SAFEGUARDING YOUR DATA

WITH RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

www.redhat.com

WHY NOW?

The need to protect sensitive data has increased dramatically in the past several years. This can be attributed to a continually-evolving environment in which business requirements have changed and in which new regulatory mandates have come into existence. A careful examination of these trends is required in order to fully understand the present and future relevance of data security in enterprise organizations.

CHANGING BUSINESS REQUIREMENTS

The IT boom and subsequent bust of the late 1990s made long-lasting, positive impacts on global productivity. Long after the demise of Pets.com, Webvan, and other symbols of the "new economy", the fact remains that the infrastructure and technology investments made during that time period resulted in many of the tools and capabilities upon which today's workforce relies. Miles of fiber-optic cables were laid underneath the oceans, data exchange protocols were standardized, and memory and processing power experienced tremendous capability gains at decreasing price points.

As a result, the enterprise workforce is now much more mobile in nature. While this mobility brings with it tremendous benefits in terms of flexibility and cost savings, it also presents a tremendous challenge to IT administrators who are tasked with ensuring that personal, confidential, and proprietary information doesn't fall into the wrong hands. As employees increasingly work from home offices and hotel rooms, the traditional physical boundaries which have previously defined the perimeters of enterprise networks no longer exist. These employees are routinely transporting data outside of their enterprise networks, leaving it vulnerable to loss or theft.

Additionally, many environments that were previously unconnected are now network-enabled and network-dependent. Hospitals and other clinical settings, for example, now use numerous interconnected devices for transmitting patient health information and delivering diagnoses. Primary and secondary schools depend on networked systems to store and transmit their students' personally identifiable information (PII). Finally, enterprises' greatly increased reliance on offshore resources has resulted in a requirement that proprietary data be readily accessible from half a world away. This expansion in connectivity has created a new information security challenge for the organizations whose operations depend on these environments.

There is a third contributing factor that may seem obvious but is no less important. There is simply more data in existence today, and it's growing at an exponential rate. The capabilities of a globally networked economy have made it possible for a greater number of digital transactions to take place at a much quicker pace. More transactions mean more data, and that data needs to be protected. Likewise, a greater number of paper records are now being digitized. Patient records, for example, are now being commonly converted to electronic medical records (EMR). This greatly increases the efficiency of health care operations, but it also introduces great risk if those records are not securely stored and transmitted.

COMPLIANCE

Evolving business requirements often result in new regulation, and this has certainly been the case in the area of data privacy and protection. Beginning in the mid-1990s, new U.S. and international compliance regulations began to come into existence. These regulations apply to a wide range of organizations and seek to protect the personal and financial information of individuals. Table 1 summarizes the most significant and broad-reaching of these regulations.

REGULATION	JURISDICTION	APPLIES TO	PROTECTED DATA
Payment Card Industry Data Security Standard (PCI DSS)[1]	International	All organizations which hold, process, or pass cardholder information from any of the branded cards	Cardholder data: • Primary Account Number (PAN) • Cardholder name • Service code • Expiration date Sensitive authentication data: • Full magnetic stripe data • CAV2/CVC2/CVV2/CID • PIN/PIN block
Health Insurance Portability and Accountability Act (HIPAA)[2]	United States	Health care providers who transmit or store any information in an electronic form, including: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing homes • Pharmacies Health plans : • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs Health care clearinghouses Medicare Prescription Drug Card Sponsors	Individually identifiable health information, including demographic data, that relates to: • An individual's past, present, or future physical or mental health or condition • A provision of health care to an individual • The past, present, or future payment for the provision of health care to an individual
Gramm-Leach Bliley Act (GLBA)[3]	United States	Financial institutions, which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are 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, and an array of other activities.	Nonpublic personal information (NPI), i.e., any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.

Table 1: Examples of data privacy and protection regulations currently in existence

[1] https://www.pcisecuritystandards.org

[2] http://www.hhs.gov/ocr/privacy/

[3] http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

These regulations all take very different approaches in terms of how they mandate the protection of data. Some consist of specific requirements, while others simply provide generally-worded implementation guidelines and recommendations. All of them, however, involve provisions related to the storage, transmission, and disposal of personal information.

UNDERSTANDING THE RISK OF DATA LOSS

An analysis of recent statistics illustrates just how significant the risk of data loss has become:

- Since early 2005, more than 150 million personal records have been exposed[4]
- Reports of data breaches in the U.S. rose almost 50% in 2008[5]
- 85% of organizations polled in a recent survey reported that they have had a data breach event[6]

A further analysis of recent statistics illustrates the potential impacts of data loss:

- A data security breach costs a company an average of $197 per lost record, with 65% of this cost resulting from lost business[7]
- A data breach that exposes personal information could cost companies an average of $268,000 to inform their customers, even if the lost data is never used[8]
- 20% of customers terminated their relationships with a company after being notified of a security breach[9]

Additionally, many of the regulations pertaining to data privacy and protection carry significant civil and criminal penalties for non-compliance, as summarized in Table 2.

