Achieving A “PCI” Trusted Cloud

George Gerchow – Director, Center for Policy & Compliance, VMware

Professional Techniques - T13

Agenda

- Challenges in Virtualization & Cloud Adoption
- VMware Trusted Cloud Solutions
- Trusted Cloud Ecosystem
- VMware Center for Policy & Compliance
- Project San Blas
- Key Takeaways

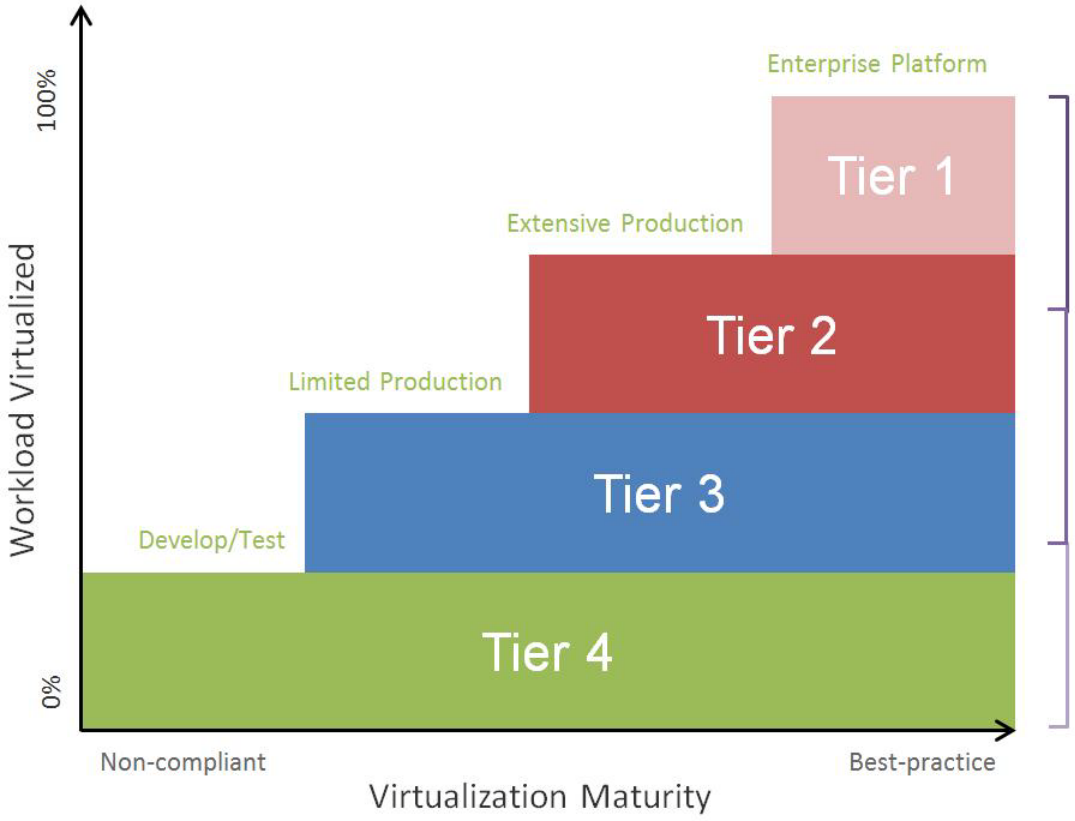
Security and Compliance are Key Concerns For CIOs Moving To Cloud

Q. What are the top challenges or barriers to implementing a cloud computing strategy?

Top 4 Concerns are on Security and Compliance

Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

Compliance is Key to Virtualizing the Next 35% of the Datacenter



The journey

Security and compliance will be required for 100% adoption

Management tools enabled expansion to 65%

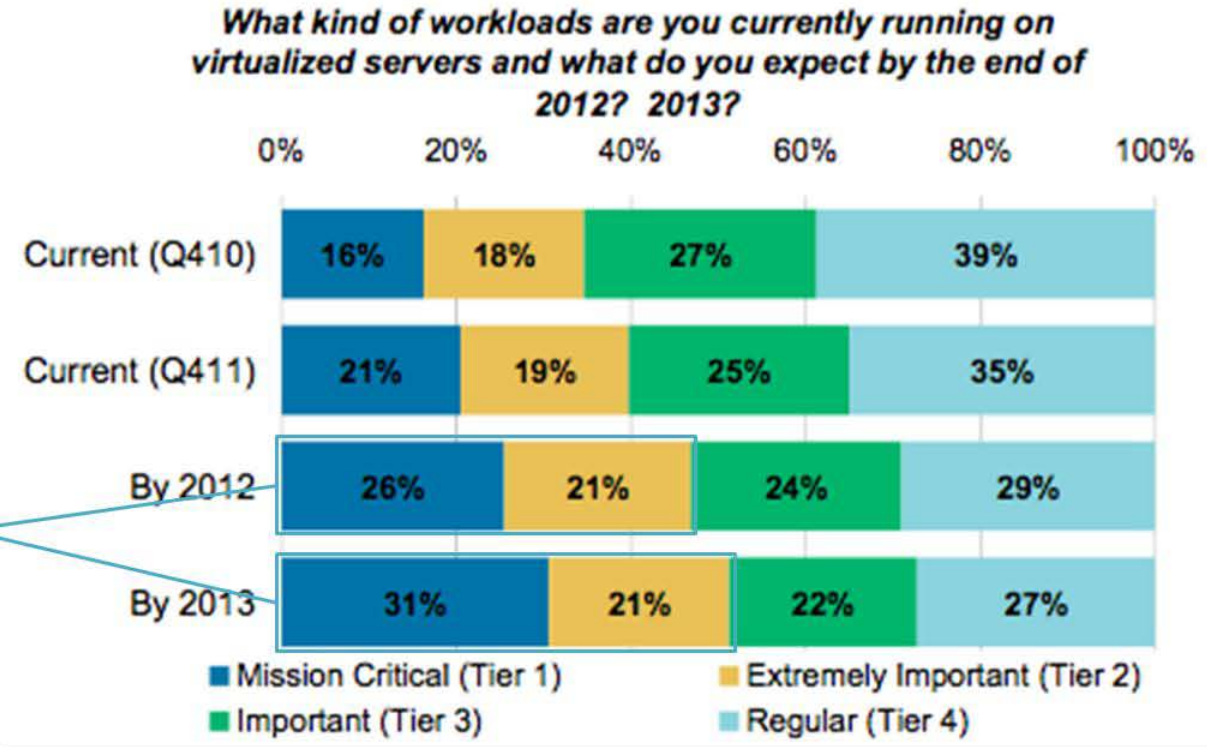
vSphere enabled the initial 35% of workloads to be virtualized

Areas of Growth

Tier 1 & 2 are the greatest priority and growth areas for virtualization

Exhibit 12

Tier 1 Workloads Up >25% From Last Year, Expected to Be Greatest Use Case by 2013

