Achieving Continuous Compliance with PCI DSS 3.0 in the Private Cloud

PCI Conference, Moscow Russia

Edmundo C
CEO
May 29, 201

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?

WHAT IS NEEDED?

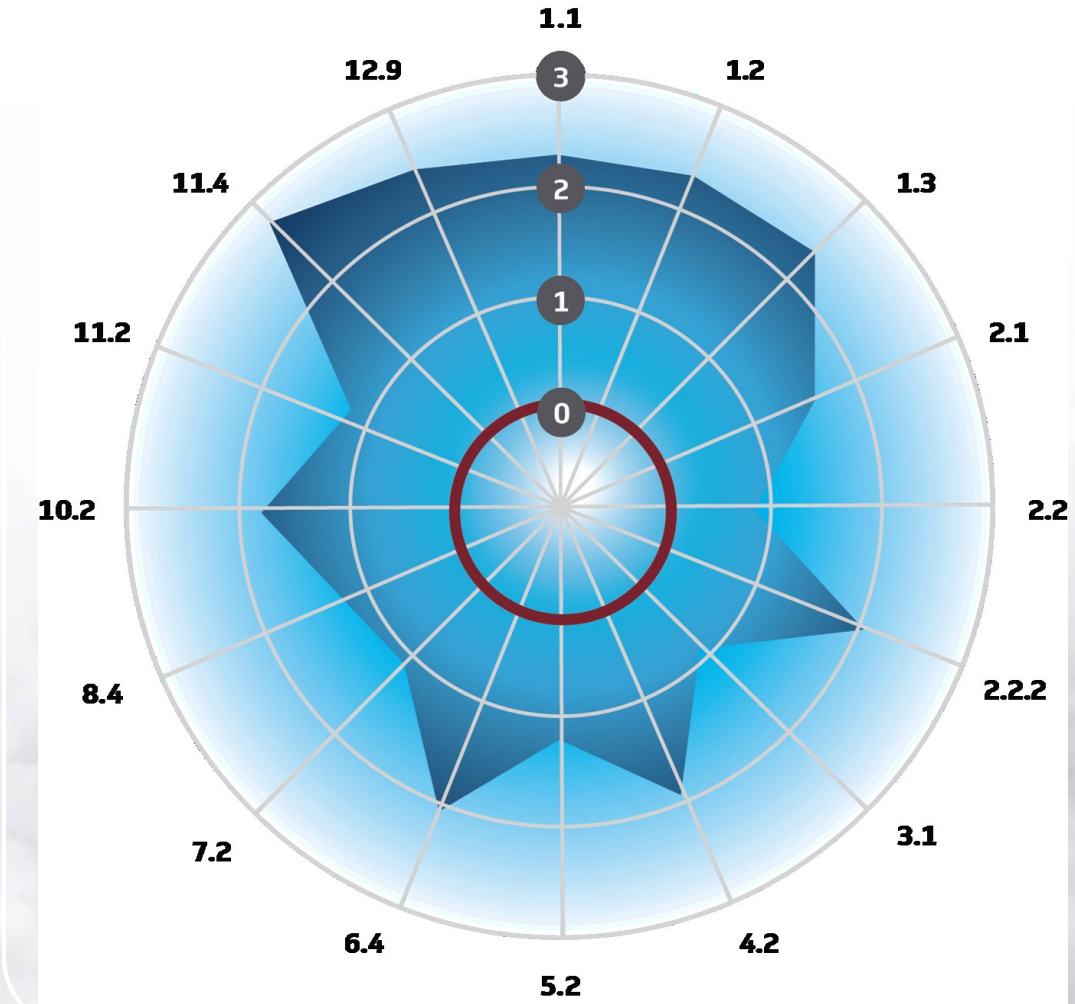
- Trust: Automated security controls to policy
- Verify: Continuous monitoring for proof of control, demonstrate compliance
- Enforce: Mitigation to assure compliance to standards

