



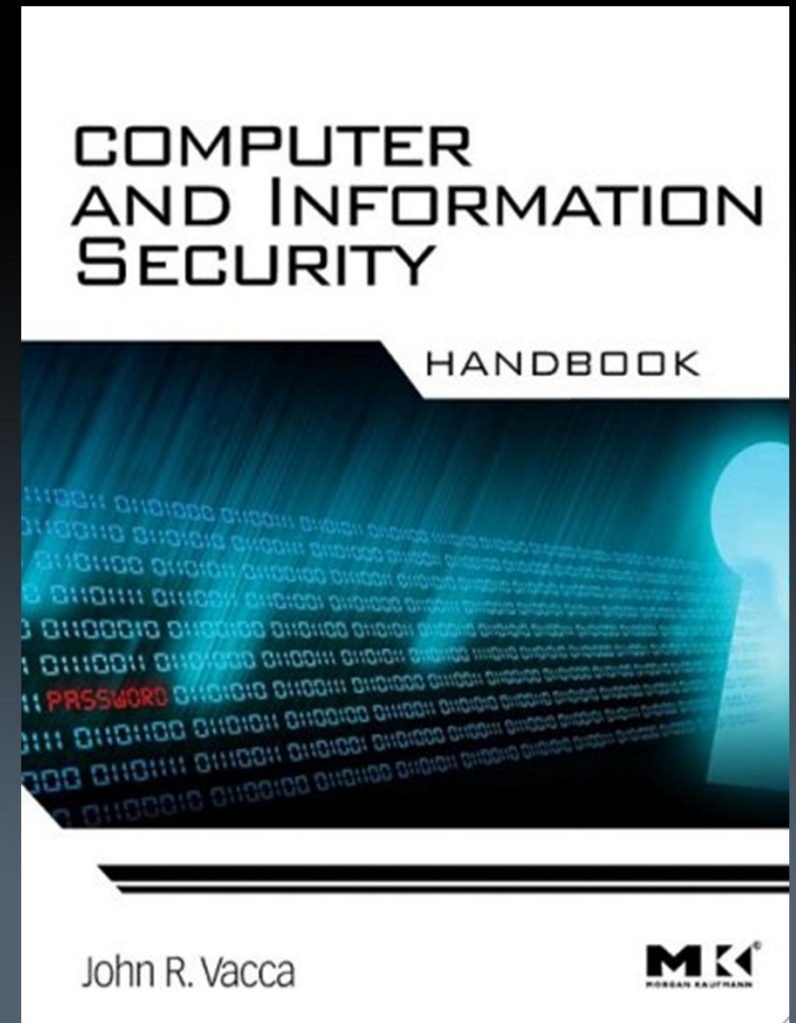
TAKEDOWNCON 19 MAY 2011

ADVANCES IN TRUSTED COMPUTING

Your Presenter

Robert Rounsavall

Director Secure Information Services
Cloud Security Alliance SME (SP)
Security Wanna-be
Former Navy Cryptologic Chief



Agenda

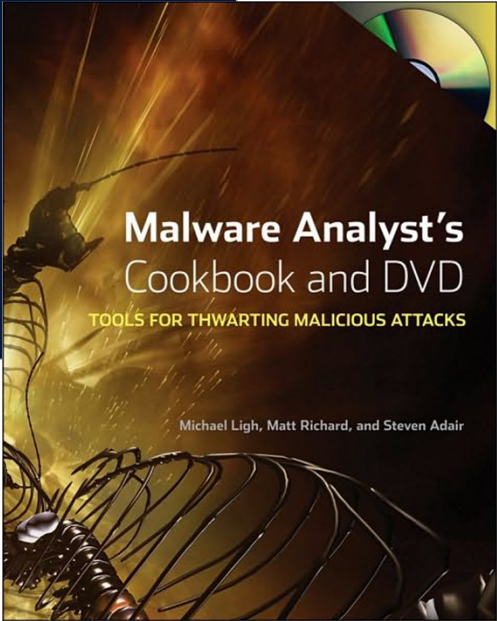
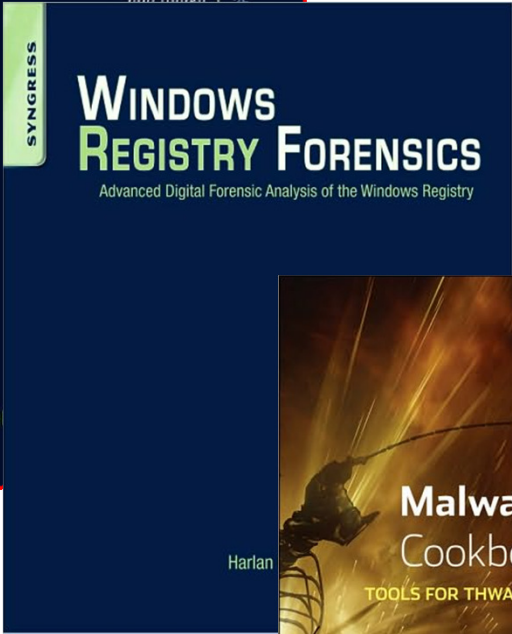
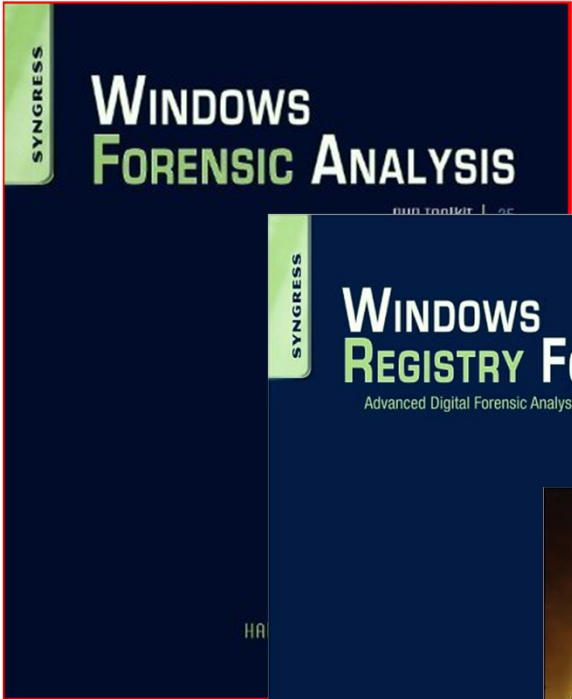
- Quick intro to my org and team
- What is “The Cloud” and what does it have to do with Trusted Computing
- What is Trusted Computing
- What are we doing with Trusted Computing
- Where I think it is going to go