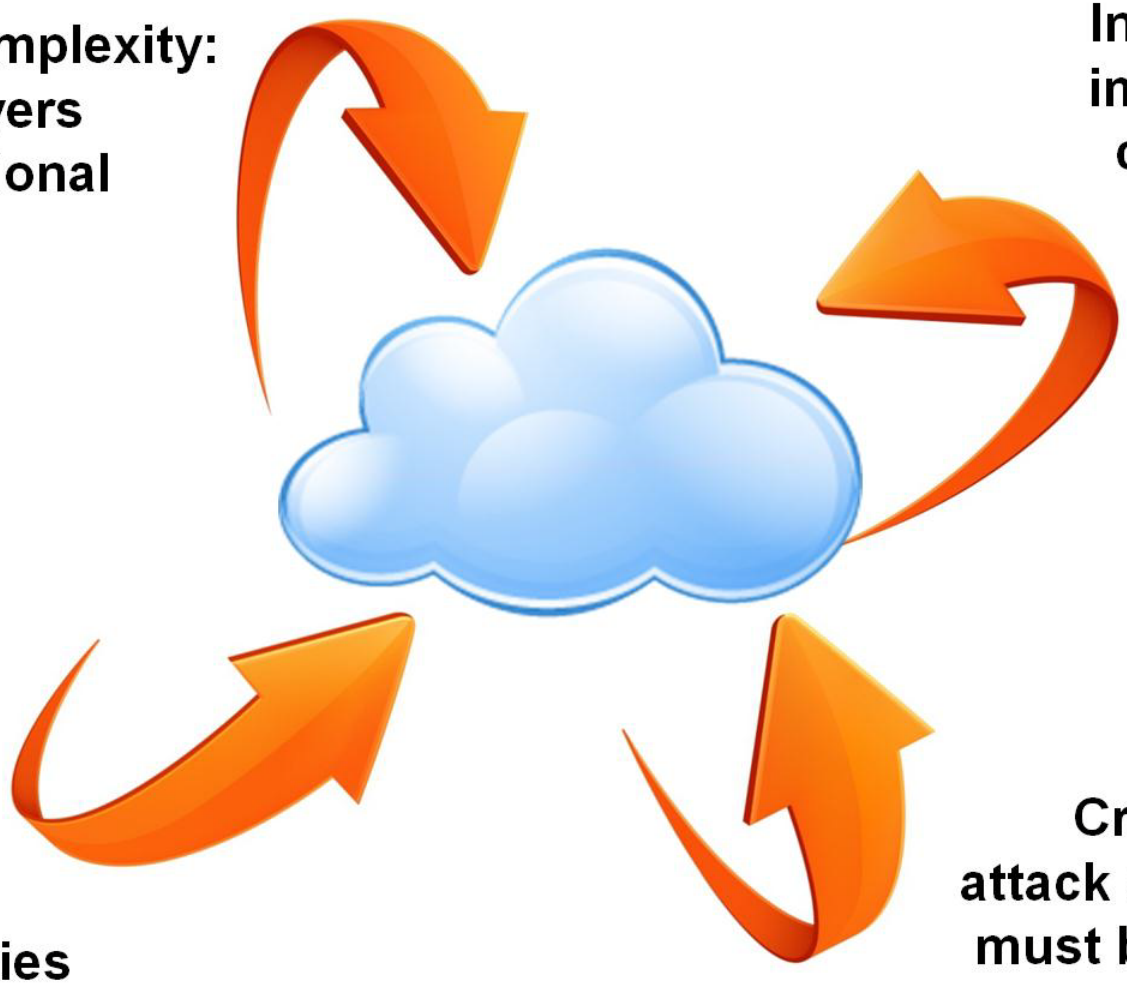


Source: Morgan Stanley Research. N = 24 respondents that answered both of our Q410 and Q411 surveys.

Compliance is More Complicated in the Cloud

Increases complexity: additional layers require additional controls

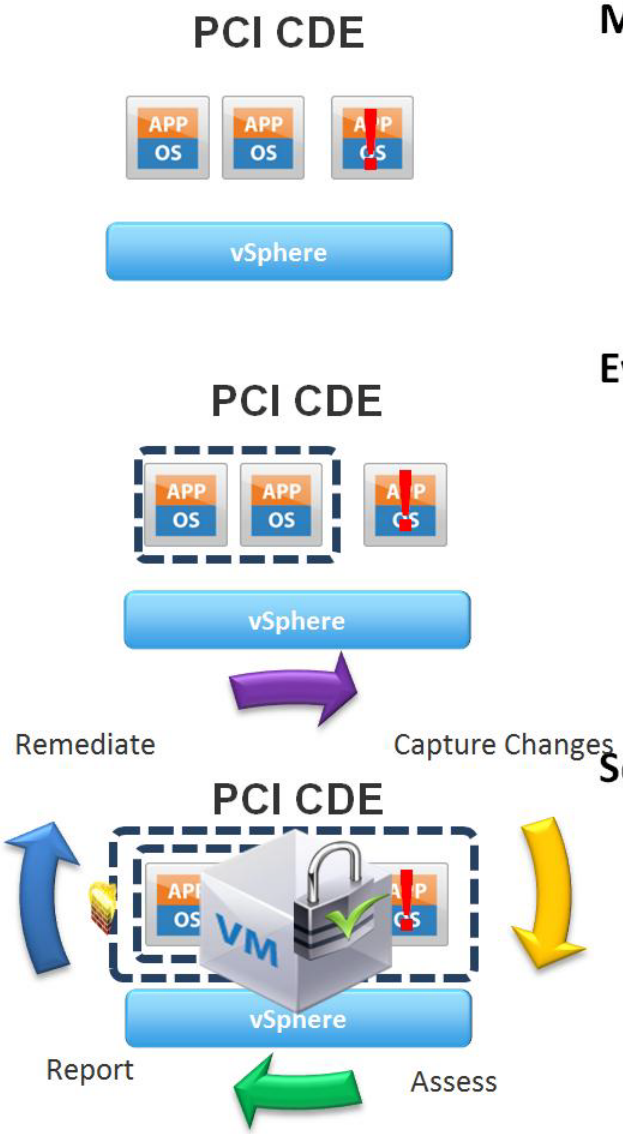
Increases the impact of any compromise



Impacts roles and responsibilities

Creates a new attack surface that must be hardened

Challenges Cloud Brings and the Issue of Trust



Mixed Mode Levels of Trust

- VM's riding on the same Guest with different Trust Levels (PCI)
- Multi-Tenancy protecting Intellectual Property (IP) with shared Resources
- Auditor, QSA Approval of Design

Evidence Based Compliance

- How is my data being protected and segmented by level of security?
- What standards and frameworks do I adopt to minimize risk?
- How do I Automate best practices, regulatory guidelines and vendor standards?

Separation of consumer and provider

- Consumer needs governance around its workloads
  - Evidence from provider around its infrastructure compliance
  - How do I address data governance, privacy, etc?
  - **How do we account for Change? (Loss of Service)**

Partner with the Right Auditor for Virtualized Compliance

How is your relationship with your auditor?

