6th Annual IT Security Automation Conference

September 27-29, 2010 • Baltimore, Maryland
Baltimore Convention Center

Trustworthy Cloud Computing

Creating Trustworthy Cloud Systems

Steve Orrin

Director of Security Solutions
Software and Services Group
Intel, Corp.

Security Preventing Adoption of The Cloud

51% Security is the greatest concern surrounding cloud computing adoption.

- Gain visibility
- Maintain control
- Prove compliance

Source: CIO Magazine 2010 State of the CIO Study

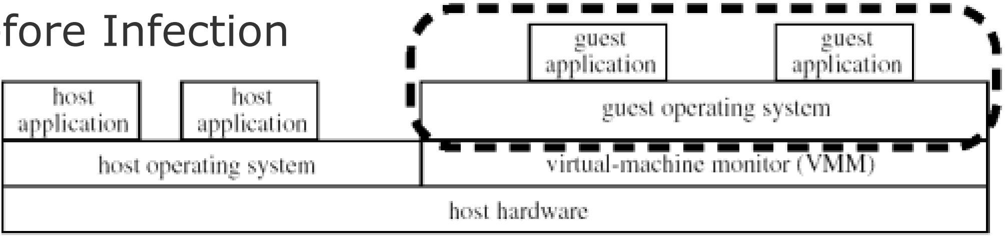
Key Challenges for Cloud Security

- Attacks on the infrastructure
- Co-tenancy threats
- Regulation Compliance
- Visibility and Audit Challenges

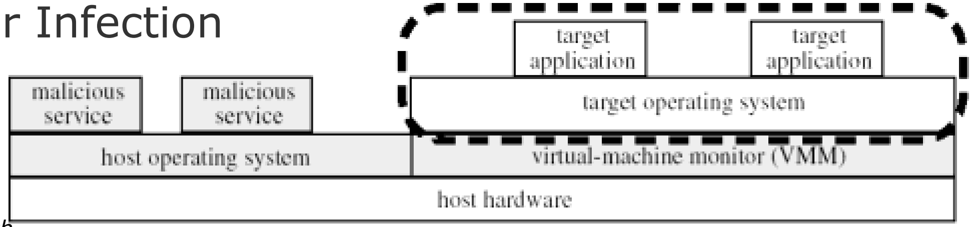
HyperJacking

- Hyperjacking involves installing a rogue hypervisor that can take complete control of a server. Regular security measures are ineffective because the OS will not even be aware that the machine has been compromised.
- Blue Pill/SubVirt use virtualization technology to create an ultra-thin hypervisor that takes complete control of the underlying operating system.

Before Infection



After Infection



SubVirt: Implementing malware with virtual machines
Samuel King & Peter Chen, University of Michigan
Yi-Min Wang, Chad Verbowski, Helen Wang, Jacob Lorch, Microsoft Research
BluePill
Joanna Rutkowska, Invisible Things

Clouds Under Attack, an Example
The Co-tenancy Problem

- Researchers at the UCSD and MIT were able to pinpoint the physical server used by programs running on the EC2 cloud and then extract small amounts of data from these programs, by placing their own software there and launching a side-channel attack.

For more on the details of the attacks see:
http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf

Title: Researchers find a new way to attack the cloud
Author: Robert McMillan
Source: IDG News Service
http://www.computerworld.com/s/article/9137507/Researchers_find_a_new_way_to_attack_the_cloud

Regulations abound

- Some Examples:
- FISMA, NIST’s SP 800-53 rev 3 guidelines, & FedRAMP
  - Tackling issues of multi-tenancy, shared resource pooling, lack of trust, visibility, and control of the service provider’s infrastructure.
- PCI DSS Section 2
  - 2.2.1 Implement only one primary function per server.
  - 2.2.2 Disable all unnecessary and insecure services and protocols
- HIPAA & Security Standards Technical Safeguards
  - “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”

Tenant-in-Control User Requirements

A tenant wants to run a business critical application in the cloud. Their requirements:

They want their provider to be following security best practices:

e.g., VMware Hardening guidelines

They want to be able to pass a FISMA audit (they handle federal data)

They want to be assured that they are booting from a secure root of trust (protection from inserted root kit)

