

**SUMMIT**

**JBoss  
WORLD**

**PRESENTED BY RED HAT**

**LEARN. NETWORK.  
EXPERIENCE OPEN SOURCE.**

[www.theredhatsummit.com](http://www.theredhatsummit.com)

# Achieving Compliance in an Increasingly Virtual World

Akash Chandrashekar & Dave Russell  
Solutions Architects, Red Hat  
Friday, June 25

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# SHIFTING INVESTMENTS



**CURRENT IT SPENDING**

- INFRASTRUCTURE MAINTENANCE**
- APPLICATION MAINTENANCE**
- APPLICATION INNOVATION**
- INFRASTRUCTURE INNOVATION**



**DESIRED IT SPENDING**

**SUMMIT**

JBoss  
WORLD

PRESENTED BY RED HAT

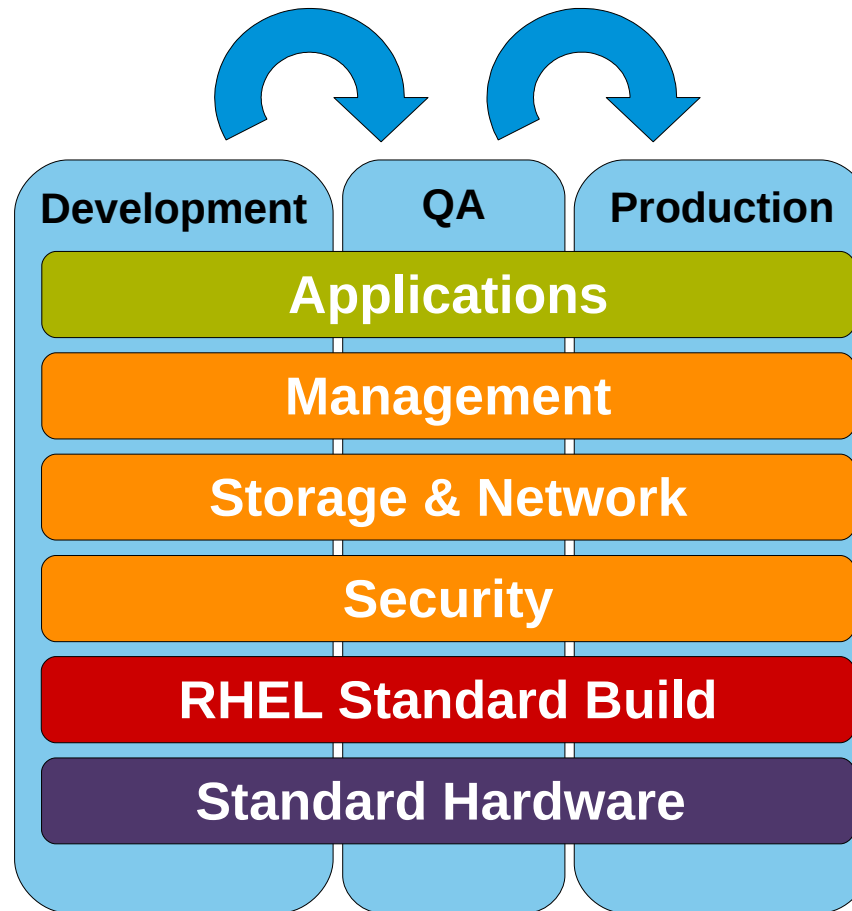


# Virtualization possibilities

- Effective and efficient use of hardware
- Reduce the number of idle hardware
- Migration of environments to different systems
- Better flexibility in utilizing hardware
- Leverage the possibilities that lie within Cloud Computing



