FUJITSU

Driving Agility in Financial Services:
How IDaaS Can Help Firms Innovate their Way to Success

Introduction

To succeed in a highly competitive market, Financial Services (FS) companies have to be agile and collaborative. Competition is coming from traditional, well-established financial services organizations that have seen the need for investing in greater business agility to make quick, flexible decisions to empower their customer. But it is also coming from born digital, innovative Fintech players that have quickly stolen market share from the larger players by building more customer-centric business models for the 21st Century consumer.

In this fast-paced landscape of mobile, cloud-driven innovation and rapid development cycles, cybersecurity can often be an afterthought. But FS companies hold some of the most highly sensitive and regulated customer data, and IP, that must be protected. Proper Identity and Access Management (IAM), ensuring that only the right people can get to the right information at the right time, therefore becomes a key for business success. Get this right and you've laid the foundations for a business that can attract customers and retain customers. But it's not easy to do this yourself, which is why many leading organizations outsource this vital role to a trusted provider using Identity as a Service (IDaaS) solutions.

What's driving the need for agility in financial services?

In an ultra-competitive marketplace, firms are leveraging digital transformation to become more agile. The need to do so is being driven by several factors:

- Fierce competition for customers
- Changing business models shifting from product-centric to customer-centric
- Tight profit margins
- Rapidly changing product portfolios and accelerated rollouts of innovative services
- Enhanced regulation increasing government oversight and intervention
- Alignment of IT strategies and goals with the business

Cloud computing and the need for IAM

Many IT leaders have turned to cloud computing, to help drive the rapid, continuous development of application-based services, enabling firms to react quickly to market demand with innovative new offerings. Applications are the new innovation and productivity engine for FS and the cloud helps accelerate their development and smooth their consumption.

Cloud infrastructure is now the default choice to support growth through innovation because it:

- **Delivers cost savings:** organisations are saving 14% of their budgets by switching to the public cloud
- **Moves spending from CapEx to OpEx:** which removes the need for large upfront investments
- **Provides Scalability/Elasticity:** Helps support a more agile development of new services thanks to unlimited resource availability
- **Supports anytime, anywhere access:** for a mobile, app-driven world

Given these benefits many organizations have moved core business systems to the cloud, and that trend is likely to continue as the thirst for innovation and competitive-edge grows in the FS sector.

The importance of cybersecurity

This move to digital, cloud-based services puts an even greater pressure on cyber security. FS organizations store, manage and process sensitive financial and personal data which is highly sought-after by cybercrime groups and even nation states. User account credentials are the key that can unlock this data for malicious third parties. In fact, Verizon claims that 80% of hacking-related breaches used stolen and/or weak or guessable passwords.

Whilst compromised customer credentials are a serious problem, it is just as important to manage the cybersecurity risk associated with your employees. Both human error and malicious intent could lead to damaging data loss/theft. Mistakes made by staff accounted for 62% of all breach incidents reported to UK watchdog the Information Commissioner's Office (ICO), according to research from 2016. Staff can easily be tricked into clicking on convincing-looking phishing links designed to harvest their credentials, especially given the rise in executive email spoofing attacks. Malicious insiders are even harder to spot as they know what to look for and will have a better idea of how to cover their tracks. These insiders can turn malicious for a huge number of reasons but many are motivated by money, others by personal and professional grievances, and some may even take data with them to a competitor when they leave.

Recent research estimates that 90% of global organisations feel vulnerable to insider-related risk. The main contributing factors highlighted by IT leaders are too many employees with excessive access privileges (37%), and an increasing number of devices with access to sensitive data (36%). In the FS sector these problems are particularly prevalent because of the continuous stream of new employees and ever-evolving systems. This makes it even more important to ensure that:

- New employees get access to systems, apps and platforms in a secure manner
- Staff are only allowed access to the systems necessary to do their job – and no more
- Those leaving have access rights removed as soon as they no longer work for the company

Keeping up with this is crucial as regulatory compliance requirements such as GDPR give greater power to authorities to enforce stricter controls. The Financial Conduct Authority (FCA) also requires firms to report "material breaches" under Principle 11. In fact, the regulator wants more than that: it demands "a security culture", driven from the top down.

At a fundamental level, the effort of investigating, remediating and reporting incidents harms business agility. But that need not be the case. Effective cyber-tools enable FS firms to drive greater agility and growth by proactively identifying threats and vulnerabilities and putting a stop to them before they can impact the business and block innovation. When considering the insider risk effective cyber security controls are also a key part of protecting Intellectual Property from being stolen by exiting employees.

In this context, Identity and Access management (IAM) is vital to managing security risks and providing that foundational layer on which success can be built.

The need for change in IAM

The adoption of cloud- and app-driven approaches means that legacy IAM solutions are no longer fit-for-purpose. On-premise IAM simply does not work with modern, cloud infrastructure. It's costly and time-consuming to integrate and maintain, and lacks the visibility and speed required to support business agility. In fact, legacy IAM is that block on innovation that security should never be.

These legacy tools are unable to adapt to your cloud and app-based infrastructure as it grows over time. Costly new connectors must be built each time a new cloud app is added, adding as much as £75,000 per new integration, while the apps themselves also require more maintenance and updates. The possibility of frequent, costly downtime is a risk no-one wants to expose themselves to.

Cloud–based identity, or Identity-as-a-Service (IDaas), addresses these problems as they are easy to set-up and deploy and offer the kind of scalability and reliability that on-premise alternatives cannot provide.

It's all about securing access at the cloud app-layer rather than attempting to follow the outdated model of security at the perimeter. IDaaS offers a 360-degree view of all apps, users and devices in your environment. There's no need to take cloud services offline and new apps can easily be added and managed, providing the business with the secure agility it needs to stay competitive in an ultra-competitive market place.

Fujitsu can help you enhance your agility and empower your employees to innovate securely by providing you with the right mix of IAM and IDaaS solutions.

IDaaS Solutions

- Single Sign-On (SSO) access across multiple applications and platforms
- Adaptive Multi-Factor Authentication (MFA) for enhanced security, with support for SMS push notifications, Google authentication and Okta Verify with Push
- Lifecycle Management allows integration with Slack, and comprehensive control over lifecycle states with automation and customisation
- Compliance with complex financial regulations across diverse regions
- Consistent user experience globally for customers and employees
- 100% of employees protected with Adaptive Multi-Factor Authentication (MFA)

Empowering Financial Services

True Identity and Access Management that ensures that the right people, access the right information, at the right time means that IT Security teams can:

Support Digital Transformation: Cloud-based identity will help to speed up your innovation agenda by connecting any employee, vendor, partner, or customer to anything with security that doesn't sacrifice ease of use, and easily interoperates with the tools you already have in place.

Provide Secure and Efficient Access for Employees, Partners and Customers: Online access to CRM, order booking, and enablement tools for external brokers is mission-critical yet difficult to do efficiently with legacy IAM solutions. We make it easier to collaborate in a more secure way than ever before possible so you can drive more revenue.

Empower Your Customers with a Secure and Seamless Experience: Customers want to engage on their own terms. Whether you want to acquire new customers online, or unify a constellation of customer portals, we make web and mobile access secure, compliant, and frictionless.

The result is a solution which reduces operational expenses and minimises security risk providing the ideal foundation to innovate and build success.