IT'S TIME TO (SECURELY) INNOVATE FINANCIAL SERVICES

Antonina Skrypnyk and Pavlo Mikhaelian

softserve

Financial Services businesses are 300 times more likely to be hacked than those in other industries. Valuable financial records are a prime target for those with bad intentions, and breaches not only affect individual customers but cause significant brand damage.

As the financial services industry evolves to include better—and more innovative—technology, measures must be taken to keep data sealed tight, and within regulatory compliance.

Give consumers what they want—but take care

Today's financial customers demand convenient, fast, and personalized digital experiences. The ability to have on-demand access to all financial parameters at the tap of an app is no longer a nice to have, it is essential.

But for an industry notorious for legacy systems, meeting those needs can be a challenge. Fortunately, there are many paths for financial services businesses to update systems and reach customers—securely. To that end, two clear paths have emerged: cloud migration and distributed ledger technology (DLT).

Migrating to the cloud augments storage space while reducing power consumption and costs, allowing companies to scale up and deliver more quickly. For financial services specifically, this means a faster turnaround for service areas such as credit scoring, statements, consumer payments, and billing.

DLT has also taken the industry by storm, offering a faster, more transparent way of doing business. By its own structure—which stacks data block-by-block—security is intrinsic within the structure of the code, making transactions and contracts secure by nature.

Unfortunately, there is an inherent misperception of security in both technologies: that full security is "built in." **This could not be further from the truth**. For companies looking to leverage either technology, or any new technology for that matter, in-depth scrutiny is required before implementation. Let's dive deeper into common misconceptions—and what to do about them—in cloud migration and DLT.

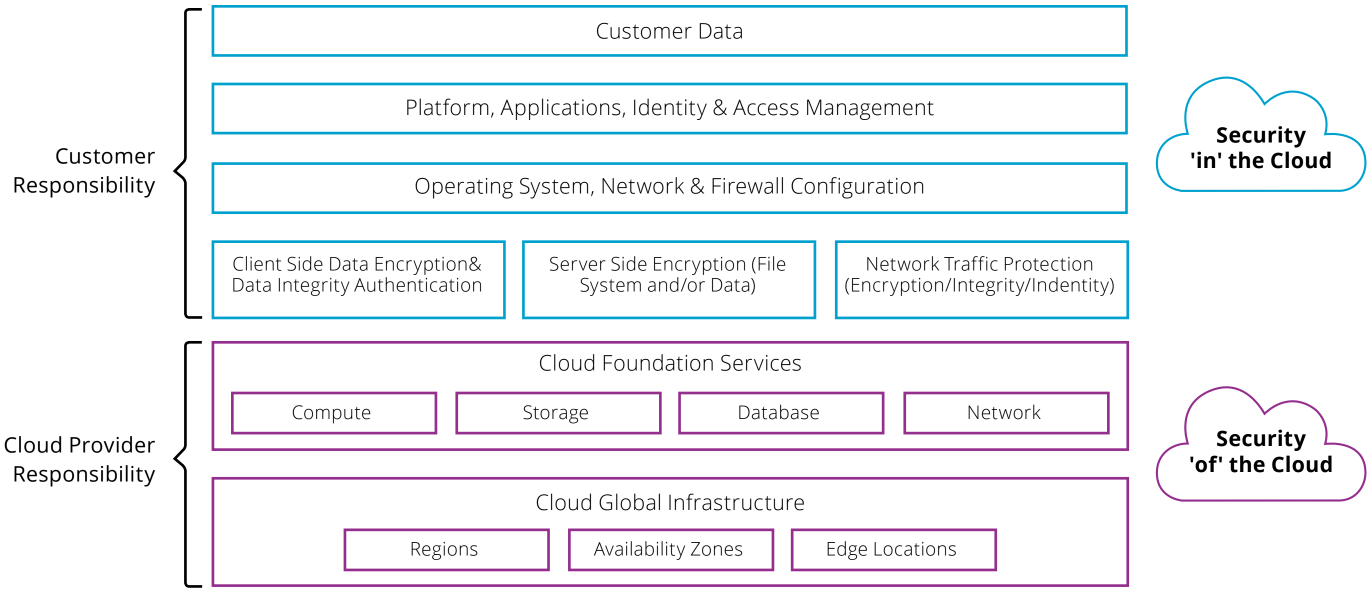
Cloud migration

Within cloud migration, scalability and performance often take the spotlight over security. And assumptions about the nature of cloud security itself can lead to vulnerabilities.