Industry Knowledge

- Have you successfully taken a virtual environment through a PCI Certification
  - Submitted an ROC to the Council (Report On Compliance)

Scope

- Does your virtual environment require for you to put everything in scope?
  - What would they (Auditor) do to reduce scope

Segmentation

- What does it mean to segment in a Virtual Environment?
  - Firewall, IDS, IPS (Statefull or Stateless)

Mixed Mode / Multi-tenant is Better than Physical

Automated and self-healing

Security & compliance trust zones

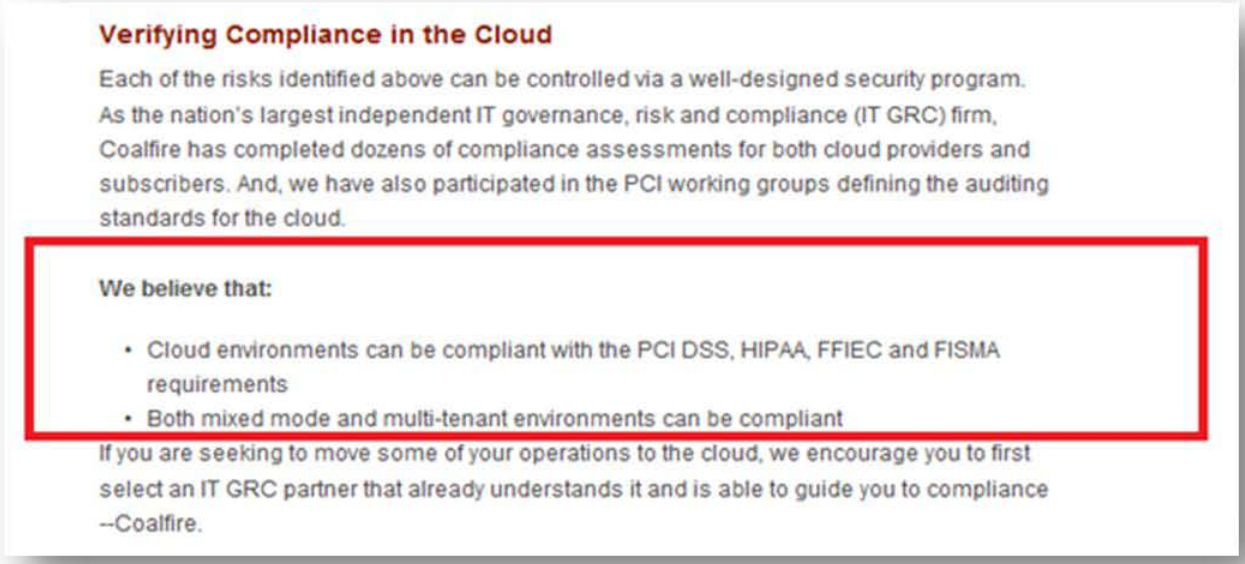
Power of cloud infrastructure automation

We are not alone:

Coalfire

ACCUVANT

K3DES



Verifying Compliance in the Cloud

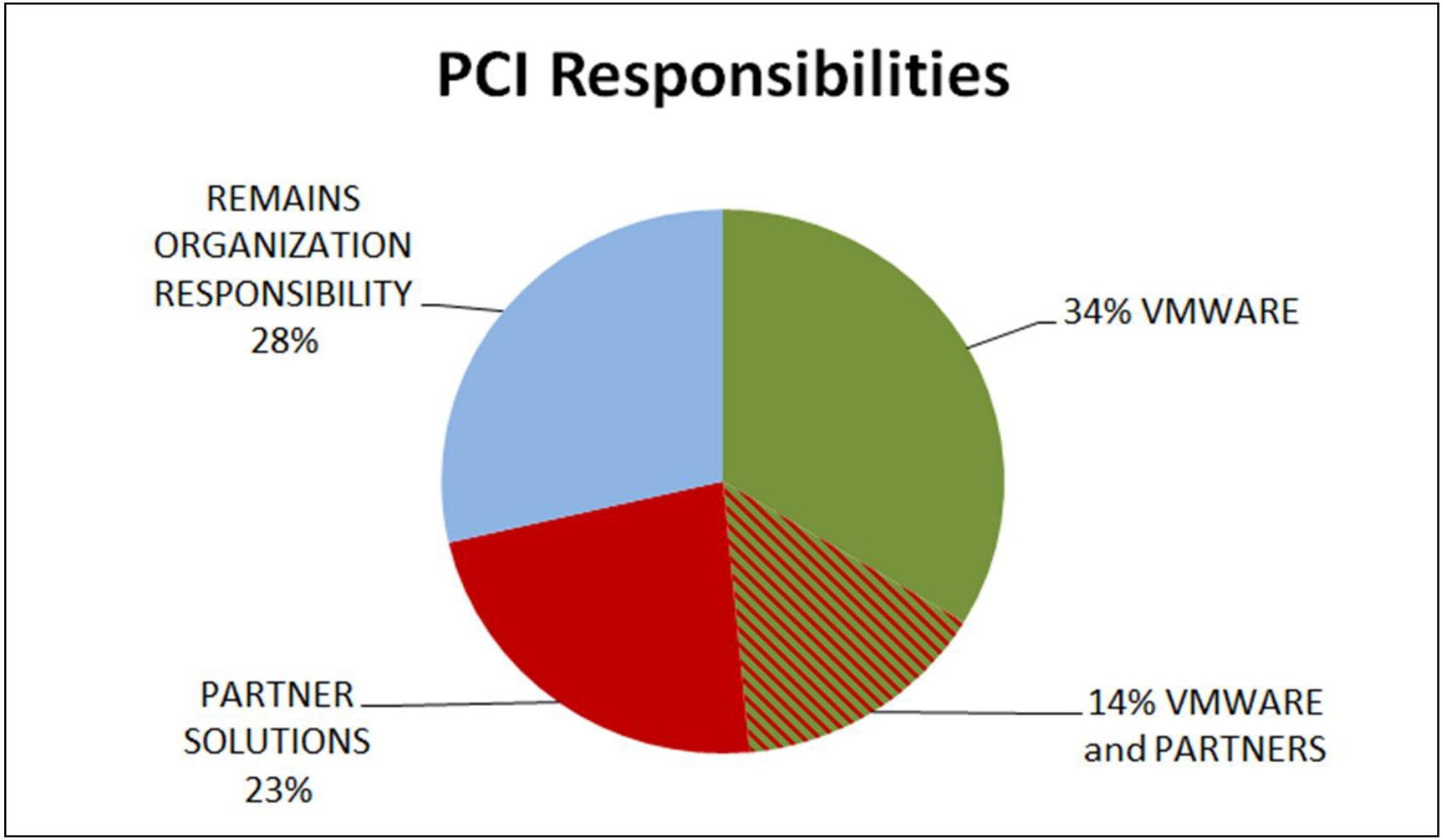
Each of the risks identified above can be controlled via a well-designed security program. As the nation's largest independent IT governance, risk and compliance (IT GRC) firm, Coalfire has completed dozens of compliance assessments for both cloud providers and subscribers. And, we have also participated in the PCI working groups defining the auditing standards for the cloud.

