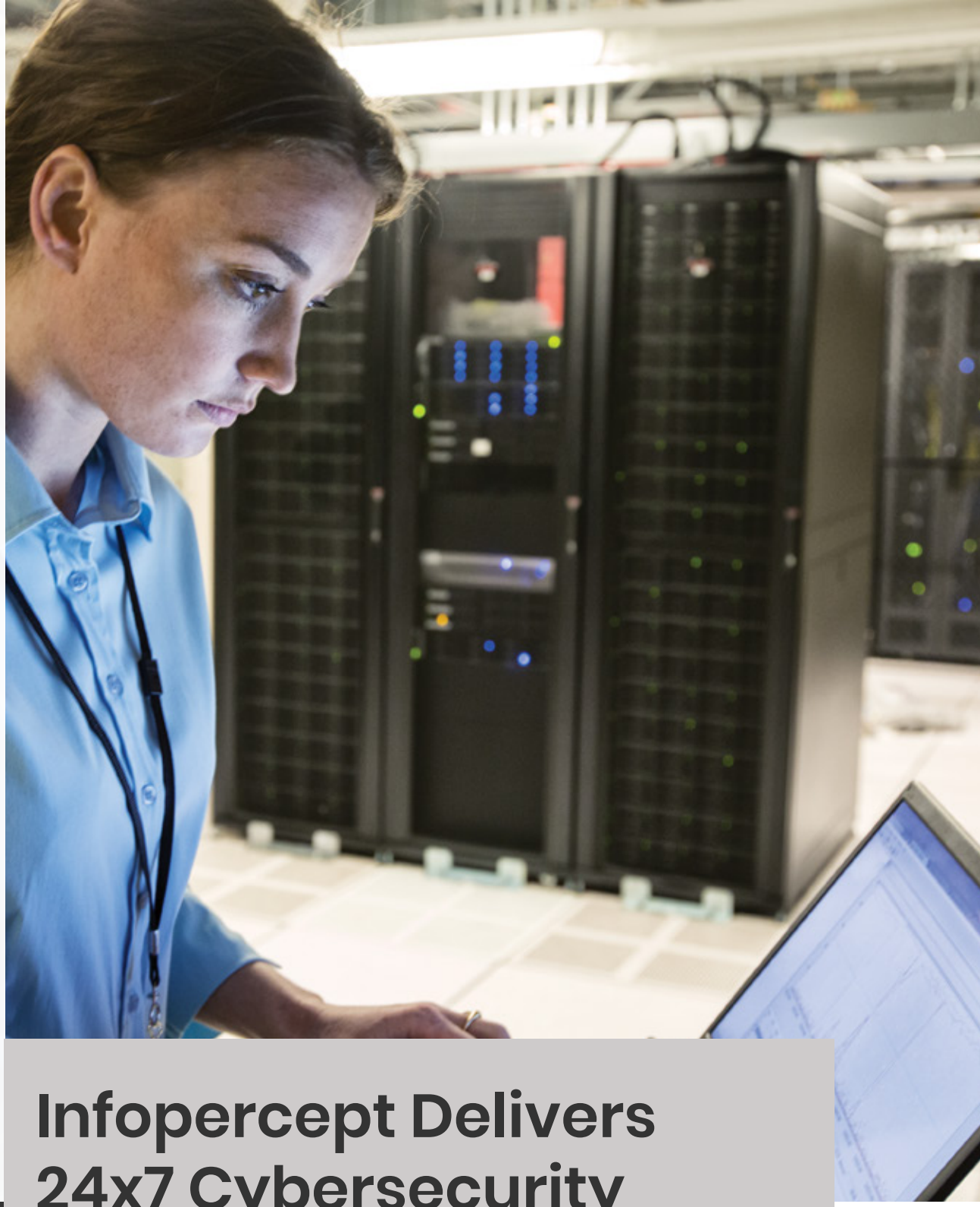
2020

CASE STUDY



Infopercept Delivers 24x7 Cybersecurity Coverage Across Multiple Cloud Scenarios to Global Fintech

Infopercept

CASE STUDY:

Background:

The client, a fintech with global footprint, associated with us when they were taking their first steps vis-à-vis platform development and in the process of giving a proof of concept to their target customers – banks and regulatory bodies. While the product was in its inception stage, the nature of the product meant that the parameters its efficacy would be judged on would be data security, vulnerability management, inherent strength of the architecture, risk mitigation, continuous risk assessment, compliance and more.

Since the relationship began in earnest right at the inception stage, we were able to conduct a thorough vulnerability assessment to identify and plug all security gaps. This gave confidence to the Fintech's target audience that the product had merit.

The Fintech and its platform climbed the next step in the approval ladder when banks and other bodies started getting interested in the platform. At every stage of the approval ladder, their area of concern revolved around the security framework and protocols in place to ensure complete data security.