Building Blocks of Trustworthy Clouds

- Creating a chain of trust rooted in hardware that extends to include the hypervisor.
- Hardening the Virtualization Environment using known best methods
- Providing Visibility for Compliance and Audit
- Using Automation to bring it all together

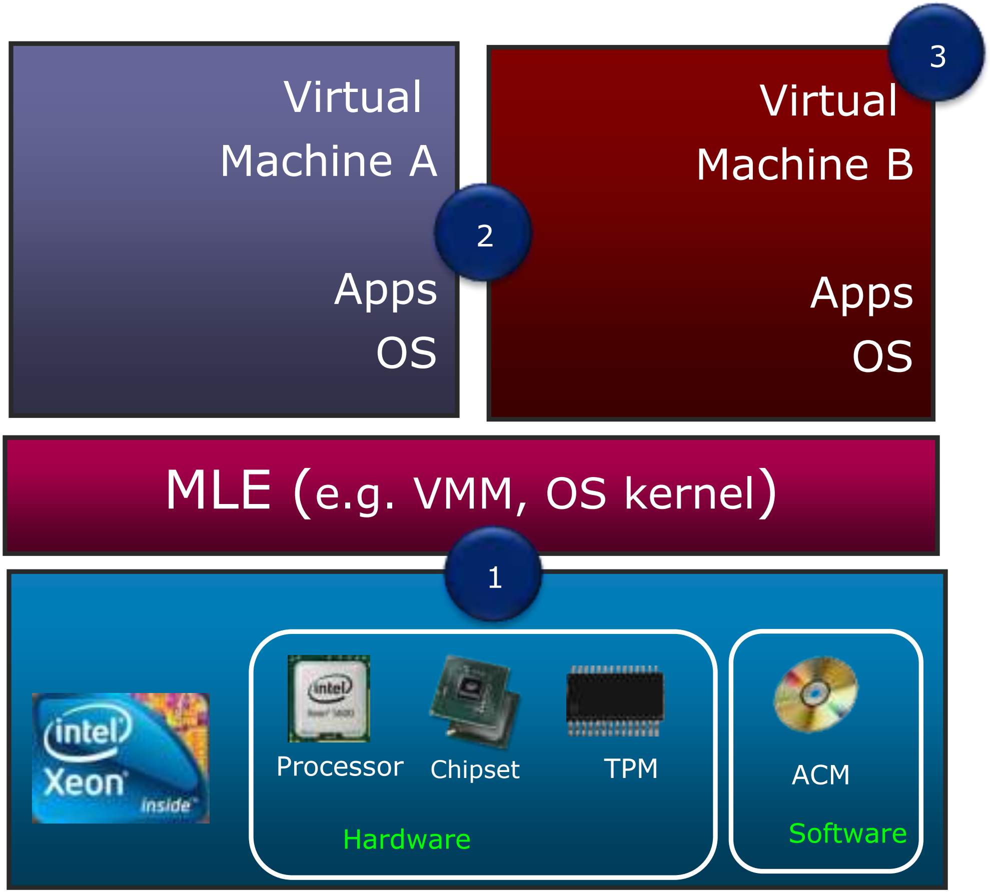
Intel Trusted Execution Technology (TXT)TM

A hardware based security foundation to build and maintain a *chain of trust*, to protect the platform from software based attacks

1 Verified Launch: Intel TXT hardware-based chain of trust enables launch of MLE into a known, expected state. Changes to MLE can be detected via hash-based measurements

2 Protected Configuration: Intel TXT hardware protects the launched configurations from malicious SW. Maintaining integrity of the measured launched environment identity

3 Secret Protection: Intel TXT hardware removes residual data at improper MLE shut down, protecting data from memory snooping software.



Virtual Machine A

Apps

OS

Virtual Machine B

Apps

OS

MLE (e.g. VMM, OS kernel)

Intel TXT enhances and complements the capabilities of VT to provide more robust trusted platforms

Harden the virtualization infrastructure

- Use established published methods like VMware's Hardening Guidelines
  - http://www.vmware.com/files/pdf/techpaper/VMware_vSphere_HardeningGuide_May10_EN.pdf

