RED HAT :: CHICAGO :: 2009
SUMMIT

Safeguarding your Data with Desktop Virtualization

Jim Brennan
Sr. Product Marketing Manager
Red Hat

John Pirc
Product Line Executive
IBM Internet Security Systems and
Security Thought Leader, The SANS Institute

presented by

Agenda

Addressing the data security challenge with hosted desktop virtualization

Understanding the risks

Best practices for securely deploying desktop virtualization

Q & A

The Data Security Challenge: Why Now?

The need for remote data accessibility has increased:

- Increasingly mobile workforce
  - Work-from-home employees
  - Traveling employees
- Newly connected environments
  - Offshore
  - Clinical
  - K-12 Schools
- Increasing amounts of data
  - Increased number of electronic transactions
  - Newly-digitized records (ex: electronic medical records)

The Data Security Challenge: Why Now?

New regulations mandating protection of data:

Payment Card Industry Data Security Standard (PCI DSS)

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

The Data Security Challenge: Why Now?

Payment Card Industry Data Security Standard (PCI DSS):

Applies internationally to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands

Mandates safeguarding of:

- Cardholder data (name, account number, expiration date, security code)
- Sensitive authentication data (pin, magnetic stripe data)

12 defined requirements grouped into six categories:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The Data Security Challenge: Why Now?

Gramm-Leach-Bliley Act (GLBA):

Applies to all firms that provide financial products or services in the US (lending, brokering, tax preparation, financial advising, credit counseling, etc)

Mandates safeguarding of all nonpublic personal information (NPI)

Two primary rules

- Financial Privacy Rule:
  - Governs the collection and disclosure of customers' personal financial information by financial institutions
- Safeguards Rule:
  - Requires all financial institutions to design, implement and maintain safeguards to protect customer information
  - Rule does not define specific requirements, only recommendations

The Data Security Challenge: Why Now?

Health Insurance Portability and Accountability Act (HIPAA):

Applies to all health care providers, health plans, and health care clearinghouses with operations in the US

Mandates safeguarding of all protected health information (PHI) and electronic protected health information (EPHI)

Two primary provisions:

- Privacy Rule: Sets the standards for who may have access to PHI
- Security Rule: Sets the standards for ensuring that only those who should have access to EPHI will actually have access
  - Defines three sets of safeguards:
    - Administrative
    - Physical
    - Technical
  - Some safeguards have associated "implementation specifications" (either “required” or “addressable”)

The Data Security Challenge: How Serious Is It?

Since early 2005, more than 150 million personal records have been exposed[1]

A data security breach costs a company an average of $197 per lost record[2]

65% of data security breach costs are the result of lost business[2]

20% of customers terminated a relationship with a company after being notified of a security breach[3]

Non-compliance penalties:

- Up to $100,000 fine per incident
- Imprisonment up to 20 years

[1] Privacy Rights Clearinghouse, A Chronology of Data Breaches, April 9th, 2007
[2] The Cost of Data Breach. Ponemon Institute, LLC, 2007
[3] Ponemon Institute, December 2005

The Data Security Challenge: What Are We Up Against?

Common data breach scenarios*:

Insider Theft: Data stolen by someone inside the company)

Data on the Move: Laptop, thumb drive, PDA, etc

Subcontractor: Stolen or lost by a second party

Hacking: Stolen by someone outside of the company

Accidental Exposure: Inadvertent Internet/Web posting)

Notes: careless vs. malicious, physical vs. digital

* Identity Theft Resource Center (http://www.idtheftcenter.org)

How much of this is due to data on the move?

The Data Security Challenge: Data On The Move

30% of all 2008 data breaches were the result of a lost or stolen laptop, desktop or drive[1]

- 136 breaches[2]
- 18.74M records[2]

FBI statistics:

- Every 43 seconds a computer is reported stolen[3]
- 1 in 10 laptop computers will be stolen within the first 12 months of purchase[4]
- 97% of lost and stolen laptops are never recovered[4]
- 57% of corporate crimes are linked to stolen laptops[3]

[1] DataLossDB
[2] Identity Theft Resource Center 2008 Data Breach Data On The Move Summary
[3] CSI/FBI Computer Crime and Security Survey, 2006
[4] CSI/FBI Computer Crime and Security Survey, 2005

The Data Security Challenge: Data On The Move

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)

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)

