

## PCI DSS Section 6.6 Compliance

In June of 2008 the PCI council required compliance to section 6.6 of the DSS. This section outlined the need for a third party code review, or the implementation of a web application firewall. The significance of these two options is that for many companies compliance can be extremely difficult and cost prohibitive. The first option of code review, while thorough may prove difficult if the application is older and undocumented. Bringing in a third party to conduct a review of this nature can be time consuming and may result in overlooked issues. If performed properly however, this is an excellent road to choose, but it will require resources, time, and money. The alternative path is to leverage the network level protections of a web application firewall or WAF. This technology sits in front of a web application and buffers it from attack. The cost and steep learning curve however can be a deterrent to small IT staff that may not have the time to dedicate towards setup and maintenance. With SaaS becoming increasingly common this does not have to be the case. CT Infosec has designed and built a cloud based web application firewall offering allowing companies the protection of an onsite WAF without the burdens created by such a deployment. Keeping this layer in the cloud has several advantages such as 24/7 monitoring, reduction in maintenance, lowered bandwidth costs, and the expertise of full time Infosec staff. It has also been shown that a properly deployed WAF will protect against threats in the event that developers have not had their code reviewed before deployment. Cloud computing is an excellent answer for today's growing networks. The WAF SaaS model fits perfectly into today's web and PCI compliance needs. For companies looking for quick, dependable and low maintenance solutions, they should pay strong attention to these offerings.