We believe that:

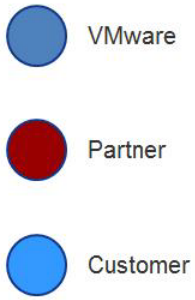
- Cloud environments can be compliant with the PCI DSS, HIPAA, FFIEC and FISMA requirements
- Both mixed mode and multi-tenant environments can be compliant

If you are seeking to move some of your operations to the cloud, we encourage you to first select an IT GRC partner that already understands it and is able to guide you to compliance --Coalfire.

PCI – Functional Responsibilities



PCI Architecture – Responsibilities Matrix



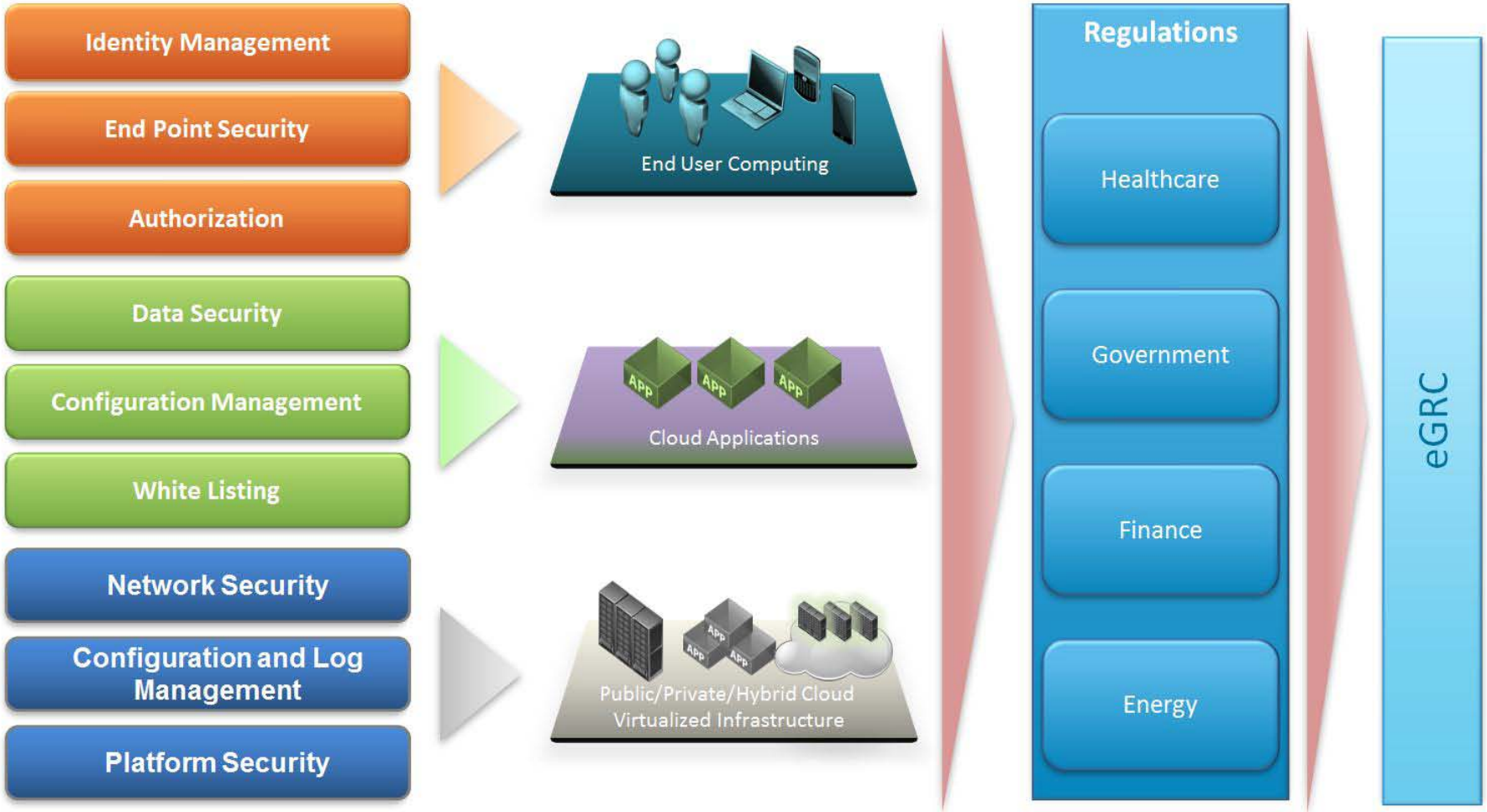
Pie Chart	PCI DSS Requirement	# of PCI Assessment Tests	Addressed in VMware's Suites	Addressed or Enhanced by Partners	Not Addressed by VMware or Partners
	Requirement 1: Install and maintain a firewall configuration to protect cardholder data	25	21	23	5
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	24	22	22	2
	Requirement 3: Protect stored cardholder data	33	12	29	4
	Requirement 4: Encrypt transmission of cardholder data across open, public networks	9	7	9	0
	Requirement 5: Use and regularly update anti-virus software or programs	6	6	6	0
	Requirement 6: Develop and maintain secure systems and applications	32	12	30	2
	Requirement 7: Restrict access to cardholder data by business need to know	7	7	7	2
	Requirement 8: Assign a unique ID to each person with computer access	32	20	30	2
	Requirement 9: Restrict physical access to cardholder data	28	0	0	28
	Requirement 10: Track and monitor all access to network resources and cardholder data	29	26	27	2
	Requirement 11: Regularly test security systems and processes.	24	3	16	8
	Requirement 12: Maintain a policy that addresses information security for all personnel.	40	1	39	39
	Requirement A.1: Shared hosting providers must protect the cardholder data environment	8	7	7	1
	**TOTAL** **Note: Some controls are enhanced by Partners, so the same control may be double counted.**	**297**	**144**	**245**	**95**

