



## Virtualization Security & PCI Compliance

By David de Valk, Reflex Systems

Virtualization of x86 computing platforms has rapidly become one of, if not the most, significant computing technologies of the last 10 years. Server virtualization adoption is rapidly growing and expected to significantly increase in the next 3 to 4 years where upwards of 50 percent of all servers will be virtualized. Fueling this dramatic shift is the tremendous and quantifiable benefits provided by virtualizing servers, including reduced CAPEX & OPEX, energy savings, increased flexibility, improved disaster recovery, better systems management, and of critical importance increased security.

As organizations evaluate, plan, and adopt virtualization strategies it is critical to take a holistic approach that includes thoughtful analysis of not only what business applications can benefit from virtualization but also what 'IT applications' can benefit from virtualization. In the same manner that an organizations' email, print, file server, and functional business systems benefit by embracing virtualization as a trusted computing platform, so can specialized 'IT applications' such as security. By adopting such an approach organizations are able to extend virtualizations benefits, protect and increase their virtualization ROI and increase overall data security. For organizations that have specific compliancy requirements, such as the Payment Card Industry (PCI) Data Security Standard, this approach yields both increased levels of compliancy as well as lower overall costs of compliancy.

The PCI Data Security Standard provides specific requirements based on industry best practices for maintaining secure systems and applications. Included in the requirements are numerous network security features and functions such as network firewalls, intrusion detection/prevention systems, application firewalls, patch management, and logging systems. These systems are critical to ensuring network security and overall data security far beyond just those systems that are required to be PCI compliant. This is best illustrated by the increasing trend of organizations adopting the PCI standard for protecting private information such as employee and customer data. It is here that by adopting virtualization as a trusted computing platform and implementing the PCI mandated network security features and functions within the virtual infrastructure organizations are not only able to maintain PCI compliancy at a lower overall cost, but they are also able to increase their overall network security for no or little incremental cost.

Virtual Security Appliances provide the required features and functions mandated by PCI. While many of the features and functions parallel those currently available in physical security devices, Virtual Security Appliances are purpose built and designed to meet unique virtualization security challenges. Physical security devices residing outside the virtual infrastructure may be able to provide basic levels of visibility and

control, but they provide zero visibility and control within the virtual infrastructure. Additionally, Virtual Security Appliances are able to take advantage of virtualization as a trusted computing platform to enable customers to adopt and deploy "defense in depth" best practices without the traditional high costs and complexities of physical infrastructure.

Through a holistic view and approach to virtualization, that includes products purpose built and optimized for virtualized environments, organizations are able to not only maintain their PCI compliance but also improve their overall data security through the virtualized data center.

To learn more about virtualization management, security and PCI Compliance view an informative Webinar given by several leaders in virtualization, including Citrix, Reflex Security, and Fortisphere. The Webinar is free and is available by visiting [http://www.reflexsecurity.com/reflex\\_podcasts\\_download.php](http://www.reflexsecurity.com/reflex_podcasts_download.php) .