2021

CASE STUDY

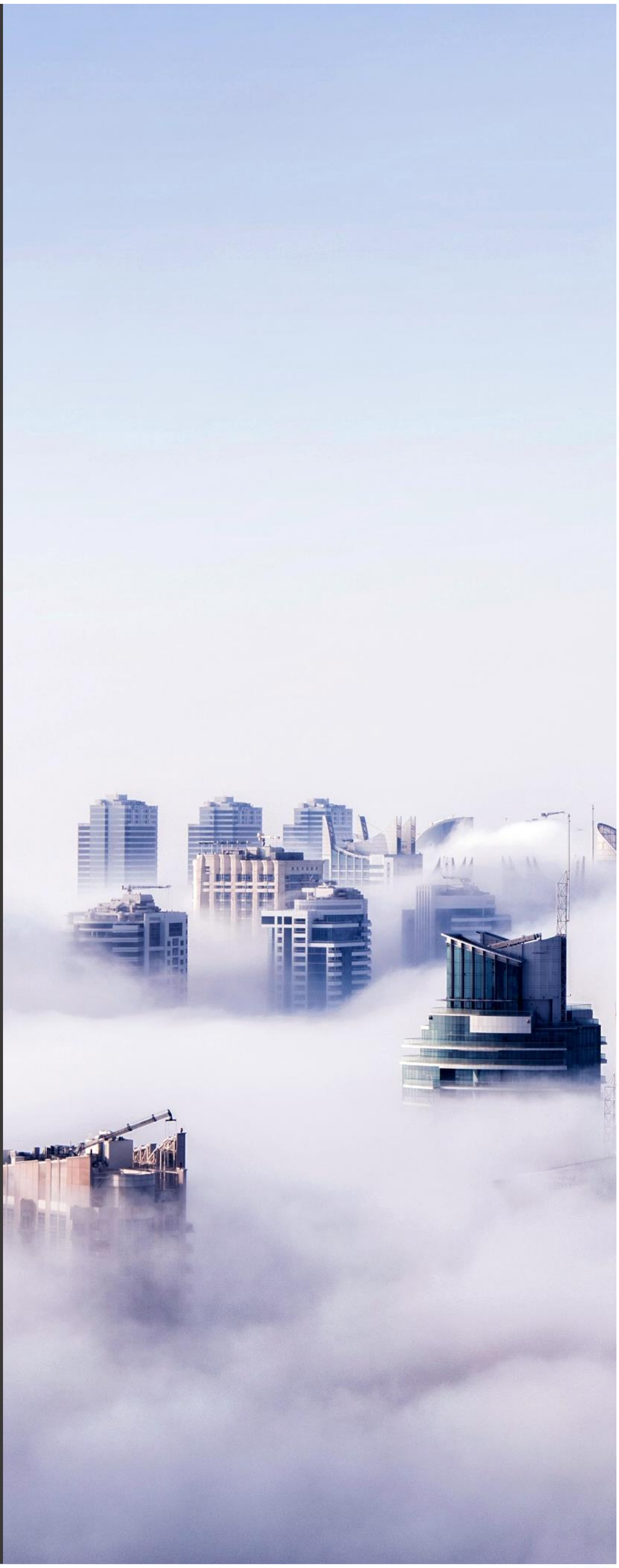
# Tailormade Solutions for a Global Leader in Fintech on Cloud

Infopercept

# Introduction

A global leader in investment banking and financial services, this company provides solutions to governments, corporations, and institutions alike in over 100 countries. It has a strong hold over consumer and commercial banking as well.

The company had plans to acquire a fintech company that delivers financial services through online banking, mobile apps etc. As is crucial in the banking sector, a lot of private and confidential information needs to be protected and safe-guarded against malicious attacks. The company was keen that all security requirements and compliance standards were met before the acquisition.



# The Problem

Traditional financial infrastructure is being replaced by digital technology that brings about a major paradigm shift in the use of old banking methods and services. A massive surge in numbers in the user database of the fintech services, fueled by the global pandemic has catapulted the use of technology that is largely dependent on cloud computing services. This leaves the firms vulnerable to malware attacks, data breaches, digital identity risk, application security risk, cloud-based security risks etc.

In order to cater to the growing database of customers using the fintech applications, the businesses need speed, agility and accuracy. This minimizes the use of local servers and increases dependency on cloud servers.

