



Achieving Continuous Compliance with PCI DSS 3.0 in the Private Cloud

PCI Conference, Moscow Russia

Edmundo C
CEO
May 29, 2014



THE STATE OF THE PRIVATE CLOUD

- Server/compute virtualization fully embraced by IT-Savvy industries and generally accepted as the standard going forward for all
- Security technologies must follow suit, yet very few players currently
- Physical security appliances, along with many other dedicated networking "boxes" will diminish in role/importance as a result
- Network Function Virtualization (NFV / SDN) is gaining traction and presenting new security challenges



CURRENT CHALLENGES FOR PRIVATE CLOUD

“ My physical security solution can't keep up with my virtual infrastructure ”

“ We spend months Preparing for audits”

“ We have too many tools required to manage our infrastructure”

“ We don't have complete visibility on changes in the virtual infrastructure”

“ I'm concerned about migrating my compliant physical workloads to virtualized infrastructure ”

“ Can you prove that my workloads are segmented? I need to pass my PCI Audit next quarter ”



POLICY IN THE CLOUD ERA?

2012

PCI_DSS

ISO 27001

2012
PCI_DSS Rev 2



WHAT IS NEEDED?

- Trust: Automated security controls to policy
- Verify: Continuous monitoring for proof of control, demonstrate compliance
- Enforce: Mitigation to assure compliance to standards



Trust: Cloud Security Requires Logical Zoning

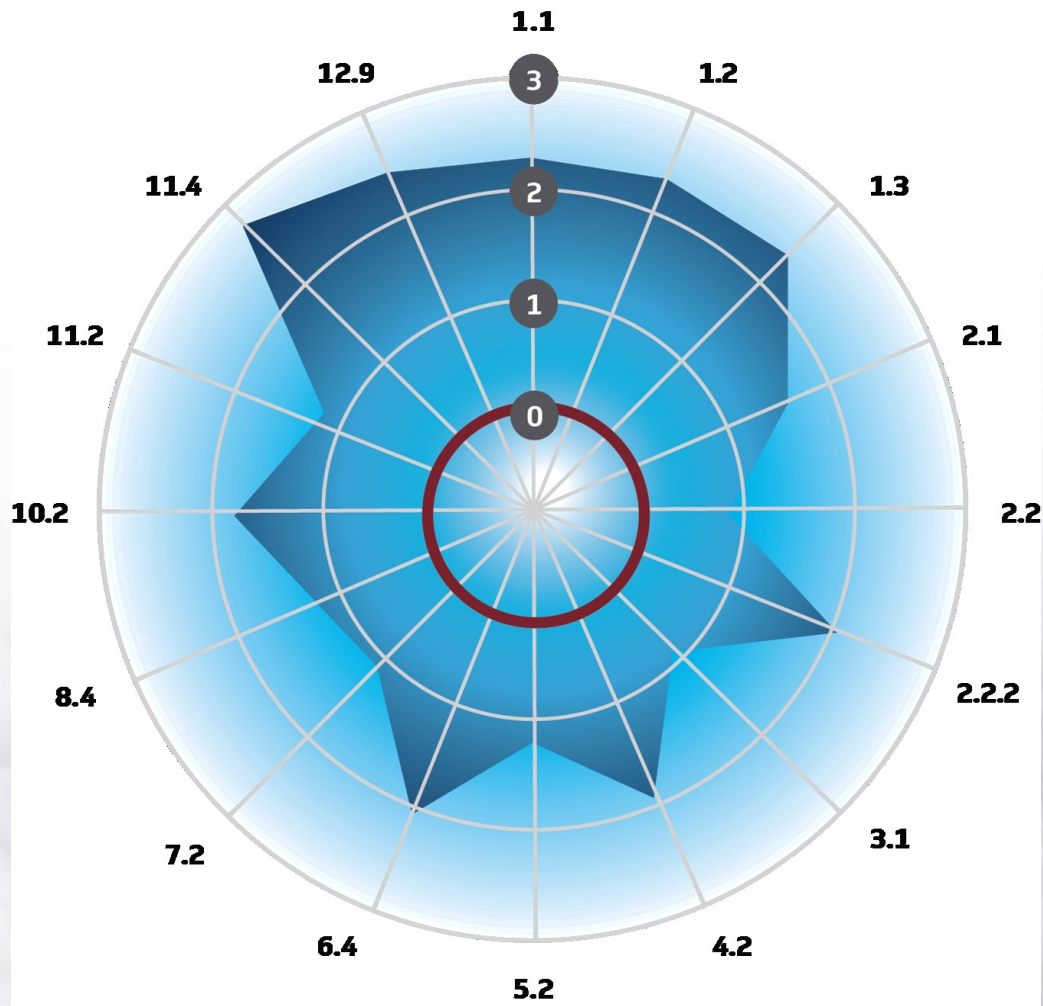
- All assets are controlled using Trustzone containers
- TrustZones policies apply controls to standards, i.e. PCI
- CDE workloads placed automatically into a PCI zone
- PCI Zone automates and enforces controls
- Policies are automatically applied to all new assets
- Default membership into an "Staging/Quarantine" zone as an option