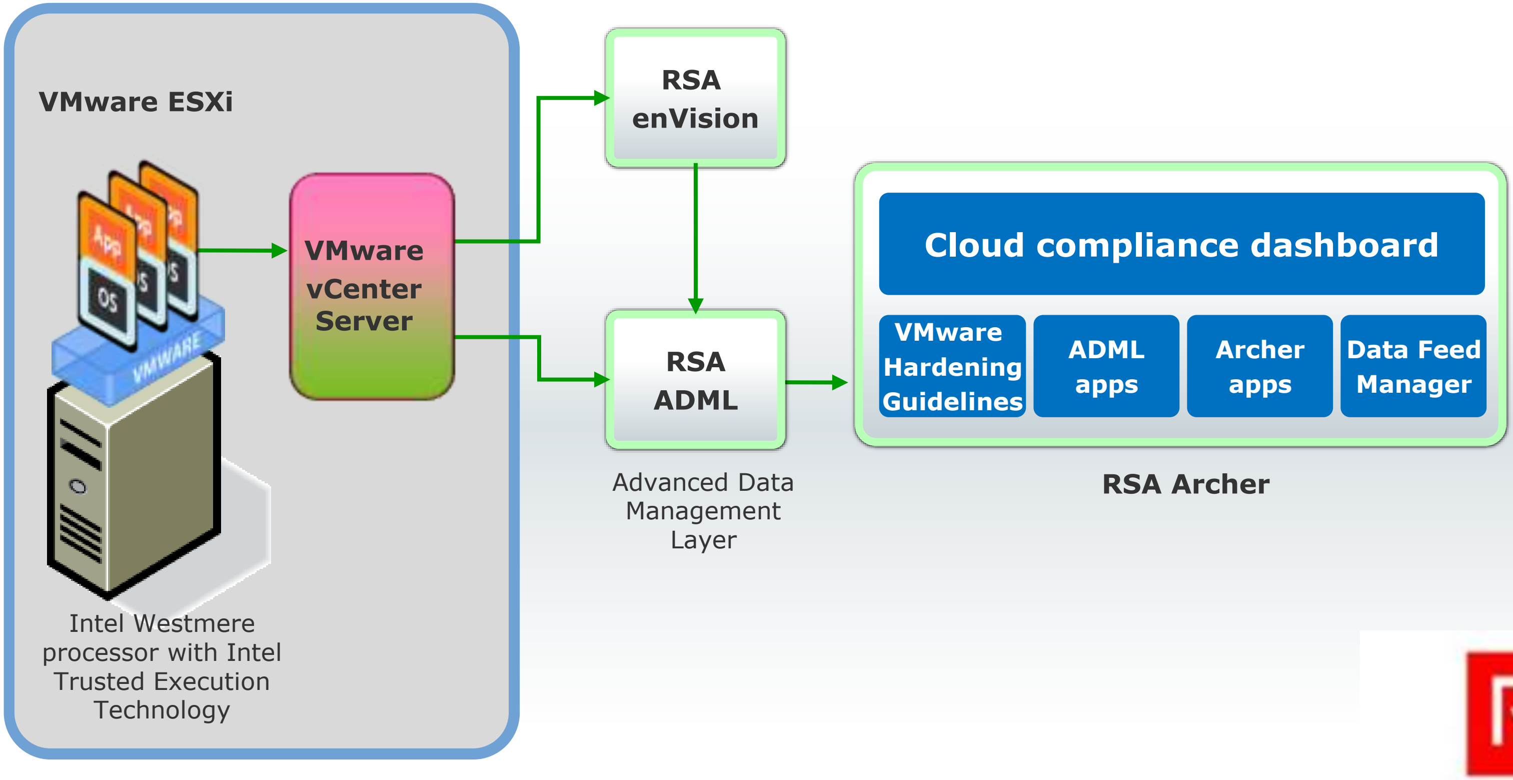
VMware

Security Hardening Guide

May 2010

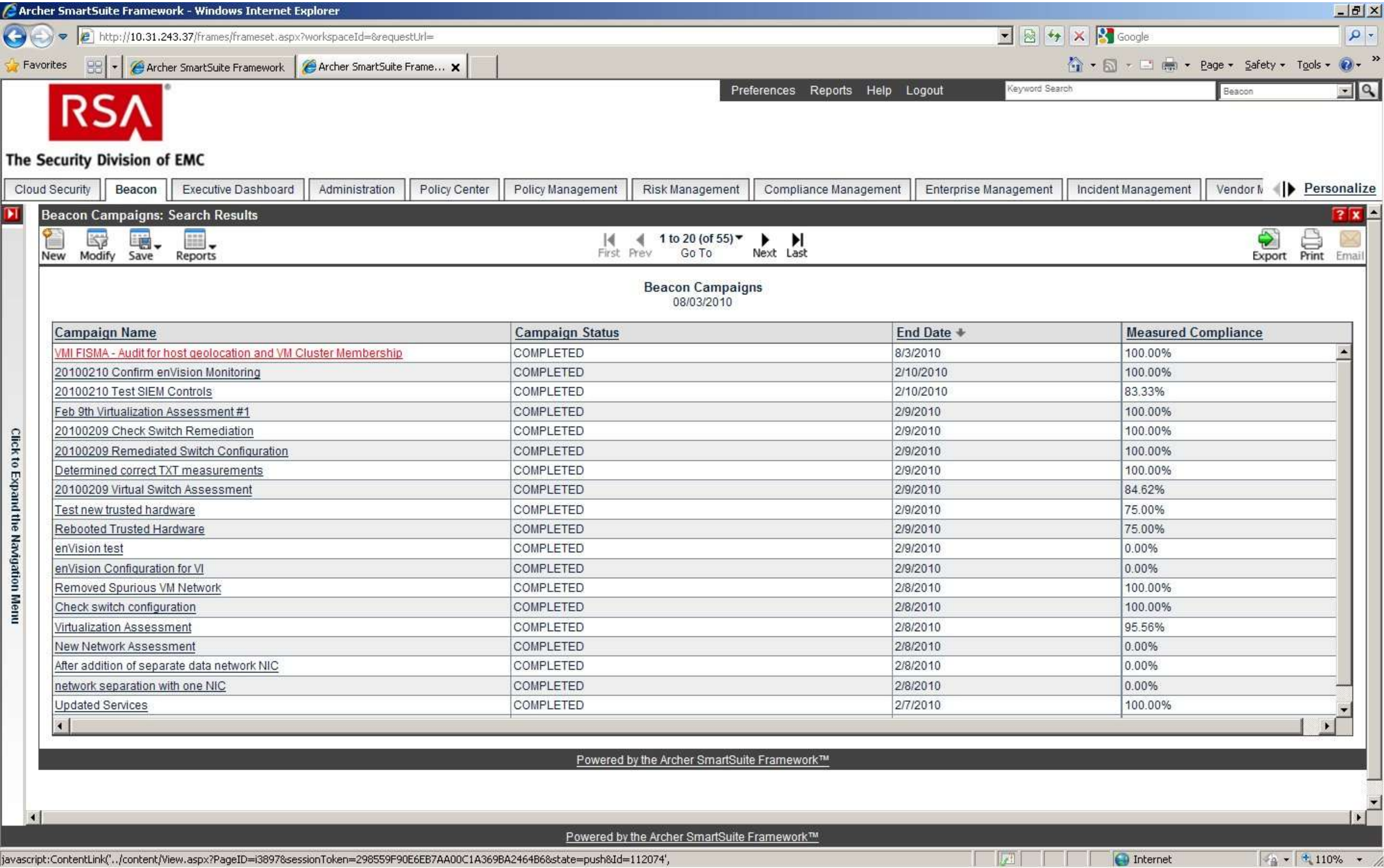
Cloud Compliance Architecture

Measuring and Monitoring Cloud Infrastructure Security


VMware ESXi
App
App
App
OS
OS
OS
VMWARE
VMware vCenter Server
Intel Westmere processor with Intel Trusted Execution Technology
RSA enVision
RSA ADML
Advanced Data Management Layer
Cloud compliance dashboard
VMware Hardening Guidelines
ADML apps
Archer apps
Data Feed Manager
RSA Archer