TERREMARK



OUR SECURITY TEAM



The Cloud

- Definitions: Gartner, NIST, Wikipedia all have definitions
- SPI model
- Elastic Computing
- Self Provisioning
- Alternate Definition: Where attackers go to do fun and interesting things with credit card data that they have obtained



Front end of the cloud

The screenshot shows a web browser window with the URL <https://icenter.digitalops.net/Default.aspx>. The page title is "Enterprise Cloud" and the user is logged in as "Robert Rounsavall - Terremark-Citrix". The interface has a navigation bar with "Resources", "Devices", and "Network". Under "Devices", there are several action buttons: "Create Row...", "Create Group...", "Create Server...", "Create Blank Server...", and "VPN Connect...". Below these, there is a "Vulnerable" section and an "Internal Devices" section. The "Internal Devices" section is divided into "SIEM" and "clients". Under "clients", there are three server icons: "POC", "pocrhel", and "pocwindows" (which is highlighted in yellow). Below the "clients" section is a "SANS" section. At the bottom, there is a "Selected: Internal Devices > clients > pocwindows" breadcrumb and a toolbar with actions like "Rename...", "Configure...", "Manage IPs...", "Move...", "Shut Down...", "Delete", "Copy...", "Connect...", and "View Tasks...". A "DETAILS" panel is open for the selected server, showing the following information:

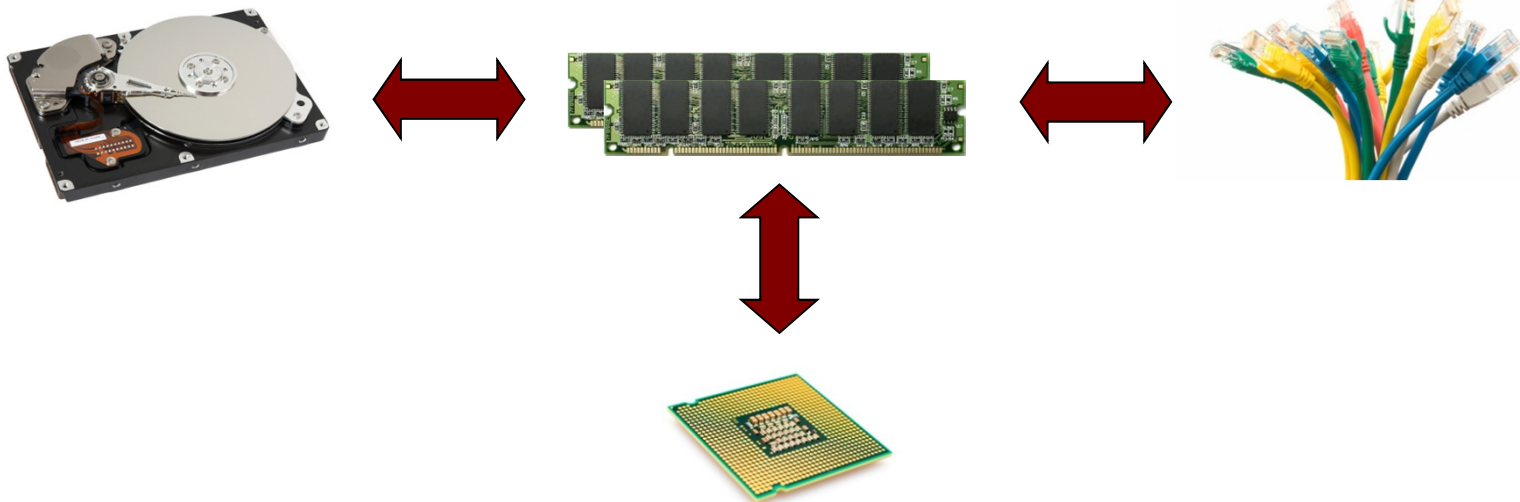
Detected IP:	10.153.34.53	Operating System:	Microsoft Windows Server 2003, Standard Edition (32-bit)	Active Tasks:	0
Processors:	1	Licensed By:	Service Provider	VMware Tools Status:	Current
Memory:	256 MB	Licensing Costs:	\$33.00/mo.		
Storage:	20 GB	Type:	Template		

What is really important

Hard Disk Image + Volatile Memory + Network Traffic

=

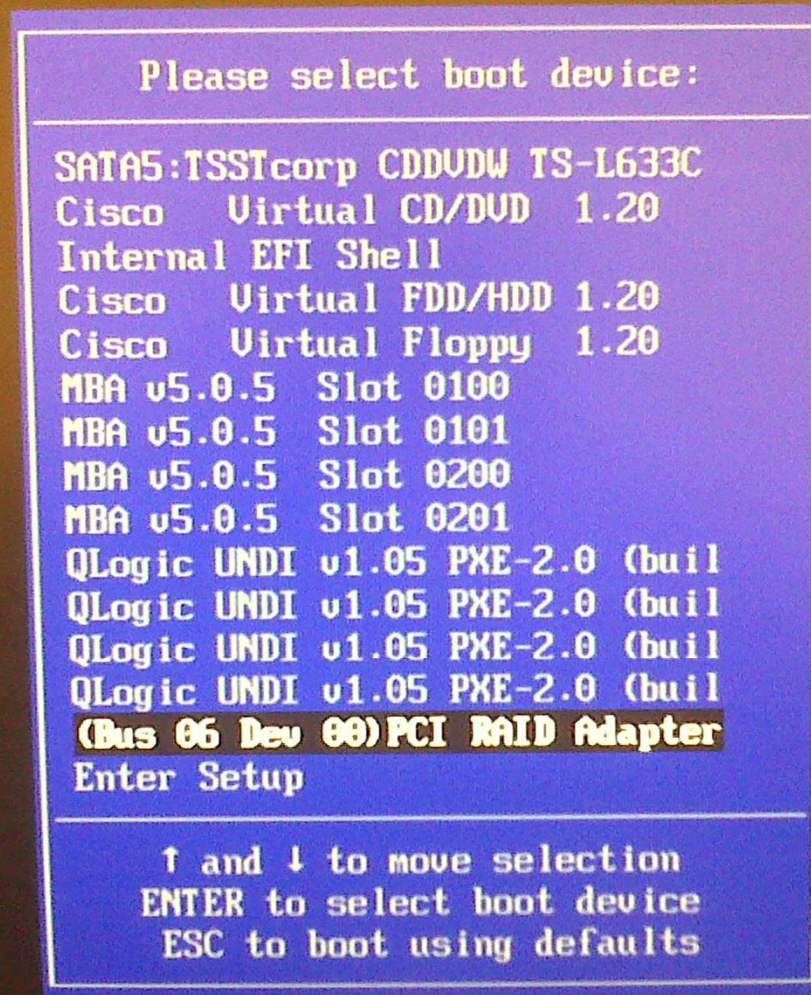
Rapid Detection, Effective Analysis and Good Decisions



