PCI Virtualization and Cloud Controls

Kennet Westby
President
Coalfire
1. Why are companies moving to the Cloud?

2. Defining Virtualization and Cloud Computing

3. Assessing Risks and challenges with Cloud Computing

4. Compliance and Regulation in Virtual and Cloud Environments (PCI, HIPAA, FEDRAMP)

5. Recommendations

6. Key Takeaways
Cost savings comes from a variety of areas and varies with the size and complexity of the environment.

Examples of savings:
- Reduced hardware costs
- Reduced energy consumption and energy costs
- Improved server to admin ratio
- Reduced server maintenance and operation costs
- Reduced facilities maintenance and operations costs
- Improved automation for server management and provisioning
Cloud Computing
“IT should be planning, moving to private clouds”
- Gartner – June 16th, 2011

Cloud computing is a means “for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Virtualization
**Virtualization**, in computing, is the creation of a virtual (rather than actual) version of something...

- *Wikipedia*

**Virtualization** separates applications, desktops, machines, networks, data and services from their physical constraints. Virtualization is an evolving concept, encompassing a broad range of technologies, tools, and methods, and can bring significant operational benefits to organizations that choose to leverage them.

- *PCI Info Sup P.3*

45% of servers today are using virtualization, increasing to 77% by 2015.

60% of virtual servers will be less secure than their physical counterparts through 2012.

80% of enterprises now have a virtualization program or project.
What’s wrong with my home PC?

- Software
- Operating System
- Hardware
Let's consolidate

Virtual Machine 1

Virtual Machine 2

Virtual Environment

Hypervisor

Operating System

Hardware
What Virtual Environment are you Running?

Virtual Environment

Virtual Machine 1

Virtual Machine 2

Virtual Environment

Virtual Machine 1

Virtual Machine 2

Type 1 Hypervisor
(“Bare Metal”, “Native”)

Type 2 Hypervisor
(“Hosted”)

Hypervisor

Hardware

Software

Hypervisor

Server O/S

Hardware
“Hypervisors are not created equal, and it is particularly important to choose a solution that supports the required security functions for each environment. “

- PCI Info Sup p. 10
“Mixed-mode” refers to a virtualization configuration where both in-scope and out-of-scope virtual components are running on the same hypervisor or host.
Multi-Tenancy?

Tenant 1

Tenant 2

Virtual Environment

Multi-Tenant
Assessing Risk
Risk and uncertainty

Table 3-6. Risk-Level Matrix

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>Impact</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Low (10)</td>
<td>Medium (50)</td>
<td>High (100)</td>
<td></td>
</tr>
<tr>
<td>High (1.0)</td>
<td>Low</td>
<td>10 X 1.0 = 10</td>
<td>Medium</td>
<td>High</td>
<td>100 X 1.0 = 100</td>
</tr>
<tr>
<td>Medium (0.5)</td>
<td>Low</td>
<td>10 X 0.5 = 5</td>
<td>Medium</td>
<td>Medium</td>
<td>100 X 0.5 = 50</td>
</tr>
<tr>
<td>Low (0.1)</td>
<td>Low</td>
<td>10 X 0.1 = 1</td>
<td>Low</td>
<td>Low</td>
<td>100 X 0.1 = 10</td>
</tr>
</tbody>
</table>

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

All quantitative assessments start with qualitative assessments. We assume we know the rules of the game.
Risk #1/2 – Subcontracting – Up/Down Stream Risks

- Agency / Organization
- Slow Adoption of direct cloud service providers (but increasing)
- Cloud Service Provider
- Fast adoption of the cloud to reduce costs, keep up with changing demands, increase service offerings.
- Classic Service Provider
- Rapid Adoption of Service Providers
Risk #3 Encryption

- Does encrypted data need to be protected with the same controls as non-encrypted data?
- Are there advantages to using hardware-based encryption that can’t be duplicated through software?
- How does an assessor validate the effectiveness of the encryption process.
- Can encryption reduce the scope/accreditation boundary?
- Do we need different test procedures for encryption in memory, applications, storage, transmission?
Risk #4 Scope Reduction

Apply all controls to all systems.
Apply some controls to some systems.
Apply new processes to address new risks.