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

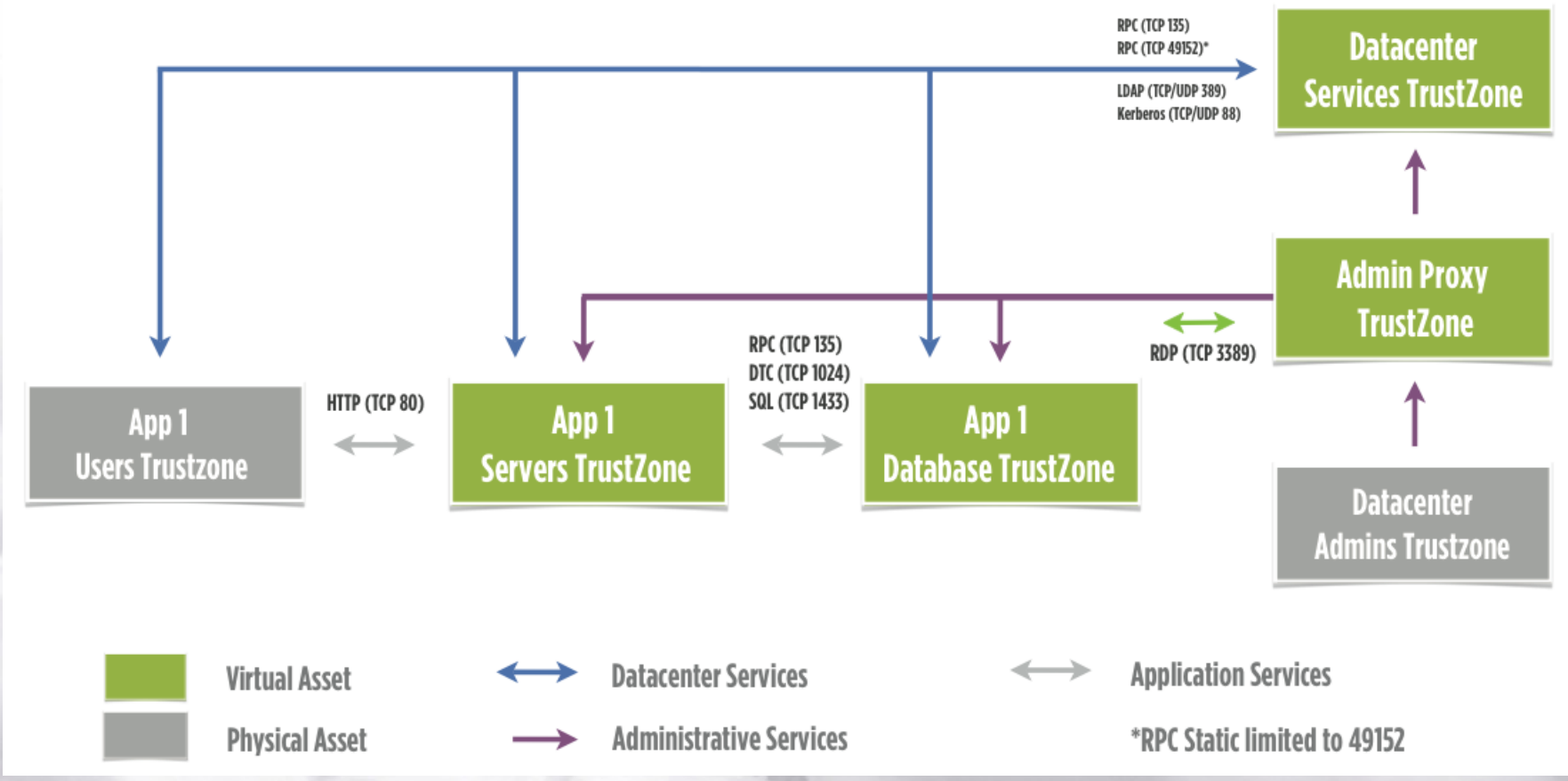
- CDE Isolation:
  - Secondary controls for VLAN isolation
  - Orchestrate virtual firewall from VMware or Cisco
- Automatic quarantine of untrusted virtual assets
- Alert on, and revert, non-compliant changes to virtual network configurations
- Actively block network attacks with IPS

