



QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

## **Security Control Variations Between In-House and Cloud-Based Virtualized Infrastructures**

Virtualization-related components (such as Hypervisor, Virtual Network and Virtual Machines [VMs]) in a virtualized data center infrastructure need effective security controls. However, the differences in scope of control (among stakeholders) over this component set between in-house and cloud-based virtualized infrastructures introduce variations in security control measures that can be deployed by the respective stakeholders.

This paper, from the National Institute of Standards and Technology, analyzes those variations and their efficiency and security impacts. The authors also suggest technology enablers that can minimize those impacts and improve the overall security robustness of the basic computing units of a virtualized infrastructure (i.e., VMs).

Use this detailed NIST document to help guide your own virtualized infrastructure security measures.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- Security Control Variations Between In-House and Cloud-Based Virtualized Infrastructures.pdf