Do all controls have to apply to all systems?
Many virtual components do not have the same level of access control, logging, and monitoring as their physical counterparts.

In this example, a third party vendor (Hytrust) has created a centralized way to enforce access control, view logs, and centralize data.
Risk #6 Intra-Cloud Communication
Risk #7 – Training and Certification Programs

Without training, what is the value of our risk assessments?
From a mere handful of malicious apps at the start of the year, it skyrocketed to more than a thousand malicious Android apps by the middle of December 2011. The average month-on-month growth rate for the second half of 2011 was more than 60%. If this growth rate is sustained this year, then 2012 will definitely be an “exciting” year for Android. Why is this so? If current trends hold, we may be able to see more than 120,000 malicious Android apps by December 2012.
Risk #9 – Nested Accreditation - Scope
#10 Continuous Monitoring – Centralized Data

- Use vSDS to scan environment
- VMs with credit card data are reported
- Create CDE and Non-CDE

What VMs need to be considered in my PCI Environment?
Technical Challenges

Vulnerability Scanning
What is the “standard” for scans? Do they have to be authenticated? How are vulnerabilities ranked? How do you scan dormant virtual machines? Do we have appropriate vulnerabilities for cloud components in the NVD? Do risk rankings apply equally to the cloud?

Penetration Testing
What is the “standard” for penetration testing? White box, black box, grey box? What level of credentials? What do internal penetration tests require? What is an “acceptable” penetration test?

Mixed Mode
Can virtual machines of different security levels reside on the same physical hardware? Can they share memory, networking, storage, etc.? If one component is SECRET, does that make all routers, servers, and the hypervisor SECRET?

Multi - Tenancy
What are the minimum controls necessary to ensure that the security posture of one client cannot affect the security posture of another client? What’s the difference between segmentation using software and virtualization over physical segmentation? Are firewalls enough?

Configuration Management
Clouds are built from hardware, software, and virtual components? What benchmarks are there for virtual switches, virtual firewalls, hypervisors, SANS, routers, etc. Are the vendor recommendations good enough, or do we need Federal standards (such as FDCC), CIS, NIST, DISA? What reference architectures exist?
Compliance in the Cloud
Compliance is built from standards. Today there are several emerging standards attempting to solve the question “what are reasonable controls “

- **Big Issues**
  1. What is the Cloud?
  2. What are the appropriate controls for the cloud?
  3. What is the scope/boundary of the assessment?
  4. What are the appropriate tests?
  5. What are the required skillsets?

- **Other Issues**
  1. What tools are required?
  2. What education is required?
  3. How much testing can be leveraged from other audits/assessments?
  4. How do different approaches affect scope (encryptions, access control, authentication)?
  5. What does the report look like?
  6. How often should it be conducted?
  7. How does it integrate with continuous monitoring?
  8. What’s the appropriate sample size for a dynamic environment?
Different Industries have similar challenges.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Regulations</th>
<th>Evaluation</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD</td>
<td>8500, STIGS</td>
<td>C&amp;A</td>
<td>NEED FOR SIMILAR CLOUD TECHNOLOGIES AND AUDIT READY CONTROLS</td>
</tr>
<tr>
<td>BANKING</td>
<td>FFIEC</td>
<td>EXAMS AUDITS</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>PCI DSS</td>
<td>QSA</td>
<td></td>
</tr>
<tr>
<td>FEDRAMP</td>
<td>NIST 800-53</td>
<td>3PAO</td>
<td></td>
</tr>
<tr>
<td>UTILITIES</td>
<td>NERC CIP</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>HEALTHCARE</td>
<td>HIPAA HITECH</td>
<td>TBD</td>
<td></td>
</tr>
</tbody>
</table>
PCI in Virtual or Cloud Environments
PCI - Special Interest Group’s

PCI SSC Special Interest Groups (SIG)

Objective: Recommend changes, clarifications or improvements to the PCI Standards and the programs that support them

Approach: Leverage PCI SSC Participating Organizations’ valuable business and technical experiences, to collaborate with the PCI SSC on any supporting guidance or special projects relating to the PCI Security Standards

Result: Deliver actionable support documentation, specific instruction or recommendations to clarify how a specific technology can affect an organization’s compliance with specific PCI DSS requirements

