nCircle

Proactive Network Security

The Evolution of Identity Management and its Effect on IT Systems

Sweta Duseja

Compliance Marketing Manager

What is Identity Management?

- A system of procedures, policies and technologies to manage the lifecycle and entitlements of users and their electronic credentials
  - Uniquely identifying a person and their roles and responsibilities
  - Attributes for each person, including relationships, affiliations and profile
  - A unique identifier for each person for authentication and authorization
  - User accounts and systems accesses for network resources

An Abbreviated History of Identity Management

- Customized Legacy Systems
  - Internal – Applications, Directories, Databases
  - External – Partner systems
- Proprietary Identity Centralization
  - Cookies, Agents, Single Sign On
- Identity Portability via Interoperable Standards (X.509v3, SAML, WS-*, XACML)
  - Vendor Independent, System Independent

Classic Identity Management Benefits

- **Improved Efficiency**
  - Improve manageability, reduce complexity, streamline administration
  - Reduced user management (user provisioning, deprovisioning, help desk tasks)
- **Simplified Compliance**
  - Current regulatory environment affects virtually all large organizations
  - Penalties solidifying – fines, litigation, bad press, Wall St reaction
- **Increased Security**
  - Automated account cleanup for former or re-assigned employees
  - Better access control and strong authentication
  - Automated auditing, logging, and reporting
- **Real Return On Investment**
  - Automating IDM tasks improves operational effectiveness
  - Reduces administration resource burden and lost user productivity

Identity Management Costs

- Costs are high
  - Procurement costs can range from $18-$100 per user, depending on deployment size*
  - Implementation costs are, on average, **5x** procurement costs*
  - Often not included are internal resource costs
- Adoption continues
  - Costs are high, but OMB is pushing agencies to implement
  - Provable ROI regarding help desks, password resets, etc.
  - There are other benefits that justify the cost – within other IT systems

*Source: Gartner

Unexpected Benefits:
Identity Management's Effect On IT Systems

Implementation of IDM has had some unexpected ancillary benefits:

- Appropriate Access
- Remote Access
- Centralized Control

Identity Management and IT Systems & Security - Classic Categories

Blocking Attacks: Network Based			
Intrusion Prevention	Intrusion Detection	Firewall	Anti-Spam

Blocking Attacks: Host Based			
Intrusion Prevention	Spyware Removal	Personal Firewall	Anti-Virus

Eliminating Security Risk			
Vulnerability Mgmt	Patch Management	Configuration Mgmt	Security Compliance

Safely Supporting Authorized Users			
ID & Access Mgmt	File Encryption	Authentication / PKI	VPN

Tools to Minimize Business Losses			
Forensic Tools	Backup	Compliance	Business Recovery

Source: SANS.org
Defense-in-Depth Model

Identity Management and IT Systems & Security - Classic Categories

Blocking Attacks: Network Based

Intrusion Prevention	Intrusion Detection	Firewall	Anti-Spam

Blocking Attacks: Host Based

Intrusion Prevention	Spyware Removal	Personal Firewall	Anti-Virus

Eliminating Security Risk

Vulnerability Mgmt	Patch Management	Configuration Mgmt	Security Compliance

Safely Supporting Authorized Users

ID & Access Mgmt	File Encryption	Authentication / PKI	VPN

Tools to Minimize Business Losses

Forensic Tools	Backup	Compliance	Business Recovery

**Source: SANS.org
Defense-in-Depth Model**

Identity Management and IT Systems & Security - Classic Categories

Blocking Attacks: Network Based

Intrusion Prevention	Intrusion Detection	Firewall	Anti-Spam

Blocking Attacks: Host Based

Intrusion Prevention	Spyware Removal	Personal Firewall	Anti-Virus

Eliminating Security Risk

Vulnerability Mgmt	Patch Management	Configuration Mgmt	Security Compliance

Safely Supporting Authorized Users

ID & Access Mgmt	File Encryption	Authentication / PKI	VPN

Tools to Minimize Business Losses

Forensic Tools	Backup	Compliance	Business Recovery

Source: SANS.org
Defense-in-Depth Model

Identity Management and IT Systems & Security - Growth Categories

Blocking Attacks: Network Based

Intrusion Prevention	Intrusion Detection	Firewall	Anti-Spam

Blocking Attacks: Host Based

Intrusion Prevention	Spyware Removal	Personal Firewall	Anti-Virus

Eliminating Security Risk

Vulnerability Mgmt	Patch Management	Configuration Mgmt	Security Compliance

Safely Supporting Authorized Users

ID & Access Mgmt	File Encryption	Authentication / PKI	VPN

Tools to Minimize Business Losses

Forensic Tools	Backup	Compliance	Business Recovery

Source: SANS.org
Defense-in-Depth Model

So, What Changed?

