ACHIEVING PCI DSS COMPLIANCE

WITH RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that was created in 2004 by the five major credit card companies: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The PCI DSS standard seeks to prevent credit card fraud by requiring the implementation of certain controls and processes by all entities involved in the processing of credit cards. The five founding credit card companies subsequently formed the Payment Card Industry Security Standards Council (PCI SSC) in 2006. Since the formation of the council and the establishment of the security standard, cardholders have benefited from increased protection of both their personal information and their assets. Complying with the standard, however, has proven to be challenging for the entities required to do so. This paper will illustrate how Red Hat Enterprise Virtualization for Desktops can help these organizations comply with specific PCI DSS mandates while increasing overall efficiency and agility.

OVERVIEW OF REGULATIONS

PCI DSS applies to all organizations that hold, process, or pass cardholder information from any credit card branded with the logo of one of the participating company brands. This includes the financial institutions issuing the cards, the merchants accepting payments from cardholders, the financial institutions accepting payment on behalf of the merchants, and the entities operating the networks on which all of these transactions take place. The standard mandates the protection of two types of data:

- **Cardholder data**
  Name, account number, expiration date
- **Sensitive authentication data**
  Magnetic stripe data, card validation code, and personal identification number (PIN)

The primary distinction between these two types of data is with regards to storage. PCI DSS explicitly forbids the storage of sensitive authentication data following a transaction, even if that data is encrypted. Cardholder data, on the other hand, can be stored, as long as it is done so in accordance with the standard.

PCI DSS outlines twelve requirements that must be met in order for an organization to be considered compliant. These requirements cover a wide range of system components found in a cardholder data environment, and they are grouped into six categories:

- **Build and maintain a secure network**
  Requirements 1 and 2 specify the use of network protection technologies and techniques, password policies, and controlled systems configurations.
- **Protect cardholder data**
  Requirements 3 and 4 specify what data may be stored and transmitted and in what form.
- **Maintain a vulnerability management program**
  Requirements 5 and 6 contain broad-reaching mandates regarding anti-virus technologies, patch management, secure application development, change control procedures, and web application protection.
- **Implement strong access control measures**
  Requirements 7, 8, and 9 specify controls related to identity and access management, both electronic and physical.
- **Regularly monitor and test networks**
  Requirements 10 and 11 mandate regular and comprehensive auditing and assessment of all systems and networks upon which cardholder data is stored or transmitted.
- **Maintain an information security policy**
  Requirement 12 mandates the development and implementation of a comprehensive security policy that clearly outlines the responsibilities of employees. The development of a rigorous incident response procedure is also mandated.

Requirements 3 and 9 present a unique set of challenges to organizations with broad deployments of laptops, desktops, and portable media that are used by employees who have access to cardholder data. Often times this data ends up on these devices, which are then moved outside of organizations' physical boundaries. This mobility makes it extremely difficult to ensure the security of cardholder data or to maintain an accurate inventory of it.

In order to more easily comply with requirements 3 and 9, a new deployment model is needed for the laptops and desktops used by organizations governed by PCI DSS. This new deployment model needs to be one in which cardholder data is easily protected, inventoried, and disposed.

RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

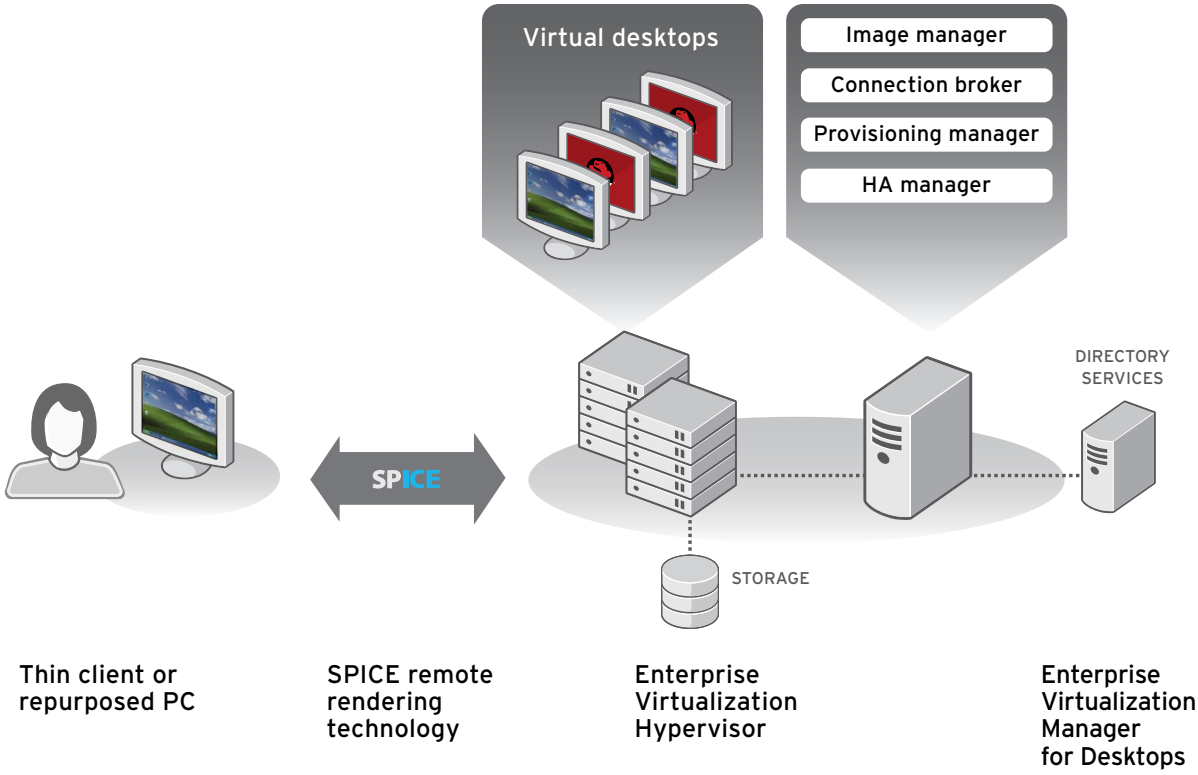
The traditional model used by organizations to deploy desktop computing involves the use of personal computers. Each of those PCs has a fully featured operating system installed on it, usually either Windows or Linux, that provides all of the basic computing operations and functions. Applications such as word processors, spreadsheet programs, and web browsers are then installed on top of that operating system to provide users with the tools that they need to perform their jobs. All of the data associated with the operating system and the applications is stored on the internal hard drive of the PC itself.

With Red Hat Enterprise Virtualization for Desktops, the operating system and applications that make up a user's desktop environment actually reside on servers located in a centralized datacenter. Users connect to these desktop environments, known as virtual desktops, using a thin client with a network connection and a minimal amount of software installed upon it. Unlike with traditional desktop deployments, no data is stored on these thin clients. This type of architecture is referred to as hosted desktop virtualization.

Red Hat Enterprise Virtualization for Desktops is an end-to-end desktop virtualization solution featuring everything an organization needs to deploy virtualized desktops:

- **Red Hat Enterprise Virtualization Hypervisor**
  A standalone, high-performance, secure hypervisor based on the Red Hat Enterprise Linux kernel with Kernel-based Virtual Machine (KVM) technology.
- **Red Hat Enterprise Virtualization Manager for Desktops**
  A centralized management console with a comprehensive set of management tools that administrators can use to create, monitor, and maintain their virtual desktops.
- **SPICE (Simple Protocol for Independent Computing Environments)**
  An adaptive remote rendering protocol able to deliver an end user experience comparable to that of a physical desktop.
- **Integrated connection broker**
  A web-based portal from which end users can log into their virtual desktops.

FIGURE 1: RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS



By moving desktop environments off of the endpoint and into the datacenter, Red Hat Enterprise Virtualization for Desktops helps organizations more easily address the specifications set forth in PCI DSS. Many of the specifications found in Requirements 3 and 9 are either addressed or made irrelevant with this new architecture:

- **Requirement 3.1** mandates that organizations "keep cardholder data storage to a minimum." With Red Hat Enterprise Virtualization for Desktops, the footprint of cardholder data is essentially reduced to that of the servers in the datacenter on which the virtual desktops are hosted, making it easy to comply with this requirement.
- **Requirement 9.6** mandates that organizations "physically secure all paper and electronic media that contain cardholder data." Because fewer computers actually store data in a Red Hat Enterprise Virtualization for Desktops deployment, fewer machines need to be physically secured. Additionally, datacenters are typically outfitted with numerous layers of physical security, including access cards and rack locks. This means that the the virtual desktops residing on servers in those datacenters are often already physically secured.