# Standard Operating Environment (SOE)



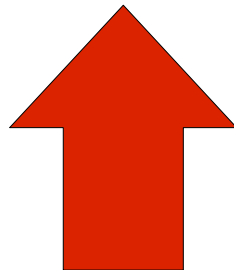
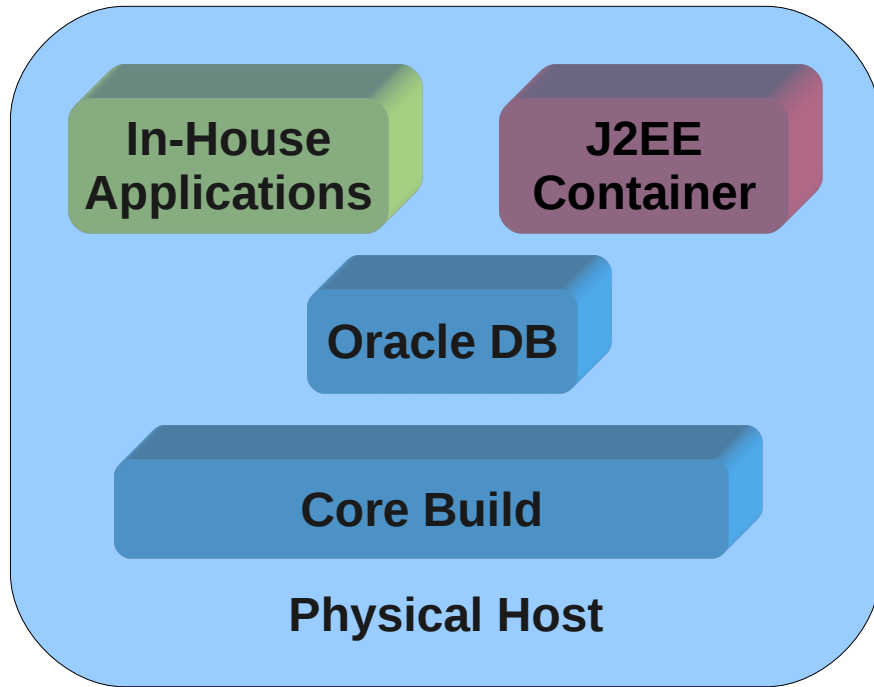
**SUMMIT**

JBoss  
WORLD

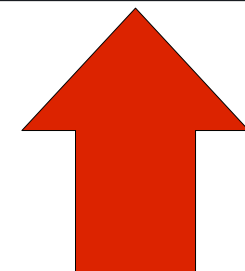
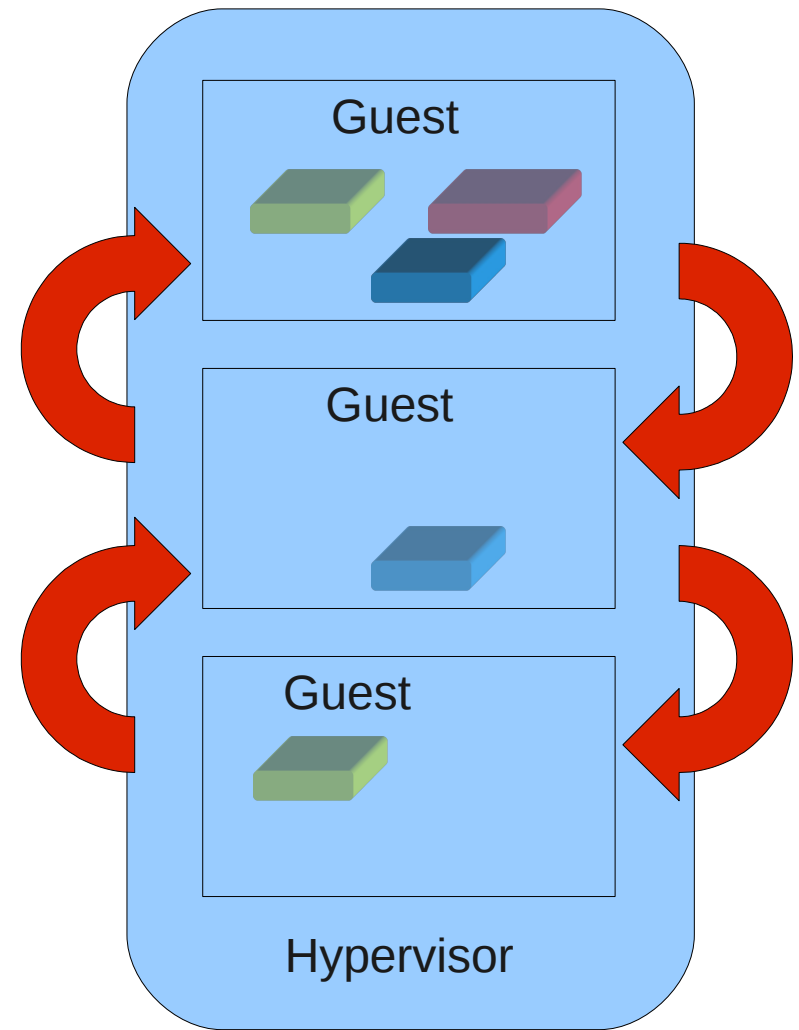
PRESENTED BY RED HAT