For many financial businesses, one of the attractive features of the cloud (beyond the possibilities for saving costs and increasing agility) is the level of built-in security. But this is often a misreading of the cloud's shared responsibility model.

Cloud security and liability on the part of the cloud provider is limited. To clear any doubt, let us be clear: **turnkey security does not mean a risk-free cloud**. In fact, there is a shared responsibility between both the cloud customer and the cloud provider.

The shared responsibility model means that while the cloud provider is responsible for the security *of* the cloud, the customer is responsible for security *in* the cloud. Essentially the cloud provider is responsible for the security of the cloud infrastructure, and for the security of foundational services such as compute, storage, database, and network. The cloud customer, meanwhile, has a long list of his own security responsibilities, such as client and server encryption, network traffic protection; OS, network, and firewall configuration; platform, application, identity, and access management; and—of course—customer data.


Customer Responsibility
Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client Side Data Encryption& Data Integrity Authentication
Server Side Encryption (File System and/or Data)
Network Traffic Protection (Encryption/Integrity/Indentity)
Security 'in' the Cloud
Cloud Provider Responsibility
Cloud Foundation Services
Compute
Storage
Database
Network
Cloud Global Infrastructure
Regions
Availability Zones
Edge Locations
Security 'of' the Cloud

All solutions, data, and applications that exist within the cloud need their own, customized security on the part of the cloud customer (i.e. the business).

Another problem is using legacy security solutions that simply don't belong anywhere in the cloud. It isn't unusual for a cloud migration to be a direct shift of existing legacy systems from one location to another. But while the increased agility of the cloud increases market share and volume, using outdated security systems to guard them is often inadequate. Security should therefore be updated to match the technology or platform upon which the solution is placed.

As for those who are doubting the importance of security (if there are any doubters left in our readership): corporate managers need not look deep into press archives to identify recent security breaches—**action must be taken to regularly assess the health and security of your system to ensure that vulnerabilities are mitigated.** Security is something that needs to be monitored around the clock, as well as regular security assessments and health checks that test vulnerabilities within the system and improve or upgrade it as needed.

Let’s get distributed

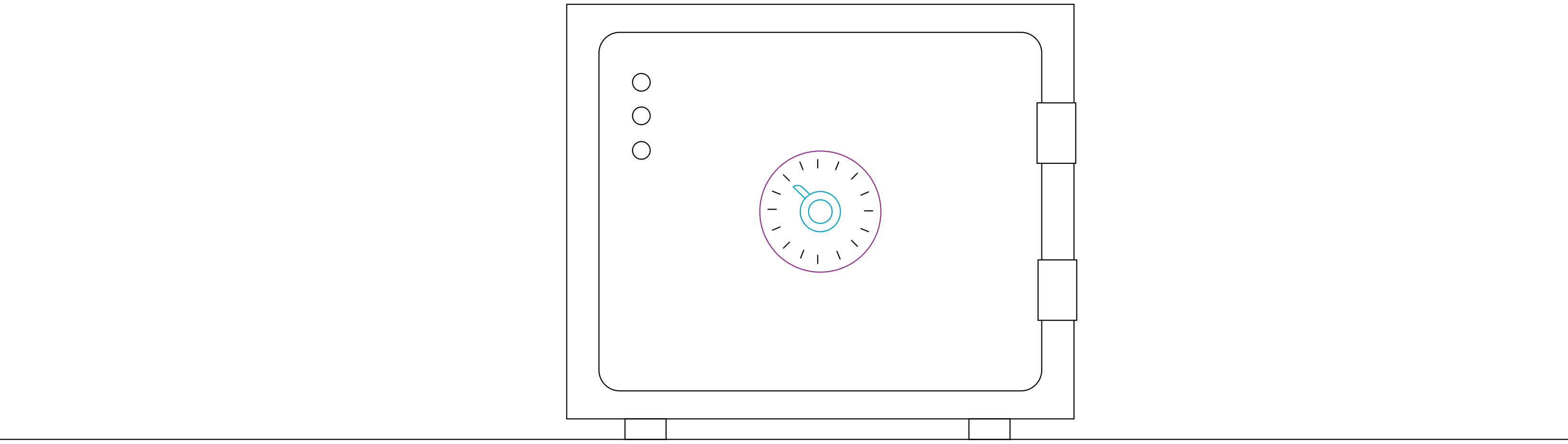
DLT enables direct transactions, increases speed and transparency, and reduces fraud. But for financial leaders, introducing DLT into the ecosystem means new and potentially more complex security risks.