PCI Applicability – VMware + Partner Matrix

- Detailed PCI Applicability Matrix for VMware and VMware Partners

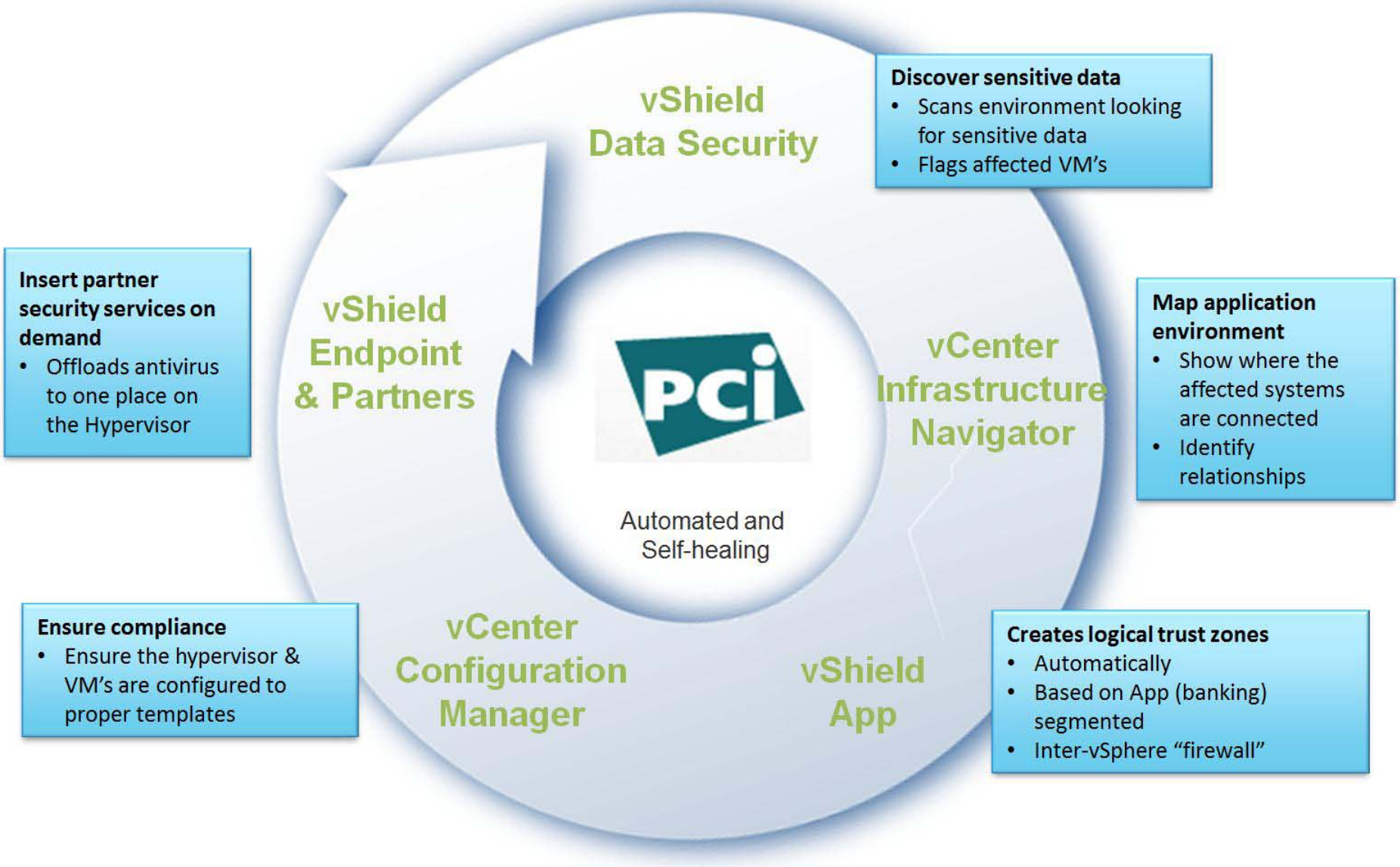
PCI Requirement	Testing Procedures	VMware Solutions					Partner Solutions						
		vSphere	vShield	vCOPs	vCloud	View	1. Hardware	2. Authentication	3. Logging, Monitoring	4. Endpoint Security	5. Encryption	6. Availability	7. Other
	Number of PCI DSS Controls Addressed	108	135	112	108	103	0	0	0	0	0	0	0
Requirement 1: Install and maintain a firewall configuration to protect cardholder data													
1.1 Establish firewall and router configuration standards that include the following:	1.1 Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:												
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	x	x	x	x								
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	x	x	x	x								
	1.1.2.b Verify that the diagram is kept current.	x	x	x	x								
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.3.a Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.					x							
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.					x							

Trusted vCloud: Compliance – Functional View

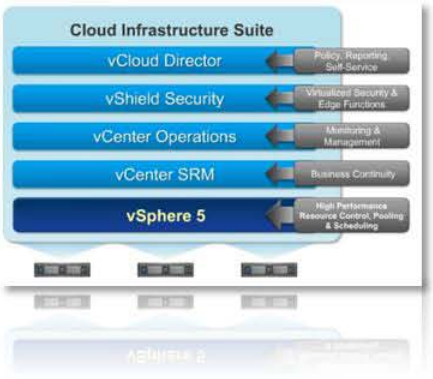


Meet Customers' Compliance Requirements to Migrate Tier 1 Apps to CIS

Continuous Compliance for Business Critical Applications



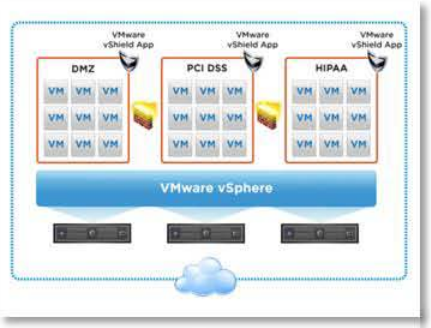
VMware for the Trusted Cloud



Cloud Infrastructure Suite

Trusted Platform

- vSphere, vCloud Director, vCenter



vShield

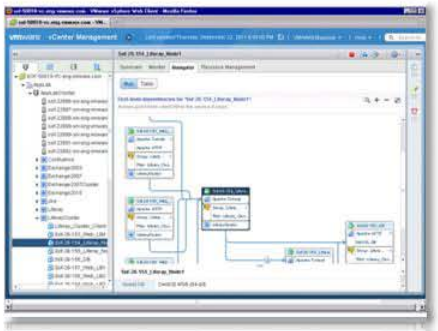
Enable Security Controls

- Securing Perimeter
- Segmenting Applications
- Data Discovery and Protection

vCenter Configuration manager

Continuous Compliance

- Adherence to regulatory Guidelines
- Out of the Box Benchmarks
- Auto Remediate Non Compliant Results



vCenter Infrastructure Navigator & vCenter Orchestrator

Automated discovery and orchestration

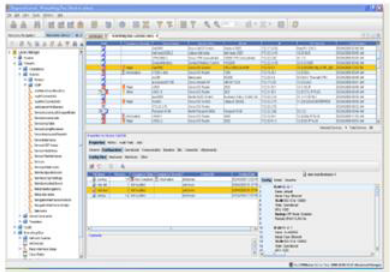
- Cloud Framework
- Application Relationships

Trusted vCloud Ecosystem

ARCHER

Centralized, access-controlled environment for automating enterprise compliance

- Scan critical IT assets automatically
- Check compliance status
- Return assessment results
- Import results automatically
- Map to other solutions or policies
- Show relevant reports in dashboard



NETWORK CONFIGURATION MANAGER (EMC)

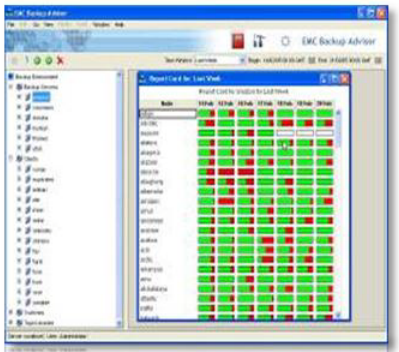
Manage network device configuration

- Create network configuration policies & templates
- Automate assessments and schedule reports
- Drill down for details and remediation scheduling

STORAGE CONFIGURATION ADVISOR (EMC)

Manage storage device configuration

- Assess SAN compliance by policy or breaches of storage devices
- Provide audit data for support matrix, policies, user log and changes
- Automate import to centralized repository