Blade Computing



A Few Additional Boot Options



What does this have to do with Trusted Computing?

- As a cloud provider we get asked questions like:
- Where are my servers?
- How do you know?
- How do you protect against a hypervisor compromise?
- What do you do to validate against hardware attacks?
- How do you handle secure multi-tenancy?
- Up to now it has been a missing piece of our security instrumentation...



Timeline

- 2008: Invisible Things Lab reports some TXT bugs to Intel
- 2009: ITL presents at BlackHat on some vulnerabilities
- 2009: Our fed customers were asking about trusted computing
- 2010: RSA Conference: RSA/Intel/VMWare start talking about what they are doing with Trusted Computing
- 2010: Dell ships replacement system boards with malware on them
- 2010: Our commercial customers were asking about trusted computing
- 2011: RSA Conference: Intel shows working code and integrations with vSphere
- 2011: You will see GA support in VMWare
- 2011: ITL releases qubes OS that will support txt



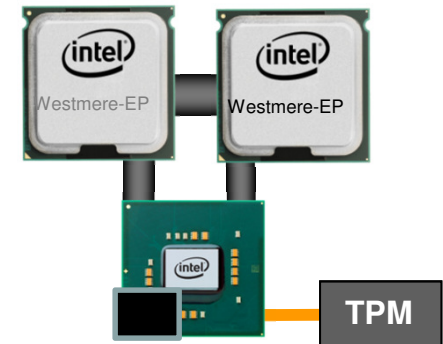
What is trusted computing?

- The term "trusted computing" refers to applications that leverage hardware-based "roots of trust" at the edge of the network and at the endpoints - sometimes referred to as "hardware anchors in a sea of untrusted software" - for higher assurance.
- Better virtual machine separation based on hardware controls
- Cryptographic channels based on hardware controls
- Validation and attestation of the platform

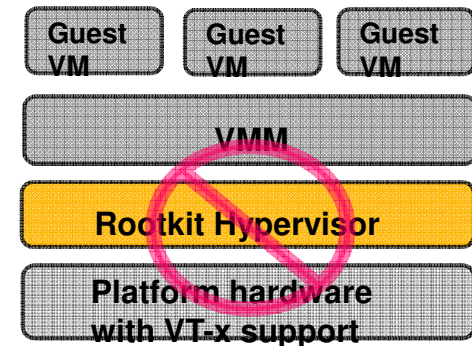


Intel Trusted Execution Technology (TXT)

- TXT enforces control through measurement, memory locking and sealing secrets
 - Allows greater control of launch stack and enables isolation in boot process



- TXT helps prevent attacks
 - Attempts to insert non-trusted VMM (rootkit hypervisor)
 - Reset attacks designed to compromise platform secrets in memory
 - BIOS and firmware update attacks



Helps prevent hijacking by rootkit

**Makes Platforms More Robust
Against Software-based Attacks**



Who Cares?

The Feds

Enterprises

Service Providers

Hardware and Software Vendors



Terms and definitions

- TPM- Trusted Platform Module
- PCR- Platform Configuration Register
- TXT- Trusted Execution Technology
- MLE- Measured Launch Environment
- Attestation- Reliably measuring and reporting on a configuration
- GRC- Governance Risk Compliance



POC

- Demonstrate that the technology actually worked
- What does working mean?
 - BIOS supports TXT/TPM
 - We can boot to a hypervisor on a trusted platform
 - We can validate whether or not the hypervisor is trusted
- Identify some use cases for the technology
 - How does this fit in with our existing security?