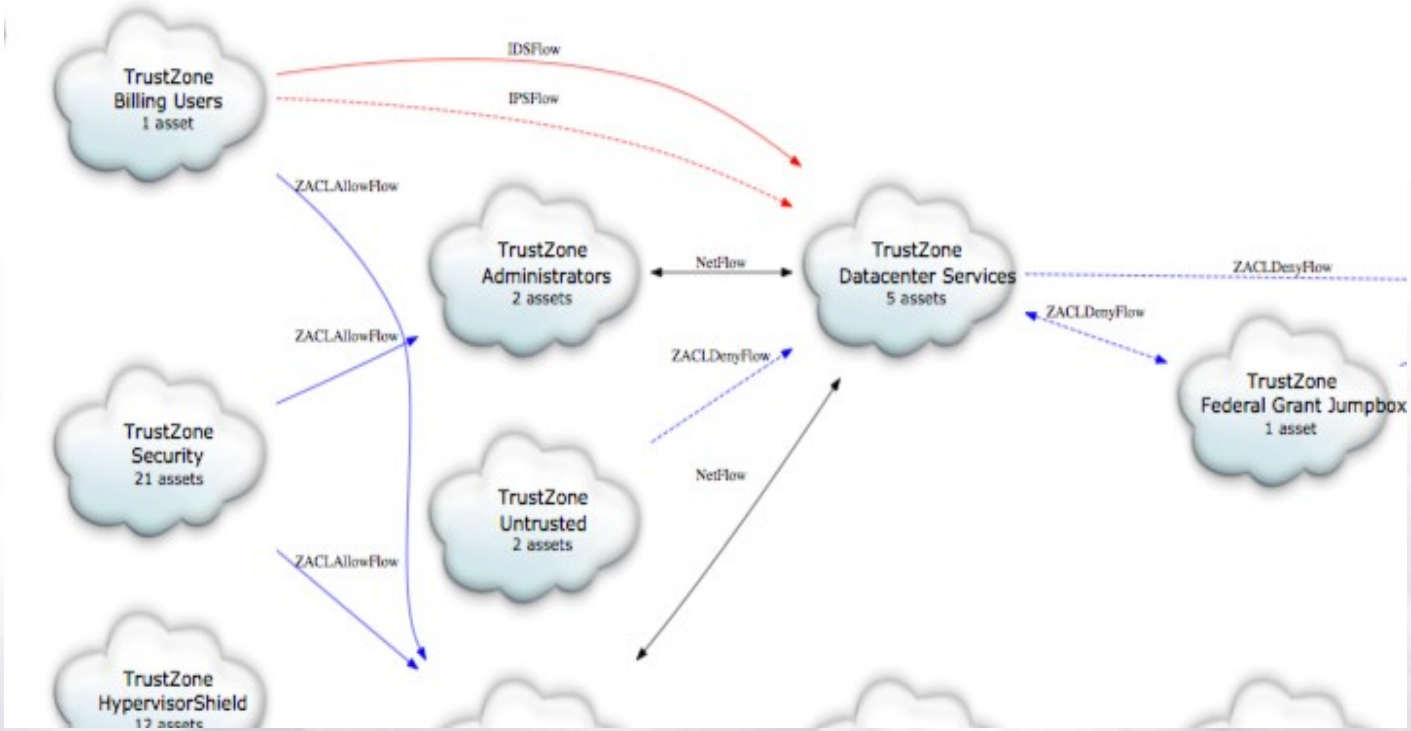
CASE STUDY

LEADING FINANCIAL INSTITUTION

CUSTOMER	CHALLENGE
• Fortune 500 Financial Inst. • 2 datacenters • 7200 employees	Needed strong security solution prior to deploying mission critical apps into private cloud
SOLUTION REQUIREMENT	CUSTOMER QUOTE
• Workload isolation on physical host • Control private cloud network • Continuously monitor for and assure regulatory compliance for mission critical apps	"If I had Catbird last year it would have saved us $2M in audit costs."