# Physical vs Virtualized



VS



**SUMMIT**

JBoss  
WORLD

PRESENTED BY RED HAT



# Virtual or Not? What's the Difference?

- The protection of sensitive data
- PCI/DSS, Sarbanes-Oxley, HIPAA

## Stationary



## In Flight



## Isolation



**SUMMIT**

**JBoss  
WORLD**

**PRESENTED BY RED HAT**



# Virtualization and Compliance

- How will virtualization affect my compliance?
- What steps are required to ensure continued compliance in a virtualized space ?
- What standards will affect me in a virtualized space?
- How can I protect my virtualized guests and host?
- What exactly should I need to do to address these concerns?

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# Typical Compliance Requirements

- Segregation of systems
- Segregation of networks
- Protect virtualized media
- Logging and auditing
- Patching and change control
- Subscription/license/commercial considerations
- Control system sprawl

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# RED HAT<sup>®</sup> NETWORK SATELLITE



Provisioning



Patch Management



Monitoring



Configuration Management

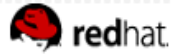
**SUMMIT**

JBoss  
WORLD

PRESENTED BY RED HAT



# http://www.redhat.com/security/data/cve



## Security Response Team

2009 CVE

**CVE-2009-0040**

2008 CVE

2007 CVE

2006 CVE

2005 CVE

2004 CVE

2003 CVE

2002 CVE

2001 CVE

2000 CVE

1999 CVE

## CVE-2009-0040

**Impact:** Moderate ([classification](#))

**Public:** February 19 2009

**Bugzilla:** [486355](#): CVE-2009-0040 libpng arbitrary free() flaw

### Details

The MITRE CVE dictionary describes this issue as:

The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png\_read\_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.

Find out more about CVE-2009-0040 from the [MITRE CVE dictionary](#) and [NIST NVD](#).

