



ACHIEVING GLBA COMPLIANCE

WITH RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

The Gramm-Leach-Bliley Act (GLBA) was introduced into U.S. law in 1999. The main intent of the GLBA was to open up financial markets by repealing some portions of the Glass-Steagall Act of 1933. A secondary objective of the act was to ensure the privacy and protection of individual financial information by requiring financial institutions to institute appropriate controls and procedures. These requirements have introduced additional complexity into the operations of these organizations and have forced them to rethink how they store, transmit, and dispose of customer data. This paper will illustrate how Red Hat Enterprise Virtualization for Desktops can help organizations comply with specific GLBA mandates while increasing overall efficiency and agility.

OVERVIEW OF REGULATIONS

GLBA seeks to protect the nonpublic personal information (NPI) of individuals. NPI is defined as financial information collected by a financial institution that is personally identifiable and not otherwise available in a public forum. NPI includes:

- Information provided by an individual applying to receive a financial product or service. Examples include name, address, Social Security number, and income.
- Information received from a transaction involving a financial product or service. Examples include account numbers, balances, credit/debit charges, and payment history.

GLBA applies to any type of financial institution, which it defines as any entity that is “significantly engaged” in “financial activities.” These activities include but are not limited to the following:

- Lending, brokering, or servicing any type of consumer loan
- Transferring or safeguarding money
- Preparing individual tax returns

- Providing financial advice or credit counseling
- Providing residential real estate settlement services
- Collecting consumer debts

GLBA also applies to any entity that receives NPI from a financial institution. A company who purchases a customer list from a financial institution for marketing purposes, for example, is required to implement the same controls and procedures as those that are required for the originating financial institution. The reach of GLBA, therefore, goes well beyond those organizations that consider themselves to be operating in the financial services sector.

There are two primary regulations of GLBA:

- **The Privacy Rule**
Governs the collection and disclosure of NPI and requires that financial institutions periodically provide their customers with a written notice describing their privacy policies and practices.
- **The Safeguards Rule**
Requires that financial institutions design, implement, and maintain safeguards to protect NPI.

The Safeguards Rule does not outline specific implementation guidelines for organizations to follow. It is instead designed to be flexible, requiring only that organizations implement safeguards that are appropriate to their environments and operations. As such, organizations are encouraged to consider several factors related to the storage, transmission, and disposal of NPI. Some of these considerations present a unique set of challenges to organizations having broad deployments of laptops, desktops, and portable media that are used by employees who have access to NPI. This data often ends up on these devices, which are then moved outside of the organizations' physical boundaries. This mobility makes it extremely difficult to ensure the security of NPI or to maintain an accurate inventory of it.

In order to more easily comply with GLBA, a new deployment model is needed for the laptops and desktops used by organizations governed by the Safeguards Rule. This new deployment model needs to be one in which NPI is easily protected, inventoried, and disposed.

RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

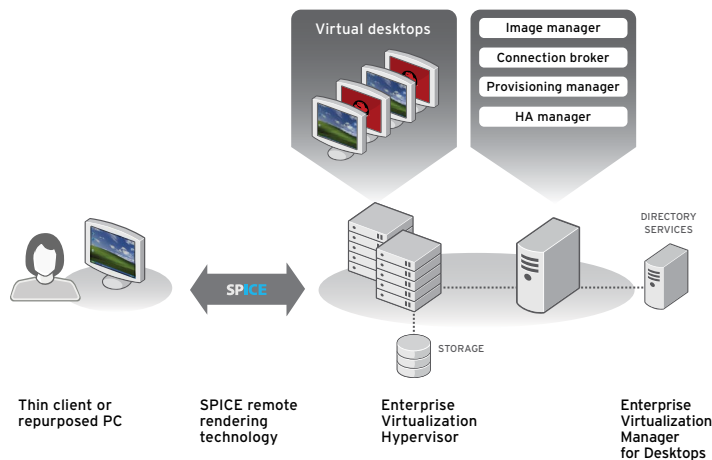
The traditional model used by organizations to deploy desktop computing involves the use of personal computers. Each of those PCs has a fully featured operating system installed on it, usually either Windows or Linux, that provides all of the basic computing operations and functions. Applications such 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 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 following GLBA recommendations:

- **Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use.**

With Red Hat Enterprise Virtualization for Desktops, stolen laptops become a non-issue, as all data – operating system, application, and user – is stored within secure datacenters. If a thin client is lost or stolen, those who recover it will gain access to nothing more than the hardware itself.

- **Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home.** With Red Hat Enterprise Virtualization for Desktops, employees can access NPI remotely, without that data ever leaving the datacenter. There is therefore no need for those employees to keep any NPI at home.

- **Know where sensitive customer information is stored and store it securely.**

With Red Hat Enterprise Virtualization for Desktops, organizations know exactly where NPI resides at all times – in the safety and security of their datacenters.

- **Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.**

Due to the reduced footprint of NPI in a Red Hat Enterprise Virtualization for Desktops deployment, disposal policies and procedures only need to be implemented for the servers and storage infrastructure on which the virtual desktops are hosted, as opposed to a vast number of deployed end points and portable media devices.

In addition to helping organizations address these recommendations, Red Hat Enterprise Virtualization for Desktops is designed in such a way that it does not introduce any-

thing that would violate compliance with the standards set forth in the other GLBA requirements:

- **Take steps to ensure the secure transmission of customer information.**

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.

BEYOND COMPLIANCE

In addition to helping organizations achieve GLBA 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 GLBA 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 that can be hosted 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 GLBA mandate that organizations dealing with personal financial 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 recommendations set forth in the Safeguards Rule of GLBA. By reducing their NPI footprints 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

ASIA PACIFIC

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

EUROPE, MIDDLE EAST AND AFRICA

00800 7334 2835
www.europe.redhat.com
europe@redhat.com

LATIN AMERICA

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