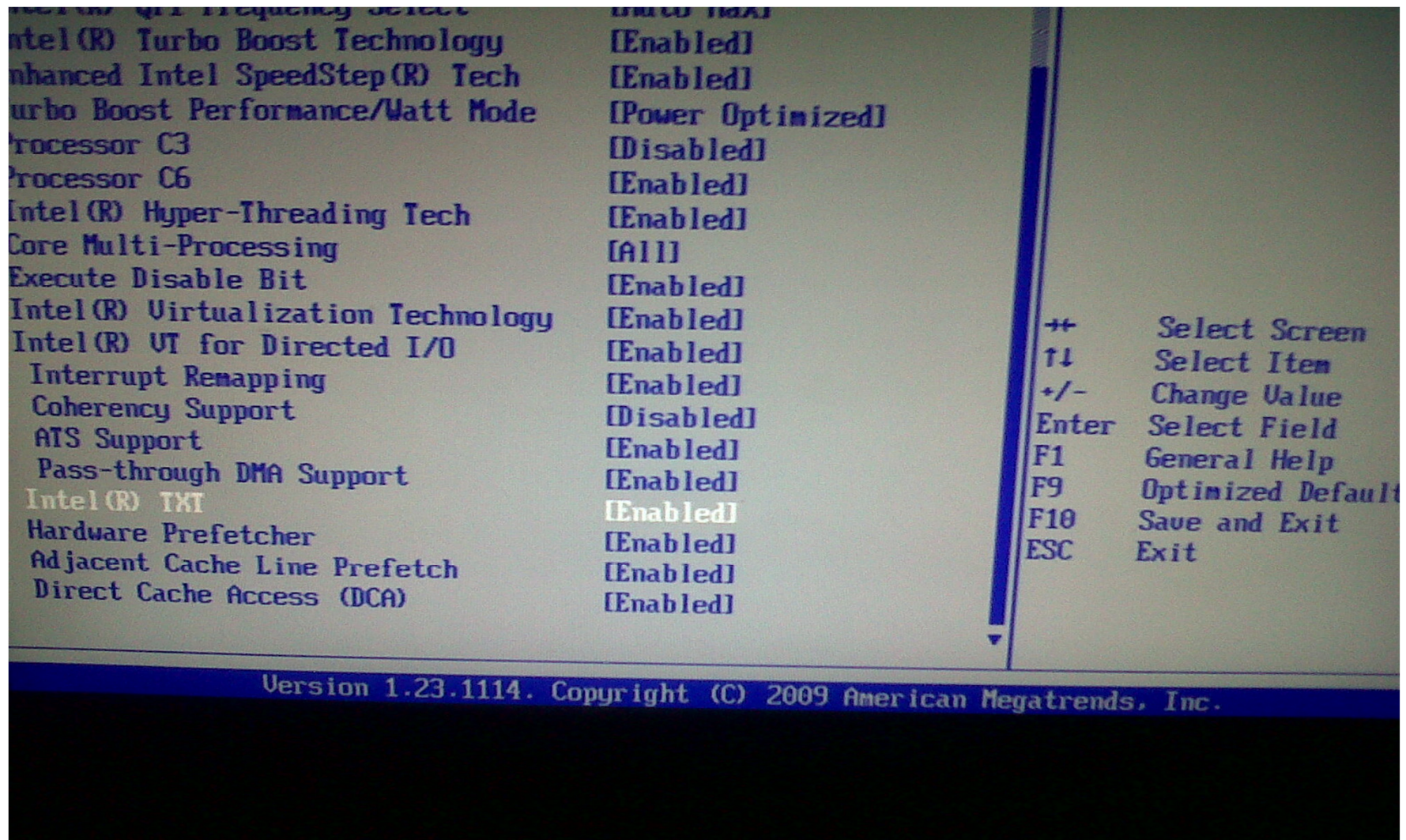
POC

Embedded vSphere Hypervisor Using Intel TXT

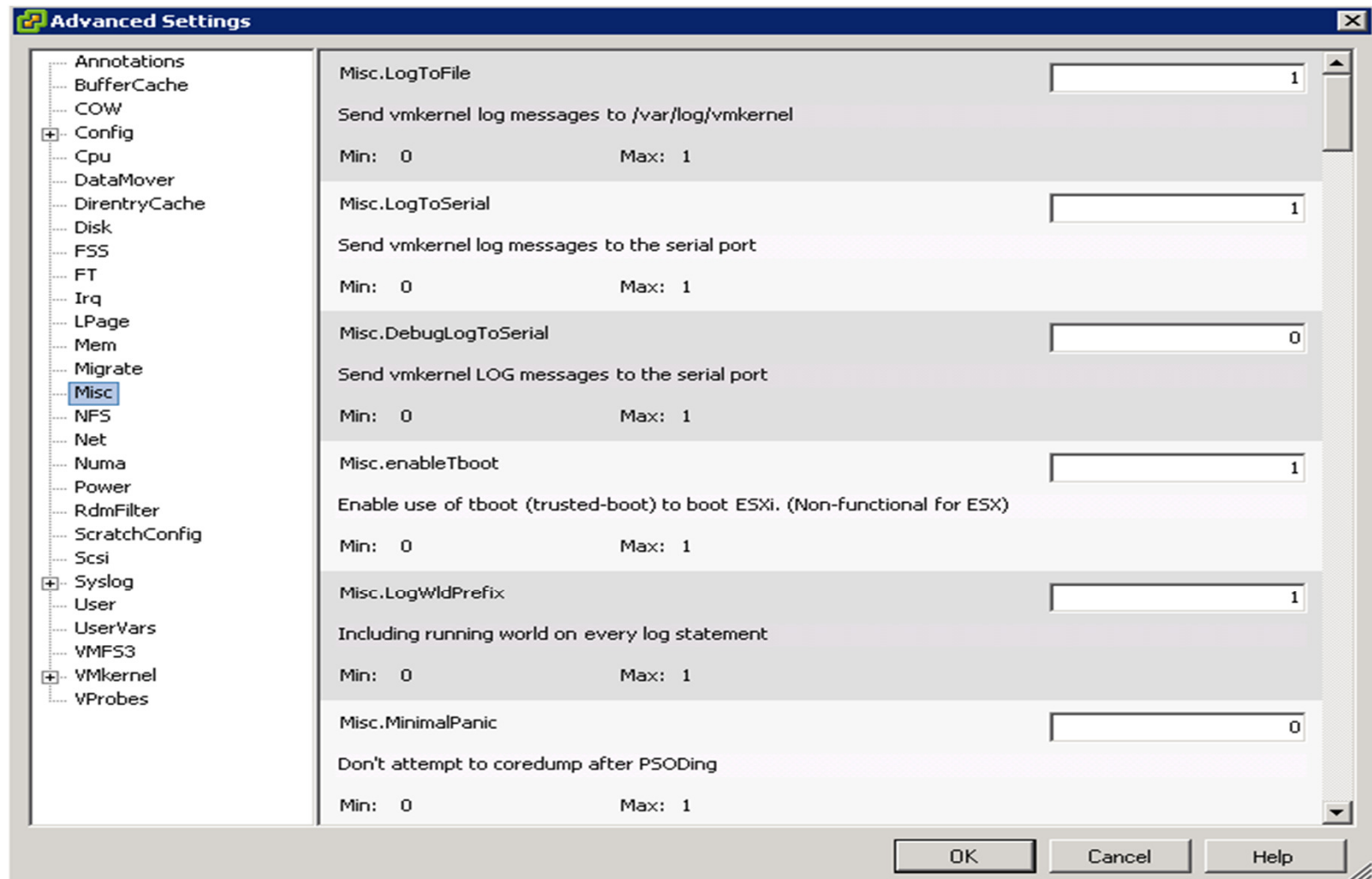
- All layers of the cloud require trust and security guarantees, even HW platforms that launch & run the VMware vCloud operating system
 - *Recently, hypervisors (e.g. VMware ESXi Server) are being “embedded” in platforms as they leave the factory*
 - *Future versions of VMware vSphere will provide these guarantees at the software, network, and storage levels.*
- VMware's vSphere hypervisor can be optimized to use Intel TXT to provide these guarantees at the hardware level:
 - *Allows vSphere to securely boot and measure its launch environment.*
- Measurements provided to VMware's vCenter can attest to integrity of each platform running vSphere hypervisor
- vCenter Apps can allow the customer to build policies & compliance activities that leverage these attestations
 - *Can be used to manage the operation and migration of workloads within the cloud*