### CVSS v2 metrics

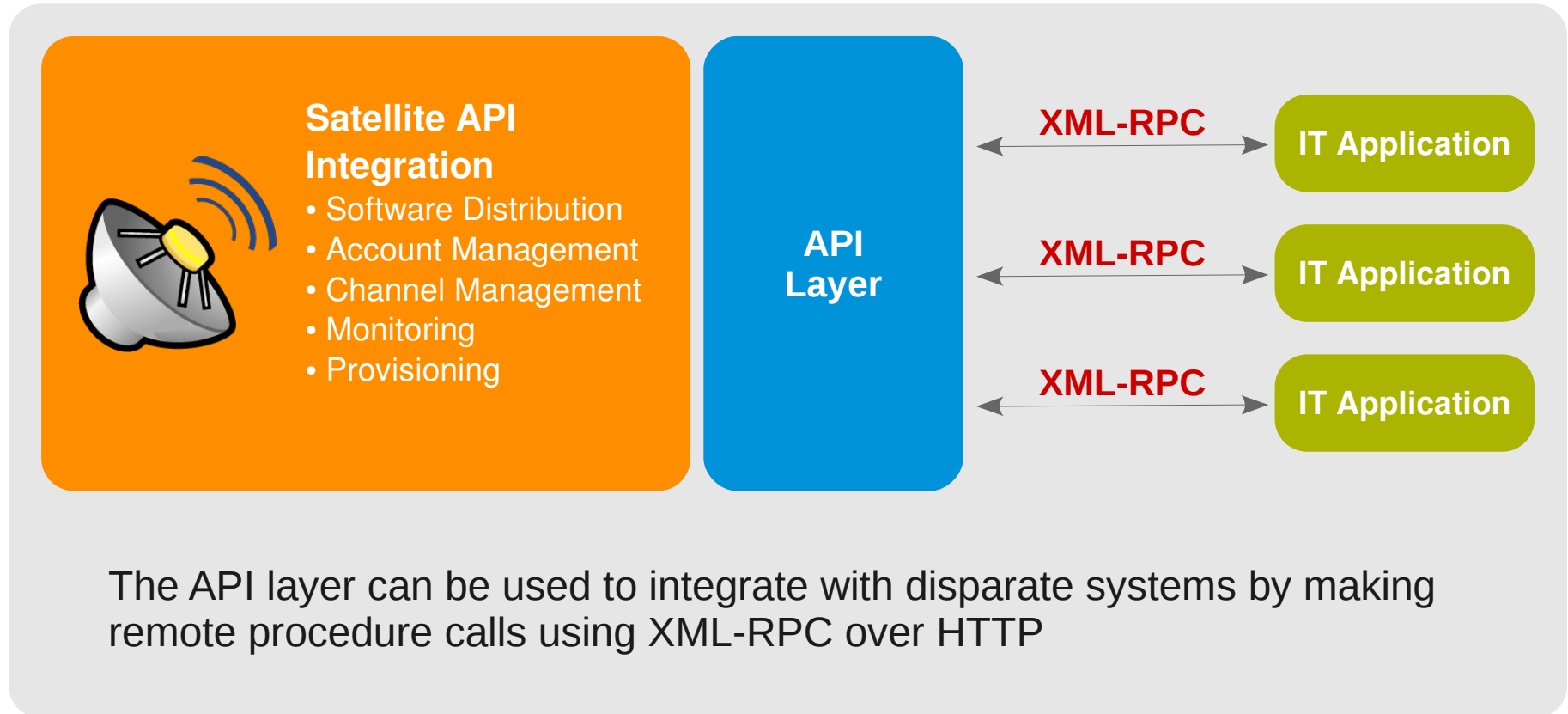
**Base Score:** 6.8      **Base Metrics:** [AV:N/AC:M/Au:N/C:P/I:P/A:P](#)  
**Access Vector:** Network      **Confidentiality Impact:** Partial  
**Access Complexity:** Medium      **Integrity Impact:** Partial  
**Authentication:** None      **Availability Impact:** Partial

Find out more about [Red Hat support for the Common Vulnerability Scoring System \(CVSS\)](#).

### Red Hat security errata

Platform	Errata	Release Date
Red Hat Enterprise Linux version 4 (firefox)	<a href="#">RHSA-2009-0315</a>	March 05 2009
Red Hat Enterprise Linux version 5 (firefox)	<a href="#">RHSA-2009-0315</a>	March 05 2009
Red Hat Enterprise Linux version 2.1 (seamonkey)	<a href="#">RHSA-2009-0325</a>	March 05 2009

# API layer Integration



# Satellite Reporting

## server.example.com

### System Information

- **RHN ID:** 1000010028
- **Reg Date:** 2009-06-24 T00:59:45
- **Last Check-in:** 2009-08-28 T22:18:28
- **Vendor:** Dell Computer Corporation
- **System:** PowerEdge 1850
- **Asset Tag:** 3VCRJ91
- **Bios Version:** A04