- Identity Management evolved from an agent-based to an agentless architecture
  - Large, expensive deployments hosted on OS/390 mainframes
  - Moved to Service Oriented Architecture (SOA)
  - Agentless communication is becoming the norm for identity management

So, What Changed?

- Identity Management's evolution from an agent-based to an agentless architecture…

  … *helped to model* other IT systems' evolution from agent-based to agentless architecture

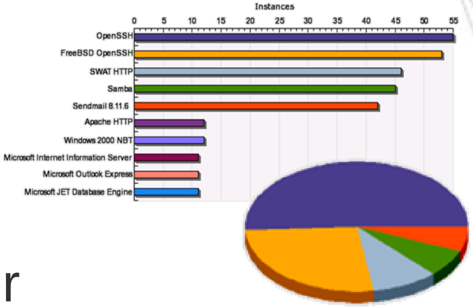
- Instead of having to physically examine a machine, or load an agent on a machine, we can:
  - Create fine-grained, limited privilege accounts
  - Centrally consolidate these accounts

So, What Changed?

What could previously only be accomplished with a separate agent for each solution is now routinely done without installing software on the endpoints

- If you want to find out:
  - If a system contains obsolete or prohibited software
  - If a system is running the latest version of anti-virus
  - If a user has disabled their personal firewall
  - If a server had been reconfigured from its approved secure state, and by whom
- Can accomplish this for *all* systems on the network

Security Auditing Leverages Identity Management



- Vulnerability Assessment, Vulnerability Management
  - Automated assessment of networked systems for vulnerabilities, e.g. buffer overflows, DoS, etc.
- Most VA/VM solutions provide remote testing without credentials
  - Assesses network-facing services and applications
- Thanks to IDM, some solutions can also perform deep system testing using credentials
  - Read-only registry and/or file access on Windows
  - SSH on UNIX, Cisco IOS, Linux, OS X, etc.

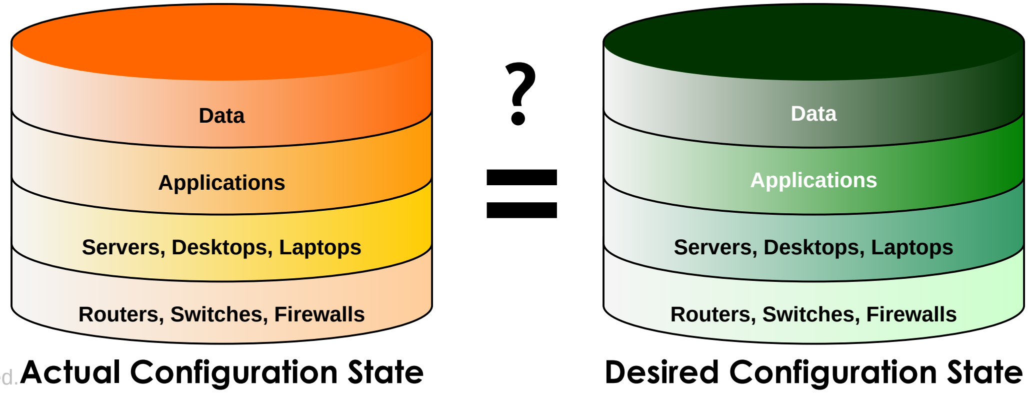
nCircle
Proactive Network Security

Configuration Auditing Leverages Identity Management

Before IDM, configuration auditing could only be accomplished using agents, and was therefore relegated to a small number of systems…