RSA® The Security Division of EMC

Archer Dashboard – FISMA Compliance Report

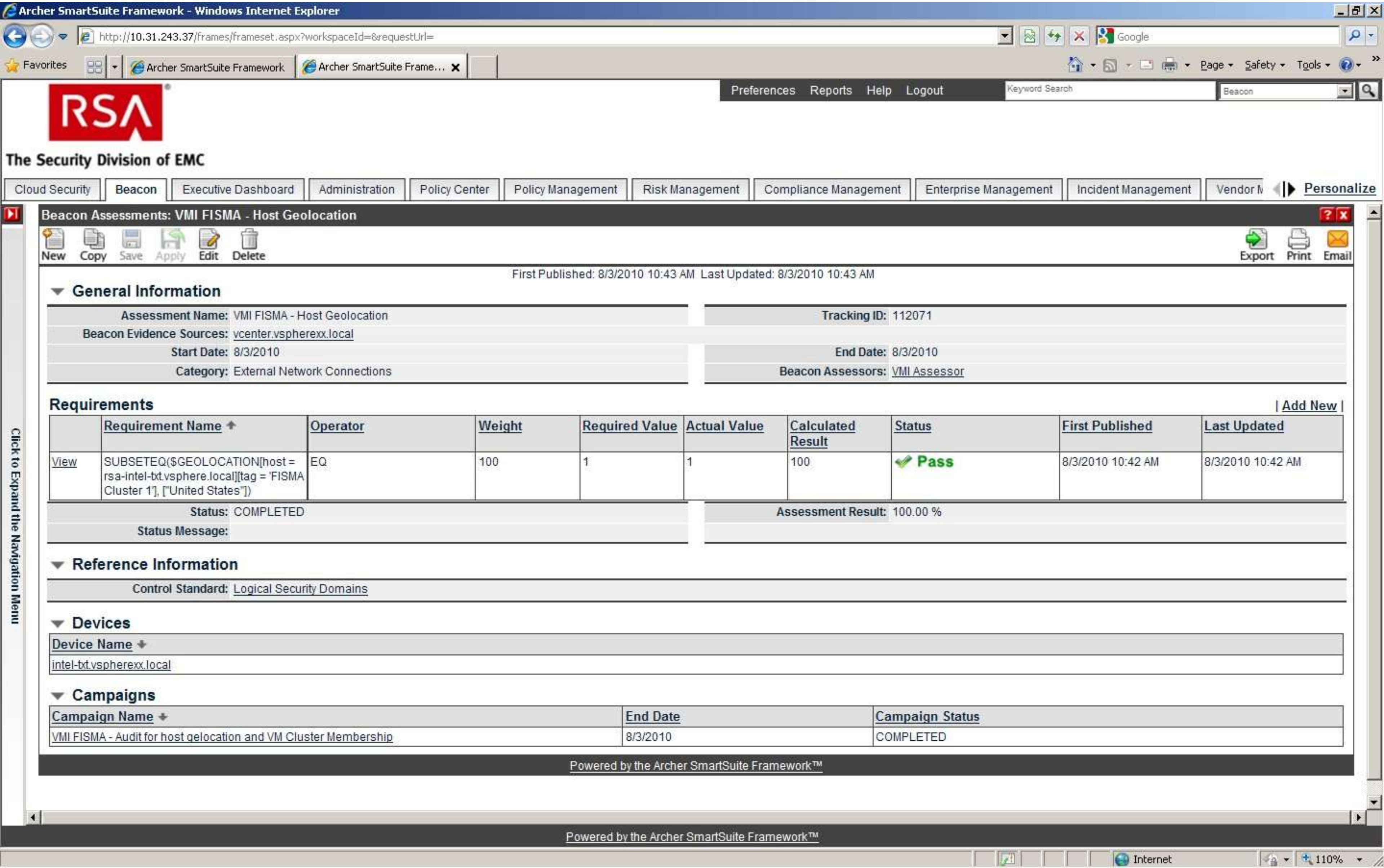


Beacon Campaigns
08/03/2010

Campaign Name	Campaign Status	End Date	Measured Compliance
VMI FISMA - Audit for host geolocation and VM Cluster Membership	COMPLETED	8/3/2010	100.00%
20100210 Confirm enVision Monitoring	COMPLETED	2/10/2010	100.00%
20100210 Test SIEM Controls	COMPLETED	2/10/2010	83.33%
Feb 9th Virtualization Assessment #1	COMPLETED	2/9/2010	100.00%
20100209 Check Switch Remediation	COMPLETED	2/9/2010	100.00%
20100209 Remediated Switch Configuration	COMPLETED	2/9/2010	100.00%
Determined correct TXT measurements	COMPLETED	2/9/2010	100.00%
20100209 Virtual Switch Assessment	COMPLETED	2/9/2010	84.62%
Test new trusted hardware	COMPLETED	2/9/2010	75.00%
Rebooted Trusted Hardware	COMPLETED	2/9/2010	75.00%
enVision test	COMPLETED	2/9/2010	0.00%
enVision Configuration for VI	COMPLETED	2/9/2010	0.00%
Removed Spurious VM Network	COMPLETED	2/8/2010	100.00%
Check switch configuration	COMPLETED	2/8/2010	100.00%
Virtualization Assessment	COMPLETED	2/8/2010	95.56%
New Network Assessment	COMPLETED	2/8/2010	0.00%
After addition of separate data network NIC	COMPLETED	2/8/2010	0.00%
network separation with one NIC	COMPLETED	2/8/2010	0.00%
Updated Services	COMPLETED	2/7/2010	100.00%

