Virtualization has dramatically reduced IT costs while greatly improving efficiency. Now businesses need rapid access to IT resources to support faster time-to-market. IT needs to deliver this while ensuring that the data center is fully managed and secured. VMware vCloud® Suite is an integrated set of products that includes the basic components you need to build a private cloud infrastructure and operationalize your VMware vSphere® virtualized environments.

VMware vCloud Networking and Security™ provides networking and security capabilities for virtualized compute environments built using vCloud Suite. It provides a broad range of services delivered through virtual appliances, such as a virtual firewall, virtual private network (VPN), load balancing, NAT, DHCP and VXLAN-extended networks while also providing a comprehensive framework to integrate third-party solutions.

These foundational networking and security capabilities of the vCloud Suite enhance operational efficiency, improve agility with control and enable extensibility to partner solutions. Management integration with VMware vCenter Server™ and VMware vCloud Director® reduces the cost and complexity of data center operations.

With vCloud Networking and Security and integrated VMware partner solutions, enterprises can:

- Virtualize business-critical applications with confidence.
- Build secure and agile private clouds.
- Secure VMware Horizon View™ deployments.

This solution brief describes the security and compliance considerations for each of these initiatives, and how VMware solutions and products address them.

### Solution Overview

#### Protect Business-Critical Applications

As organizations continue their journey to the cloud, they virtualize more of their business-critical applications. It follows that ensuring the security of these applications becomes a crucial step in cloud adoption. In a virtual environment, organizations need to have visibility into the traffic between virtual workloads. They need their critical applications and databases protected from threats from less secure or un-patched systems. And they need to implement audit and compliance controls on in-scope hosts. The challenge is to ensure security and compliance while still maintaining flexibility and the ability to scale rapidly.

VMware solutions support compliance objectives and protection of applications in the virtual data center, without compromising the benefits of cloud computing. They enable organizations to create business-based security groups and protect critical applications from network-based threats. The App Firewall component of vCloud Networking and Security provides adaptive security that travels with virtual machines as they migrate from host to host. This approach makes it easy for customers to support applications belonging to different trust levels in the same virtual data center, and ensures that proper segmentation and trust zones are enforced for all application deployments. Organizations gain visibility into and control over network communications between virtual machines. Policy enforcement is agile, because it is based on logical constructs centered on the workloads to be protected, and not on infrastructure constructs such as IP addresses or VLANs.

Ensuring configuration compliance of the underlying VMware infrastructure and in-scope virtual servers is another critical concern of organizations deploying business-critical applications to the cloud. VMware vCenter™ Configuration Manager™ is a full featured server-configuration and compliance-management solution. It automates critical configuration and compliance management tasks including configuration-data collection, change execution and reporting; change auditing; compliance assessment; patch management; OS provisioning; and software package distribution. vCenter Configuration Manager capabilities ensure the infrastructure that underlies your business-critical applications is hardened against security best practices, vendor hardening guidelines, and regulatory mandates such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX).
Finally, a shared virtual infrastructure raises concerns about the ability of an organization to identify and protect sensitive business information. Exposure or leakage of such data (e.g., credit card information or health records) can cost an enterprise millions of dollars and harm its reputation. The data security component of vCloud Networking and Security enables organizations to identify sensitive business information on unstructured file shares and ensure that it is protected. With a large number of pre-defined templates for country and industry-specific regulations, it quickly identifies and reports on sensitive data exposures. It also improves performance by offloading data discovery functions to a virtual appliance.

Secure Your Private Cloud

Today more and more organizations are leveraging the benefits of private cloud computing to increase flexibility and reduce costs. Yet many have not changed their traditional approach to architecting networks and security. Physical networking and security topologies severely limit flexibility and the ability to scale. They are not virtualization-aware, making it all too easy to become noncompliant as changes occur in a dynamic infrastructure. Also, a heavy reliance on hardware-based solutions leaves organizations with multiple special-purpose appliances, each with its own interface. The lack of a common management interface adds to the cost and complexity of maintaining the security of virtual data centers.

VMware vCloud Suite reduce the complexity of private clouds by enabling organizations to deploy virtualization-aware networking and security infrastructure. The VXLAN component of vCloud Networking and Security, in conjunction with VMware vSphere Distributed Switch (VDS), creates layer 2 logical networks across non-contiguous clusters or pods, without the need for VLANs. VXLAN requires multicast to be turned on. VXLAN enables customers to scale their applications across clusters and pods and improve management and utilization of compute resources across physical network boundaries. It also reduces manual networking provisioning and simplifies deployment by eliminating VLANs.

The Edge component of vCloud Networking and Security delivers an operationally efficient, simple and cost-effective security-services gateway to secure the perimeter of the virtual data center. The included load balancer helps manage inbound web traffic across virtual machine clusters. The Edge virtual appliance delivers other gateway services as well, such as network address translation (NAT), remote access and site-to-site VPN and DHCP. Fully integrated with VMware vCenter Server™ and VMware vCloud Director®, Edge enables role-based access control and separation of duties as part of a unified framework for managing virtualization security.

Secure Virtual Desktop Deployments

Virtual Desktop (VDI) deployments are growing rapidly, but VDI introduces new security challenges. Since virtual desktop solutions consolidate desktop processing onto centralized servers, resource intensive tasks like virus scanning can have a significant impact on performance. Legacy virus scanning approach can necessitate additional server hardware and resulting in lower consolidation ratios. Virtual desktops also need proper access controls, to limit third-party extranet users from accessing internal resources that they shouldn’t.

VMware enables optimized antivirus and anti-malware security for virtual environments via integration with VMware partners. VMware vShield Endpoint™, part of vShpere 5.x, allows security technology partners to offer more efficient antivirus and anti-malware protection for virtual hosts, including VMware Horizon View desktops. It does so by offloading antivirus and anti-malware functions from individual virtual machines to a centralized secure virtual appliance that protects the host and all virtual machines on it. This approach streamlines security management and provides added protection against antivirus “storms,” performance bottlenecks and botnet attacks.

In order to control access within VDI environments, the App component of vCloud Networking and Security is used to create logical security perimeters around virtual desktops. This capability ensures that VDI users can only access applications and data they are authorized to use. It also prevents unauthorized access into the VDI desktops from the rest of the network.

VMware capabilities, along with trusted solutions from VMware partners, ensure that enterprises can virtualize business-critical applications with confidence, build secure and agile private clouds and secure Horizon View deployments.

Learn More

For more information please visit http://www.vmware.com/products/datacenter-virtualization/vcloud-suite/features.html