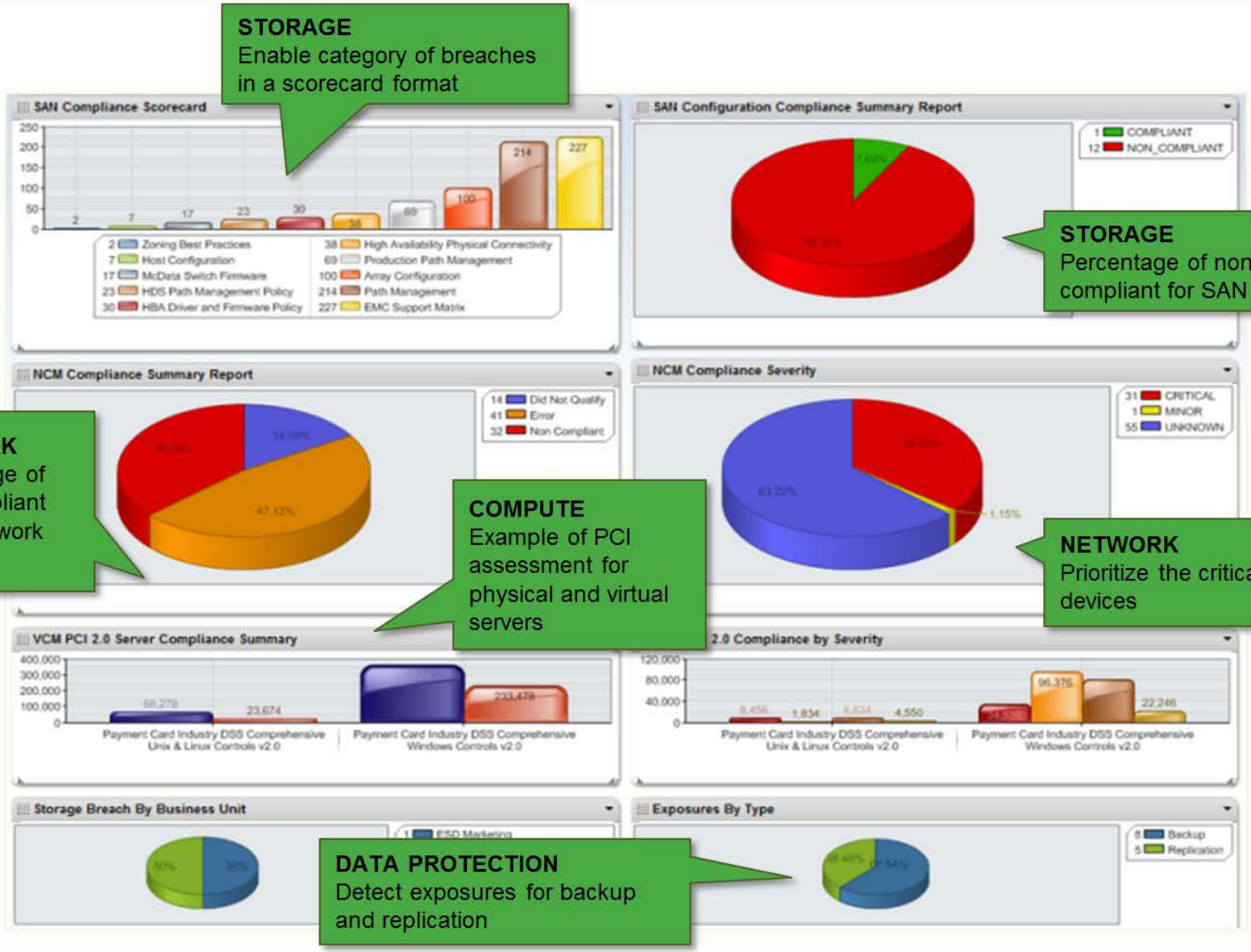


DATA PROTECTION ADVISOR (EMC)

Monitor data protection environments

- Discover exposures of backup and replication environments
- Identify recoverability gaps and drill down to specific clients
- Link compliance system for business continuity

eGRC Ecosystem Example - VMware + EMC + RSA



Summary of Archer Key Benefits

Automated technology control assessment

- Allow assessment automation of IT infrastructure configuration
- Enable mapping of configuration violations to defined IT controls

IT compliance reporting

- Summarize IT information relative to existing compliance programs
- Enable device grouping to overall business hierarchy
- Reduce time spent to prepare for audit via single reporting engine

Compliance efficiency

- Automate remediation to close compliance gaps quickly with minimal effort

VMware IT Business Management

- Transition from managing technology to managing services
- Expose the cost and value of IT & Compliance to your entire organization
- Understand impact of business demand and change
- Identify where money saving opportunities exist
- Communicate and improve quality of service
- Manage the relationships with your customers and external vendors

VMware Center for Policy & Compliance (CP&C)

- Dedicated group of security and compliance policy experts, analysts and technical specialists established in 2000
- Chartered to research and develop compliance solutions specifically for Cloud computing environments
- Staff averages 18+ years experience and hold certifications such as CISSP, CCNA, ITIL, MCSE, MCDBA, and of course vCP
- Global presence and frequently meets with customers, auditors and analyst to provide guidance & thought leadership in PCI, Healthcare and Trusted Cloud environments

Evolving Healthcare Compliance Challenges

- HIPAA- circa 1996 is long in tooth, but had a pretty small bite
- Along comes HITECH in 2009 (Government)
  - Expands scope of privacy and security protections under HIPAA, including breach notification. Enforcement is ramped up. HHS/OCR publishes activity
  - New detailed security rule sections §164.302 through §164.318.
  - Mandatory penalties up to $1.5M for extended/repeated violations
  - $50k fine per infraction, up to $1.5M
- HITRUST 2K10 (Public sector)
  - If you are covered by HIPAA & HITECH you should be ready for Certification
- PCI DSS v 2.0 is here
- DISA Content being used by most Healthcare organizations

PCI matters in Healthcare

Most Covered Entities (healthcare providers) are also Merchants

- subject to PCI DSS compliance; not optional
- it is mandatory for those accepting credit cards
- 45 Common Controls between PCI & HIPAA

- PCI remains the focal point for compliance with data security initiatives
- **PCI is prescriptive, encompassing more than one-half of all controls mandated by HIPAA**

- HIPAA compliance on the other hand is risk-based, and 'addressable' and 'required' controls are justified within the context of their operation
- **HIPAA HITECH stresses privacy in addition to security whereas PCI does not address privacy**

HIPAA Violations that hurt!