Secondly, for the acquisition to be complete it is imperative that all compliance standards also be met. The National Institute of Standards and Technology (NIST) set up by the United States Department of Commerce has framed guidelines to help organizations set up a cyber security framework which helps identify, detect and rectify cyber threats.  Auditing procedures such as System and Organization Controls (SOC) and ISO 270001 have to be in place in order to secure the business and protect the data and privacy of the clients.

## Infopercept - A Global Leader in Managed Security Services Provider (MSSP)

Infopercept was engaged to help identify security threats/loopholes in the fintech company. It also had to ensure that all compliance requirements were met for a smooth takeover by the parent company.

The Infopercept top management signed a retainer and assigned a *shadow CISO* to work in tandem with the CISO of fintech to overlook the work carried out. Together along with a risk/process team, they were able to resolve the security issues and straighten out the compliance requirements.

# Solutions

The Infopercept team decided to adopt the model of integrating development, security, and operation phases, often referred to as *DevSecOps*. This requires fusing the development of software applications with information technology, and simultaneously working on securing the infrastructure. The idea was to be able to address security issues even as they crop up and resolve them immediately. It makes the entire operation easy, fast, and less expensive. This enables the entire IT team to come together and shoulder the responsibility of securing the network.

Infopercept then set up a *Compliance Optimization Center (COC)* team to look after the compliance requirements. This ensured that all international professional standards were met for smooth and efficient business. Some of the functions of the COC were regular audits, management review meetings, random spot checks, etc.

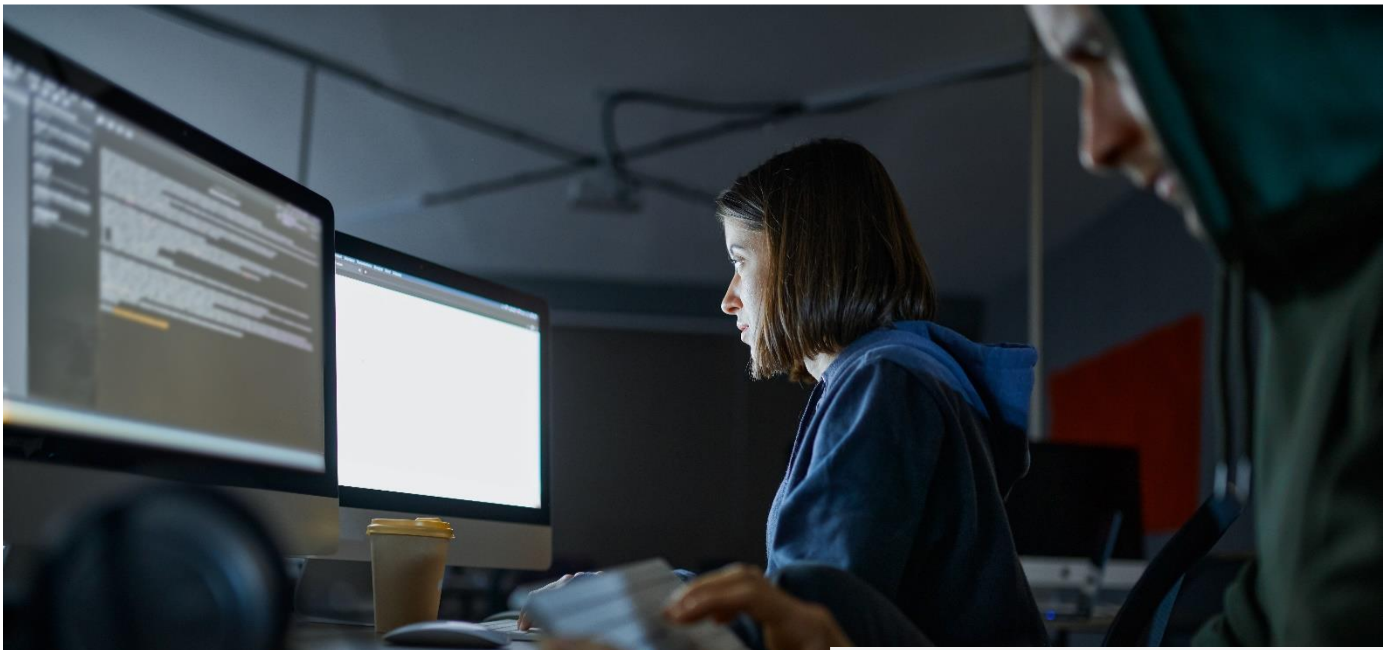
As most of the applications were cloud-based and *API (Application Programming Interface)* was used, it was critical to assess security risks periodically. A large amount of sensitive data is usually shared and exchanged among internal and external systems. A robust API management system was put in place by Infopercept to ensure that data is transmitted securely. A network is secure only as long as periodic checks are in place, as it is a continuous and ongoing process.

