

PCI Compliance in the Cloud: What are the Risks?

Ward Spangenberg, Director of PCI and Compliance

It is no surprise that the emergence of cloud computing and virtualization are creating a noticeable buzz across the IT space. As the market puts pressure on companies to increase productivity and decrease capital investments, solutions like distributed computing, that offer scalable systems with low overhead, are attractive options for management to consider. However, when you are responsible for the security of your network, the thought of migrating everything to an environment you don't actually own or control probably makes you cringe.

By now you've undoubtedly heard the mantra: "know where your data is, and know where your data is going." This concept is the cornerstone to data security, and plays a significant role in achieving and maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS). Most of the requirements hinge upon a merchant's ability to implement network access controls, and periodically test their effectiveness, which may be difficult to do in a cloud platform, where the underlying infrastructure is outsourced.

So how does a company leverage the benefits of cloud systems without jeopardizing security, or PCI compliance? The same way you would approach any new technology: by understanding the architecture, and selecting a platform that exposes you to the least amount of risk.

Cloud systems essentially come in three sizes: software as a service, platform as a service and infrastructure as a service. Each level has its own benefits and challenges.

At the top of the pyramid, you have software as a service. Everything is provided and managed for you, limiting the scope of your PCI exposure. The catch here, is you still pay for the work the vendor does to maintain their compliance.

In the next layer, platform as a service, you have more opportunity to benefit from the power and flexibility of the cloud. However, you also assume more risk. The vendor provides the application programming interface (API), leaving you responsible for developing and securing your web applications. This is where it gets tricky, because until someone can present a clear demarcation point between the application, virtualization and the physical layers and the controls offering protection between them, no Qualified Security Assessor (QSA) can really say the system is compliant.

In this case the merchant's argument might be that they are using a shared hosting provider. In shared hosting the provider is generally responsible for managing servers, installing server software, security updates, technical support, and other aspects of the service. However, housing data in a hosting environment does not automatically impose the requirements for data security upon the hosting provider.

This translates to one of two options: either the merchant proves they are using a hosting provider that complies with the PCI; or the merchant assures they can manage their own systems in accordance with PCI. I have yet to meet a shared hosting provider who is willing to accept the liability of PCI compliance in a cloud environment. Examine a typical user agreement for a cloud hosting plan, and you will find it is primarily concerned with up time. There is no mention, or guarantee, of security. There are, however, restrictions on conducting port scans for vulnerabilities and penetration testing, both of which are required to pass PCI scans.

The introduction of services like Amazon EC2 and GoGrid shift the focus from the middleware layer to a raw infrastructure as a service model. The challenge here is the technology is ahead of the PCI requirements. Cloud platforms rely heavily on virtualization, and most QSAs are struggling with how to interpret the PCI requirement of running one primary function per server in a virtualized environment. The simplistic view is to demand that merchants run exactly one service on one machine, however, this defeats the purpose and benefits of virtualization.

The way around this stalemate is to simply build your web applications on the cloud, but leave your payment gateway in more traditional hands. Whether you use a third-party credit card processing service, or handle payment functionality through a trusted application on your own network, you can effectively firewall with your API through an SSL wrapper and encryption. Employing a hybrid of cloud and traditional architecture gives you the best of both worlds.