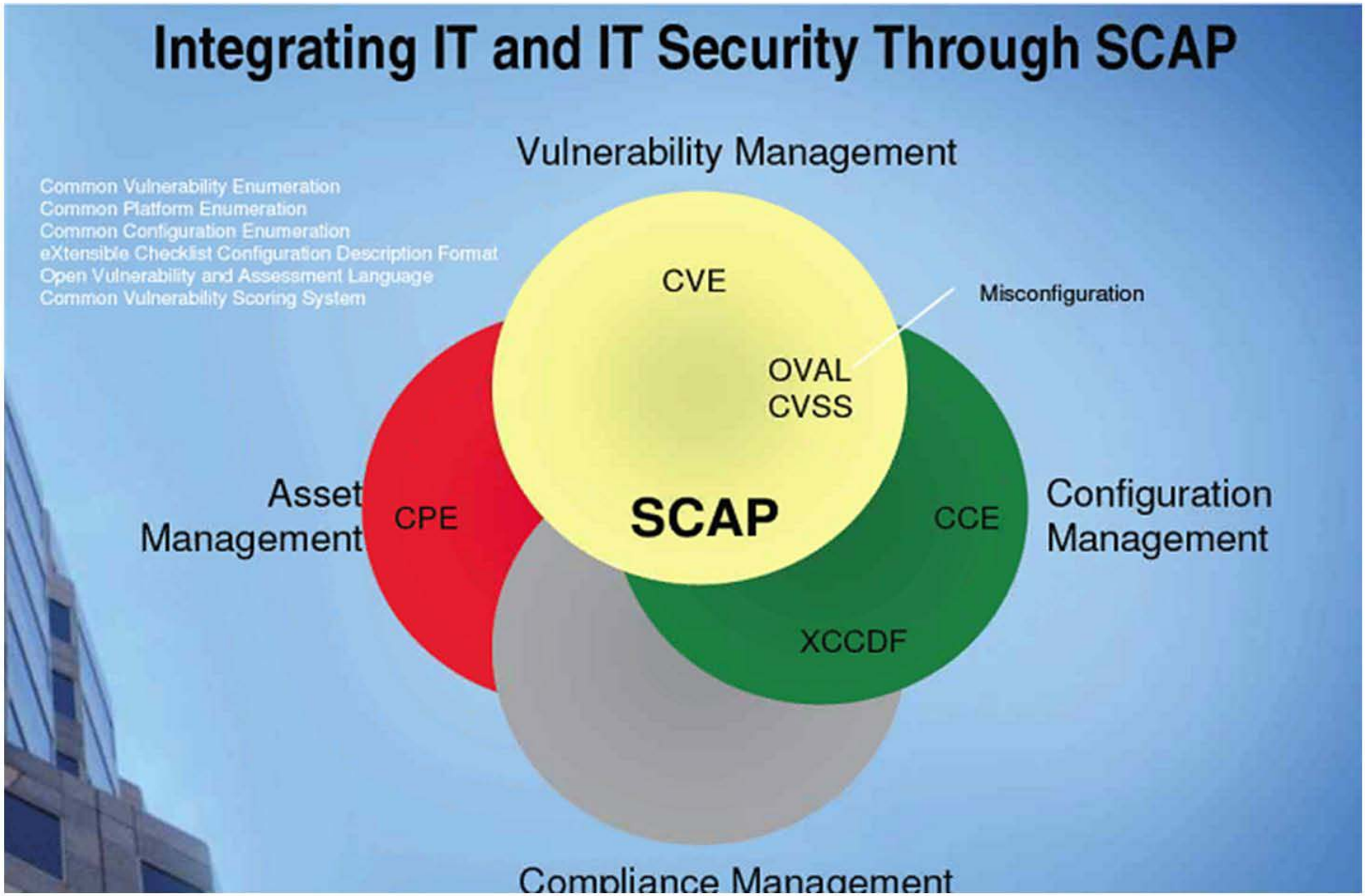
- A Massachusetts General Hospital employee took some work home, but accidentally left 192 paper billing records—containing detailed protected health information—on the subway. Fined $1M.
- Howard University Hospital says a former contractor's personal laptop containing patient information was stolen in January. Fine expected to be 1.5M
- South Shore Hospital contracted with a Pennsylvania company, to erase and re-sell 473 data tapes containing information on 800,000 individuals. None of the data was encrypted. Fined 750k.
- UCLA Health Services (UCLAHS) settles two claims that unauthorized employees accessed records of celebrities that received care at UCLAHS. Settled for $875k
- April 2012 - Utah Health Care Data Breach Exposed About 780,000 Patient Files".. A weak password is to blame for the hacking of a Utah Department of Technology Services server containing patients' Social Security numbers and data on children's health plans..."

By the Numbers*:

- 385 breaches of protected health information (PHI)
- 19,016,894 patient health records affected
- 49,396 average # of patient records per breach in 2011
- 59% of all breaches involved a business associate
- 39% occurred on a laptop or other portable device
- 25% occurred on a desktop PC or server
  - 64% can be avoided with VMware solutions!
- 60% resulted from malicious intent (theft, hacking)
- 525% growth in records breached due to loss 2010-2011
- 20 the top 20 major incidents resulted in 88% of all patient records breached

*Redspin PHI 2011 Breach Report

SCAP in Virtualization & Cloud



Project San Blas Overview

Today, security Controls for virtual and cloud environments:

- **Overly complex**
- **Different hardening guidelines are not reconciled**
- **Difficult to implement**

Author vendor-agnostic
Trusted Cloud Controls best practices
for publication and distribution

A simplified, non-vendor specific, best practice approach distributed by trusted organizations

- **Simple path to follow for migrating automated workloads to Virtual & Cloud Platforms**

Benefits

- Typical hardening guidelines are organized by product – this is across the ecosystem
- Parameters (Descriptions)
- Prescriptive
- Critical & "Simple"

Target Audience

- VI Admin\ Architects
- Need Standard of Compliance (Evidence)
- Auditors

Deliverable

- PDF – (Human readable)
- Enable SCAP – security automation content Controls (XML, XCCDF)
- OVAL (open vulnerability assessment language)

Draft standards

TCC02 - Do not use default self-signed certificates

Description:

Using self-signed certificates is a good start for securing your servers by setting up temporary SSL mechanism in development and test environments. However, this practice is not recommended for a production environment where security is a prime requirement. You must use certificates from a trusted certificate authority (CA).

Rationale:

Using default self-signed certificates leave the SSL connections prone to Man-in-The-Middle attacks. Self-signed certificates also pose a higher risk since more often they are not properly implemented and secured as done by the commercial CA vendors.

Certificates use a chain of trust, where each certificate is signed (trusted) by a higher, more credible certificate. At the top of the chain of trust are the root certificates, owned by CA.

Remediation:

1) Identify all the components / systems in the cloud environment that use digital certificates for SSL.
2) Follow your organization's digital certificate management policy and use certificates from trusted CAs only.

Audit:

1) Ensure that all the components /systems were identified to cover all the layers of cloud delivery technologies.
2) Check details of digital certificate management procedure followed by the organization.
3) Check the certificates used by these components / systems to find out gaps, if any.