Enable in BIOS (dependent on HW Vendor)



Enabling Trusted Boot



PCR (Platform Config Register) Values

Home

Data Object Type: HostTpmDigestInfo[]

Parent Managed Object ID: host-19

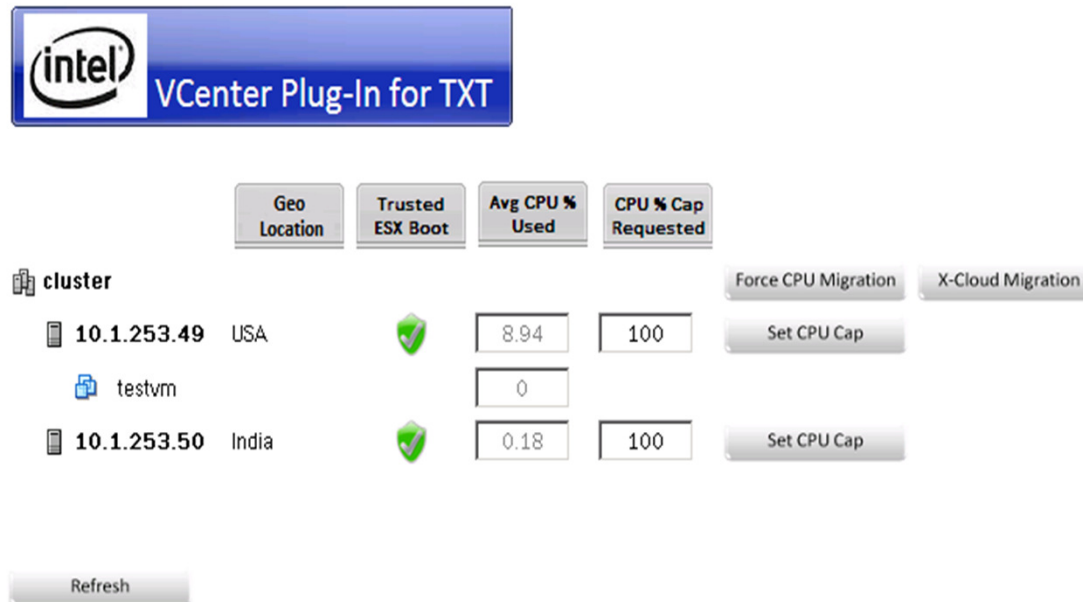
Property Path: runtime.tpmPcrValues

Properties



NAME	TYPE	VALUE																		
[0]	HostTpmDigestInfo	<table border="1"> <thead> <tr> <th>NAME</th> <th>TYPE</th> <th>VALUE</th> </tr> </thead> <tbody> <tr> <td>digestMethod</td> <td>string</td> <td>"SHA1"</td> </tr> <tr> <td>digestValue</td> <td>byte[]</td> <td> <ul style="list-style-type: none"> • -28 • 53 • -6 • -36 • 43 • -112 • -71 • 70 • 101 • 38 • -122 • -87 • -82 • -121 • 22 • -60 • 60 • -9 • -51 • -113 </td> </tr> <tr> <td>dynamicProperty</td> <td>DynamicProperty[]</td> <td>Unset</td> </tr> <tr> <td>dynamicType</td> <td>string</td> <td>Unset</td> </tr> <tr> <td>dynamicValue</td> <td>string</td> <td>Unset</td> </tr> </tbody> </table>	NAME	TYPE	VALUE	digestMethod	string	"SHA1"	digestValue	byte[]	<ul style="list-style-type: none"> • -28 • 53 • -6 • -36 • 43 • -112 • -71 • 70 • 101 • 38 • -122 • -87 • -82 • -121 • 22 • -60 • 60 • -9 • -51 • -113 	dynamicProperty	DynamicProperty[]	Unset	dynamicType	string	Unset	dynamicValue	string	Unset
NAME	TYPE	VALUE																		
digestMethod	string	"SHA1"																		
digestValue	byte[]	<ul style="list-style-type: none"> • -28 • 53 • -6 • -36 • 43 • -112 • -71 • 70 • 101 • 38 • -122 • -87 • -82 • -121 • 22 • -60 • 60 • -9 • -51 • -113 																		
dynamicProperty	DynamicProperty[]	Unset																		
dynamicType	string	Unset																		
dynamicValue	string	Unset																		