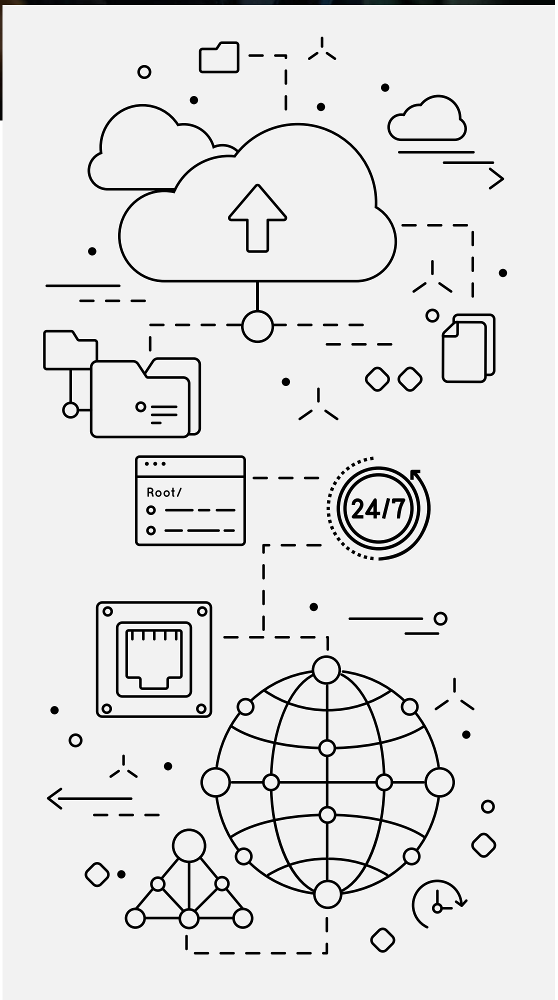
The application team is required to deliver the changes in codes frequently and reliably. For this purpose, a strategy of *Continuous Integration and Continuous Delivery (CI/CD)* was adopted. It is a coding policy that aids development teams to efficiently deliver minor changes in code.

Furthermore, as applications use different platforms and tools, it needed a mechanism to integrate and validate changes. The primary aim of CI was to automate the entire process so that teams involved were able to provide better software quality. An automated CD system further delivered the applications to selected environments.

A delicate balance had to be maintained while delivering quality code at top speed. For this purpose, a *static code analysis* was done. As an advanced practice, static code analysis not only saves time and money but also improves code security. While the application was up and running *dynamic code analysis* was established. It checked the code for quality, reliability and security even as the software was being executed. Dynamic code analysis helped prevent bad code from being executed and helped troubleshoot incidents while the code was in production.

# Security Operations Center (SOC) - 24X7





People, processes and technology come together to continuously monitor and improve an organization's cyber security posture. This includes either preventing threats or identifying, analyzing, and remediating them. A SOC ensures that all events that are logged in are continuously monitored. The events could be internet traffic, desktops, databases, applications, endpoint systems, etc. The security operation teams put together a collaborative effort to assess and defend against cyber hacks. In a nutshell, an SOC keeps activity logs, ranks events according to severity, takes proactive and reactive measures, provides updates and backup systems, oversees compliance requirements among other features.

## Benefits

Using the above mentioned practices, Infopercept was able to meet the security and compliance requirements of the fintech company in a short time. Having worked with large fintech companies in the past, Infopercept with its international exposure, was able to set up the DevSecOps cycle that kept the system running efficiently. The data was secured in the cloud environment using *Amazon Web Service (AWS)* cloud computing. It provided an **easy to use** platform, and a number of **cost-effective** solutions that were **reliable** and **scalable.**

### About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

### Imprint
© Infopercept Consulting Pvt. Ltd. 2021

### Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

### Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

### Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consu lting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Infopercept