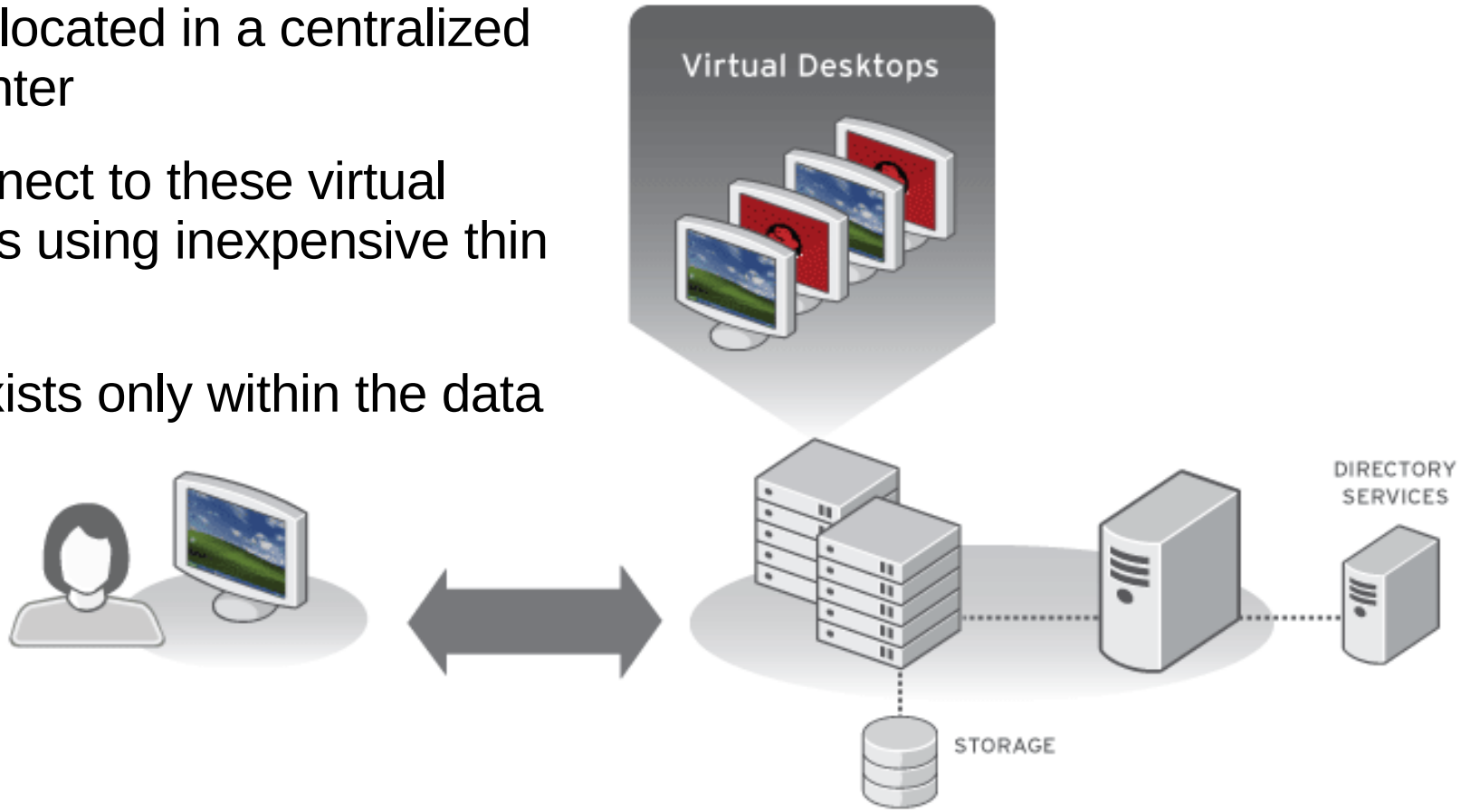
What if data no longer needed to be on the move?

Hosted Desktop Virtualization: Enabling Secure Remote Access to Data

Complete desktop environments are hosted as virtual desktops on servers located in a centralized data center

Users connect to these virtual desktops using inexpensive thin clients

All data exists only within the data center



Hosted Desktop Virtualization: Meeting Compliance Regulations

Payment Card Industry Data Security Standard (PCI DSS) requirements addressed:

Requirement 3

- 3.1: Keep cardholder data storage to a minimum

Requirement 9

- 9.1: Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
- 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.
- 9.8: Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).
- 9.9.1: Properly inventory all media and make sure it is securely stored
- 9.10.2: Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed

Hosted Desktop Virtualization: Meeting Compliance Regulations

Gramm-Leach-Bliley Act (GLBA) Safeguard Rule recommendations addressed:

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.

Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home.

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

Hosted Desktop Virtualization: Meeting Compliance Regulations

Health Insurance Portability and Accountability Act (HIPAA):

Required physical safeguards addressed:

- Disposal – 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"
- Media Re-Use – 164.310(d)(2)(ii): "Implement procedures for removal of electronic protected health information from electronic media before the media are made available"

Addressable physical safeguards addressed:

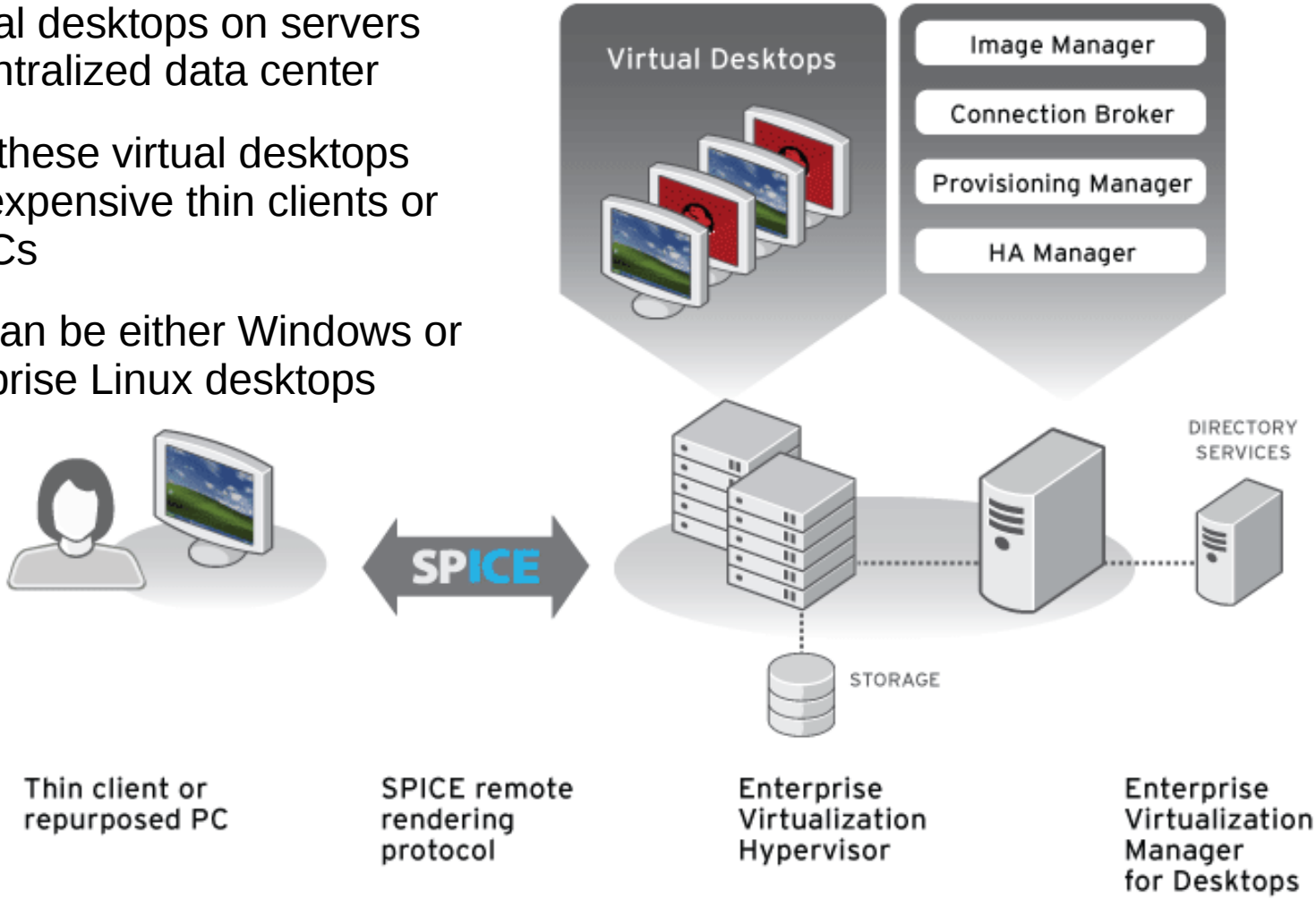
- Accountability – 164.310(d)(2)(iii): "Maintain a record of the movements of hardware and electronic media and any person responsible therefore."
- Data Backup and Storage – 64.310(d)(2)(iv): "Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

