CUSTOMER SUCCESS STORY

Royal College of Physicians
Setting higher medical standards

Royal College of Physicians Sails Past PCI Exam

About Royal College of Physicians

The Royal College of Physicians of London (RCP), a registered charity based in the United Kingdom, is a professional membership organization dedicated to ensuring that doctors are educated and trained to the highest of standards, and that patient care is delivered consistently with maximum quality. To help meet this aim, RCP, which represents more than 21,000 Fellows and Collegiate Members, provides education, training, medical examinations, and other services that aim to further the practice of medicine.

Strong security essential for new Web infrastructure

The IT department of Royal College of Physicians of London runs the medical examination Web site on behalf of the Federation of Royal Colleges of Physicians of the UK. When the department sought to make certain its new Web site met PCI DSS compliance, it turned to Barracuda Networks, which acquired leading Web application and security vendor NetContinuum in 2007, and found a way to not only meet Payment Card industry Data Security Standard (PCI DSS) requirements, but also to simplify the management of its entire Web DMZ architecture.

Further, when RCP readied the rollout of its new Web infrastructure, it wanted to be certain all 14 of its Web sites were deployed and maintained as securely as possible. The rollout kicked off with the launch of a new e-learning site dedicated to providing physicians easy access to educational resources and support, as well as an enhanced site for the Membership of The Royal Colleges of Physicians of the United Kingdom, MRCP (UK), on behalf of the Federation of Royal Colleges of Physicians of the UK. The MRCP (UK) site provides physicians with all of the information they need to take the three-part MRCP (UK) examination enabling physicians to apply, register, as well as pay for their exams, and receive their results all on one site.

Virtualized Web architecture and PCI Data Security Standard compliance

RCP expects several million pounds of transactions to flow through the site, with most payments conducted by credit card. Therefore it was crucial that the examination site be highly secured to protect the privacy of the physicians' personal information as well as the availability of the applications, and the site had to be PCI DSS compliant before it could go live.

Like most organizations, RCP operates on a tight budget with IT support and development teams closely integrated. Building an end-to-end Web infrastructure that was easy to manage and maintain was essential. With that goal in mind, RCP decided to architect and build a virtualized Web server farm. The internally-hosted Web architecture comprises six servers, or blades, including a VMWare management server, a server dedicated to the management of RCP's domain addresses, and four servers that make up the virtual server farm. In addition, the Web applications are based on Microsoft Windows SharePoint Services 3.0.

"This architecture makes it easy for us to centrally manage our SharePoint front-end, the mid-tier systems, as well as our backend databases," said Christopher Venning, IT network and support manager at RCP.

The issue yet to be solved was how RCP could give its new architecture the highest level of security and availability possible, and be able to prove to a team of external auditors that it met PCI DSS compliance, as required by its acquiring bank. Like its Web site architecture, RCP wanted its security to be centrally managed and to feather well with the virtualized application server infrastructure.

"PCI compliance was a strict requirement from the bank. We had to be able to show our compliance before we would be able to conduct transactions," said Venning.

> *"As part of the process members use to register for examinations, we collect a variety of information, including credit card data. The banks insisted that our Web systems were PCI compliant. Barracuda Networks helped us to get there without a struggle."*
>
> -Christopher Venning
> Network Manager
> Royal College of Physicians

Barracuda Application Gateway NC-1100 AG Fast Facts:

- Easily helps organizations comply with PCI DSS requirements
- Delivers best practices security out of the box
- Single point of protection for inbound and outbound traffic for all Web applications
- Protects Web sites and Web applications against application layer attacks
- Monitors traffic and provides reports about attackers and attack attempts

Of particular importance to RCP was PCI DSS version 1.1, established by the independent PCI Security Standards Council in September 2006. This version included significant changes in how the standard addresses Web application security. For instance, the updated version requires all custom-built application software to be reviewed by an application security specialist for vulnerabilities, or that merchants that accept or store credit card transaction information deploy a Web application firewall.

Venning and his team carefully examined a number of ways to fulfill these standard requirements while maintaining the highest levels of security, including deploying a network firewall, a Web application firewall, or a load balancer, as well as securely managing all of the individual routers and switches in their infrastructure. But none of the architectures they investigated seemed to be easily manageable.

"Everything seemed more complex than it needed to be," said Venning. "We really needed a single point of control for the whole DMZ environment."

While RCP evaluated its options, its solution provider, Matrix Communications Systems, recommended that it look at the application firewalls and gateways provided by Barracuda Networks. Following a careful appraisal, RCP chose to secure its entire application architecture with the Barracuda Application Gateway NC-1100 AG. The Barracuda Application Gateway NC-1100 AG combines best-in-breed application firewall technology with full-load balancing and traffic management that includes connection pooling, caching, compression, and application acceleration from within a single appliance.

"The installation went flawlessly," said Venning. To meet all of its security and high-availability needs, the RCP deployed two Barracuda Application Gateway NC-1100 AG appliances: one dedicated to protect all of its live Web traffic, and the second as part of its fail-over strategy in the event something goes awry with the primary device.

Comprehensive Web application security and streamlined PCI compliance

With the complete implementation of the Barracuda Application Gateway NC-1100 AG, RCP's Web applications are protected from increasingly prevalent forms of attack, including buffer overflows, SQL injections, cross-site scripting, forms tampering, cookie and session stealing, and a multitude of other Web application attack techniques.

Equally important, the Barracuda Application Gateway NC-1100 AG helped RCP easily pass its first two PCI DSS compliance audits. After completing both the e-Learning and MRCP (UK) examination sites, RCP had those sites audited independently to validate that they met the specification. In addition, the device helped RCP streamline the audit process which requires everything to be documented, including configurations for everything from firewalls to routing and switching.

"With this setup, I only have one sheet for the audit, not a raft of documents," added Venning.

Web application security for the long haul

RCP is currently bringing a dozen additional sites online, each is protected by the Barracuda Application Gateway NC-1100 AG.

"The administrative framework is very well suited for front ending a virtualized server environment," said Venning. "Adding new applications behind the Barracuda Application Gateway NC-1100 AG is very easy."

With the Barracuda Application Gateway NC-1100 AG Venning and the RCP IT team no longer have to worry about rapidly spreading, new application threats, or significant portions of the PCI DSS standard.

"With Barracuda Networks we realized that these appliances not only help us to achieve PCI compliance, but also simplify our network infrastructure," said Venning. "As an added bonus, we have improved availability and simplified our management."

About Barracuda Web Application Controllers

Barracuda Web Application Controllers, including both the Barracuda Web Application Firewall and Barracuda Application Gateway, protect Web sites from attackers leveraging protocol or application vulnerabilities to instigate unauthorized access, data theft, denial of service or defacement. Designed to deliver comprehensive Web security, the Barracuda Web Application Controllers acts as a proxy for Web traffic to insulate Web servers from direct access by hackers, enforces data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS), and secures Web sites against the top 10 major Web vulnerabilities compiled by Open Web Application Security Project (OWASP).

Barracuda Networks, Inc.
www.barracuda.com
info@barracuda.com