javascript:ContentLink('../content/View.aspx?PageID=i3897&sessionToken=298559F90E6EB7AA00C1A369BA2464B6&state=push&Id=112074',

Archer Dashboard – FISMA Compliance Report



Beacon Assessments: VMI FISMA - Host Geolocation

First Published: 8/3/2010 10:43 AM Last Updated: 8/3/2010 10:43 AM

General Information

Assessment Name:	VMI FISMA - Host Geolocation	Tracking ID:	112071
Beacon Evidence Sources:	vcenter.vspherexx.local		
Start Date:	8/3/2010	End Date:	8/3/2010
Category:	External Network Connections	Beacon Assessors:	VMI Assessor

Requirements

	Requirement Name	Operator	Weight	Required Value	Actual Value	Calculated Result	Status	First Published	Last Updated
View	SUBSETEQ($GEOLOCATION[host = rsa-intel-txt.vsphere.local][tag = 'FISMA Cluster 1'], ['United States'])	EQ	100	1	1	100	✓ Pass	8/3/2010 10:42 AM	8/3/2010 10:42 AM

Status:	COMPLETED	Assessment Result:	100.00 %
Status Message:			

Reference Information

Control Standard: Logical Security Domains

Devices

Device Name
intel-txt.vspherexx.local

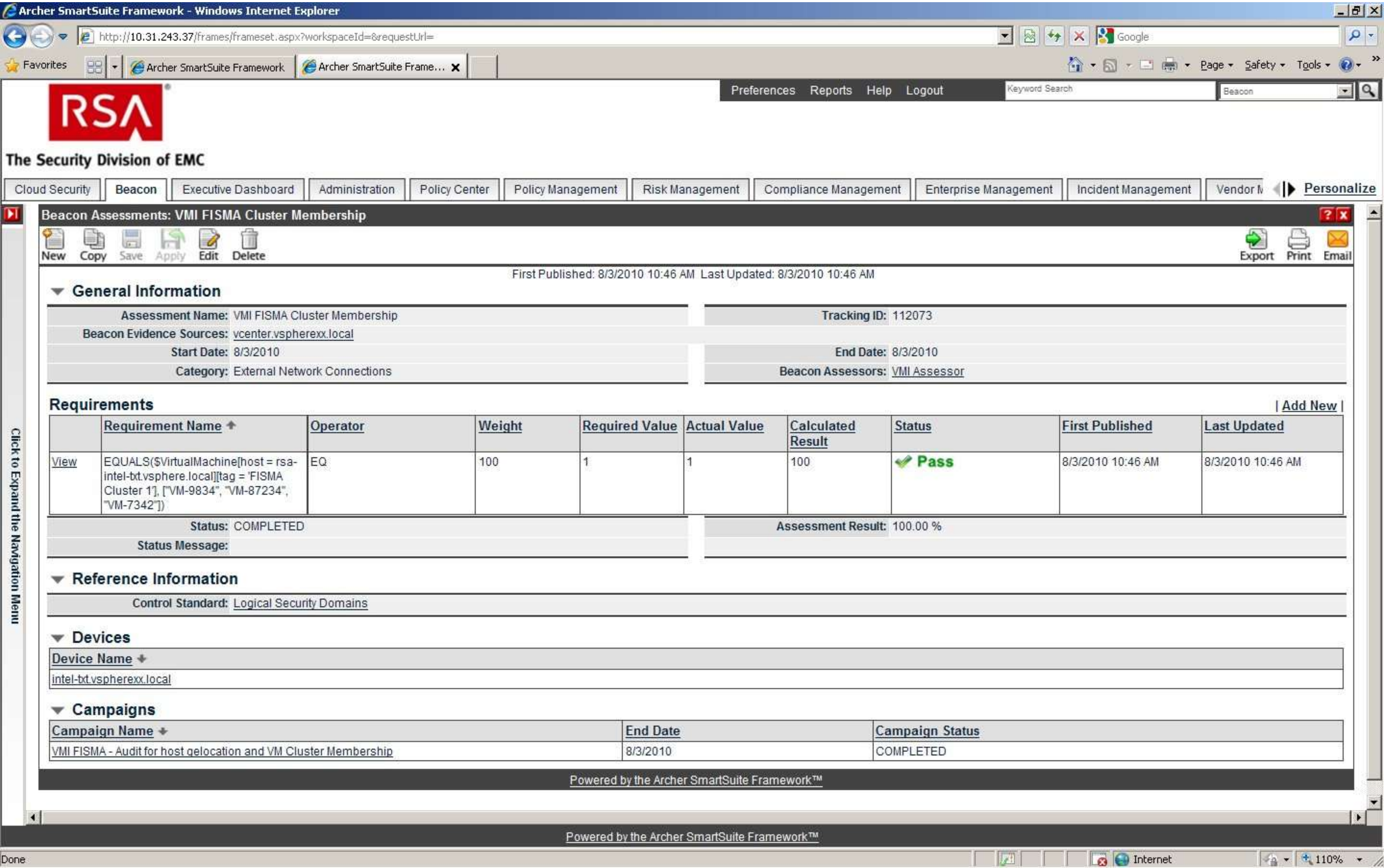
Campaigns

Campaign Name	End Date	Campaign Status
VMI FISMA - Audit for host gelocation and VM Cluster Membership	8/3/2010	COMPLETED

Powered by the Archer SmartSuite Framework™

Powered by the Archer SmartSuite Framework™

Archer Dashboard – FISMA Compliance Report



Beacon Assessments: VMI FISMA Cluster Membership

First Published: 8/3/2010 10:46 AM Last Updated: 8/3/2010 10:46 AM

General Information

Assessment Name:	VMI FISMA Cluster Membership	Tracking ID:	112073
Beacon Evidence Sources:	vcenter.vspherexx.local		
Start Date:	8/3/2010	End Date:	8/3/2010
Category:	External Network Connections	Beacon Assessors:	VMI Assessor

Requirements | Add New |

	Requirement Name	Operator	Weight	Required Value	Actual Value	Calculated Result	Status	First Published	Last Updated