Red Hat Enterprise Virtualization Manager for Desktops

Complete desktop environments are hosted as virtual desktops on servers located in a centralized data center

Users connect to these virtual desktops using either inexpensive thin clients or re-purposed PCs

Virtual desktops can be either Windows or Red Hat Enterprise Linux desktops



Red Hat Enterprise Virtualization Manager for Desktops

An end-to-end desktop virtualization solution:

Red Hat Enterprise Virtualization Hypervisor

SPICE

Integrated connection broker

Centralized management console

Red Hat Enterprise Virtualization Hypervisor

Standalone hypervisor

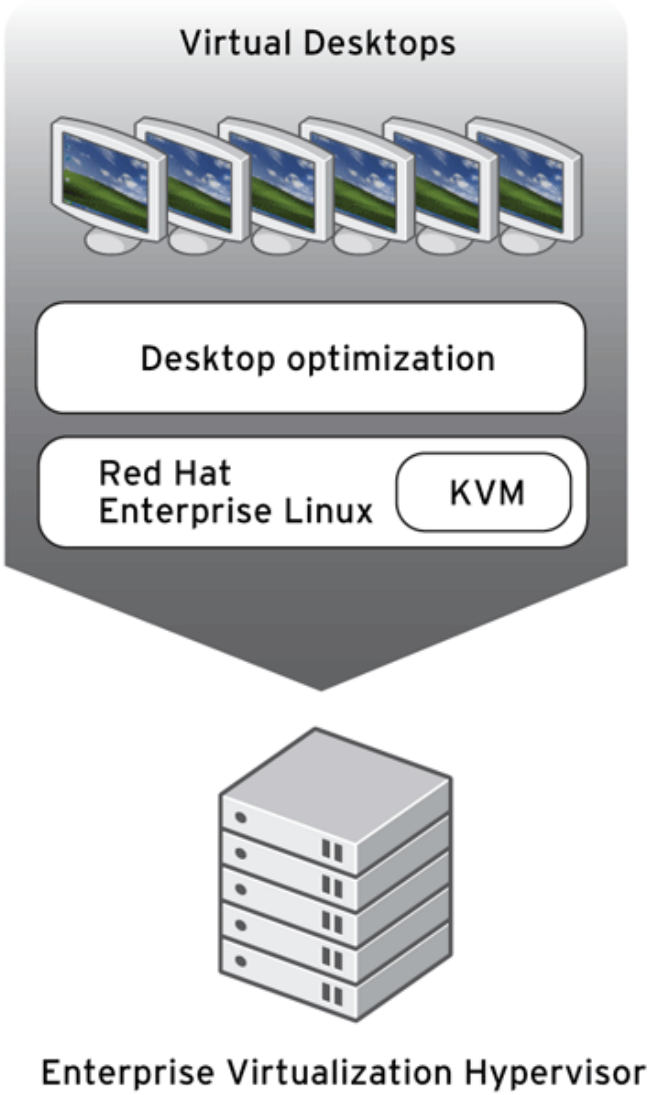
- Only runs virtual machines
- No support for running applications

Reduced footprint – optimized image

- Lightweight < 100MB
- Easy to install and manage
  - Boot from network via PXE
  - Run from flash drive
  - Installed on local disk or SAN

