



# Meeting PCI DSS Compliance in Virtual Environments with Vyatta Network OS

As virtualization technology continues to change the datacenter and deliver new cloud computing models, it is more important than ever to understand its impact on compliance requirements. The PCI Security Standards Council has delivered guidance on recommended security measures to meet the Payment Card Industry Data Security Standard (PCI DSS) in virtual and cloud environments. This paper describes how Vyatta helps businesses to meet the security requirements recently published in a report by the PCI Security Standards Council's Virtualization Special Interest Group (SIG). This report outlines detailed recommendations and best practices for everything from risk assessment strategies to technology selection.

Vyatta enables customers to closely follow specific guidelines from this report, by providing an integrated software solution for deploying advanced networking and security in the virtual data center and cloud. This functionality includes Layer 2 and 3 traffic forwarding and routing, stateful firewall, VPN and IPS, optimized specifically for any virtual environment.

The PCI Virtualization SIG has identified four key principles related to virtualization of infrastructure that houses payment card information.

## CASE STUDY

### Securing Cardholder Data Transmissions for Delta Sonic Car Wash

"Vyatta allows Delta Sonic Car Wash Systems to segment the network, so cardholder data transmissions are secure from any VoIP, video, or other data flowing across the network. In addition, Vyatta has enabled Delta Sonic Car Wash Systems to secure internet-facing virtual machines in its Citrix Xen-Server-based virtual datacenter."



### PCI DSS Guidelines - Key Principles

- a. If virtualization technologies are used in a cardholder data environment, PCI DSS requirements apply to those virtualization technologies.
- b. Virtualization technology introduces new risks that may not be relevant to other technologies, and that must be assessed when adopting virtualization in cardholder data environments.
- c. Implementations of virtual technologies can vary greatly, and entities will need to perform a thorough discovery to identify and document the unique characteristics of their particular virtualized implementation, including all interactions with payment transaction processes and payment card data.
- d. There is no one-size-fits-all method or solution to configure virtualized environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented.

To conform to the PCI DSS standard in virtual environments, the PCI Security Council report outlines detailed recommendations and best practices for everything from risk assessment strategies to technology selection. The two key points highlighted in this report that Vyatta Network OS enables users to address are outlined below.

## ISOLATE SECURITY FUNCTIONS - PCI DSS Virtualization Guidelines Section 4.1.5

**Problem:** Migrating applications and data into virtual and cloud environments forces administrators to rearchitect network controls and isolation schemes that already exist in the physical network, since The movement of applications and data to a virtual server infrastructure makes using traditional firewalling, VPN and IPS deployed as hardware devices difficult, if not impossible, to replicate physical network security policies in the virtual datacenter.

### PCI DSS Guidance - Isolating Security Functions

"The security functions provided by VMs must be implemented with the same process separation required in the physical world."

"Preventive controls such as a network firewall should never be combined on a single logical host with the payment card data it is configured to protect"

"Processes controlling network segmentation and the log-aggregation function that would detect tampering of network segmentation controls should not be mixed"

"If security functions are to be hosted on the same hypervisor or host, the level of isolation between security functions should be such that they can be considered as being installed on separate machines"

**Vyatta Solution:** The Vyatta Network OS allows users to have a single software and virtualization optimized security solution that can run on x86 hardware or within a hypervisor as needed, enabling users to realize the benefits of consolidation and automation that are inherent to virtualization while solving any proximity issues introduced by hardware-based solutions.

For customers required to maintain isolated process separation policies in the hypervisor, the Vyatta Network OS can be deployed on a per-server or on a per-customer basis. A Vyatta virtualized architecture delivers to each individual department or customer, a fully isolated network security stack running as a completely separate virtual instance within the hypervisor from other logical hosts, with VPN for data encryption -- enabling not only secure data in transit, but the required logical separation between network controls and the data they are configured to protect.

In addition, security administrators can deploy additional instances of Vyatta, this one with Vyatta IPS enabled, to monitor and identify network reconnaissance and intrusion attempts, and to suppress anomalous traffic such as propagation-type attacks, effectively preventing compromises to customer data privacy. As a separate virtual instance, the IPS-enabled instance of Vyatta runs alongside the Vyatta firewall instances in the hypervisor, but with complete logical separation from any Vyatta firewall instances within that hypervisor.

Any and all virtual Vyatta deployments consist of fully isolated security functions – each Vyatta system is installed or imported as a specific hypervisor container template and provisioned on any x86-based virtual hardware, rendering it a specific, fully isolated virtual appliance, equivalent to running on a separate physical x86 hardware platform.

## EVALUATE VIRTUALIZED NETWORK SECURITY FEATURES

- PCI DSS Virtualization Guidelines Section 4.1.12

**Problem:** Not all virtual network security solutions are created equal. Feature and function checklists are not an adequate evaluation of virtual security options. To properly secure next-generation dynamic environments, a security solution must be engineered as a complete operating system and optimized for virtual environments to define and enforce policies in the same way that physically separate devices would. A virtual network security solution must be optimized for the chosen hypervisor to properly leverage virtual and physical server resources that are available to it for proper isolation, performance and auditing.

### PCI DSS Guidance - Evaluating Virtualized Network Security Features

“Any deployment of virtualized network infrastructure should include effective security measures at the data plane, control plane, and management plane”

“Isolation between virtualized network devices should be such that the virtual systems can be effectively regarded as separate hardware.”

“Each virtualized device should maintain individual and independent access-controlled configurations.”

“Audit trails for virtual infrastructures should be granular and detailed enough to identify individual access to and activities performed on each specific virtual component.”

“Access controls should enforce least privilege, both individually for each device and across the entire platform.”

**Vyatta Solution:** The Vyatta Network OS has been designed from the ground up to leverage x86 system resources and is the only network virtual machine optimized for all popular virtualization hypervisors.

The data plane, control plane, and management plane for each Vyatta system (for each virtual machines network security functions) are completely isolated at the virtual hardware layer, IP space and VPN tunnel endpoints and management, and routing tables / firewall rules – both logical and physical. Each Vyatta system uses completely separate virtualized x86 hardware resources – CPU, memory allocation, hard disk and network interfaces, so that each Vyatta system can effectively be regarded as a discrete virtualized hardware appliance.

Configuration data and management for each Vyatta instance is completely separate and involve separate system kernel- and user-space isolation. Within the Vyatta system, the configuration database and management plane, including logging subsystem, are dedicated to that instance alone, and is completely independent of any other virtual machines or virtual services running on that hypervisor.

**Conclusion:** Vyatta’s application-centric approach to networking delivers the industry’s most comprehensive solution for complete migration of firewall, VPN, IPS and dynamic routing to virtual environments. Vyatta ensures that organizations can segment, isolate and secure data to meet the compliance requirements of next-generation virtual environments. Following the best practices from the (PCI Security Standards Council report (LINK)) and implementing the Vyatta Network OS as virtual machines can ensure your organization maintains compliance with PCI DSS requirements.