[4] Privacy Rights Clearinghouse, A Chronology of Data Breaches, April 9th, 2007

[5] ITRC 2008 data breach report

[6] Scott and Scott LLP and Ponemon Institute LLC, May 15th, 2007

[7] 2007 Annual Study: The Cost of Data Breach. Ponemon Institute, LLC, 2008

[8] McAfee and Datamonitor's Data Loss Survey, 2007

[9] Ponemon Institute LLC, December 2005

REGULATION	CIVIL PENALTIES	CRIMINAL PENALTIES
Payment Card Industry Data Security Standard (PCI DSS)	Increased transaction processing fees Fines of up to $550,000 Suspension of credit card transaction processing abilities	None
Health Insurance Portability and Accountability Act (HIPAA)	For violations occurring prior to 2/18/2009: • Penalty amount: up to $100 per violation • Calendar year cap: $25,000 For violations occurring on or after 2/18/2009 : • Penalty amount: $100 to $50,000 or more per violation • Calendar year cap: $1,500,000	A person who knowingly obtains or discloses individually identifiable health information may face a criminal penalty of up to $50,000 and up to one year imprisonment. Criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm.
Gramm-Leach Bliley Act (GLBA)	Civil penalty of not more than $100,000 for each violation Some or all of the following sanctions may be imposed: • Termination of FDIC insurance • Implementation of cease and desist orders barring policies or practices deemed in violation of the act's privacy provisions • Removal of the financial institution's management including directors, officers, etc. and potentially barring them permanently from working in the banking industry • Fines of up to $1,000,000 for an individual or the lesser of $1,000,000 or 1% of the total assets of the financial institution	Imprisonment of institution officers and directors for not more than five years

Table 2: Non-compliance penalties for data privacy and protection regulations

While the impact of data loss is clearly significant regardless of how it occurs, it's important to understand that data loss can take place under a variety of scenarios, each having its own likelihood of occurring and each presenting its own unique challenges. The most common scenarios, as defined by the Identity Theft Resource Center[10], are as follows:

- **Insider Theft**
  Data is stolen by someone employed or recently terminated by the responsible organization
- **Data on the move**
  Data is lost or stolen while residing on a computer, thumb drive, PDA, etc. owned by the responsible organization or someone affiliated with the organization

[10] http://www.idtheftcenter.org

- **Subcontractor**
  Data is lost or stolen by someone not directly employed by the responsible organization, but rather by someone affiliated with the organization who has access to the data

- **Hacking**
  Data is remotely accessed by an unauthorized party not affiliated with the responsible organization

- **Accidental exposure**
  Data is inadvertently posted to a web site accessible by unauthorized parties

Of all the above scenarios, *data on the move* presents some of the most interesting security challenges. Something as simple as a misplaced laptop can introduce just as much risk to an organization's data security posture as a sophisticated, network-based infiltration attack. The simplistic nature of the *data on the move* scenario is evident in the fact that 30% of all 2008 data breaches were the result of a lost or stolen laptop, desktop or drive[11]. This amounted to 136 breaches involving almost 19 million compromised records[12]. The frequency of lost or stolen computers, in particular, is cause for significant alarm:

- Every 43 seconds a computer is reported stolen[13]
- 1 in 10 laptop computers will be stolen within the first 12 months of purchase[14]
- 97% of lost and stolen laptops are never recovered[15]
- 57% of corporate crimes are linked to stolen laptops[16]

Data on the move breaches represent a clear and present danger, as evident by the following recent high-profile incidents:

- A laptop was stolen from the offices of a large university, exposing the personal information of 100,000 alumni, students, and past applicants (2009)
- Burglars stole computer systems from the offices of a company that provides outsourced benefits administration, exposing the personal information of 75,000 employees of several large companies (2008)
- Laptop computers belonging to a blood donation center were stolen, exposing the names and social security numbers of 321,000 donors (2008)
- An unencrypted hard drive containing 330,000 names, addresses and social security numbers was lost when it was shipped back to its owner by a computer repair company (2006)

[11] DataLossDB

[12] Identity Theft Resource Center 2008 Data Breach *Data On The Move* Summary

[13] CSI/FBI Computer Crime and Security Survey, 2006

[14] CSI/FBI Computer Crime and Security Survey, 2005

[15] CSI/FBI Computer Crime and Security Survey, 2005

[16] CSI/FBI Computer Crime and Security Survey, 2006

- A file server and several laptop computers were stolen from a regional office of a major insurance company, exposing the private data of 970,000 potential customers (2006)
- A laptop containing the personal information of 28.6 million veterans was stolen from a VA employee's home (2006)