Built on Red Hat Enterprise Linux 5 kernel with KVM

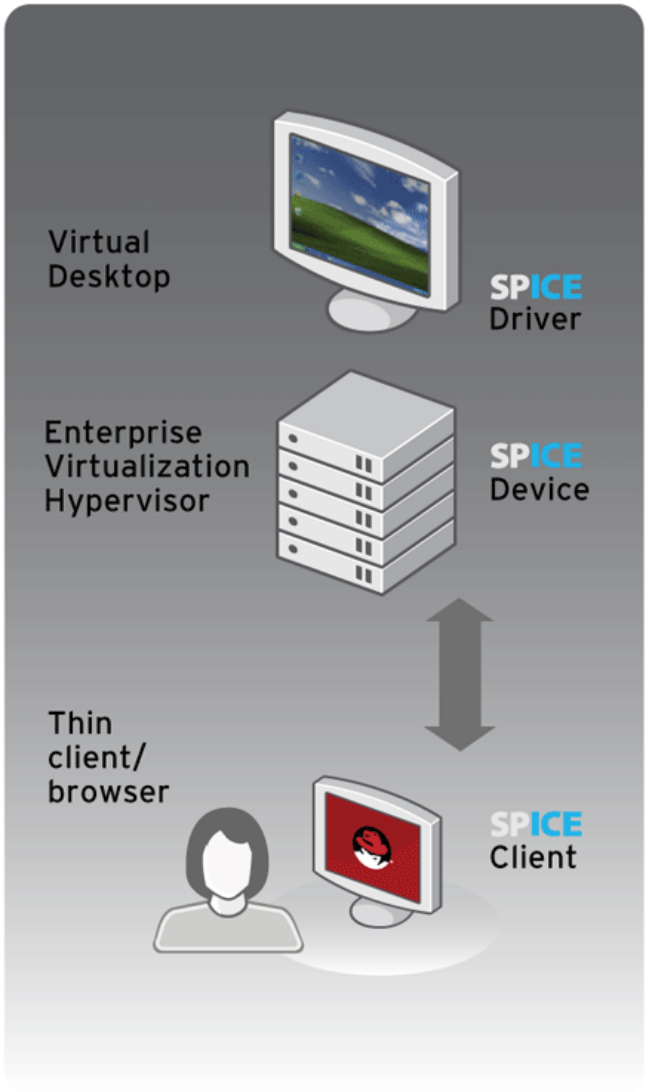
- Supports wide range of certified hardware platforms