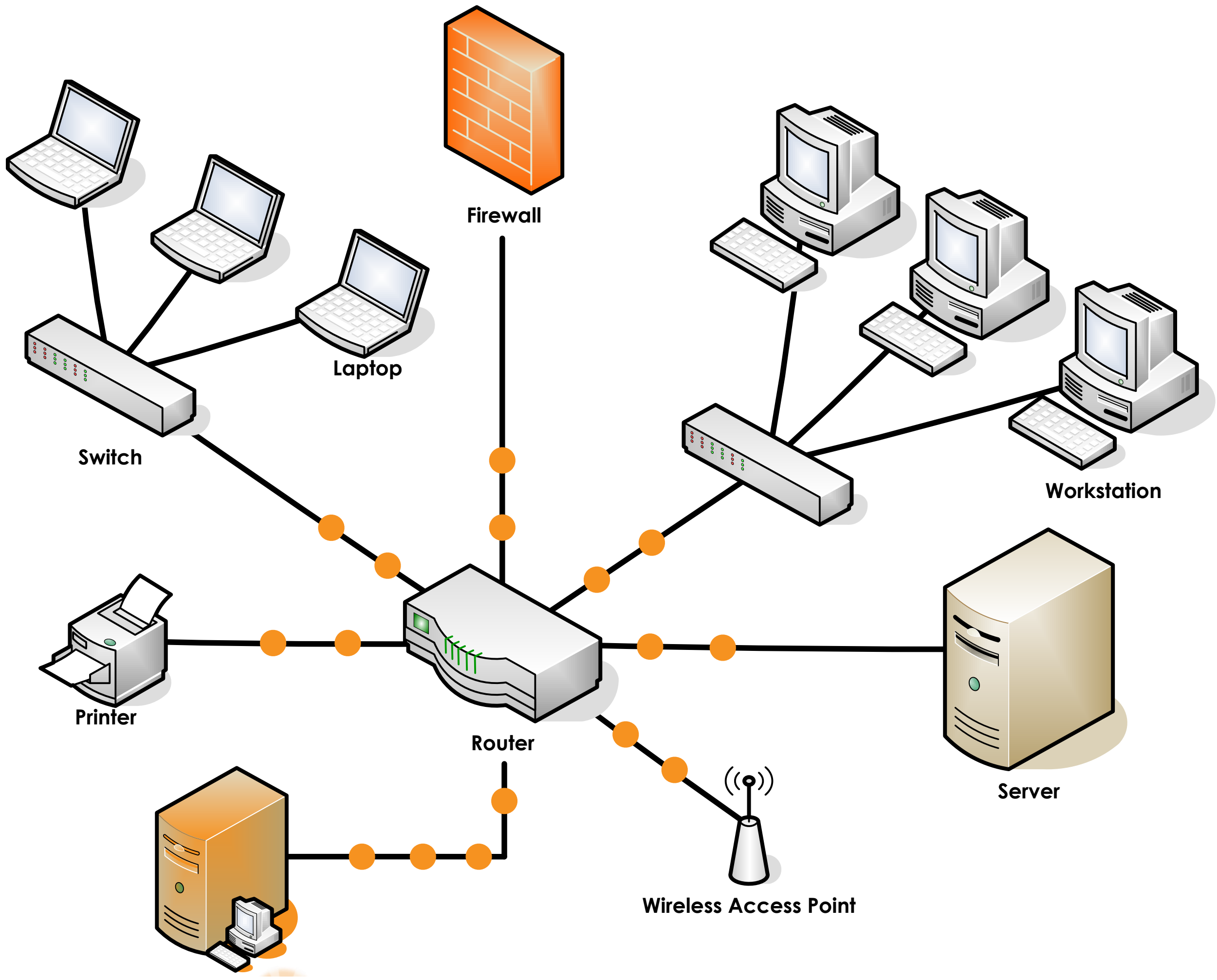
Configuration auditing discovers:

1. How IT systems are configured
2. Whether these configurations comply with established policy
3. How system configurations are changing
4. Whether these changes are OK or not