TRUSTZONE ARCHITECTURE—TIERED APP MODEL

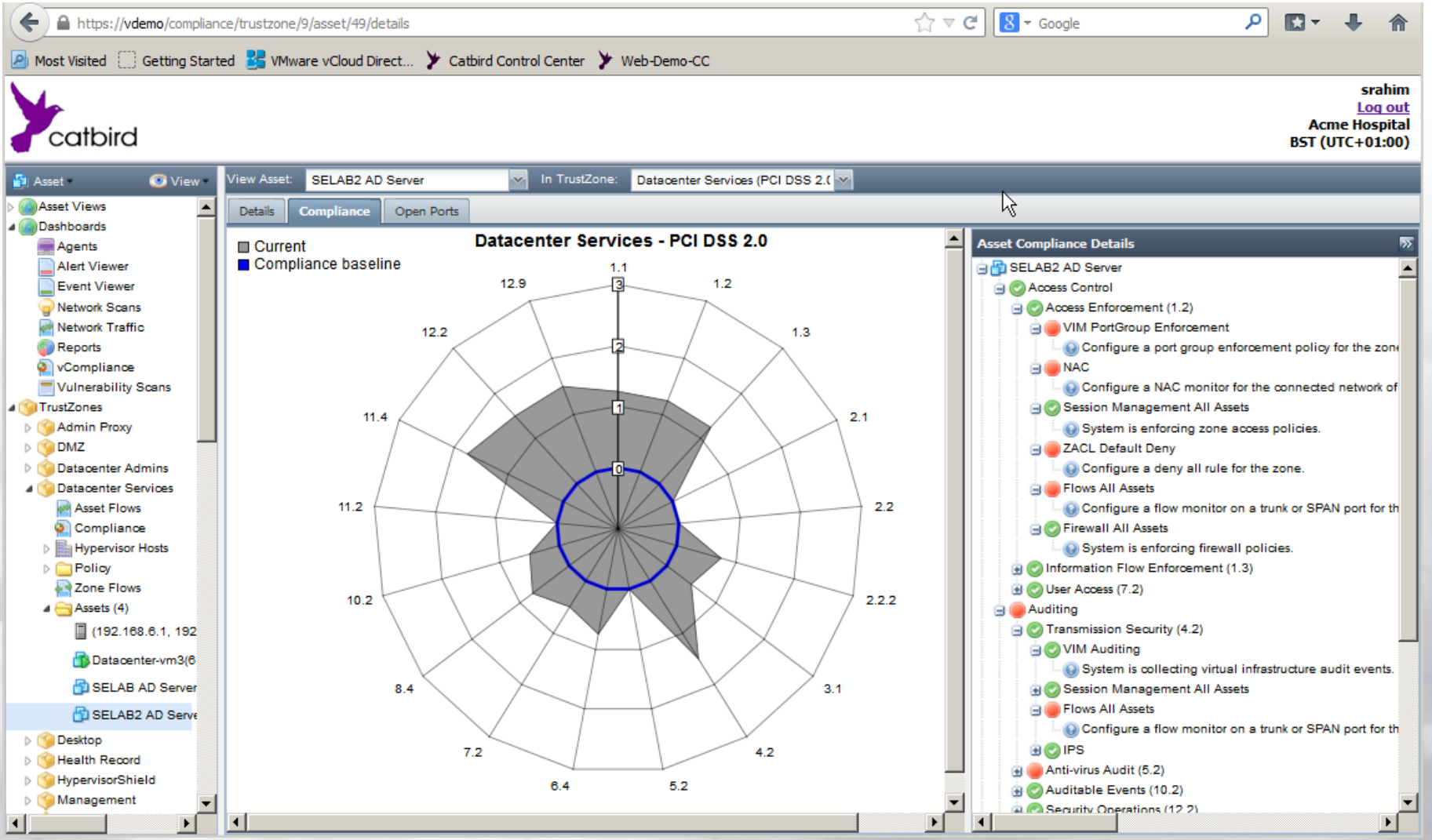




Real Time CDE Data Flows