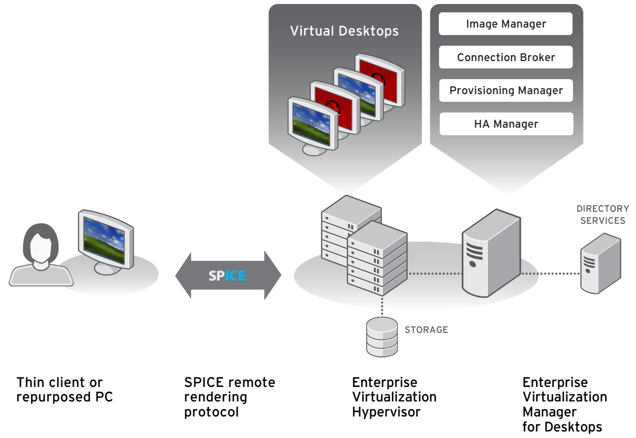
The solution to the *data on the move* scenario requires a different approach to the way in which enterprise organizations deploy computing power to their employees and affiliates. It involves the application of digital principles to a physical problem, and it involves answering a fundamental question: What if data no longer had to be on the move?

RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

The traditional model for deploying desktop computing within an enterprise involves the use of personal computers (PCs). 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 in order to provider users with the tools 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 installed software. Unlike with traditional desktop deployments, no data is stored on these thin clients. This type of architecture is referred to as hosted desktop virtualization.

FIGURE 1: RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS


Virtual Desktops
Image Manager
Connection Broker
Provisioning Manager
HA Manager
DIRECTORY SERVICES
SPICE
STORAGE
Thin client or repurposed PC
SPICE remote rendering protocol
Enterprise Virtualization Hypervisor
Enterprise Virtualization Manager for Desktops

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

- **Red Hat Enterprise Virtualization Hypervisor**
  A standalone, high-performance, and secure hypervisor based on the Red Hat Enterprise Linux kernel with KVM (Kernel-based Virtual Machine) technology
- **Red Hat Enterprise Virtualization Manager for Server**
  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 indistinguishable from that of a physical desktop
- **Integrated connection broker**
  A web-based portal from which end users can log into their virtual desktops

ENABLING SECURE REMOTE DATA ACCESS

By moving desktop environments off of the end point and into the datacenter, Red Hat Enterprise Virtualization for Desktops enables enterprises to centralize and secure their data. Stolen computers or unencrypted hard drives become a non-issue, as all data—operating system, applications, and user—is now 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. Additionally, all data can be easily and centrally backed up within the datacenter, ensuring that it is always available, even in the event of a hardware failure. With Red Hat Enterprise Virtualization for Desktops, the enterprise workforce can be mobile, but the data they depend on doesn't need to be.

MEETING COMPLIANCE REGULATIONS

Red Hat Enterprise Virtualization for Desktops also enables enterprises to better meet the compliance regulations pertaining to data privacy and protection. Because data is no longer distributed across multiple laptops and desktops, it is easier to inventory and control. Some regulatory requirements, such as those pertaining to the disposal of data from laptops and desktops, even become irrelevant with Red Hat Enterprise Virtualization for Desktops, since that data never existed on those computers in the first place. Table 3 illustrates specific ways in which this new deployment model helps enterprises address key data privacy and protection regulations.

REGULATION	REQUIREMENTS AND RECOMMENDATIONS ADDRESSED
Payment Card Industry Data Security Standard (PCI DSS)	Requirement 3.1: Keep cardholder data storage to a minimum Requirement 9.1: Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data Requirement 9.6: Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data Requirement 9.8: Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals) Requirement 9.9.1: Properly inventory all media and make sure it is securely stored Requirement 9.10.2: Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed
Health Insurance Portability and Accountability Act (HIPAA)	Specification 164.310(d)(2)(i): Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored Specification 164.310(d)(2)(ii): Implement procedures for removal of electronic protected health information from electronic media before the media are made available Specification 164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore Specification 164.310(d)(2)(iv): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment
Gramm-Leach Bliley Act (GLBA)	Safeguard rule recommendations: Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices Develop policies for employees who telecommute Know where sensitive customer information is stored and store it securely 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

Table 3: Regulatory requirements/recommendations addressed by Red Hat Enterprise Virtualization for Desktops

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 enterprises looking to safeguard their data 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 enterprises 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 enterprises 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 enterprises 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

Changing business requirements and new compliance regulations have made data privacy and protection a top priority for enterprise organizations, with data loss representing a clear and present danger to the overall security and viability of these organizations. Red Hat Enterprise Virtualization for Desktops can mitigate the risk of data loss and address regulatory requirements by taking sensitive data off of laptops and desktops and confining it within the safety and security of an enterprise data center. Built on the industry-leading security of Red Hat Enterprise Linux, with support for both Microsoft Windows and Red Hat Enterprise Linux desktops, Red Hat Enterprise Virtualization for Desktops helps enterprises safeguard their data and keep pace with today's fast-changing environment.

Learn more at redhat.com/virtualization-strategy.

RED HAT SALES AND INQUIRIES NORTH AMERICA

1-888-REDHAT1
www.redhat.com