Virtualization

Information Supplements

- Protecting Telephone-based Payment Card Data 03/18/2011
- Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance v1.0 10/2010
- PCI DSS Applicability in an EMV Environment v1.0 10/2010
- Skimming Prevention: Best Practices for Merchants 08/2009
- Requirement 6.6 Application Reviews and Web Application Firewalls Clarified v1.2 08/2009
- Requirement 11.3 Penetration Testing v1.2 08/2009
- PCI DSS Virtualization Guidelines v2.0 06/2011
- Wireless Guidelines 07/2002
Note the difference between “security” and “compliance”.

**PCI DSS Virtualization Guidelines**

- Different technology, same rules apply
- Benefits must be commensurate with risks
- No one size fits all approach

For optimal security, it’s recommended that all virtualization components meet PCI DSS requirements (out-of-scope systems can benefit from PCI security, too!)
PCI – Key Recommendations

At a Glance – Key Recommendations

- Evaluate the risks
- Virtualization leverages “virtual system components" that must meet PCI DSS requirements
- Implement ‘defense in depth’
- Isolate security functions
- Control access, even more than physical systems
- Choose your hypervisor carefully
“PCI Certified” Clouds?

The burden for providing proof of PCI DSS compliance for a cloud-based service falls heavily on the cloud provider, and such proof should be accepted only based on rigorous evidence of adequate controls.

The cloud provider should be prepared to provide their hosted customers with evidence that clearly indicates what was included in the scope of their PCI DSS assessment as well as what was not in scope; details of controls that were not covered and are therefore the customer’s responsibility to cover in their own PCI DSS assessment; details of which PCI DSS requirements were reviewed and considered to be —in place and —not in place; and confirmation of when the assessment was conducted.
The Virtualization Guidelines does not supersede the PCI DSS.

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate an entity’s network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce the scope of the cardholder data environment. A Qualified Security Assessor (QSA) can assist in determining scope within an entity’s cardholder data environment along with providing guidance about how to narrow the scope of a PCI DSS assessment by implementing proper network segmentation.
Examples of Scope

*Example of how scope and responsibility may differ* by type of cloud service:

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Type of Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IAAS</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Software, user applications</td>
<td></td>
</tr>
<tr>
<td>Operating systems, databases</td>
<td></td>
</tr>
<tr>
<td>Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)</td>
<td></td>
</tr>
<tr>
<td>Computer and network hardware (processor, memory, storage, cabling, etc.)</td>
<td></td>
</tr>
<tr>
<td>Data center (physical facility)</td>
<td></td>
</tr>
</tbody>
</table>

*Note: This is an example only. Cloud service offerings should be individually reviewed to determine how responsibilities between the cloud provider and cloud customer are assigned.*
FEDRAMP
Federal Risk and Authorization Program (FEDRAMP)

1. Apptis Inc. (Amazon Web Services)
2. AT&T
3. Autonomic Resources (Carpathia, Enomaly and Dell)
4. CGI Federal
5. Computer Literacy World (Electrosoft, XO, Secure Networks)
6. Computer Technology Consultants (Softlayer, Inc.)
7. Eyak Tech LLC
8. General Dynamics Information Technology (Carpathia)
9. Insight Public Sector (Microsoft)
10. Savvis Federal Systems
4 Key Takeaways

1. Fundamentals – virtualization, cloud, encryption, mobile, applications, business.

2. Agreements – what’s in writing?

3. Requirements – read them

4. Trust - but verify
### Additional Resources

<table>
<thead>
<tr>
<th>Document</th>
<th>Synopsis</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI DSS virtualization Guidelines</strong></td>
<td>Payment Card Industry (PCI) guidance in meeting PCI Data Security Standards (DSS) in a virtual and cloud environment.</td>
<td><a href="https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf">https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf</a></td>
</tr>
<tr>
<td><strong>Coalfire Website</strong></td>
<td>Many resources on Virtualization and Cloud Computing security and compliance trends.</td>
<td><a href="http://www.coalfire.com">www.coalfire.com</a></td>
</tr>
</tbody>
</table>
Questions?

www.Coalfire.com