Digital Trust in the Cloud

Liquid Security in Cloudy Places

Ron Knode

October 2009
Are You Afraid of the Dark?
Are You Afraid of the Dark?
Are You Afraid of the Dark?
Are You Afraid of the Dark?
Information Assurance is Cloud-Complicated
“Clouds are cloudy”

As visibility is lost …
- Where is the data?
- Who can see the data?
- Who has seen the data?
- Is data untampered?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

... Security, compliance, and value are lost as well
Cloud Processing
Three Big Obstacles to Value Capture

- Lack of standards
- Lack of portability
- Lack of transparency

Leading to problems with ...

controls …, compliance …, sustained payoff …, reliability …, liability …, confidentiality …, privacy …,

Compliance issues

- FRCP
- ISO27001
- HMG Infosec Standard 2
- U.K. Manual of Protective Security
- HIPAA
- HITECH in ARRA 2009
- GLBA
- PCI DSS
- ITAR
- DIACAP
- NIST 800-53 and FISMA
- SAS70
Absent Transparency … Some Big Problems

For example, … without transparency …

• No confirmed chain of custody for information
• No way to conduct investigative forensics
• Little confidence in the ability to detect attempts or occurrences of illegal disclosure
• Little capability to discover or enforce configurations
• No ability to monitor operational access or service management actions (e.g., change management, patch management, vulnerability management, …)
Weatherproofing the Enterprise for Cloud Services Today
Waiting for liquid security to evolve

Private Clouds

“Safe Computing” for Cloud Processing

Presumptive Security
Relationship between Transparency and Elastic Payoff Potential based on Deployment Model
Transparency Restores Information Assurance
Working with a “glass cloud” delivers the elastic benefits of the cloud

As visibility is gained …
• Configurations are known and verified
• Data exposure and use is collected and reported
• Access permissions are discovered and validated
• Processing and data locations are exposed
• Compliance evidence can be gathered and analyzed
• Processing risks and readiness become known

… Security, compliance, and value are captured as well
The Real Value Question for Cloud Processing

- How do we create digital trust in the cloud so we can reap the greatest elastic benefit?

- How do we bring transparency to the cloud so we can reap the greatest elastic benefit?

Without disqualifying any cloud provider or consumer … ?!
The Orchestration Core
Translation of Business Needs to Trusted Cloud Service Delivery

1. Trusted Cloud Service decision support
   - Trusted cloud services business needs analysis and recommendations (CloudAssist)

2. Orchestrator of Orchestrators
   - The automated arrangement, coordination, connection, and accountability for individual cloud service contributions

Business and technical needs integration knowledge

CloudTrust Protocol

Service Interface

Service Interface

Service Interface

Service Interface

Service Interface

Service Interface

Service Interface

Service Interface
<table>
<thead>
<tr>
<th>Type</th>
<th>Family</th>
<th>Information Request or Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Identity / Session</td>
<td>1. Identify service owner and initiate evidence session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Terminate evidence session</td>
</tr>
<tr>
<td></td>
<td>Evidence Requests</td>
<td>[for all cloud service units supporting service owner …]</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>3. What is current configuration for {Hypervisor? Guest O/S’s? Virtual switches? Virtual firewalls?}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. How does current configuration of {service unit type} differ from {service owner configuration specification/policy}</td>
</tr>
<tr>
<td></td>
<td>SCAP</td>
<td>[for all cloud service units supporting service owner …]</td>
</tr>
<tr>
<td></td>
<td>Vulnerability</td>
<td>5. Results of latest vulnerability assessment on {hypervisor; guest O/S’s; virtual switches; virtual firewalls}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Date of latest vulnerability assessment on {hypervisor; guest O/S’s; virtual switches; virtual firewalls}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Perform vulnerability assessment now on {hypervisor; guest O/S’s; virtual switches; virtual firewalls}</td>
</tr>
<tr>
<td></td>
<td>Anchoring</td>
<td>[for all cloud service units supporting service owner …]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Provide geographic location and affirmation (by unit identity)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Provide platform separation affirmation and identities (by unit identity)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Provide process separation affirmation – positive or negative - (by process name, e.g., storage encryption, storage de-duplication, …)</td>
</tr>
<tr>
<td></td>
<td>Audit Log</td>
<td>[for all cloud service units supporting service owner …]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11. Provide log of policy violations {in last ‘n’ hours} (e.g., malware elimination, unauthorized access attempts, …)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12. Provide audit/event log (for last ‘n’ hours)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13. Provide list of currently authorized users/subjects and their permissions</td>
</tr>
<tr>
<td></td>
<td>Policy introduction</td>
<td>14. …</td>
</tr>
<tr>
<td></td>
<td>Users &amp; permissions</td>
<td>15. … And more …</td>
</tr>
</tbody>
</table>
Research Conclusions Summary

- The desire to benefit from the elastic promise of cloud processing is blocked for most enterprise applications because of security and privacy concerns.
- The re-introduction of transparency into the cloud is the single biggest action needed to create digital trust in a cloud and enable the capture of enterprise-scale payoffs in cloud processing.
- Even today there are ways to benefit from cloud processing while technologies and techniques to deliver digital trust in the cloud are evolving.
- CSC has created a definition and an approach to "orchestrate" a trusted cloud and restore needed transparency.
- Resist the temptation to jump into even a so-called “secure” cloud just to save money.
  - Aim higher!
  - Jump into the right “trusted” cloud to create and capture new enterprise value.

www.csc.com/security/insights/32270-digital_trust_in_the_cloud
Or at
www.csc.com/lefreports
Imagine This!