VERIFY: Continuous Measurements Against PCI Standard

- Continuously monitor:
 - Security events
 - Emerging threats
 - Intrusion detection
 - Firewall events
 - Vulnerabilities
- Hypervisor events
- Configuration drift of infrastructure and workloads





PCI TrustZone

Real time compliance Posture



ENFORCE: Machine-speed Mitigation

- CDE Isolation:
 - Secondary controls for VLAN isolation
 - Orchestrate virtual firewall from VMware or Cisco
- Automatic quarantine of untrusted virtual assets
- Alert on, and revert, non-compliant changes to virtual network configurations
- Actively block network attacks with IPS





CASE STUDY



LEADING FINANCIAL INSTITUTION

CUSTOMER

- Fortune 500 Financial Inst.
- 2 datacenters
- 7200 employees

CHALLENGE

Needed strong security solution prior to deploying mission critical apps into private cloud

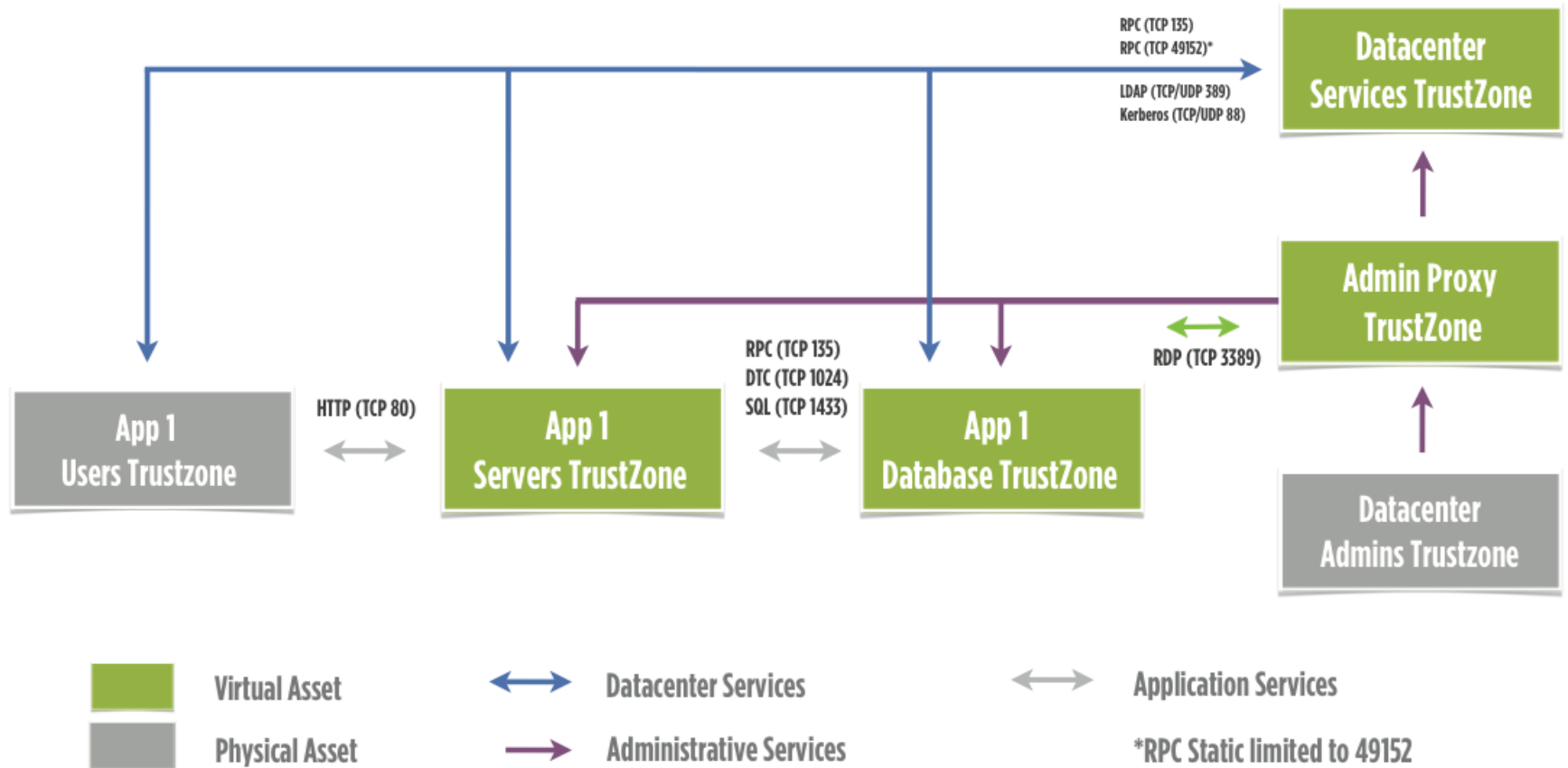
SOLUTION REQUIREMENT

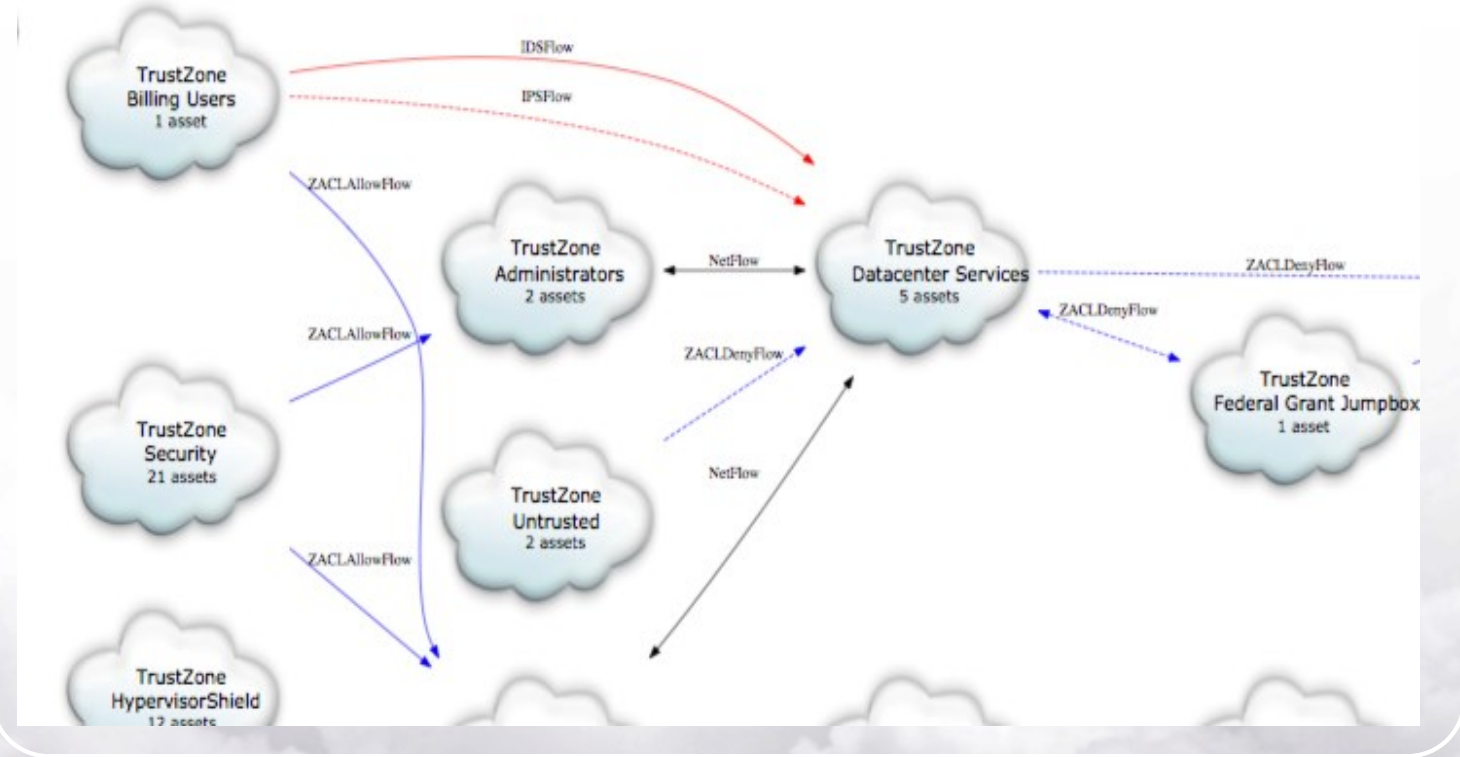
- Workload isolation on physical host
- Control private cloud network
- Continuously monitor for and assure regulatory compliance for mission critical apps