Meets Requirements 1.2 and 1.3

CATBIRD ASSET AND ZONE COMPLIANCE

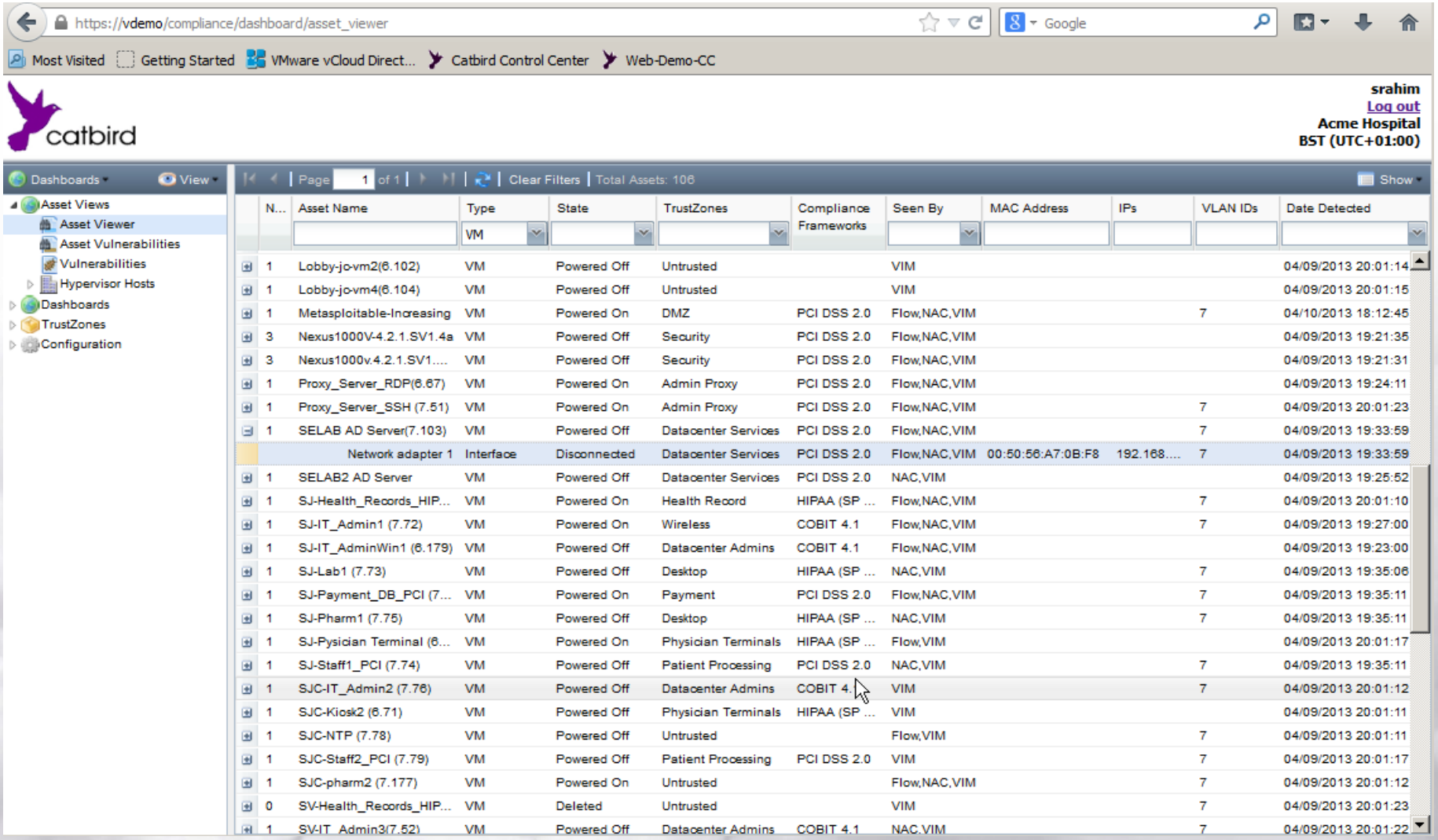


Catbird: Security and Compliance