Medical practice

18 GP’s

2 Specialists

3 different hospitals and clinics in 2 different states

The Opportunity

• Public, “for profit” enterprise in the Midwest US
• Accept Medicare and Medicaid, … but only if …
  – Major credit card to cover deductibles
• In-house electronic patient health record system (EHR)
  – Not certified by HHS
• Independent audits (financial and otherwise)
  – IT controls plan
  – Configuration specific
• Email and word processing assigned to public cloud already
• Desire to receive ARRA incentives for deploying fully certified EHR

The Payoff

• Double the size of the practice
• Reduce patient wait times
• Practice doctors spend 12% more time with patients
• Competitive advantage + Better care
CSC Trusted Cloud Services™ Make New Enterprise Value Possible

“Is my data still in the U.S. operating center?”

“Are the configurations I requested still being used for me?”

• Visibility is sustained
• Evidence is requested/delivered
• Digital trust is amplified
• Enterprise value is created

“…Right cloud. Right way.”
CloudTrust Protocol in Action

Turning on the lights
CloudTrust Protocol in Action
Checking the lights

CloudVision
DIGITAL TRUST IN THE CLOUD

CTP Request Status

<table>
<thead>
<tr>
<th>Status</th>
<th>#</th>
<th>Name</th>
<th>Requester</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>3</td>
<td>Current Configuration</td>
<td>Bob</td>
<td>CTP Response delivered by provider</td>
</tr>
<tr>
<td>Ready</td>
<td>8</td>
<td>Proximity Hosting Report</td>
<td>Bob</td>
<td>CTP Proximity response was delivered, if provided:</td>
</tr>
<tr>
<td>Waiting</td>
<td>18</td>
<td>Proximity Hosting Policy</td>
<td>Bob</td>
<td>Please press the Waiting button to configure your geographic location information.</td>
</tr>
</tbody>
</table>

Click on the green Ready button when the response is available.

This is the (12) time this page has been refreshed.
SCAP-based Configuration Request and Reply

NETWORK CONFIGURATION

IP Ranges

10.1.0.0/24
10.2.3.4

Network Connections:
- Maryland_General_Solaris
- Harbor_Hospital_Vista02
- Harbor_Hospital_Vista01
- Harbor_Hospital_W2K3
- Harbor_Hospital_Novell
- Harbor_Hospital_RedHatWeb
- Harbor_Hospital_EMEA

NETWORK SYSTEMS

Harbor_Hospital_W2K3
- Key: Harbor_Hospital_W2K3
- Type: STRING
- Value: running

Harbor_Hospital_Vista02
- Key: Harbor_Hospital_Vista02
- Type: LONG
- Value: 0

Harbor_Hospital_Novell
- Key: Harbor_Hospital_Novell
- Type: LONG
- Value: 1

Harbor_Hospital_XP01
- Key: Harbor_Hospital_XP01
- Type: LONG
- Value: -1

Harbor_Hospital_RedHatWeb
- Key: Harbor_Hospital_RedHatWeb
- Type: NULL

Harbor_Hospital_Vista01
- Key: Harbor_Hospital_Vista01
- Type: LONG
- Value: 1000

Harbor_Hospital_EMEA
- Key: Harbor_Hospital_EMEA
- Type: LONG
- Value: 512

vmnic3
- Key: vmnic3
- Type: STRING
- Value: Harbor_Hospital_W2K3

...
CloudTrust Protocol in Action
All the lights to check

<table>
<thead>
<tr>
<th>No.</th>
<th>Import Name</th>
<th>Quick Run</th>
<th>Edit in Background</th>
<th>Run</th>
<th>Published</th>
<th>Schedule</th>
<th>Edit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alarm Assignments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Alarm Transpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Alarm Cleared</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Alarms Closed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Application Inventory Per Day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Application Inventory Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Applications Per VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Closed VM Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Detected Applications Per VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Hosts By Version</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Infrastructure Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Network Connections Per VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Port Group Connection Density</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Port Group Connection Density By Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Repet VM Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Security Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Textual Difference</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Top 10 VMs With change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>VM Life Cycle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>VM Mismatch Drill Roll</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>VMs with Evolve Pass Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You Can Help

Are we at the fraying ends of a fad, or the beginning of a bonanza of IT value and performance?

- Secure cloud processing must offer more than just economy.
  - Security in the cloud is not enough
  - Trust in the cloud is necessary to create new enterprise value

- Partnership with government agencies and service and technology enterprises to solidify standards is necessary and inevitable.

- Join the cloud standards community of the OMG to help complete the open definition and application of cloud standards, including CloudTrust!

- Do not wait too long ... participate with your own cloud pilots for yourselves as well as your own communities ... Things are looking up!
Clouds Come with Rainbows

- Visibility brings trust
- Trust brings payoffs
- CloudTrust elements of transparency let everyone deliver visibility
- Join the OMG effort and help complete the definition

We are here

Digital Trust

CloudTrust

SCAP

Aim here