Infopercept's continuous association with the Fintech ensured it could meaningful allay fears around data security as the company followed the security prescription carefully and diligently developed, implemented, monitored and optimized by us.

Challenges

- A cloud-based platform whose prospective clients were banks was always going to be highly scrutinized with respect to security protocols around data security; the client had to make a strong demonstrable argument for the product from the security perspective.

- As AWS was found to be the ideal cloud service to host the client platform, the challenge was to meet the security best practices of AWS that is 'of the cloud' security.

- Apart from meeting the demanding standards of AWS' 'of the cloud' security, achieving comprehensive 'in the cloud' security was a herculean task considering the scope and scale of the platform, as well as its, target users.

- The client wanted to cover all security bases and wanted a layered approach to security that had perfect synergy with one another. Considering the nature of the platform the layers needed to work towards achieving the highest standards of cybersecurity and maintaining these standards.

- A key challenge was multiple patches were pending across Operation Systems, Network, Application and there were configuration gaps in the current security posture.

- Banks and regulatory bodies require information on security compliance and health on a continuous basis and therefore the focus needed to be on a proactive approach to security that assesses security weaknesses and leverage a range of security technologies to plug vulnerabilities; optimizing the security ROI of these deployments and finally monitoring them 24x7 to ensure comprehensive visibility across the architectural framework and quickly responding to security incidents.

Solution

Infopercept and its team of cybersecurity warriors were associated with the fintech giant right at the inception stage itself, which gave us a significant advantage as we could evaluate security gaps right from the product development stage.

The initial platform was tested for architecture vulnerabilities, before it was presented to regulatory bodies and banks. We conducted a continuous security monitoring of the platform during development and kept watch on its security architecture. This meant, when the platform was deployed in its entirety, it met (and continues to meet) all industry-best security practices for cloud-based platforms.

The platform generated interest from the get-go, but the elephant in the room was 'data security'. The logical question was, "If all platform data is going to live in the cloud, how will it be protected?". As security advisors to the fintech, we were called for a meeting by the banks who had expressed interest in the platform. We conveyed our expertise in securing cloud deployments and took them through the various security controls we had already implemented (and planned to implement) for protecting confidential banking information that would be stored in AWS by our clients, and how these protocols can reduce the risk of data breaches.

Our in-depth presentation on securing client platform from both known/unknown advanced threats left room no doubt that that the platform's security framework was on point.

Security 'of the cloud'

With AWS, businesses get the benefit of a data center and network architecture built to meet the requirements of the most security-sensitive organizations. But it is businesses who must ensure that their cloud deployment is able to meet the demanding security standards set by AWS. We worked alongside the client to architect a security framework that seamlessly achieves the best practices underlined by AWS' 'security of the cloud'.

Security 'in the cloud'

We adopted a 4-pronged approach to secure the platform in the cloud.

- **Offensive Approach – Red Team Operations**

  We took the client platform and its cloud deployment through the paces to test weaknesses across its framework and deployment. These security gaps were then aligned with the right security solutions

- **Technology Deployment**

  The use of web application firewall, an intrusion prevention system sandboxing were the defensive technologies we implemented that give drill-down 24x7 monitoring, visibility and insights into all network traffic and also identify suspicious or malicious threats on the network to immediately prevent advanced attacks, hacks and breaches.

  Server Protection and endpoint protection (enhanced with moving target defense) and deception technology tools were pressed into services to deliver next level of threat hunting to detect both known and unknown threats.

A SIEM solution was also deployed that collects security log events from various sources, conducts centralized analysis and reports on all security related events. Another critical requirement from banks was monitoring the performance of all the security solutions and we picked an advanced performance monitoring tool to serve this purpose.

- **Security Solutions Optimization**

  Infopercept's team of security optimizers took the fintech's IT security team through a thorough process of technology onboarding and implementation and demonstrated ways and means to maximize the potential of the technology deployment. Patch management is also a critical component of this security layer and our services ensure that the fintech client isn't behind on any patch update.

- **Achieving Compliance**

  Any and every security deployment is useless if it does not help clients meet the needed compliance standards. Our team shadowed their existing Risk and Compliance team to understand the extent of compliance and then integrated security controls that met their compliance needs. This allowed us to fine tune their compliance strategy and helped support their needs to meet all requirements under ISO -27001. We also participated in their board meetings by providing VCISO services.

Additional Security Improvements

Right from the onset we believed that a single cloud focus is never a good idea and the client needed a cloud backup, incase they were not able to access their data in AWS for some reason or the other. We therefore developed an exhaustive disaster recovery plan by creating cloud infrastructure and data backup in Azure.

Result

The security component of the platform became a key driver of success as it drove trust and more participation from banks. From the initial 5 banks that joined the platform, our fintech client increased this number to 32. What's more, the critical auditing requirements as demanded by clients and regulatory authorities were achieved seamlessly, through real-time reporting and risk mitigation.

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

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

Infopercept