CUSTOMER QUOTE

“If I had Catbird last year it would have saved us \$2M in audit costs.”

TRUSTZONE ARCHITECTURE—TIERED APP MODEL





Real Time CDE Data Flows

Meets Requirements 1.2 and 1.3



CATBIRD ASSET AND ZONE COMPLIANCE

The screenshot displays the Catbird Asset and Zone Compliance interface. The browser address bar shows the URL: <https://vdemo/compliance/trustzone/9/asset/49/details>. The page title is "Datacenter Services - PCI DSS 2.0".

The interface includes a navigation menu on the left with categories like Asset Views, Dashboards, TrustZones, and Assets. The main content area features a radar chart titled "Datacenter Services - PCI DSS 2.0" comparing the "Current" state (grey) against the "Compliance baseline" (blue). The chart has 12 axes representing different compliance requirements, with values ranging from 0 to 12.9. The current state shows a score of 1.1 for requirement 1.1, 1.2 for 1.2, 1.3 for 1.3, 2.1 for 2.1, 2.2 for 2.2, 2.2.2 for 2.2.2, 3.1 for 3.1, 4.2 for 4.2, 5.2 for 5.2, 6.4 for 6.4, 7.2 for 7.2, 8.4 for 8.4, 10.2 for 10.2, 11.2 for 11.2, 11.4 for 11.4, 12.2 for 12.2, and 12.9 for 12.9.

The "Asset Compliance Details" panel on the right lists the following compliance items for the SELAB2 AD Server:

- Access Control
 - Access Enforcement (1.2)
 - VIM PortGroup Enforcement
 - Configure a port group enforcement policy for the zone
 - NAC
 - Configure a NAC monitor for the connected network of
 - Session Management All Assets
 - System is enforcing zone access policies.
 - ZACL Default Deny
 - Configure a deny all rule for the zone.
 - Flows All Assets
 - Configure a flow monitor on a trunk or SPAN port for th
 - Firewall All Assets
 - System is enforcing firewall policies.
 - Information Flow Enforcement (1.3)
 - User Access (7.2)
- Auditing
 - Transmission Security (4.2)
 - VIM Auditing
 - System is collecting virtual infrastructure audit events.
 - Session Management All Assets
 - Flows All Assets
 - Configure a flow monitor on a trunk or SPAN port for th
 - IPS
 - Anti-virus Audit (5.2)
 - Auditable Events (10.2)
 - Security Operations (12.2)



Catbird: Security and Compliance for Private Cloud

- Trust: Automated security controls to policy
- Verify: Continuous monitoring for proof of control, demonstrate compliance
- Enforce: Mitigation to assure compliance to standards





QUESTIONS?



