RACKSPACE MEETS NEW PCI DSS COMPLIANCE WITH VMWARE NSX NETWORK VIRTUALIZATION

rackspace®
the #1 managed cloud company

INDUSTRY
MANAGED CLOUD COMPUTING

LOCATION
SAN ANTONIO, TEXAS

KEY CHALLENGES
- Segregate environments to support PCI DSS 3.1 compliance.
- Protect internal VMware vCenter deployments from customer systems.
- Implement solution quickly without burdening network team.

SOLUTION
Rackspace quickly deployed a virtual distributed firewall solution using the micro-segmentation capabilities of VMware NSX network virtualization to segregate PCI DSS systems from non–PCI DSS systems and customer and internal Rackspace environments.

BUSINESS BENEFITS
- Full PCI DSS 3.1 compliance for all internal systems, providing enhanced security
- Fast software-based deployment without burdening other networking teams
- High-performance with no added latency

Rackspace, a leading managed cloud company and a Premier Service Provider in the VMware vCloud® Air™ Network program, needed its internal infrastructure and systems to meet the new requirements of the new Payment Card Industry Data Security Standard (PCI DSS) version 3.1. Rackspace quickly deployed a virtual distributed firewall solution using the micro-segmentation capabilities of VMware NSX® network virtualization to further segregate customer and internal environments to comply with PCI DSS 3.1, the information security standard for organizations that handle major credit cards such as Visa.

Rackspace helps businesses tap the power of cloud computing without managing complex infrastructure on their own. As one of VMware's largest vCloud Air Network Service Providers, Rackspace manages tens of thousands of VMware-based virtual machines (VM) and has VMware Certified Professionals available every day of the year, around the clock, to support customers worldwide.

The Challenge

In June 2009, Visa approved Rackspace as a compliant Level 1 Payment Card Industry service provider and audits the company annually to ensure continued adherence to the requirements of the PCI DSS. Compliance is critical for keeping customer systems secure and separate and to support the company's ongoing business operations and fast-paced growth.

The Rackspace Virtualization Support team has deployed more than 100 VMware vCenter™ instances spanning eight data centers with more than 1,000 virtual machines for its back-end management and support infrastructure. "With a mindset of making things more secure for PCI compliance, we decided we had to segregate those environments," explains Luke Huckaba, a principal architect at Rackspace. More specifically, to meet the new PCI DSS requirements, Huckaba wanted an environment where "two adjacent VMs side by side on the same layer 2 subnet cannot communicate with each other."

Per Thorn, a virtualization architect at Rackspace, explains another issue: "Previously, we had a relatively flat vCenter management network to manage PCI and non-PCI environments. For PCI compliance we needed to ensure proper controls were in place to protect that network."

"We are able to isolate the PCI systems from the rest of the environment without having to re-IP anything or physically change any networking."

LUKE HUCKABA
PRINCIPAL ARCHITECT
RACKSPACE

VMWARE FOOTPRINT

- VMware NSX
- VMware vSphere
- VMware vCenter
- VMware vRealize Operations Manager

PLATFORM

- Dell PowerEdge R720 and HP ProLiant DL380 Gen9 servers
- EMC VNX and VMware Virtual SAN™ storage
- Cisco switches and firewalls

At first, the team's idea was to use physical firewalls, but that would have been extremely complicated and expensive to implement. It also would have required the help of other networking teams that were in a separate organization and incredibly busy with their own objectives. The Rackspace Virtualization Support team had a short time scale in mind for the PCI DSS compliance project, wanting to build and deploy a solution in just two or three months.

The Solution

The support team realized that the only practical option was to go virtual. "Instead of re-IP-ing the systems and using physical firewalls, which would require new routing, virtual networks, and all that entails, we decided it would be easier and better to deploy a distributed firewall," Huckaba explains. The team briefly considered Palo Alto Networks but decided to go with the VMware virtual firewall, driven by the strength of its existing VMware relationship.

Victor Sandoval, a VMware global cloud architect and VMware Certified Design Expert, worked onsite and helped Huckaba plan the solution, developing information flows and defining firewall rules and security policies. "He helped us design everything, every bit of traffic, so we could see exactly what our traffic flows will look like," says Thorn. "We spent a month planning out the traffic and policies, and that planning really helped us," concurs Huckaba.

At the same time, the Rackspace team was also moving toward a new management system, updating to VMware vSphere® 6.0u2 with VMware vCenter 6.0u2. This update would require NSX network virtualization for the vCenter deployments. So Rackspace also rolled out NSX 6.2.2 in what Huckaba calls a "retrofit deployment," tacking the NSX solution on top of the existing management infrastructure.

Once deployed, Rackspace was able to take advantage of the micro-segmentation capabilities of the NSX 6.2.2 network virtualization platform to meet the new PCI DSS compliance requirements. "We used NSX to micro-segment the environment, specifically to isolate the PCI systems and non-PCI systems," says Huckaba. With that segmentation, he says, "nothing can talk into those PCI systems unless they are explicitly allowed to. We are able to isolate the PCI systems from the rest of the environment without having to re-IP anything or physically change any networking."

Business Benefits

The new VMware NSX solution, which runs on top of existing Rackspace infrastructure and management systems, gives Rackspace the ability to create and manage flexible security policies aligned to virtual networks. NSX network virtualization supports the Rackspace Software-Defined Data Center (SDDC) approach to network security, embedding security functions right into the hypervisor. Rackspace now delivers micro-segmentation and granular security to each individual workload, enabling a fundamentally more secure and fully PCI DSS–compliant environment, while also maintaining flexibility and agility.

The fast software-based deployment didn't require network team support, new physical hardware, or physical network changes. Deployment went perfectly for the first two data centers. After they quickly resolved a small hiccup with the third data center, "deployment then continued flawlessly for the rest of our eight data centers," Huckaba says. The entire project from planning to full deployment took just eight weeks.

Huckaba says it would have taken many more months if they had made physical changes. Thorn agrees: "It was much, much easier to achieve by using NSX." Huckaba also knows the systems would have taken a performance hit with the additional bottlenecks of the physical option. Instead, the NSX solution takes advantage of the simulated 10Gb throughput directly on the host. "The latency introduced by NSX is in single-digit microseconds," says Huckaba. "As far as I'm concerned, NSX doesn't introduce any real latency."

Looking Ahead

Rackspace continues to rely on much of the VMware data center stack, including the VMware vRealize® Operations Manager™ solution for operations management, as the company adds an average of 1,000 new VMware VMs every month for new customers. Later phases of the NSX project may include extending the micro-segmentation and virtual firewall capabilities to include intrusion prevention capabilities and zero-trust application and user-aware-based security policies provided by virtual firewalls from partner companies.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com