okta

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

Introduction

The UK's Fintech sector is booming. Despite Brexit-related concerns, it remains Europe's main hub for financial technology start-ups, providing 60,000 jobs and contributing around $7 billion annually to the economy. In fact, it managed to attract $564m (£433m) of venture capital funding in the first six months of 2017 alone, a 37% increase from the same period in 2016. This puts the UK third in the Fintech stakes behind the US and China.

Investors have ploughed more than $25 billion in over 4000 UK-based Fintech companies since 2010 keen to capitalise on their relentless push to innovate, disrupt and democratise away from old, entrenched ways of doing business. From blockchain to AI, crypto-currency to peer-to-peer lending, the sheer range of new ideas permeating a once staid landscape is exhilarating—but the stakes are high.

To succeed in an already highly competitive market, Fintech players must be agile, collaborative and scalable. They're also competing against traditional financial services giants, which themselves have finally grasped the importance of business agility to make quick, flexible decisions to empower their customers.

In this landscape of mobile, cloud-driven innovation and rapid software development lifecycles, cybersecurity is often not given the attention it deserves. Yet Fintech companies hold highly sensitive and regulated customer data and IP that must be protected. Identity and access management (IAM) therefore becomes a key area for success. Getting this right will lay the foundations for a thriving business. But it's not easy to do this yourself, which is why many leading organisations outsource this vital role to a trusted provider.

They found the right way forward with Identity as a Service (IDaaS).

What's driving agility in Fintech?

In an ultra-competitive marketplace, Fintech firms are pursuing digital transformation projects to become more agile. This need is being driven by several factors:

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

Cloud computing and the need for IAM

Many Fintech IT leaders have turned to cloud computing, as it supports 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 Fintech, with the cloud helping to accelerated their development and democratise their consumption.

Here are some of the key reasons why Fintech firms are using cloud infrastructure to support innovation-fueled growth:

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

Empowers small team: Allow Fintech firms to stay lean, doing more with less

Scalability/Elasticity: Helps support a more agile organisation and could also generate big savings

Supports anytime, anywhere, any device access: for a mobile, app-driven world

Given these business benefits, it's no surprise that over a third of firms have moved core business systems to the cloud, and that figure is likely to increase in the fast-moving Fintech sector.

The importance of cybersecurity

But none of this matters without security.

Fintech firms 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 or weak passwords.

Even more important is 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 could be tricked into clicking on convincing-looking phishing links designed to harvest their credentials. They could also send sensitive data in error to the wrong recipient outside the company. Malicious insiders are even harder to spot as they will do their best to cover their tracks. Some are motivated by money, while others by personal and professional grievances. Some may even take data with them to a competitor when they leave.

Some 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%). For Fintech firms, these problems are particularly acute. Why? Because these are companies with a 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

Security incidents could have huge financial and reputational repercussions for Fintech firms.

Regulatory compliance requirements are more onerous now than they've ever been. The forthcoming EU General Data Protection Regulation (GDPR) places strict new controls on consumer and employee data. From 25 May 2018 it will give the ICO the ability to fine firms up to £17m, or 4% of global annual turnover, whichever is higher.

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. Since 2014, security incident reports to the FCA have risen have risen 67%.

At a fundamental level, the effort of investigating, remediating and reporting incidents can impair business agility. That's why commentators often liken cybersecurity to brakes on a car: they're not there to slow you down, but to allow you to go faster more safely. In a similar way, effective cyber-tools enable Fintech firms to drive greater agility and growth rather than blocking innovation.

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

The problem with legacy tools

However, with the adoption of cloud- and app-driven approaches, legacy IAM solutions are no longer fit-for-purpose. On-premises 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 the kind of block on innovation that has given security teams a bad name in the enterprise over the years.

The average firm spends as much as 50% more time deploying on-premise IAM as cloud identity solutions. Plus, these legacy tools are unable to adapt to your cloud and app-based infrastructure as it grows over time. Costly new connectors must be build each time a new cloud app is added, adding as much as £75,000 per new integration, while the apps themselves will also require more maintenance and updates. The possibility of frequent, costly downtime is a risk no Fintech player wants to expose itself to.

The value of IDaaS

Cloud–based identity, or Identity-as-a-Service (IDaas), is the only smart choice when it comes to supporting the agile Fintech organisation. Quick and easy to set-up and deploy, it offers the kind of scalability and reliability that on-premise alternatives simply can't compete with. As Frost & Sullivan Senior Industry Analyst, Swapnadeep Nayak, says: "The shifting of enterprise solutions to the cloud has created a complex architecture that requires more advanced IAM solutions than the ones currently offered by traditional identity management vendors."

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.

> "The emergence of IDaaS has proven beneficial to enterprises, as it will assist with regulatory compliance, reduce the expenses involved in extending on-premise solutions to the cloud, and support the same features as enterprises' legacy systems."
>
> **Frost & Sullivan Senior Industry Analyst, Swapnadeep Nayak**

This is exactly what Okta provides, offering the following to Fintech firms:

- Single Sign-On (SSO) access across multiple applications and platforms
- Adaptive Multi-Factor Authentication (MFA) for enhanced security, with support for SMS, Okta Verify with Push, and third party providers like Google Authenticator and RSA
- 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)

According to IDG, over half of firms (57%) have already deployed IDaaS for SSO and employee portals, while a third are using it to support MFA.

A case in point: Funding Circle

One firm already reaping the benefits of the Okta Identity Cloud is innovative small business lender Funding Circle. The London-headquartered Fintech player has combined cutting edge cloud tech and homegrown risk models with credit assessment expertise and experience to great effect: having contributed an estimated £2.7 billion already to the UK economy. The challenge for the firm was to federate identities for 660 employees across its multiple cloud-based apps, managing and enhancing security for the extended enterprise and meeting compliance requirements while maintaining a consistent user experience.

Head of infrastructure Ayotunde Obasanya praises Okta's flexibility and ease-of-management.

"What that meant was the applications we wanted to integrate today, and potentially applications we wanted to integrate in the future, were already a part of their network," he says. "In terms of the security features we were looking for, in terms of the work flow management and automation, Okta [was] spot on."

The firm has seen an 80% reduction in helpdesk password reset requests for Okta-integrated apps, in part thanks to identity capabilities like SSO, which remove the need for users to remember multiple complex passwords. It has boosted security for 100% of employees with AMA, enabling the creation of robust access policies based on user data such as location, IP address or device. Automated provisioning has

driven significant productivity gains and IT savings—vital for a fast-growing company like Funding Circle—and offboarding is quick and easy through Lifecycle Management.

Empowering Fintech

Let's recap the benefits of the Okta Identity Cloud:

Supports Digital Transformation: Cloud-based identity will help to speed up your innovation agenda. Okta is designed to connect 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. Okta makes B2B collaboration easier and more secure 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, Okta makes web and mobile access secure, compliant, and frictionless.

The result is a solution which meets compliance requirements, reduces operational expenses and minimises security risk. This provides the ideal foundation agile Fintech firms need to innovate their way to success.