ASSET INVENTORY

Browser address bar: https://vdemo/compliance/dashboard/asset_viewer

Navigation: Most Visited | Getting Started | VMware vCloud Direct... | Catbird Control Center | Web-Demo-CC

catbird logo

User: srahim | Log out | Acme Hospital | BST (UTC+01:00)

Dashboard: Asset Views | Asset Viewer | Asset Vulnerabilities | Vulnerabilities | Hypervisor Hosts | Dashboards | TrustZones | Configuration

Page: 1 of 1 | Clear Filters | Total Assets: 108

N...	Asset Name	Type	State	TrustZones	Compliance Frameworks	Seen By	MAC Address	IPs	VLAN IDs	Date Detected
1	Lobby-jo-vm2(6.102)	VM	Powered Off	Untrusted		VIM				04/09/2013 20:01:14
1	Lobby-jo-vm4(6.104)	VM	Powered Off	Untrusted		VIM				04/09/2013 20:01:15
1	Metasploitable-Increasing	VM	Powered On	DMZ	PCI DSS 2.0	Flow,NAC,VIM			7	04/10/2013 18:12:45
3	Nexus1000V-4.2.1.SV1.4a	VM	Powered Off	Security	PCI DSS 2.0	Flow,NAC,VIM				04/09/2013 19:21:35
3	Nexus1000v.4.2.1.SV1....	VM	Powered Off	Security	PCI DSS 2.0	Flow,NAC,VIM				04/09/2013 19:21:31
1	Proxy_Server_RDP(6.67)	VM	Powered On	Admin Proxy	PCI DSS 2.0	Flow,NAC,VIM				04/09/2013 19:24:11
1	Proxy_Server_SSH(7.51)	VM	Powered On	Admin Proxy	PCI DSS 2.0	Flow,NAC,VIM			7	04/09/2013 20:01:23
1	SELAB AD Server(7.103)	VM	Powered Off	Datacenter Services	PCI DSS 2.0	Flow,NAC,VIM			7	04/09/2013 19:33:59
	Network adapter 1	Interface	Disconnected	Datacenter Services	PCI DSS 2.0	Flow,NAC,VIM	00:50:56:A7:0B:F8	192.168....	7	04/09/2013 19:33:59
1	SELAB2 AD Server	VM	Powered Off	Datacenter Services	PCI DSS 2.0	NAC,VIM				04/09/2013 19:25:52
1	SJ-Health_Records_HIP...	VM	Powered On	Health Record	HIPAA (SP ...	Flow,NAC,VIM			7	04/09/2013 20:01:10
1	SJ-IT_Admin1 (7.72)	VM	Powered On	Wireless	COBIT 4.1	Flow,NAC,VIM			7	04/09/2013 19:27:00
1	SJ-IT_AdminWin1 (6.179)	VM	Powered Off	Datacenter Admins	COBIT 4.1	Flow,NAC,VIM				04/09/2013 19:23:00
1	SJ-Lab1 (7.73)	VM	Powered Off	Desktop	HIPAA (SP ...	NAC,VIM			7	04/09/2013 19:35:06
1	SJ-Payment_DB_PCI (7...	VM	Powered On	Payment	PCI DSS 2.0	Flow,NAC,VIM			7	04/09/2013 19:35:11
1	SJ-Pharm1 (7.75)	VM	Powered Off	Desktop	HIPAA (SP ...	NAC,VIM			7	04/09/2013 19:35:11
1	SJ-Physician Terminal (6...	VM	Powered On	Physician Terminals	HIPAA (SP ...	Flow,VIM				04/09/2013 20:01:17
1	SJ-Staff1_PCI (7.74)	VM	Powered Off	Patient Processing	PCI DSS 2.0	NAC,VIM			7	04/09/2013 19:35:11
1	SJC-IT_Admin2 (7.76)	VM	Powered Off	Datacenter Admins	COBIT 4...	VIM			7	04/09/2013 20:01:12
1	SJC-Kiosk2 (6.71)	VM	Powered Off	Physician Terminals	HIPAA (SP ...	VIM				04/09/2013 20:01:11
1	SJC-NTP (7.78)	VM	Powered Off	Untrusted		Flow,VIM			7	04/09/2013 20:01:11
1	SJC-Staff2_PCI (7.79)	VM	Powered Off	Patient Processing	PCI DSS 2.0	VIM			7	04/09/2013 20:01:17
1	SJC-pharm2 (7.177)	VM	Powered On	Untrusted		Flow,NAC,VIM			7	04/09/2013 20:01:12
0	SV-Health_Records_HIP...	VM	Deleted	Untrusted		VIM			7	04/09/2013 20:01:23
1	SV-IT_Admin3(7.52)	VM	Powered Off	Datacenter Admins	COBIT 4.1	NAC,VIM			7	04/09/2013 20:01:22