Intel Developing Plug-ins now



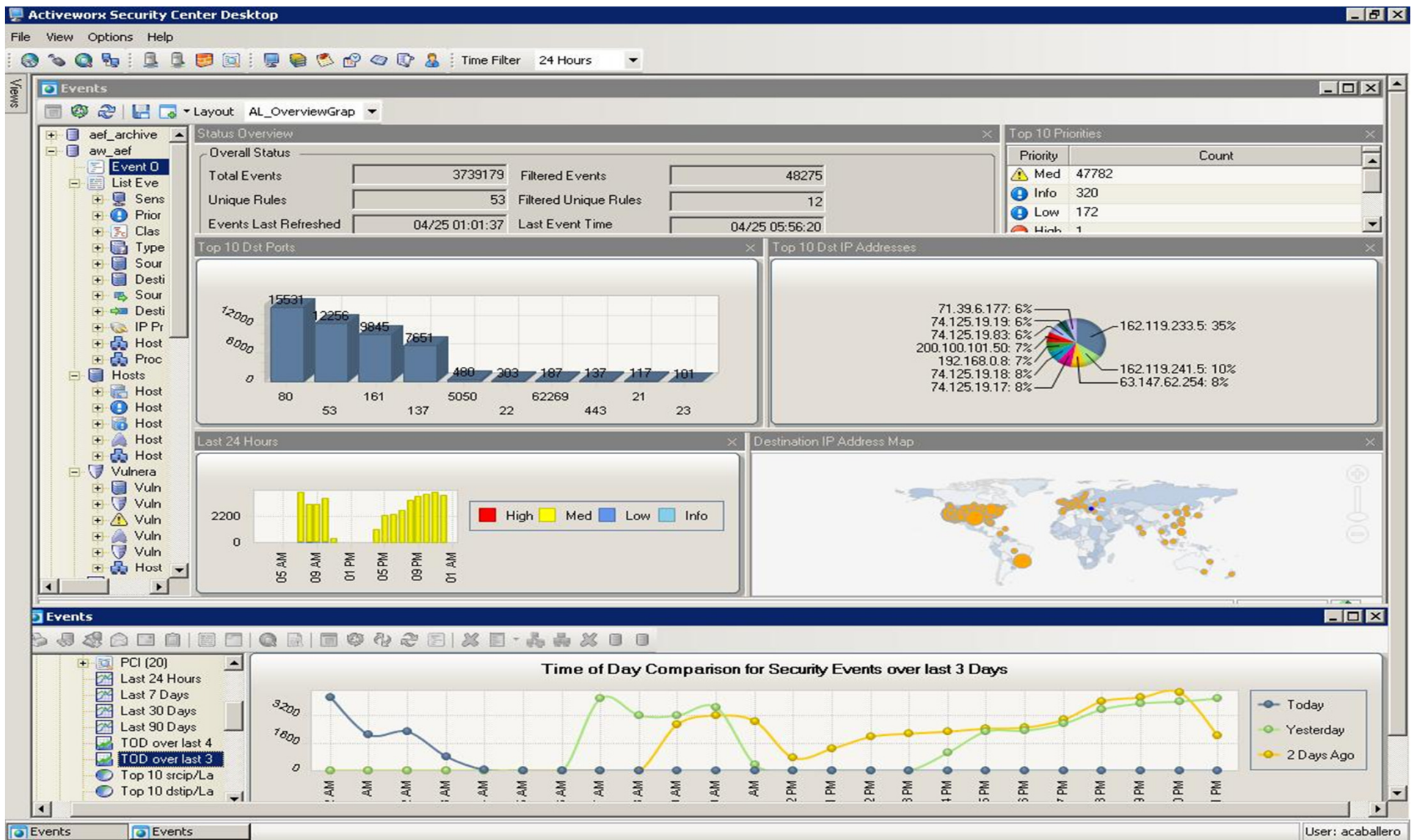
The screenshot displays the Intel VCenter Plug-In for TXT interface. At the top left is the Intel logo and the text "VCenter Plug-In for TXT". Below this is a table with columns: "Geo Location", "Trusted ESX Boot", "Avg CPU % Used", and "CPU % Cap Requested". The table lists two hosts: "10.1.253.49 USA" and "10.1.253.50 India". The "testvm" entry is indented under the first host. To the right of the table are buttons for "Force CPU Migration", "X-Cloud Migration", and "Set CPU Cap". A "Refresh" button is located at the bottom left of the interface.

	Geo Location	Trusted ESX Boot	Avg CPU % Used	CPU % Cap Requested	
cluster					Force CPU Migration X-Cloud Migration
10.1.253.49	USA		8.94	100	Set CPU Cap
testvm			0		
10.1.253.50	India		0.18	100	Set CPU Cap