for Private Cloud

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

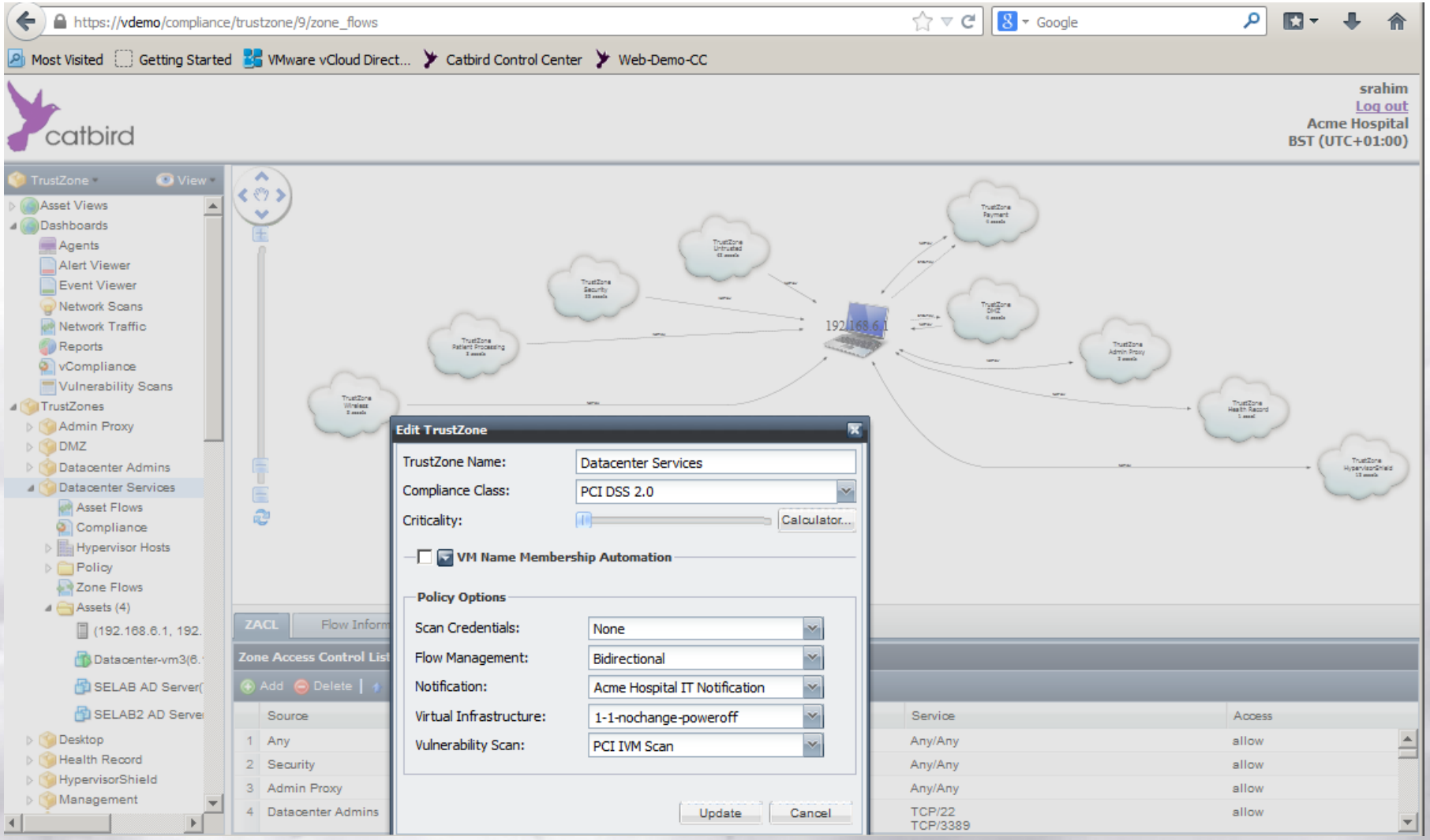
QUESTIONS?

