Secure cloud infrastructure provides powerful solution for card payment innovator

**Before**

When Coiney commenced operations, finding a secure cloud environment that satisfied PCI DSS was a big challenge.

**After**

The company used Amazon Web Services (AWS) and Trend Micro™ Deep Security™ to implement secure payment services and infrastructure within a month. PCI DSS compliance verification, a prerequisite for launching a payment business, was acquired quickly.

The launch of an enterprise to reform card payment services required a quick and secure infrastructure

“Unlike in the West, where card culture is firmly established, cash is still the dominant method of payment in Japan. Even in terms of retailers, credit cards can only be used at most large chains and department stores. Most small private stores do not accept them. I wanted to change that,” says Coiney founder and President, Naoko Samata, talking about of her company’s inception.

Coiney’s approach was simple. The company’s fundamental strategy was to use the information tools that we are comfortable with in modern life: smart phones. Smart phones can be used as credit card payment devices to promote “cashless enterprise” among businesses that up until now haven’t supported card payment, such as small retailers, restaurants, and salons.

There were a variety of hurdles when stores tried to support card payment in the past—credit checks performed by card companies while attempting to select a platform. She was particularly focused on security requirements.

But, because the security functions of AWS were not able to satisfy all of the approximately 360 requirements for PCI DSS, Samata adopted Trend Micro™ Deep Security™ to cover security needs not provided by AWS. Deep Security provided an Intrusion Detection System (IDS) and firewall, along with accompanying logs and records to satisfy the remaining PCI DSS compliance verification requirements.

Selection of AWS for PCI DSS compliance and fulfillment of additional security requirements with Deep Security was a requirement for starting the card payment service. Being able to fulfil this standard was a requirement for starting the card payment service. Coiney’s choice was a success. Cloudpack provided total support from the deployment and management on AWS to its operation and maintenance, and within a month, Coiney was able to completely implement its service in a production environment that included Deep Security.

After researching PCI DSS security requirements while utilizing cloud infrastructure, Coiney chose Amazon Web Services (AWS). The decisive factor in the selection was the platform’s security completely implemented into the company’s systems within 1 month.

Coiney’s technical team was able to complete compliance work to acquire PCI DSS compliance verification within 3 months. Secure services implemented within 1 month; Secure cloud infrastructure was acquired quickly.

Cointey’s fundamental strategy was to use the information tools that we are comfortable with in modern life: smart phones. Smart phones can be used as credit card payment devices to promote “cashless enterprise” among businesses that up until now haven’t supported card payment, such as small retailers, restaurants, and salons.

This allowed Coiney’s technical team to complete compliance work to acquire PCI DSS compliance verification within 3 months.

Outlook of Coiney’s service infrastructure utilizing Trend Micro™ Deep Security™
services, as well as requiring only a small investment when launching services.

These cloud characteristics were attractive to Samata when she started Coiney. “For startups like us with little money and time, utilizing the cloud is the best strategy. It was impossible to consider any other option,” she recalls. However, there were no other companies using the public cloud to develop and operate card payment services in Japan at the time. Consequently, Samata continued to negotiate with credit card companies while attempting to select a platform. She was particularly focused on compliance with PCI DSS (data security standards), since proving compliance with these standards was a requirement for starting the card payment service. Being able to fulfill this requirement promptly within a cloud infrastructure became the company’s greatest challenge.

Selection of AWS for PCI DSS compliance and fulfillment of additional security requirements with Deep Security

After researching PCI DSS security requirements while utilizing cloud infrastructure, Coiney chose Amazon Web Services (AWS). The decisive factor in the selection was the platform’s compliance with PCI DSS. In short, AWS was the optimum cloud service to fulfill the requirements to obtain verified PCI DSS compliance.

But, because the security functions of AWS were not able to satisfy all of the approximately 360 requirements for PCI DSS, Samata adopted Trend Micro™ Deep Security™ to cover security needs not provided by AWS. Deep Security provided an Intrusion Detection System (IDS) and firewall, along with accompanying logs and records to satisfy the remaining PCI DSS security requirements.

“Initially, we examined open source tools and security as candidates but speed and reliability were of paramount importance to us. Therefore, we selected Deep Security as it has a great track record, we didn’t have to spend time testing it, and it offers a variety of functions and tools in one package,” says Samata.

Secure services implemented within 1 month; PCI DSS compliance verification within 3 months

Coiney’s choice was a success. Cloudpack provided total support from the deployment and design on AWS to its operation and maintenance, and within a month, Coiney was able to completely implement its service in a production environment that included Deep Security. This allowed Coiney’s technical team to complete compliance work to acquire PCI DSS verification in only 3 months. The speed of this was astonishing as generally, “It’s a huge job that takes over a year,” says Samata. She adds that there have never been reports of trouble related to security management and operation and the company has high praise for the reliability and operability of Deep Security.

When moving to the public cloud, it’s critical to understand the shared responsibility model for security. Cloud providers will take care of infrastructure, but you are required to secure your workloads.

Deep Security efficiently solves high-priority security challenges in cloud environments, and features an exceedingly high return on investment. Coiney’s success story is a direct example of this.