While most consider DLT to be airtight, the security of its application is entirely reliant on those within the network. Increased transparency means transparency for all kinds of different players, and not all with the best intentions. On the edge, there is significant room for fraud to damage an otherwise secure solution.

In early 2018, Japanese cryptocurrency exchange Coincheck lost $530 million in a cryptocurrency theft. The source of the attack? Hackers gained access to the internet-connected repository where users store cryptocurrencies (the “hot wallet”). While the technology stayed intact, access to it was compromised.

In order to maintain the most secure posture, all members within a DLT network must be constantly aware of the vulnerabilities that exist in its application, and how to avoid them.

Putting your money where your mouth is



The financial services industry’s aging, legacy software and IT solutions are difficult to defend against modern cyberattacks. Running security as an add-on is risky—tools that don’t integrate seamlessly need greater scrutiny than a system that has comprehensive, custom security built into its foundation. Often, legacy systems don’t scale to include protection against modern security risks.

The best way to keep data secure is by weaving security into a solution from the beginning. Integrating security with all other components of the solution architecture ensures seamlessness, making upgrades simpler and augmenting protection.

But at what point is built-in security in need of patches or upgrades? And how much additional security is needed for a solution that incorporates legacy systems?

There are several things to keep in mind when building new solutions for financial services. Let’s walk through the top considerations:

Risk Assessment
The first step in assessing security compliance and posture is to assess risk. What are the major security risks and how can they best be addressed in order of priority?

Financial institutions should take inventory of all components within the system and assign value and risk. Customer data, back-end infrastructure, new solutions—how is each valued within the larger structure, and what is its vulnerability? By assigning value and assessing risk, financial leaders can then create a more substantial architecture.

Assessing Architecture
Once the value and the risk are clear, the next secure step is to build an architecture to protect data. Applying knowledge gained from the risk assessment, a firm architecture is then assessed and tested, made scalable, and implemented.

Architecture assessments should extend throughout the infrastructure, as well—from solutions to applications. It’s not uncommon to overlook security measures by accident, but architecture must be a consideration for everything from back-end solutions to customer-facing apps. Failing to consider comprehensive security will leave solutions vulnerable to attack.

Monitoring
What is the maintenance plan? After assessing risk and building a comprehensive architecture, the most important step in keeping data secure is ongoing monitoring.

With the evolution of attacks happening every day, security teams must constantly check for vulnerabilities within any infrastructure, solution, or application.

Conclusion

Security today is a constant, tireless reality for virtually any company. Financial businesses that defer investments in infrastructure and technology solutions to protect customer and proprietary data risk losing customers and becoming tomorrow's news headline.

As financial businesses implement more innovative solutions into legacy systems—and experiment with hot technology—the higher the risk is that data will be compromised. Whether cloud migration, DLT, or any number of recent innovations that are revolutionizing financial services, concrete steps proper steps should be taken to ensure security is airtight.

Assess risk, build a strong architecture, and continuously monitor your systems to remain secure.

Are you ready to take your infrastructure and technology solutions to the next level?
Contact SoftServe to get started today.

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience is built on a foundation of empathetic, human-focused experience design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy. No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

USA HQ

201 W 5th Street, Suite 1550
Austin, TX 75703
+1 866 687 3588

EUROPEAN HQ

One Canada Square
Canary Wharf
London E14 5AB
+44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com

softserve