Author vendor-agnostic **Trusted Cloud Controls** best practices for publication and distribution

- Industry standard based on VMware guidance and expertise
- Set of Controls to test, recommend use in audit practice (K3DES, Coalfire, Accuvant, IOActive)
- Confidence in migrating Tier 1 apps to Virtualized / Cloud platforms
- Embedded Hardening & Compliance
  - List of controls to prepare for audits
  - Configuration of Products
  - Ongoing Operational Guidance (Make sure you are following procedure)
  - Operational & Config (DISA, STIG)
  - Hardening Guide & Continuous Monitoring

Next steps

Certification

CENTER FOR INTERNET SECURITY

NIST

- CIS & NIST to certify
- Free to publish and support

Customer Council

- Customer Council (under NDA) @ VMworld US
- VP of Ops

Launch

- VMworld EMEA
- Customers
- Audit community
- CIS & NIST
- VMware

Key Elements of an Operational Trusted Cloud

- Provider
  - Select partners that have baked in Security & Continuous Compliance offerings that are cost-effective with a good understanding of your business
- Trusted Platform
  - Ensure that your provider is using a Trusted Platform and can deliver a process that accounts for change control, log information and configuration audit checks
- Integration Framework
  - Leverage some of your existing tools and applications, work with provider to build a trusted ecosystem of vendors and auditors
- Evidence-based Validation of Audit
  - Data Governance, a Compliance Framework (GRC)
    - SSAE 16/ SOC 2 – Service Oriented Control
  - Regulatory Guidelines
    - PCI, HIPAA, BASEL III, SOC
    - Segmentation of Assets, IP
    - Data Protection (Continuous Discovery and Monitoring)

Sample - Locking down Virtualized Environments

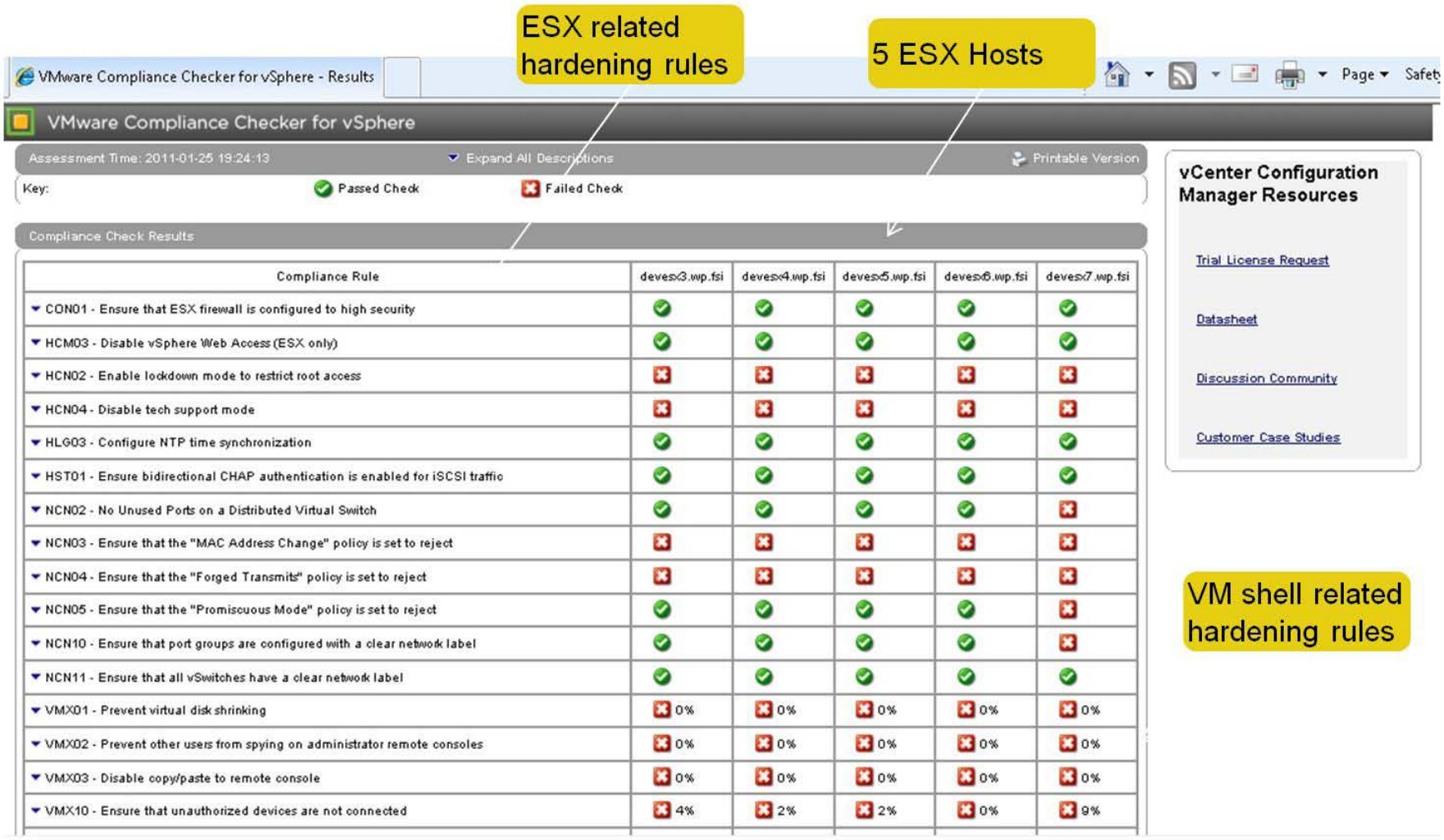
Authentication

- Restricting Admin\ Root Access

Communication\ Networking

- Making sure network is segmented properly
- Leak Prevention
  - Guest from Host
  - Guest to Guest
- Configuration\ Patching
- Changing Root Password (90 days)
- Patching Host

VCM's Free vSphere Compliance Checker (Download)



Recommendations

- Perform risk assessment *prior* to vSphere environment design
  - Physical access
  - Roles and responsibilities
  - Services and communication
- Ensure VM meet "System Components" definition
- Hypervisor of "in scope" VM always "in scope"
- Harden hypervisor
  - Multi-factor access
  - Least privilege
  - Reduced attack-surface
  - Defaults removed/changed
  - Remote logs
- Set only one primary function per VM
- Use automated hypervisor and VM patching
- Keep all management and support systems "in scope"

Call to Action

- Further Education and TCO
  - Solutions Demo
    - http://info.vmware.com/content/VCMSolutionsDemo
- *NEW* VMware/Forrester vCM ROI
  - https://www.gosavo.com/vmware/Document/Document.aspx?id=2222106&view=Preview
- Leverage CP&C with Auditors (QSA)
  - Mixed Mode Environments, Trusted Cloud Architecture & Partner Ecosystem
- More Security & Compliance Information
  - Mastermind Series
    - http://info.vmware.com/content/13090_VirtMng_NA_Security_ITCompliance?src=SALES-NPD&elq=&xyz
  - VMware Security Blog
    - http://blogs.vmware.com/security/
  - Free Compliance Checkers
  - http://communities.vmware.com/community/vmtn/vsphere/compliance-checker

Top 3 takeaways

1. **Engage Your Auditor Early in the Process**

2. **Choose a Clear Framework**

3. **Compliance Validated Architecture Requires a Partner Eco System**

Questions

"A Trusted Cloud provides enhanced reliability through enforcement of mandatory constraints, defined by policy and validated by regular audits."

Security Compliance Control

Move assets with confidence