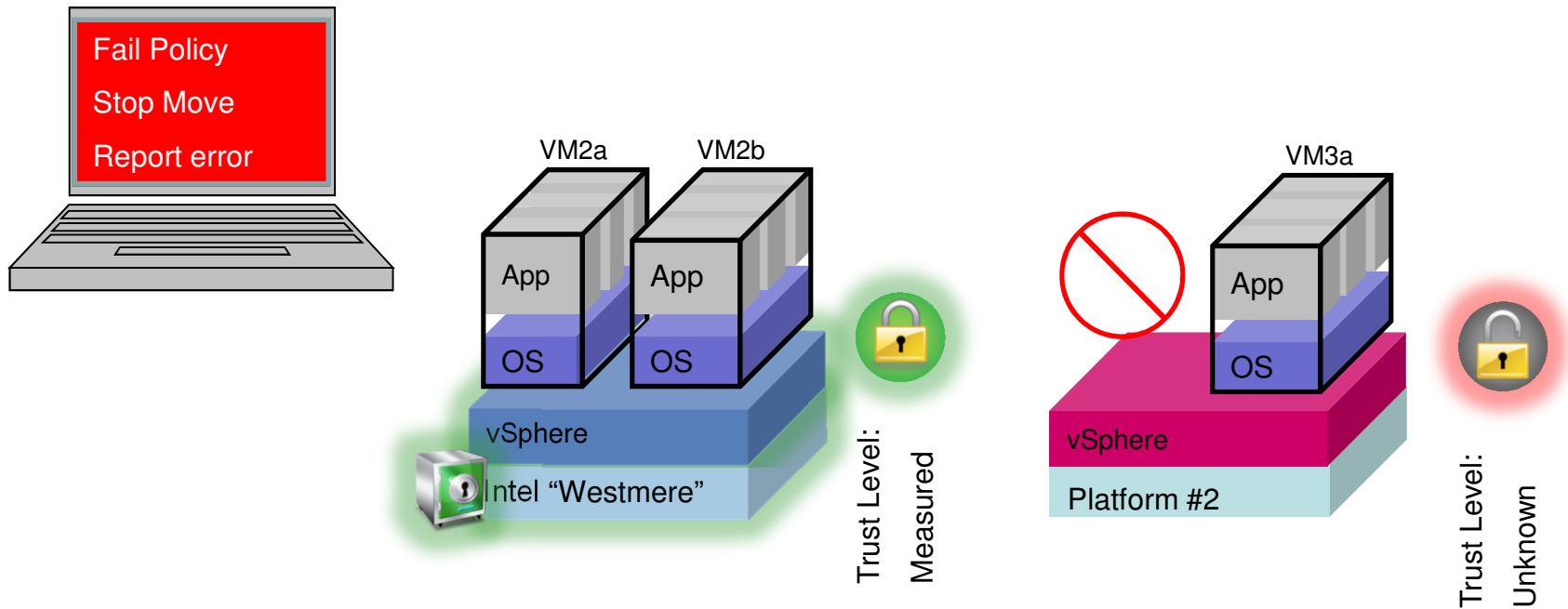
Refresh



vSphere can send alerts to your SIEM



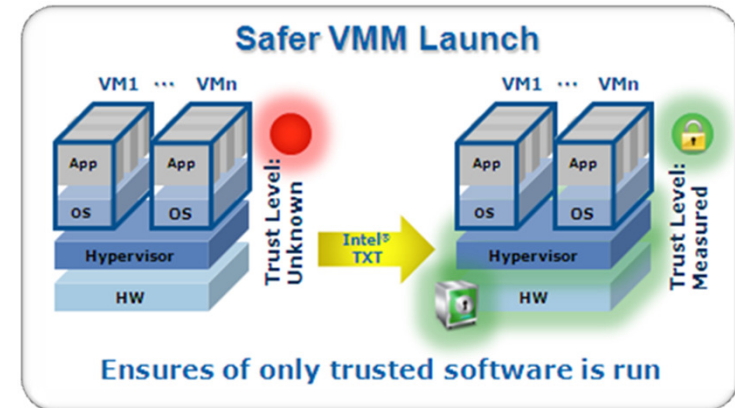
What this looks like



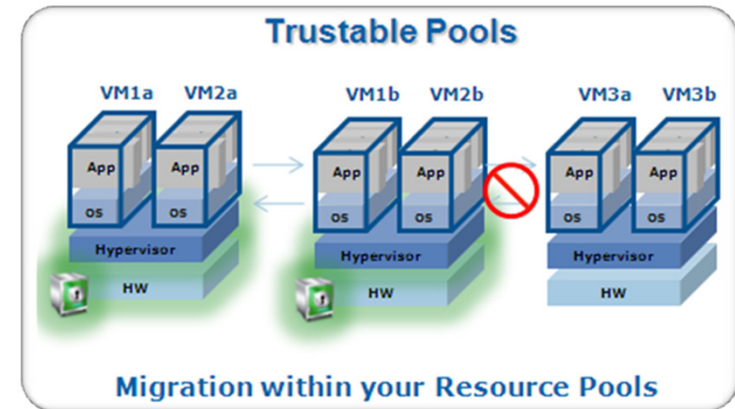
Trust established at Hypervisor launch can be utilized in migration and deployment decisions

POC Summary

- Addresses a critical need in virtualized and cloud-based use models
 - Provides control to ensure only trustable hypervisor is run on platform
 - Protecting server prior to virtualization software boot
 - Launch-time protections that complement run-time malware protections – A/V, intrusion detection, etc.
 - Supports compliance and audit activities
- Supports migration of VMs onto other trusted platforms
 - Pools of platforms with trusted hypervisor
 - VM Migration controlled across resource pools
 - Similar to clearing airport checkpoint and then moving freely between gates



Green designates Intel® TXT enabled



**Powerful Complement to Runtime Protections
in Virtualized Environments**



Limitations

- Currently only boot time checks
 - Am I going to migrate all my VM's to another platform, reboot, and re-validate? (no)
 - Plans are to add run time checks
- Not all hardware vendors support yet
 - Currently Dell and HP support, Cisco is going to but doesn't yet
- Currently no enforcement, only notification
 - Will depend on vendors writing polices to enforce
 - Hytrust
 - Catbird
 - vShield Zones
 - Cisco N1K

