ALERT LOGIC™

CASE STUDY

PCI Pal Achieves Threat Visibility And Protects Data Without Holding Back Expansion

Providing contact centres globally with the most suitable, operationally efficient and secure payment solution

PCI Pal is the provider of PCI DSS (Payment Card Industry Data Security Standard) compliant solutions for contact centres taking Cardholder Not Present (CNP) payments. Having operated from a private data centre across the UK since 2012, the company launched a global cloud offering in 2016. The organisation's leading product, PCI Pal Agent Assist, allows contact centres to take credit card payments using telephone touchtone (DTMF) masking technology in a secure and 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 dictate how credit card information must be protected whilst being passed between the card holder and the merchants bank.

PCI pal®

ABOUT

Customer: PCI Pal
Industry: Cloud Payment
Location: London, UK

The Challenge

Protecting The Surface in Depth

PCI Pal's original platform ran across three sites in London, Birmingham and Manchester, all of which were physically wired into local telephone exchange networks. As the company looked at expanding into Europe and the US, 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 re quired agility, automation, speed and scalability, and that is why the organisation 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 US, 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 utilise the power of Amazon Web Services (AWS) cloud environment.

Moving to AWS meant that PCI Pal needed a security solution that would not only perform the same stringent security controls they had in place previously, but that 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 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. 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," said Forsyth.

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. 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" explained Forsyth.

The Solution

Fully Managed, Continuous Threat Detection And Response To Provide Peace Of Mind

After comparing 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. The Alert Logic Security-as-a-Service 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.

Furthermore, Alert Logic's solution could be fully integrated with all the components of PCI Pal's solutions, such as telephony Session Border Controllers, but also application sites, web interfaces, session controllers and payment gateway interfaces.

Why Alert Logic?

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, and 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. We deployed in the US. 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," Forsyth continued.

In addition to being agile and scalable, Alert Logic's solution meant that PCI Pal could count on daily and weekly log collection and monitoring reports – produced by their Security Operations Centre (SOC) in Cardiff - which relieves enterprises of the burden of finding, hiring and retaining a large IT security function.

Since PCI Pal started using Alert Logic in October 2016, its security standpoint has remained solid: "Because of how much we invest in security, cyber threats rarely escalate. But whenever we run our own penetration tests, I tend not to inform Alert Logic, and I always receive a call from their engineers in Cardiff asking whether we are trying to breach into our own systems."

"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 in Cardiff 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.