TRUST ZONES

https://vdemo/compliance/trustzone/9/zone_flows

Most Visited Getting Started VMware vCloud Direct... Catbird Control Center Web-Demo-CC

catbird

srahim
Log out
Acme Hospital
BST (UTC+01:00)

Edit TrustZone

TrustZone Name: Datacenter Services
 Compliance Class: PCI DSS 2.0
 Criticality: [Slider] Calculator...
 VM Name Membership Automation

Policy Options

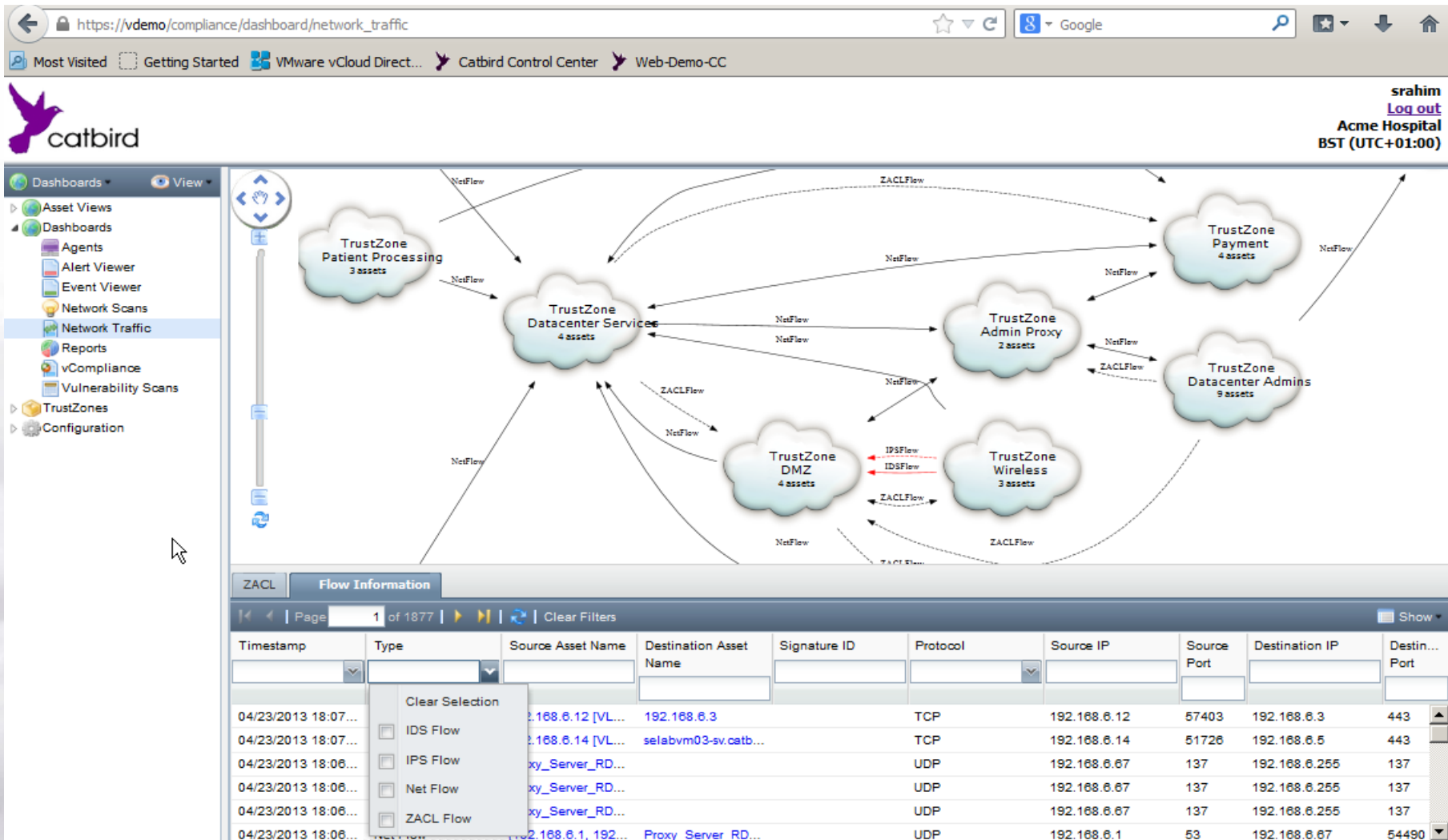
Scan Credentials: None
 Flow Management: Bidirectional
 Notification: Acme Hospital IT Notification
 Virtual Infrastructure: 1-1-nochange-poweroff
 Vulnerability Scan: PCI IVM Scan

