FORTRA

CASE STUDY

Achieving Threat Visibility & Protecting Data Without Holding Back Expansion

PCI Pal provides Payment Card Industry Data Security Standard (PCI DSS) compliant solutions for contact centers taking cardholder not present (CNP) payments. Having operated from a private data center in the United Kingdom since 2012, the company launched a global cloud offering in 2016. PCI Pal Agent Assist allows contact centers to take credit card payments using telephone touchtone (DTMF) masking technology in a secure, compliant way.

Being a PCI DSS Level 1 Service Provider, PCI Pal must adhere to the stringent regulatory requirements set out by the major credit card providers, via the PCI Security Standards Council, which dictates how credit card information must be protected whilst being passed between the card holder and the merchant's bank.

Challenge

PCI Pal's original platform ran across three sites in London, Birmingham and Manchester, England, all of which were physically wired into local telephone exchange networks. As the company looked at expanding into Europe and the United States, it faced a major infrastructure challenge – it just wasn't going to be practical to directly manage the telephony infrastructure across those regions. PCI Pal required agility, automation, speed, and scalability, which is why the organization decided to move their business-critical applications to the cloud.

Since its initial cloud launch in London in 2016, PCI Pal has expanded rapidly and today has instances in the United States, Canada, Germany and Australia. Both the speed of deployment and ability to handle large scale telephony traffic with ease has been entirely due to re-engineering their telephony offering to utilize the power of Amazon Web Services (AWS) cloud environment.

Moving to AWS meant PCI Pal needed a security solution that would not only perform the same stringent security controls they had in place previously but would also allow for the granular yet holistic continuous monitoring that seamlessly supported the quick expansion that the company was undergoing. Geoff Forsyth, Chief Information Security Officer at PCI Pal, explained that initially the company did not have the workforce to tackle the very different model of

AT-A-GLANCE

Company	PCI Pal
Location	London, UK
Industry	Cloud Payment

"Knowing that Alert Logic's SOC is constantly monitoring the security of our systems gives me the peace of mind that I will receive a notification within minutes of anything suspicious happening, giving me the chance to address it and curb potential damages immediately. I could never employ enough people to provide this kind of service, and I can't put a price on that."

Geoff Forsyth | Chief Information Security Officer, PCI Pal

security that a public cloud environment required and so they outsourced the primary build to an expert third-party security partner whilst they built up their own in-house AWS infrastructure team. AWS operates on a shared responsibility model, providing the baseline security infrastructure on top of which PCI Pal could build its telephony, web, and payment gateway interfaces.

The protective measures in place on AWS cloud infrastructure provided PCI Pal with a solid security foundation, but to close the data security loop, they required additional security measures (such as an intrusion detection system and log management) to guarantee the maximum defense of their clients' sensitive credit card data. Essentially, PCI Pal needed an extra layer of protection against the eventuality that one of their barriers could be targeted.

"Moving to the cloud changed our whole approach to security," said Forsyth. "While previously we would have had to build a traditional ring-fence and network firewalls around the perimeter, when we moved to the cloud, all of that was already integrated into the Infrastructure-as-a-Service package. We needed an equally agile security solution that would protect all of the components of our service from potential threats, without holding us back in terms of set-up time."

Given the amount of sensitive data that pours into PCI Pal's AWS hosted servers on a daily basis, the company understandably has security at the forefront of its priorities. For this reason, the threat security monitoring they needed to put in place had to be continuous, able to detect incidents in real time and alert engineers as quickly as possible.

"A successful breach would effectively undermine our very mission: PCI Pal needs a security solution that reflects how seriously we take the protection of our customers' sensitive data," explained Forsyth. "Because so many credit card and financial information details pass over our networks, we are fully aware of the risks, and it is part of our commitment to our clients to make sure that our systems are as secure as they can possibly be."

Solution

After comparing Fortra's Alert Logic's solution to that of other security providers, PCI Pal opted for Alert Logic's fully managed and continuous threat detection and response offering. Alert Logic's solution turned out to be the one that offered the most comprehensive coverage, with 24/7 security monitoring of PCI Pal environments, a proven combination of network intrusion detection system, vulnerability management, and log management.

Additionally, the service comes with the expertise of security professionals who bolster the threat detection and hunting systems by filtering out any false positives and looking out for potential false negatives.

Summary

Alert Logic's scalable security solutions assisted PCI Pal in expanding its operations overseas, faultlessly and securely. Moving to a cloud environment made the process of setting up new locations much more agile. Alert Logic was able to add their security platform nodes to PCI Pal's environment to ensure that this happened in a secure manner without compromising deployment schedules.

"Alert Logic's systems can simply add further nodes to their security net, and there is very little configuration for us to do; we get instant reports if there are problems," Forsyth continued. "We deployed in the United States. We deployed to Canada. We deployed to the EU, in Frankfurt. We deployed to Sydney in Australia. It all went seamlessly and Alert Logic just scaled up to suit."

"The biggest advantage of Alert Logic's solution is the reassurance that there won't be a security incident happening without PCI Pal's knowledge. There is nothing that could damage us more than a breach going undetected for hours – let alone days. Knowing that Alert Logic's SOC is constantly monitoring the security of our systems gives me the peace of mind that I will receive a notification within minutes of anything suspicious happening, giving me the chance to address it and curb potential damages immediately. I could never employ enough people to provide this kind of service, and I can't put a price on that," Forsyth concluded.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.