### System Events

#### Package Install 2009-07-06 23:41:33.0

Result: Failed: Some of the packages specified were on a skip list

- kernel-2.6.9-89.EL
- kernel-smp-2.6.9-89.EL
- kernel-utils-2.4-18.el4:1

#### Package Removal 2009-06-30 13:27:12.0

Result: [['cscope', '15.5', '10.RHEL4.3', '', 'i386']] removed successfully

- cscope-15.5-10.RHEL4.3

#### Package Removal 2009-07-07 04:08:12.0

Result: cairo-1.2.4-5.el5 failed because of package not installed cdparanoia-libs-alpha9.8-27.2 failed because of package not installed boost-devel-1.32.0-7.rhel4 failed because of package not installed boost-1.32.0-7.rhel4 failed because of package not installed

- boost-1.32.0-7.rhel4
- boost-devel-1.32.0-7.rhel4

# Additional Reporting from Satellite

A command-line tool that produces a handful of CSV reports with information found in the RHN Satellite server database.

Produces stock CSV reports:

- Entitlements and subscriptions
- System inventory
- Software and errata
- Users and groups



# Security Concerns with a Virtualization Platform

- Consider the complexity of the full Virtual Machine Management (VMM) stack
- External Interfaces
- Types of Exploits
- Development Environment



# External Interfaces

- Exploits need a way in
- Size of the VMM stack : Number of security-relevant flaws
- Flaw only relevant if it can be exploited
- The greater the interfaces the greater the risk



# Types of Exploits

- Hypervisor calls
- Hardware interrupts processed by the VMM
- Processor instructions processed by the VMM
- Network interfaces
- Traps that are reflected to the VMM by the CPU



# The Exposure Ratio

The likelihood of accessing flaws



The size and number of interfaces provided by privileged code to other entities.

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# Development Environment – Quality Matters

- Appropriate processes for code development as well as code review
- Flaw discovery and the release of a fixes
- Window for an attacker to mount a successful attack of the flaw



**SUMMIT**

**JBoss  
WORLD**

**PRESENTED BY RED HAT**



# VMM Security Comparison

Security Concerns	KVM	Xen	Popular VM Platform
Size of Software Stack	Medium	Medium to High	High (Based on available Info)
Number of Interfaces	Medium	High	High (Based on available Info)
Assurance of Development Environment	High	Medium	Low (Based on Information from CC evaluation)

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# KVM, RHEL6 and other cool stuff!

- Kernel Virtual Machine basics
- KVM new features in RHEL6
- Control Groups
- SELinux and sVirt