View	EQUALS($VirtualMachine[host = rsa-intel-txt.vsphere.local][tag = 'FISMA Cluster 1'], ["VM-9834", "VM-87234", "VM-7342"])	EQ	100	1	1	100	✓ Pass	8/3/2010 10:46 AM	8/3/2010 10:46 AM

Status:	COMPLETED	Assessment Result:	100.00 %
Status Message:			

Reference Information

Control Standard: Logical Security Domains

Devices

Device Name
intel-txt.vspherexx.local

Campaigns

Campaign Name	End Date	Campaign Status
VMI FISMA - Audit for host gelocation and VM Cluster Membership	8/3/2010	COMPLETED

Powered by the Archer SmartSuite Framework™

Powered by the Archer SmartSuite Framework™

Summary

- There are real and perceived risks in the Cloud
  - Real: Improper configuration, unpatched bugs can lead to loss of confidentiality, integrity, and availability
  - Real: Loss of Control and Visibility on Infrastructure
  - Perceived: Fear of the unknown
- Risks can be mitigated, but it takes an ecosystem:
  - Intel TXT - Hardware Root of Trust
  - Trusted vSphere ESXi boot, measurements in vSphere vCenter – Chain of Trust up to hypervisor
  - RSA Archer GRC – visibility and compliance management
- Work with your Cloud Service Providers, vendors, OEMs, ISVs, to achieve Security, Trust and compliance
- Help develop and improve our standards so we can continue the momentum in the cloud.

Thank You

intel®

Notices

Intel and the Intel logo are trademarks or registered trademarks of
Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

** Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. All dates and product descriptions provided are subject to change without notice. This slide may contain certain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements

***The threats and attack examples provided in this presentation are intended as examples only. They are not functional and cannot be used to create security attacks. They are not be replicated and/or modified for use in any illegal or malicious activity.

****Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.