessing the external service arrangements of banks.

The right security

Security already is a critical need for any payments infrastructure because it typically manages data that would cripple an economy in the event of a breach. However, when PII moves to the public cloud and contains payments data, there is another layer of scrutiny involved. As with all technology introduction, if institutional understanding of real and perceived risks is low, not only are regulators concerned, but those responsible for security within a bank often view this as a significant risk, despite the obvious returns and improved controls that they will have in reality.

Although the primary public cloud providers such as Microsoft Azure, Amazon AWS and Google Cloud Platform have poured significant investments into security, the task of hardening a specific environment falls to the organization that is responsible for the deployment. Cloud security controls must be set up and used correctly to ensure strong security and prevent the opening of doors that invite vulnerabilities. Security controls such as NIST 800 and Regulatory Customer Security Controls Framework are critical in securing payment deployments, and knowledge of how best to apply them is paramount.

In addition, it is important to leverage the right multiple security tools that will automatically scan all layers, analyze source code, search for known third-party product vulnerabilities, and validate runtime environment configuration. This helps to minimize the ongoing risk of introducing new vulnerabilities through code changes, environment configuration, and third-party software.

Some security controls can be very costly to implement and manage with very little risk mitigation impact. Our security approach overall maintains a healthy balance between security risks, the impact of security controls on productivity, and the costs in managing them.

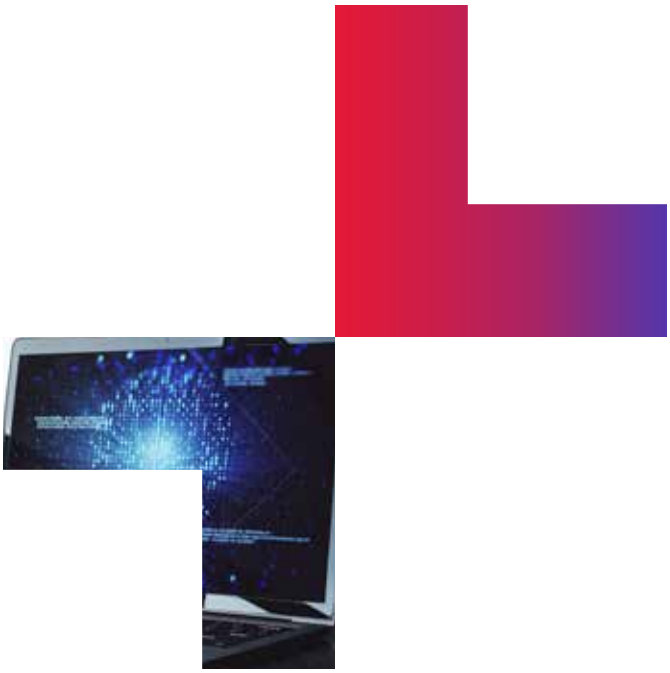
Attack tree threat modelling (threat analysis), which identifies possible attack vectors, is needed for public cloud security. Attack tree threat modelling helps to address the following primary security concerns for banks:

Extended attack surface to forge a payment or leak customer data: This type of attack can be carried out not only by bank staff with access to the bank's payments processing systems, but also by the staff of the bank's cloud service provider to some degree. The most important security controls to prevent this include:

- Multi-factor authentication for all types of accesses (e.g., user, administrator)
- Cryptography to protect payment data on multiple levels (e.g., encryption at-rest, encryption in-transit, digital signatures)
- Segregation of staff duties
- Use of continuously scanned private container registries and restricted Internet access from runtime environments

Extended attack surface to cause service unavailability: The most important security controls to prevent this are network lockdown, DDoS protection, throttling, and limited access (to essential users). Access can be limited through a private virtual network and/or a site-to-site VPN between all sites (e.g., cloud service provider and bank) in a hybrid cloud deployment. It also can be limited through jump servers, management servers, and virtual desktop infrastructure (VDI) without any option to install software.

Our security approach brings together the rocket and fuel with right controls to make them successful. With this approach, we focus on embedding security into every process, not just adding it on before the "go live" date. Security is baked in, not bolted on, and as a result, there is less chance of missing a vulnerability or inadvertently creating one.



We also recognize that security is not just about technologies; it also is about processes and people. People often can be the weakest link when it comes to security. Implementing a comprehensive security approach with proven processes helps to maintain and increase security awareness among people, which, in turn, reduces possible attack vectors.

In addition, implementing a "least privilege access" policy is an effective weapon in preventing internal and external breaches. Security vetting of all engaged staff adds another layer of protection from vulnerabilities and strongly complements all other security measures.

Bringing it all together

With clients “live” and processing payments using our regulatory-approved public cloud solution, we have been able to bring together all of the essential elements for success. Working closely with our clients, we have solved complex problems and set forward-looking banks on a pathway to sustainability, lower costs, and better use of the resources at their command.

Our clients’ success results from combining the right components with the right expertise and negating potential risks. Further, our work has led to a repeatable execution. Within a year or so, we expect public cloud deployment of payments infrastructure to become standard.

This is a great time to consider working with us to gain the benefits of either a public or a private cloud deployment. We can help you gain the advantages of whichever cloud service you choose Visit cgi.com to learn more, or contact us at info@cgi.com. We welcome an opportunity to discuss your cloud migration strategy.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com