SPICE – Simple Protocol for Independent Computing Environments

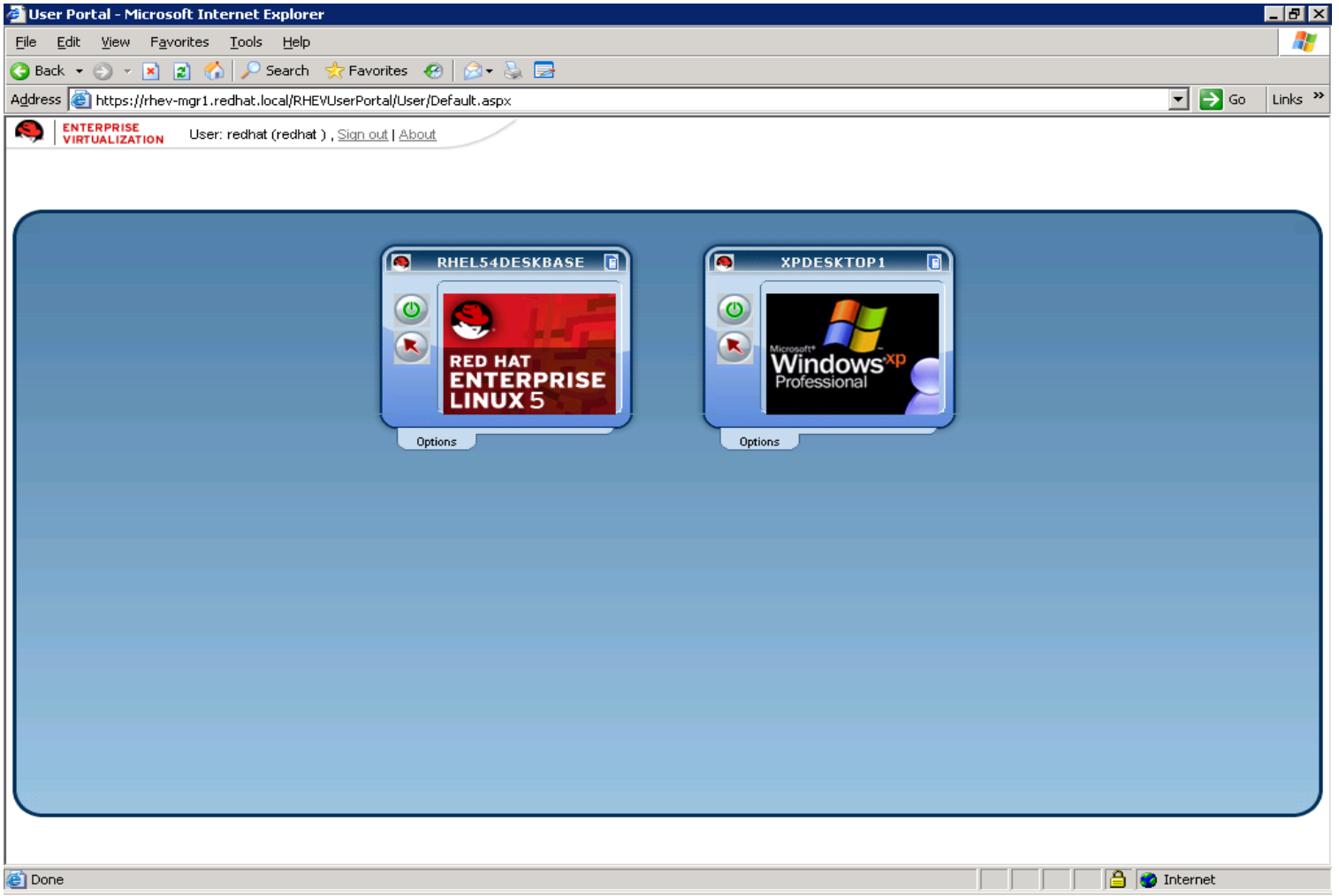
An adaptive remote rendering protocol

Able to deliver an end user experience indistinguishable from that of a physical desktop