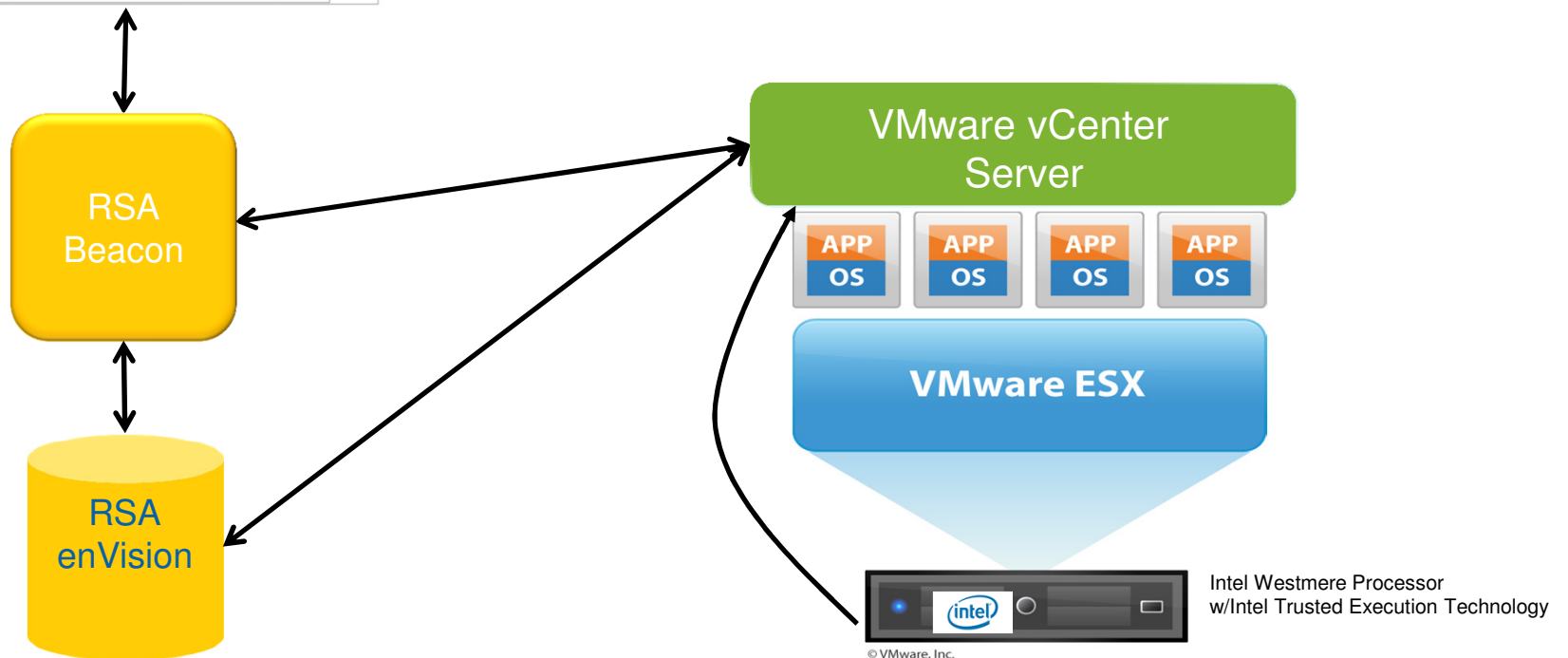


Compliance Reporting

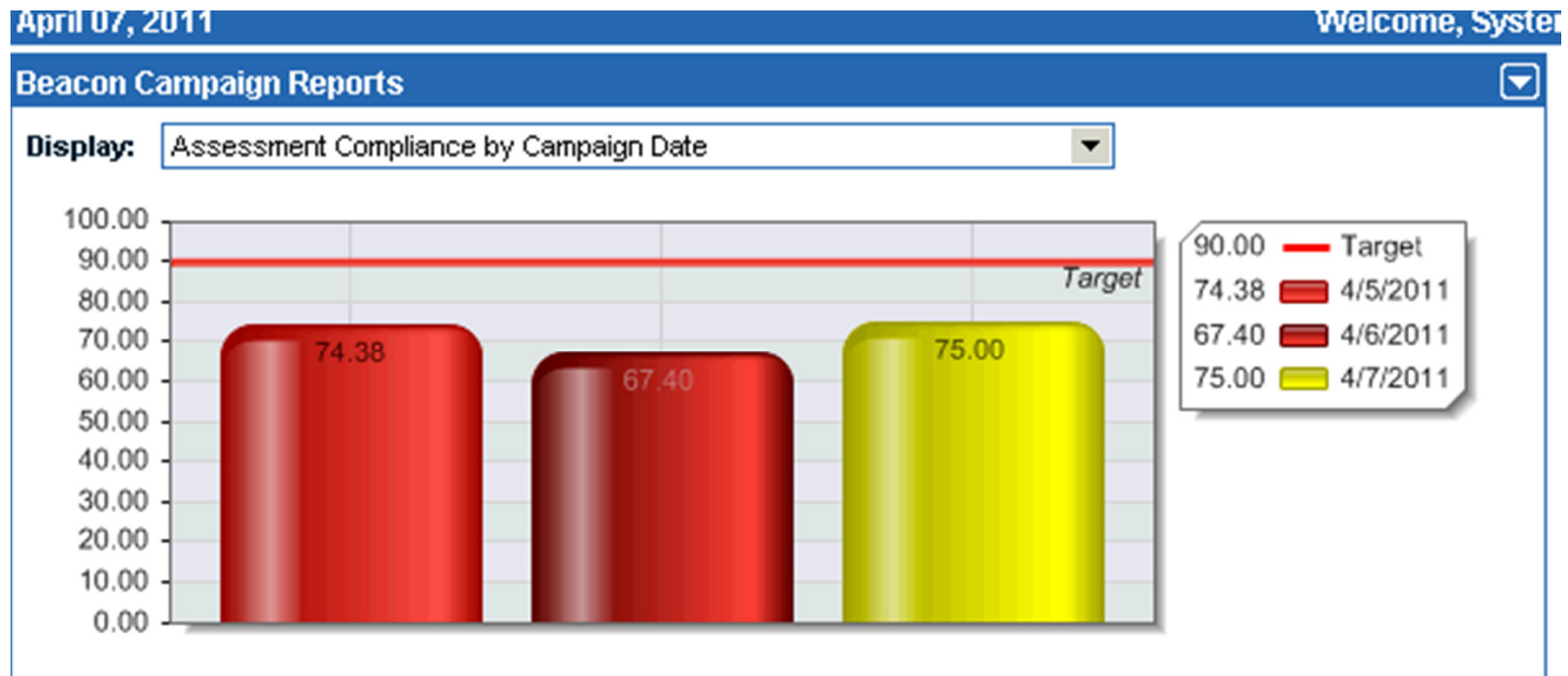


A tenant running a Tier 1 application in the cloud requires:

- Best security practices:
 - e.g. VMware hardening guidelines
- Pass a PCI audit
 - e.g. since they hold credit card data
- Assured that they are booting from a secure root of trust
 - Protection from inserted root kit, blue pill attacks



GRC Integration and Reporting



Conclusion

- Chain of trust from user device/workstation all the way to the server
- We are making some decisions on where/how/when to enable in our infrastructure
- Testing some of the tools that actually can do enforcement
- Keeping our eye on current and future developments in the space
- Technology is not a fix all super security technology that is going to save us from all things evil
- One more gap that is starting to get filled in a Defense in Depth posture



Links

- Intel® Trusted Execution Technology White Paper
- <http://www.intel.com/technology/security/downloads/arch-overview.pdf>
- Intel® Trusted Execution Technology Overview
http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf
- Intel® TXT Software Developer Guide
<http://download.intel.com/technology/security/downloads/315168.pdf>
- Intel evaluation of Intel® TXT
http://download.intel.com/it/pdf/Evolution_Integrity_Checking_Intel_Trusted_Execution_Technology_Intel_IT_Perspective.pdf>
- Intel® Trusted Execution Technology Server Platforms Availability Matrix
http://download.intel.com/technology/malwarereduction/TXT_Ready_Server_Platforms_Availability_Matrix_12_23_2010.pdf
- http://en.wikipedia.org/wiki/Trusted_Computing_Group
- <http://qubes-os.org/FAQ.html>
- <http://www.trustedcomputinggroup.org>



Thank You!

rrounsavall@terremark.com (work)

rrounsavallr@gmail.com (non-work)

@robrounsavall (twitter)