- **Requirement 9.8** mandates that organizations "ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals)." With Red Hat Enterprise Virtualization for Desktops, the laptops and desktops deployed by organizations can be mobile, but the cardholder data for which they're responsible is not. These endpoints can be absent of any storage media, making this requirement irrelevant.

- **Requirement 9.9.1** mandates that organizations "properly inventory all media and make sure it is securely stored." With Red Hat Enterprise Virtualization for Desktops, organizations know exactly where cardholder data resides at all times—in the safety and security of their datacenters.

- **Requirement 9.10.2** mandates that organizations "purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed." Due to the reduced footprint of cardholder data in a Red Hat Enterprise Virtualization for Desktops deployment, disposal policies and procedures only need to be implemented for a small number of servers, as opposed to a vast number of deployed end points and portable media devices.

In addition to helping organizations address requirements 3 and 9, Red Hat Enterprise Virtualization for Desktops is designed in such a way that it does not introduce anything that would violate compliance with the standards set forth in the other PCI DSS requirements:

- **Requirement 4.1** mandates that organizations "use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks." Red Hat Enterprise Virtualization for Desktops uses Secure Sockets Layer (SSL) technology to encrypt all communication between virtual desktops and the end point devices used to communicate with them.

- **Requirement 8.1** mandates that organizations "identify all users with a unique user name before allowing them to access system components or cardholder data." Red Hat Enterprise Virtualization for Desktops integrates directly with Active Directory, leveraging the unique user identities and policies that many covered entities already have in place.

BEYOND COMPLIANCE

In addition to helping organizations achieve PCI DSS compliance, Red Hat Enterprise Virtualization for Desktops offers the following benefits:

- **Increased manageability**
  With Red Hat Enterprise Virtualization for Desktops, desktop environments can be centrally created, monitored, and managed, reducing or even eliminating the need for on-site support in remote offices or retail locations.

- **Increased business agility and continuity**
  By eliminating the dependencies between the operating system and the underlying hardware, Red Hat Enterprise Virtualization for Desktops allows organizations to defer desktop replacements and their associated costs. Additionally, this separation allows different operating systems to be accessed from the same device.

A TRUSTED PARTNER

With a history of over 15 years of providing enterprises with the most secure operating system in the world, there is no better choice than Red Hat for organizations looking to achieve PCI DSS compliance using hosted desktop virtualization. Additionally, Red Hat Enterprise Virtualization for Desktops offers several other unique capabilities and characteristics:

- **Density**
  Industry-leading algorithms for memory management allow organizations to maximize the number of virtual desktops on a single host.
- **Cross-platform guest support**
  Support for virtual instances of Red Hat Enterprise Linux Desktop allows organizations to virtualize both Windows and non-Windows desktops.
- **Established partner ecosystem**
  An inherited legacy of over 1,000 certified hardware systems ensures compatibility with current and future systems.
- **Part of a comprehensive virtualization platform for both desktops and servers**
  A common infrastructure allows organizations to manage their complete virtual environments—both desktops and servers.
- **Open source**
  No other vendor is as well positioned and suited to bring the power and value of open source to virtualization infrastructures. KVM is open source today, and other components will be made open source in the future.

CONCLUSION

The requirements outlined in the PCI DSS require that organizations dealing with credit card information take decisive action to safeguard that information. Red Hat Enterprise Virtualization for Desktops represents a new desktop deployment model that significantly simplifies the task of complying with some of the requirements set forth in PCI DSS. By reducing their cardholder data footprint and centralizing all data in their datacenters, organizations are able to achieve this compliance while at the same time increasing the manageability and agility of their laptop and desktop deployments.

RED HAT SALES AND INQUIRIES

NORTH AMERICA
1-888-REDHAT1
www.redhat.com

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

LATIN AMERICA
+54 11 4341 6200
www.latam.redhat.com
info-latam@redhat.com

www.redhat.com
#1295885_1009