Update Cancel

Service	Access
Any/Any	allow
Any/Any	allow
Any/Any	allow
TCP/22 TCP/3389	allow



NETWORK TRAFFIC MAP



CATBIRD TRUSTZONE DASHBOARD

Browser address bar: <https://vdemo/compliance/dashboard/vcompliance>

Navigation: Most Visited, Getting Started, VMware vCloud Direct..., Catbird Control Center, Web-Demo-CC

catbird logo

User: srahim
[Log out](#)
 Acme Hospital
 BST (UTC+01:00)

Left sidebar: Dashboards, Asset Views, Asset Viewer, Asset Vulnerabilities, Vulnerabilities, Hypervisor Hosts, vCompliance, TrustZones (Admin Proxy, DMZ, Datacenter Admins, Datacenter Services, Desktop, Health Record, HypervisorShield, Management, Patient Processing, Payment, Physician Terminals, Security, Untrusted, Wireless, sr123, test123)

Datacenter Services - PCI DSS 2.0

Legend:
 ■ Current
 ■ Compliance baseline

TrustZone Compliance State									
Compliance State	TrustZone Name	Compliance Class	Auditing	Inventory Management	Access Control	Configuration Management	Change Management	Incident Response	Vulnerability Management
⊖	Security	PCI DSS 2.0	⊖	⊕	⊕	⊖	⊕	⊕	⊖
⊕	DMZ	PCI DSS 2.0	⊕	⊕	⊕	⊕	⊕	⊕	⊕
⊖	Datacenter Ser...	PCI DSS 2.0	⊖	⊖	⊕	⊖	⊕	⊕	⊖
⊖	Datacenter Ad...	COBIT 4.1	⊖	⊖	⊖	⊕	⊖	⊖	⊖
⊕	Desktop	HIPAA (SP 800-...	⊕	⊕	⊕	⊕	⊕	⊕	⊖



CATBIRD DELIVERS CONTINUOUS MONITORING USING

- SCAP configuration checking (XCCDF)
- Virtualized Vulnerability Management
- Emerging Threats
- Intrusion Detection / Prevention
- Virtual Firewall
- Hypervisor events



Thank You!