ASSET INVENTORY

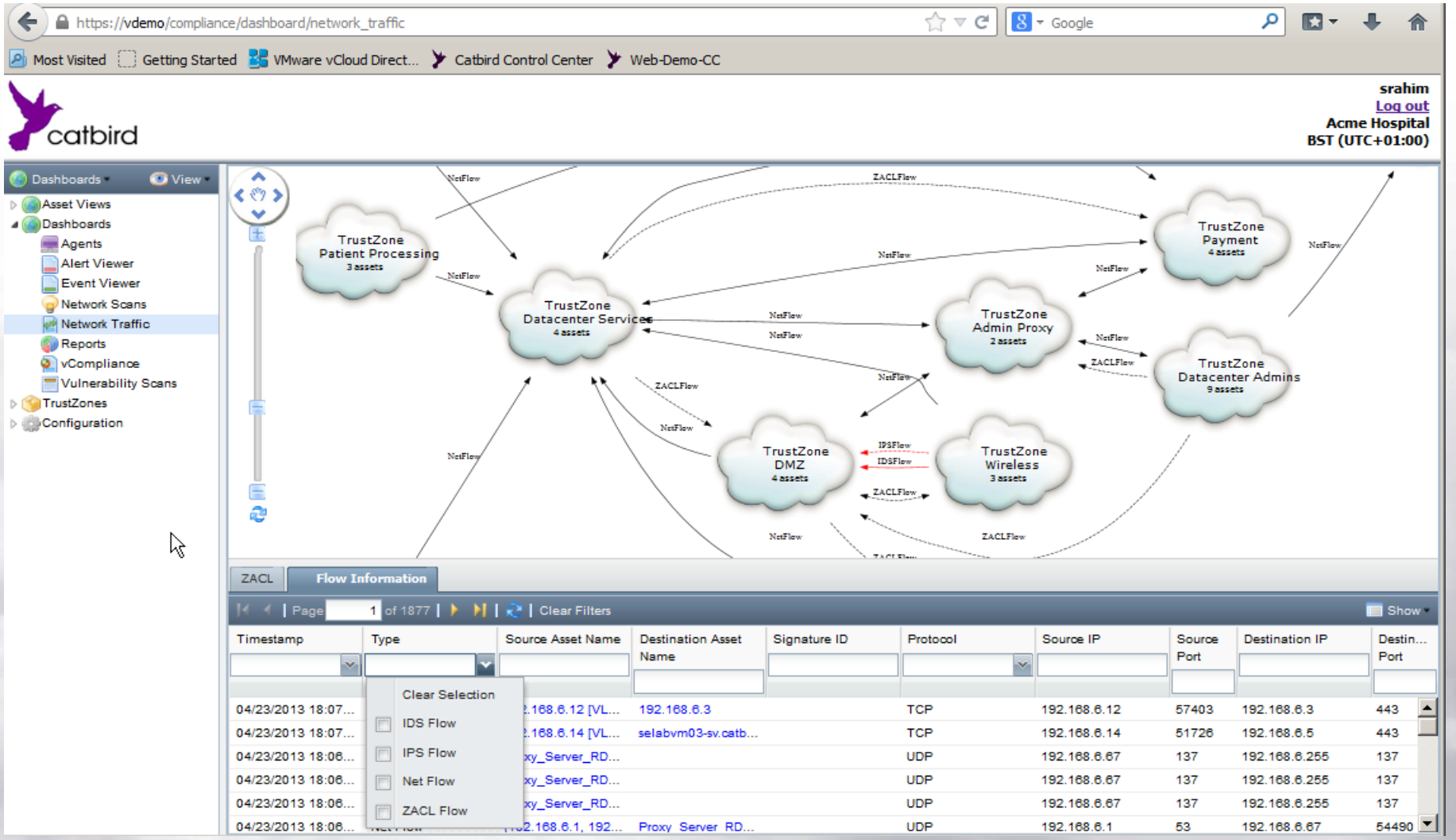


N...	Asset Name	Type	State	TrustZones	Compliance Frameworks	Seen By	MAC Address	IPs	VLAN IDs	Date Detected
		VM								
1	Lobby-jo-vm2(6.102)	VM	Powered Off	Untrusted		VIM				04/09/2013 20:01:14
1	Lobby-jo-vm4(6.104)	VM	Powered Off	Untrusted		VIM				04/09/2013 20:01:15
1	Metasploitable-Increasing	VM	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-Pysician 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

