Case Study

Security transformation and PCI-DSS compliance.

Project Name

PCI-DSS Security Transformation

Key Solutions

- Palo Alto Networks Next Generation Firewalls
- Palo Alto Networks Panorama
- Firemon
- Python

"Our aim was to renew compliance with PCI-DSS in a short period of time, but we achieved so much more with help from the team at Basis Networks.

Our business now has the confidence to roll our new digital initiatives on our network, and my operational team can now spend more time on activities other than producing compliance reports".

Client Project Manager

Background

The client is an organisation that provides mailroom management and advanced electronic services. They are responsible for the collection of information in various formats (both electronic and physical), its processing, and delivery.

As such, the information that resides and traverses the enterprise network may contain card holder data, and requires regulatory compliance with the Payment Card Industry – Data Security Standard (PCI-DSS).

Prior to this engagement, network and security infrastructure essential to compliance with PCI–DSS was managed by a third-party organisation.

Challenge

Establishing, maintaining, and demonstrating compliance with the approximately 300 PCI-DSS controls is an ongoing requirement for the customer, however complexity and lack of transparency and auditability made it difficult to assess and remediate the existing network and security solution to meet compliance obligations.

Additionally, the network and security technologies in place were only providing rudimentary protection and resiliency, and were inconsistently configured across the sites that required PCI-DSS compliance. This resulted in an environment that was not capable of mitigating against modern day threats, did not sufficiently protect the business, and was problematic and costly to operate.

Solution

Focussed

Basis Networks utilised our knowledge and experience with PCI-DSS compliance to analyse the existing environment and identify gaps that would need to be addressed as a priority. This process included a review of the devices that were in scope, and an assessment of how network segmentation may be introduced to reduce the number of system components and policies that must be brought into compliance.

Simplified

The team then rapidly developed a network and security architecture that focused on providing next-generation security capabilities across multiple sites, with simplified management capability, and an automated approach to compliance reporting.

The architecture catered specifically to the PCI-DSS card data environment, creating clear zones where application based policies and threat prevention would be applied to protect cardholder data.

Each site was provided their own Palo Alto Networks firewall pairs, with all sites being managed by a central Panorama security management platform. This approach enabled the deployment to be standardised and consistent across all locations, and provided unparalleled network and threat visibility, and vastly simplified operational management.

Phased

Implementing the new solution required multiple phases, with many being automated utilising Basis Networks developed toolsets. This approach was key in delivering the project in record time, and with minimal disruption to the business.

After migrating policy onto the new platform, Basis Networks analysed it for effectiveness and relevance, before an automated process of policy remediation was undertaken. This process removed unnecessary and insecure policies, and ensured all policies were standardised and labelled.

Each site was then cutover to the new solution in quick succession, with no reported issues.

Rapid

The transformation and remediation of the network and security architecture to meet PCI-DSS compliance was achieved in 14 weeks.

Enhanced

Early analysis had identified security to be inadequate for the criticality of data present on the network, so Basis Networks transformed the way security was applied across the enterprise.

This included the migration of firewall policy to enhanced application and user classified rules to provide granular inspection and enforcement for all traffic in to and out of the secure PCI-DSS zone. All traffic between sites was then encrypted using IPsec, with intrusion prevention enabled on all policies.

Automated

A common pain point for organisations dealing with PCI-DSS is the process for determining and proving compliance for auditing teams. This is typically a manual process requiring line by line reviews of security control points, device software versions, change management systems, and must be done twice a year to maintain compliance.

Additionally, the process of implementing new firewall policy can be complex and risk compliance if not implemented correctly. To resolve these challenges, Basis Networks introduced a number of automated capabilities:

1. Automated workflows for the design and implementation of firewall security policy. Using FireMon, policy changes can be automatically reviewed for compliance, created, deployed, and validated.
2. FireMon was also integrated into network and Palo Alto Networks security devices to automate the analysis and reporting on PCI-DSS compliance for all security policies. These reports are configured to run automatically, reducing the overhead with maintaining compliance.
3. PCI-DSS required all device software versions to maintained at specific levels, and consequently, interrogation of infrastructure is required to validate the current software versions, and to ensure non-compliant configurations are not present. Basis Networks developed a tool that runs at scheduled intervals and produces a compliance report for all devices in scope.

Products & Services

Basis Networks has built strong long-term relationships with global leaders in cyber security, and we use this to carefully choose the right technology for each customer.

The following products were deployed and services leveraged as part of this solution:

Products:

- Palo Alto Networks firewalls
    - Threat Prevention
    - GlobalProtect
    - URL Filtering

- Palo Alto Networks Panorama
- FireMon

Services:

- Business and Technology Requirements
- Current State Assessment
- Network and Security Architecture
- Network and Security Design
- Production Deployment and Configuration
- Project Management

"When Basis Networks said they could ramp up a team immediately and deliver within our very short timeframes we were sceptical.

Not only did they deliver on time, but the quality of the work was exceptional, and has resulted in them becoming our provider of choice for all network and security related work"

Client Project Manager

Results

The key outcomes of the engagement were successful compliance with the PCI-DSS, and the ability to easily report on and maintain compliance going forward.

Additional benefits to the customer included:

- A standardised, highly capable network and security architecture, deployed across several key locations.
- The ability to more rapidly deploy and modify security policy on the newer platforms deployed as part of the solution.
- A vastly improved security posture through the greater capabilities of the Palo Alto Networks next generation firewalls.
- Significantly more visibility into the network traffic traversing the new security platforms.
- Increased capability and resilience through the resolution of legacy network issues.
- An increase in confidence from the business in the ability to protect their critical customer data.
- The ability to extend security across additional sites and cloud services simply, and via a single management platform.

> *"The advanced capabilities of the new solution have given us confidence in our security posture, whilst also making it vastly easier and quicker to operate and report on the network."*
>
> **Client Project Manager**

Future Considerations

The architecture developed and deployed by Basis Networks was created to cater for a wide range of future capabilities, including; the adoption and integration of various cloud and SaaS platforms, the extension of automation capabilities, cloud based remote connectivity solution, and further segregation of non-PCI-DSS parts of the customer network.

To find out more about how Basis Networks can help your organisation, visit basisnetworks.com.au