



RETAIL PCI CASE STUDY

Foresite helped a retail client properly scope their PCI environment and outsource ongoing IT testing and monitoring requirements to meet updated compliance regulations.

INDUSTRY: RETAIL

BUSINESS CHALLENGES

- Confirming scope of Cardholder Data Environment
- Identifying gaps in compliance with new PCI DSS 3.0 standards
- Maintaining compliance for their 20+ retail locations without internal IT staff

FORESITE SOLUTIONS

- PCI DSS 3.0 Gap Assessment
- PCI DSS Managed Services
- ProVizion Security Monitoring & Alerting

OPPORTUNITIES

- Cardholder environment minimized through segmentation
- Managed Services to provide required quarterly and annual PCI testing
- ProVizion removes monitoring burden through outsourcing

THE DEAL

A large retail restaurant chain had contracted with us to perform PCI ASV scanning. The client had been gaining momentum since 2008, and was experiencing substantial growth. Since that time, they had expanded, and added restaurants to the group that were not fully aware of (or compliant with) all of the PCI requirements that were applicable to them, thus causing the entire organization to fall out of compliance.

Foresite's Threat Mitigation Team initiated a discussion to review the new PCI DSS 3.0 requirements. During this discussion, it became clear to the Chief Operating Officer that the expanding business, in conjunction with the evolving PCI DSS controls, left significant gaps in the organization's ability to achieve compliance.

Foresite proposed a PCI DSS 3.0 Gap Assessment to help them confirm what was in place, and what problems they would need to remediate in order to achieve compliance

THE COMPETITION

Part of the client's standard operating procedure is to obtain 3 proposals to compare before signing off on any work. Foresite faced a challenge when the client's payment provider told them that they could use their vendor for a turn-key compliance solution. After several group calls with the client, payment provider, and the vendor, Foresite was able to

provide sufficient evidence that there is no turn-key solution for PCI compliance, and in fact, there were numerous gaps in the vendor's offering, including ongoing testing and monitoring required to achieve compliance.

The client also had a very low-cost quote for network security monitoring, and chose not to select that solution due to the vendor's lack of understanding of how complex their environment is with 20+ retail locations. In the end, Foresite's PCI knowledge and willingness to help them evaluate competitive solutions set us apart from the competition, and we were chosen to perform all PCI-related work.

SOLUTIONS

The PCI DSS Gap Assessment confirmed the correct PCI merchant level for which the chain should file, and also identified that proper segmentation could minimize the scope of their cardholder data environment, saving them tens of thousands of dollars and ongoing audit and testing costs.

Through PCI Managed Service agreement, our client is able to outsource ongoing requirements for PCI compliance to us, including:

- Quarterly ASV and internal vulnerability scans
- Wireless testing
- Annual penetration testing
- Assistance with completing SAQs
- Real-time monitoring of firewall logs
- Outsourced Security Operations team for "as needed" Incident Response

ABOUT FORESITE

Foresite is a global service provider delivering a range of managed security and consulting solutions designed to help our clients meet their information security and compliance objectives. In the face of increasingly persistent cyber-threats, Foresite's solutions empower organizations with vigilance and expertise to proactively identify, respond to, and remediate cyber-attacks and breaches where they occur.

Our team of industry veterans work as an extension of our clients' staff providing peace of mind while securing their most important assets. For more information, visit us at <http://foresite.com> or contact us at info@foresite.com.