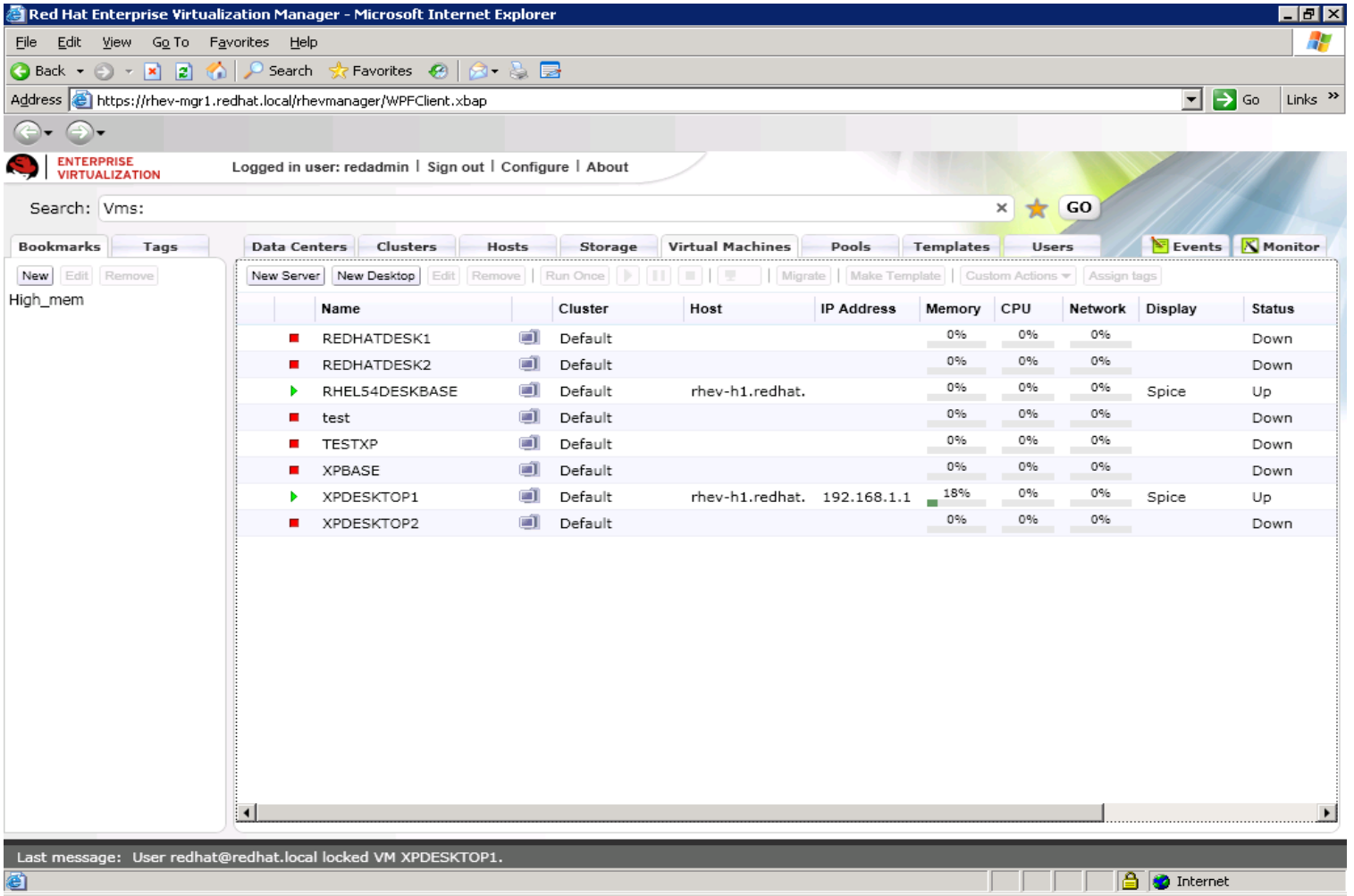
Integrated Connection Broker

Web-based portal from which end users can log into their virtual desktops.



Centralized Management Console

Web-based console from which administrators can create, monitor and maintain their virtual desktops.



Hosted Desktop Virtualization: Is It for Real?

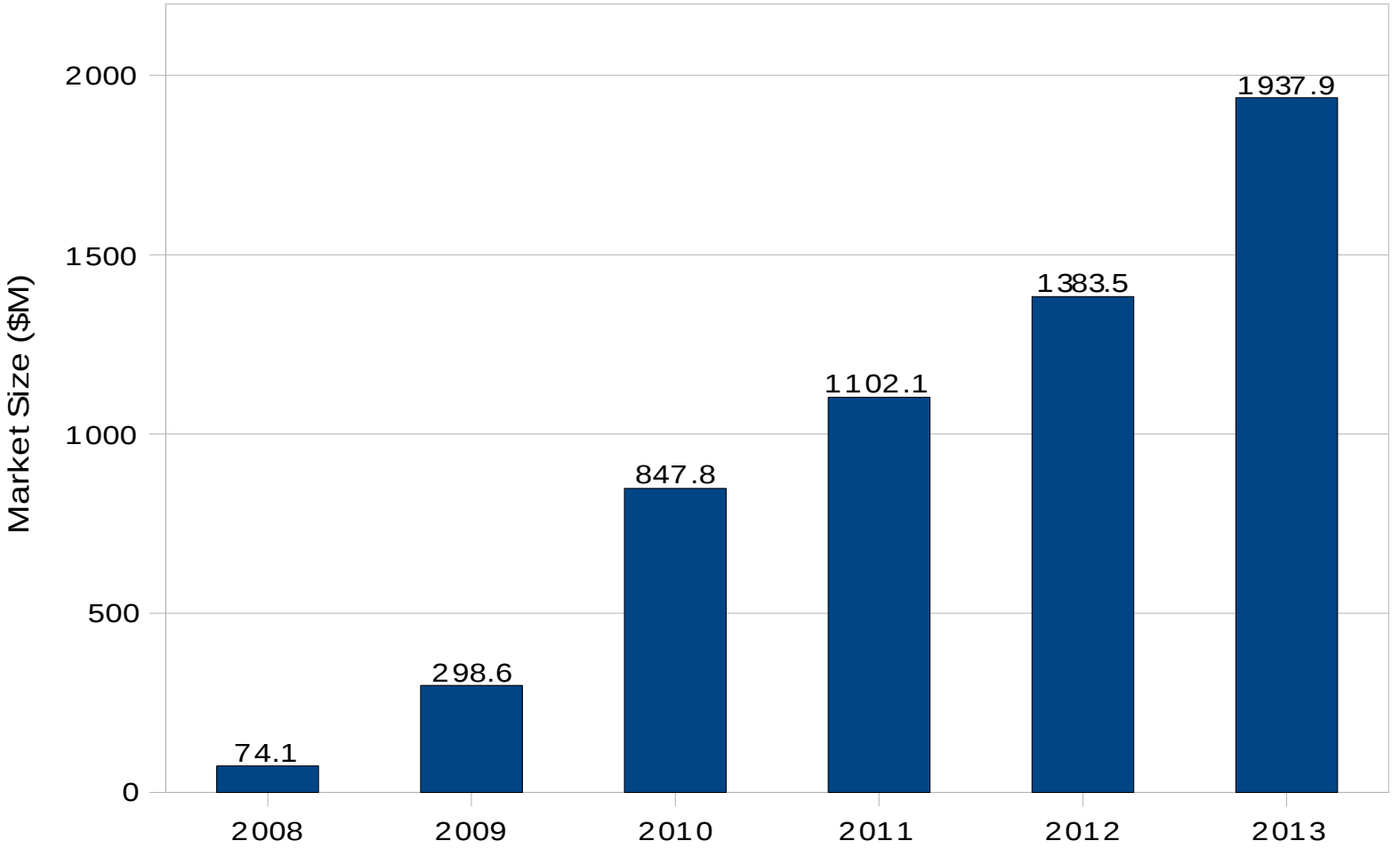
2008 IDG survey of 340 IT managers:

41% of respondents said they are already investing in desktop virtualization

22% said desktop virtualization is a critical priority of their organizations over the next twelve months

Survey participants expect 24% of their desktops to be virtualized within the next 24 months and 34% of their desktops to be virtualized by 2010

Hosted Desktop Virtualization: Is It for Real?



Source: Gartner, “Dataquest Insight: Virtualization Market Size Driven by cost Reduction, Resource Utilization and Management Advantages, January 2009

There is no free lunch

What Does Hosted Desktop Virtualization Change?

- Everything
  - Dynamic, fluid data-center
  - Resource pools
  - Commoditization of everything
  - Increased efficiency
- Nothing
  - Virtual IT is still IT
  - Security, sprawl, management, complexity, heterogeneity

Virtualization != Security

Operating System and Application Vulnerabilities

Traditional threats remain:

- Malware: viruses, worms, trojans, rootkits
- DoS/DDoS attacks
- Buffer overflows, SQL injection, XSS
- Data leakage via email
- Access control, compliance, integrity

Virtualized operating system and application threats remain:

- Disaster recovery and sandboxing are notable arguments
- However, they do not increase native resistance to OS/application threats

Virtual Machine Vulnerabilities

- Replay attacks and data retention
  - Is sensitive data being cached in unknown areas for replay purposes?
- Virtual machine stealing
  - Virtual machines are just as files, its trivial to steal a full system or groups of systems.
- Dynamic relocation (live migration)
  - Are virtual machines moving to less secure machines, networks, data centers, etc?

Management Infrastructure Vulnerabilities

- Software Threats:
  - Keys to the castle
  - Vulnerabilities in management applications
  - Secure storage of Virtual Machines and management data
- Operational Threats:
  - Managing risk requires new technology, skills and expertise.
  - We now also factor the extremely dynamic nature of virtualization into our evaluation of overall risk

Virtualization Threat Landscape

Virtualization platforms will become the will become the target of choice of the research/hacker community in the years to come

The popularity, complexity, and immaturity of x86 virtualization make it very likely that new hypervisor-compromising malware, attacks on management infrastructure, and other malicious activity will make headlines very soon

Achieving a net gain in data security

Hosted Desktop Virtualization – Best Practices for A Secure Deployment

Same OS/application security principles apply:

Defense in depth:

- Perimeter
- Network
- Application
- Host

Network design and segmentation

Unified security management:

- Firewall
- Network IDS/IPS/ADS
- Host IDS/IPS
- Anti-virus, anti-malware

Hosted Desktop Virtualization – Best Practices for A Secure Deployment

- Mitigate virtual machine vulnerabilities through isolation:
  - Isolation of virtual desktops from other virtual desktops
  - Isolation of virtual desktops from the hypervisor
- Apply Mandatory Access Control (MAC) security using technologies such as SELinux/sVirt:
  - Labels are applied to the processes that execute virtual desktops
  - Labels are applied to the files/devices on which virtual desktops are stored
  - Policy rules govern how process labels Interact with file/device labels
  - Kernel enforces these rules

Hosted Desktop Virtualization – Best Practices for A Secure Deployment

- Mitigate management infrastructure software threats:
  - Implement layered protection around management components
  - Ensure all communication channels are encrypted
  - Know your hypervisor:
    - Vulnerability history
    - Timeliness of patches
- Mitigate management infrastructure operational threats:
  - Audit systems need to account for dynamic nature of virtualized infrastructures
  - Policies needed to ensure consistent patching/versioning of clustered hypervisors
  - Staff needs to be trained on new technologies and risk factors

Key Takeaways

Data on the move represents a clear and present danger to the security and well-being of any enterprise

Hosted desktop virtualization protects data by taking it off of the end point and putting it in the data center

Virtualization introduces new technological and operational risks that require consideration

Best practices are available that can mitigate these new risks and make it possible to achieve a net gain in data security

QUESTIONS?

TELL US WHAT YOU THINK:
REDHAT.COM/SUMMIT-SURVEY