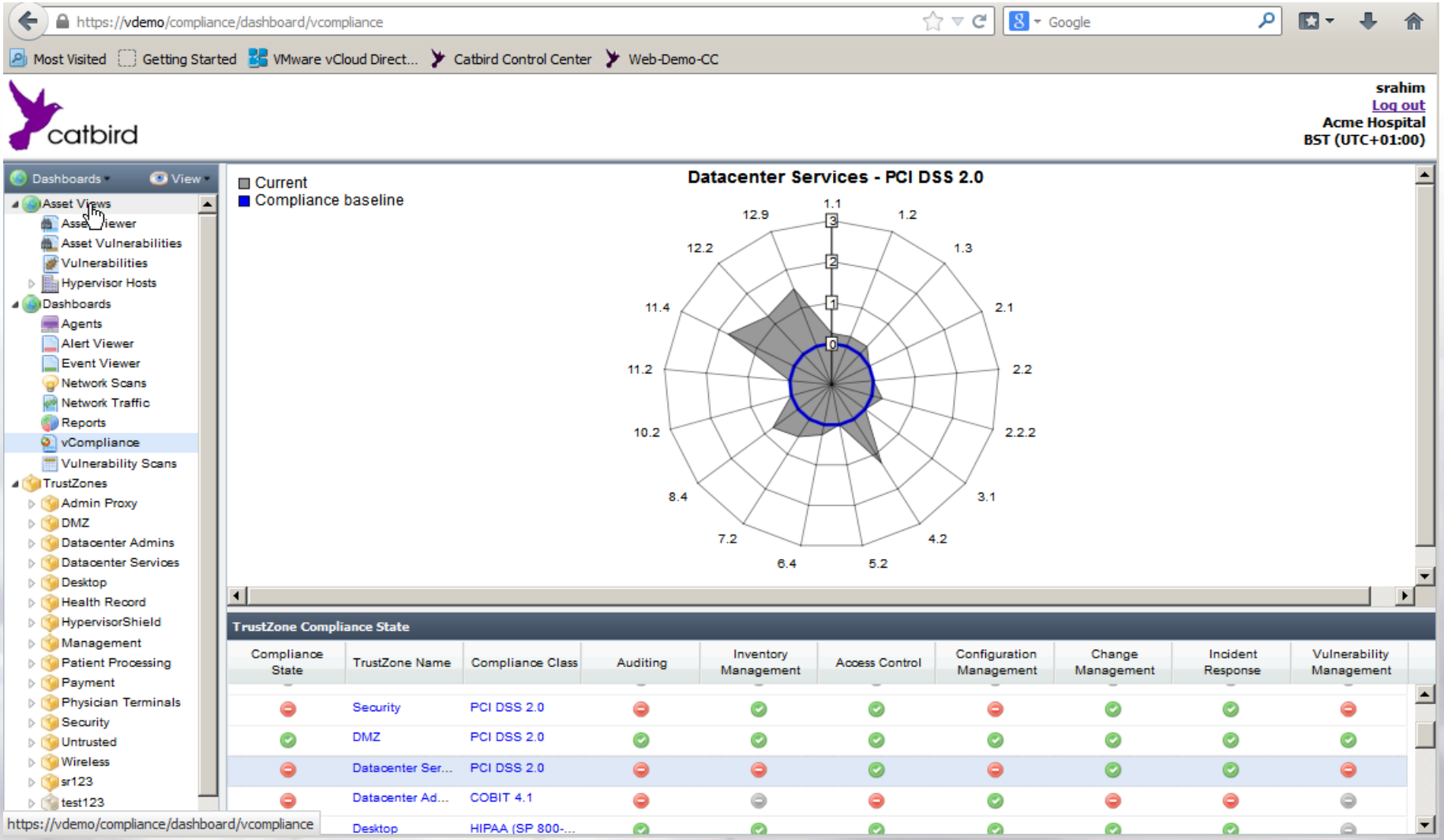
TRUST ZONES



NETWORK TRAFFIC MAP



CATBIRD TRUSTZONE DASHBOARD



CATBIRD DELIVERS CONTINUOUS MONITORING USING

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

Thank You!