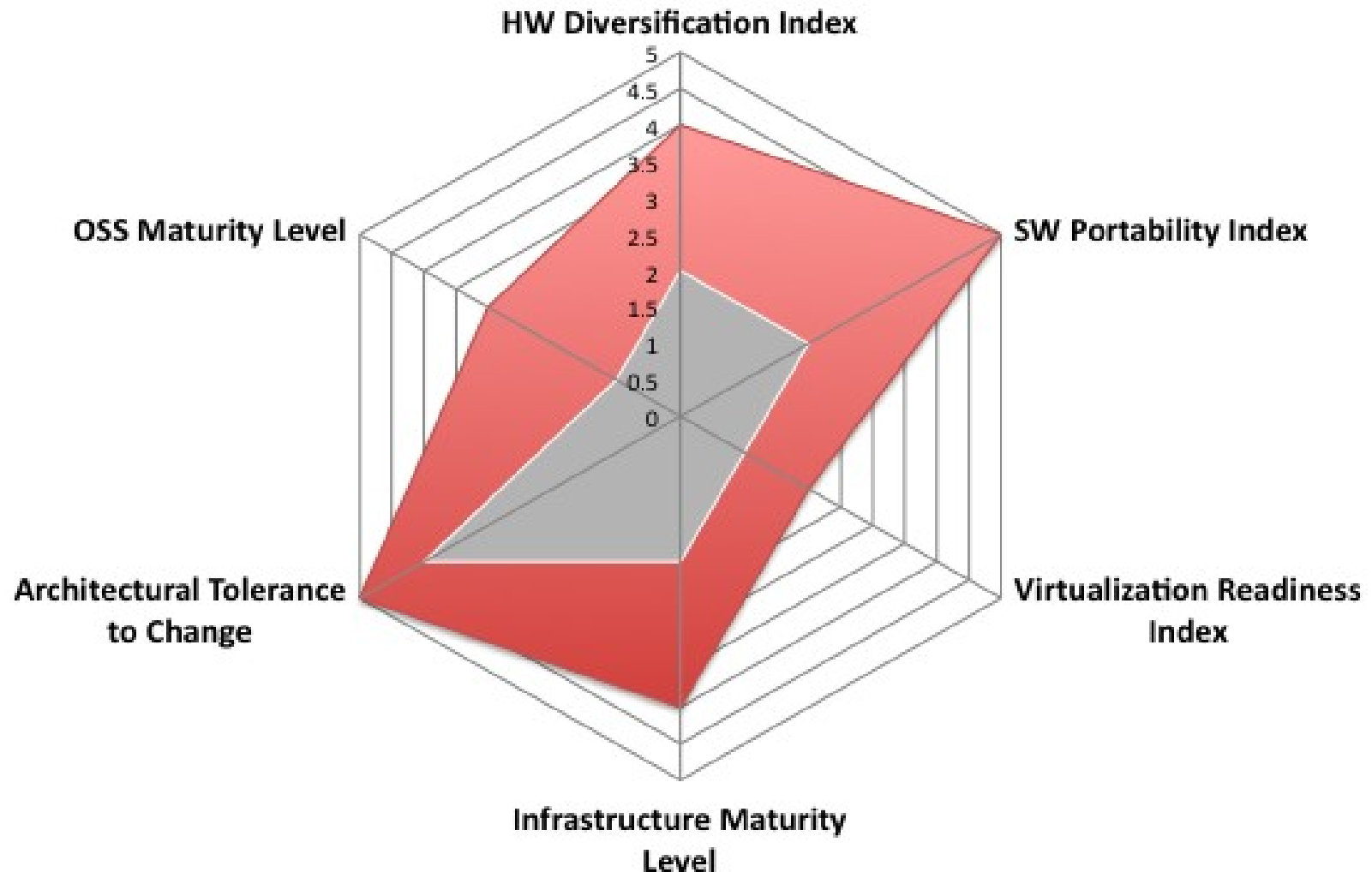
**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



# Virtualization Analysis



**SUMMIT**

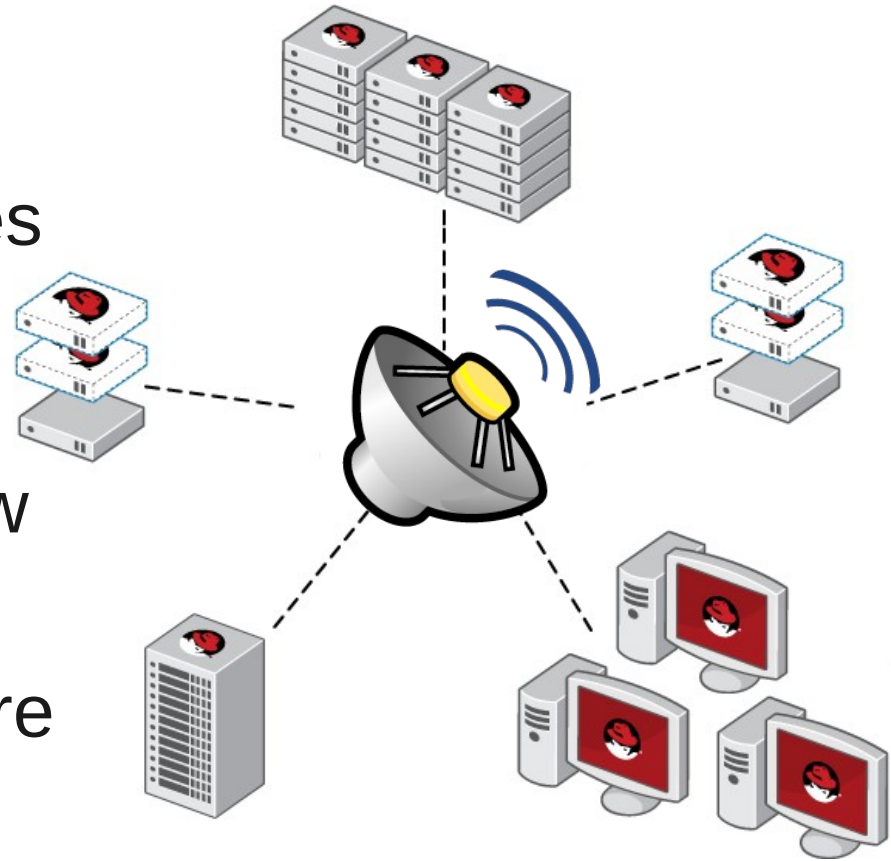
**JBoss  
WORLD**

PRESENTED BY RED HAT



# Summary

- With increased flexibility comes a significant potential for increased vulnerability
- Virtual environments bring new considerations
- Systems Management tools are key
- Process/Procedure
- Reporting and Auditing



**SUMMIT**

JBoss  
WORLD

PRESENTED BY RED HAT



# FOLLOW US ON TWITTER

[www.twitter.com/redhatsummit](http://www.twitter.com/redhatsummit)

## TWEET ABOUT IT

[#summitjbw](https://twitter.com/summitjbw)

## READ THE BLOG






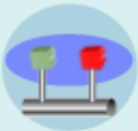

<http://summitblog.redhat.com/>

**SUMMIT**

**JBoss  
WORLD**

PRESENTED BY RED HAT



							
	<b>Silo</b>	<b>Integrated</b>	<b>Componentized</b>	<b>Services</b>	<b>Composite Services</b>	<b>Virtualized Services</b>	<b>Dynamically Re-Configurable Services</b>
<b>Business</b>	Isolated Business Line Driven	Business Process Integration	Componentized Business	Componentized Business offers Services	Processes through service composition	Geo-geographical Independent Service centers	Mix and match business and context-aware capabilities
<b>Organization</b>	Ad hoc LOB IT Strategy & Governance	Ad hoc Enterprise IT Strategy & Governance	Common Governance processes	Emerging SOA Governance	SOA and IT Governance Alignment	SOA and IT infrastructure Governance Alignment	Governance through Policy
<b>Methods</b>	Structured Analysis & Design	Object Oriented Modeling	Component Based Development	Service Oriented Modeling	Service Oriented Modeling	Service Oriented Modeling for Infra (CDSP)	Business Grammar Oriented Modeling
<b>Applications</b>	Modules	Objects	Components	Services	Process Integration via Services	Process Integration via Services	Dynamic Assembly; context-aware invocation
<b>Architecture</b>	Monolithic Architecture	Layered Architecture	Component Architecture	Emerging SOA	SOA	Grid Enabled SOA	Dynamically Re-Configurable Architecture
<b>Information</b>	Application Specific	LOB or Enterprise Specific	Canonical Models	Information As a Service	Enterprise Business Data Dictionary and repository	Virtualized Data Services	Semantic Data Vocabularies
<b>Infrastructure</b>	LOB Platform Specific	Enterprise standards	Common Reusable Infrastructure	Project-based SOA Environment	Common SOA Environment	Virtual SOA Environment; S&R	Dynamic Sense, Decide & Respond
	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>	<b>Level 6</b>	<b>Level 7</b>

**SUMMIT**

**JBoss  
WORLD**

**PRESENTED BY RED HAT**