Data
Applications
Servers, Desktops, Laptops
Routers, Switches, Firewalls
Actual Configuration State
?
=
Data
Applications
Servers, Desktops, Laptops
Routers, Switches, Firewalls
Desired Configuration State

nCircle
Proactive Network Security

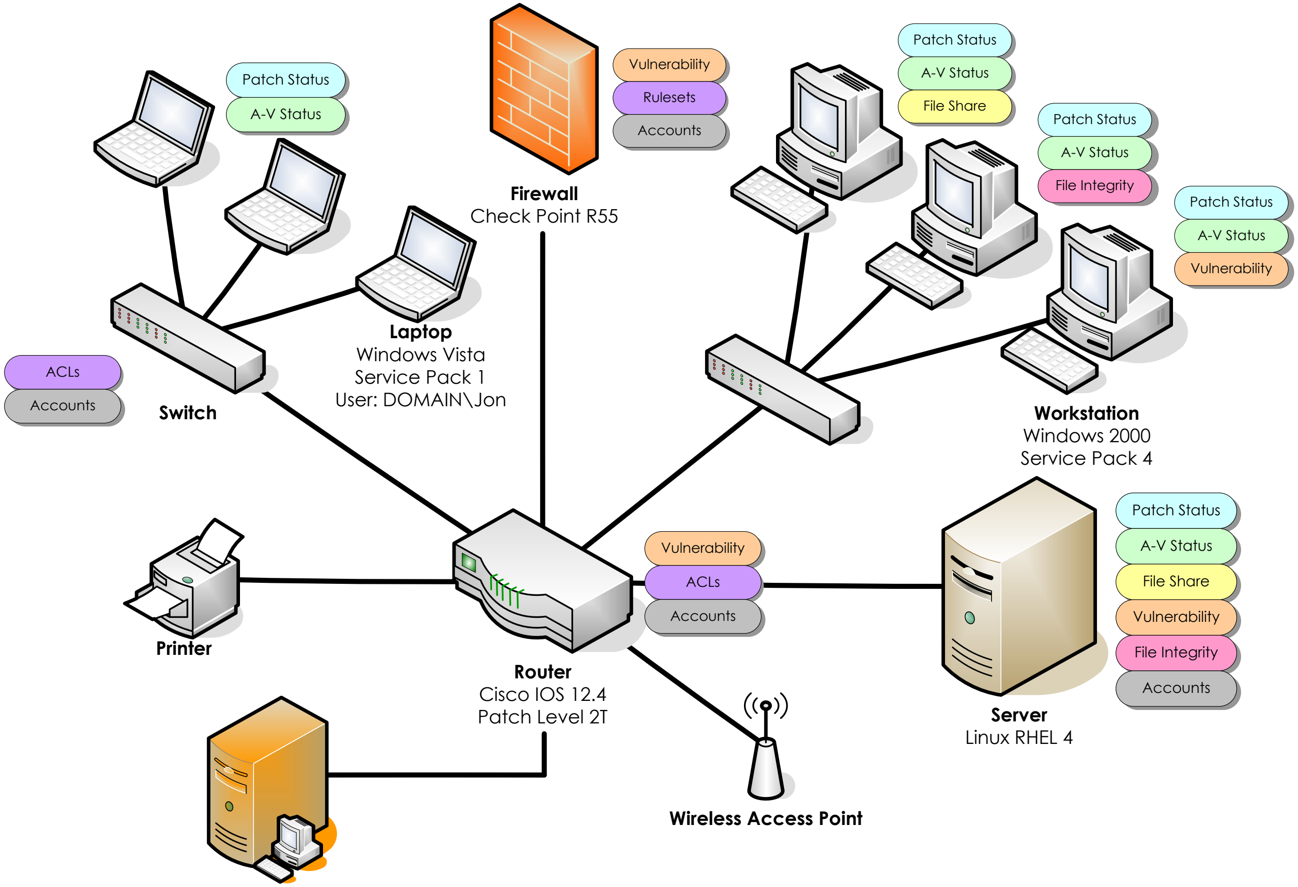
1. Enumerate Network Inventory



- Servers and endpoints
  - Windows
  - Linux
  - Solaris
  - AIX
  - HPUX
- Network infrastructure
  - Routers
  - Switches
  - Firewalls
- Enterprise applications
  - Databases
  - Web Servers
  - Anti-virus

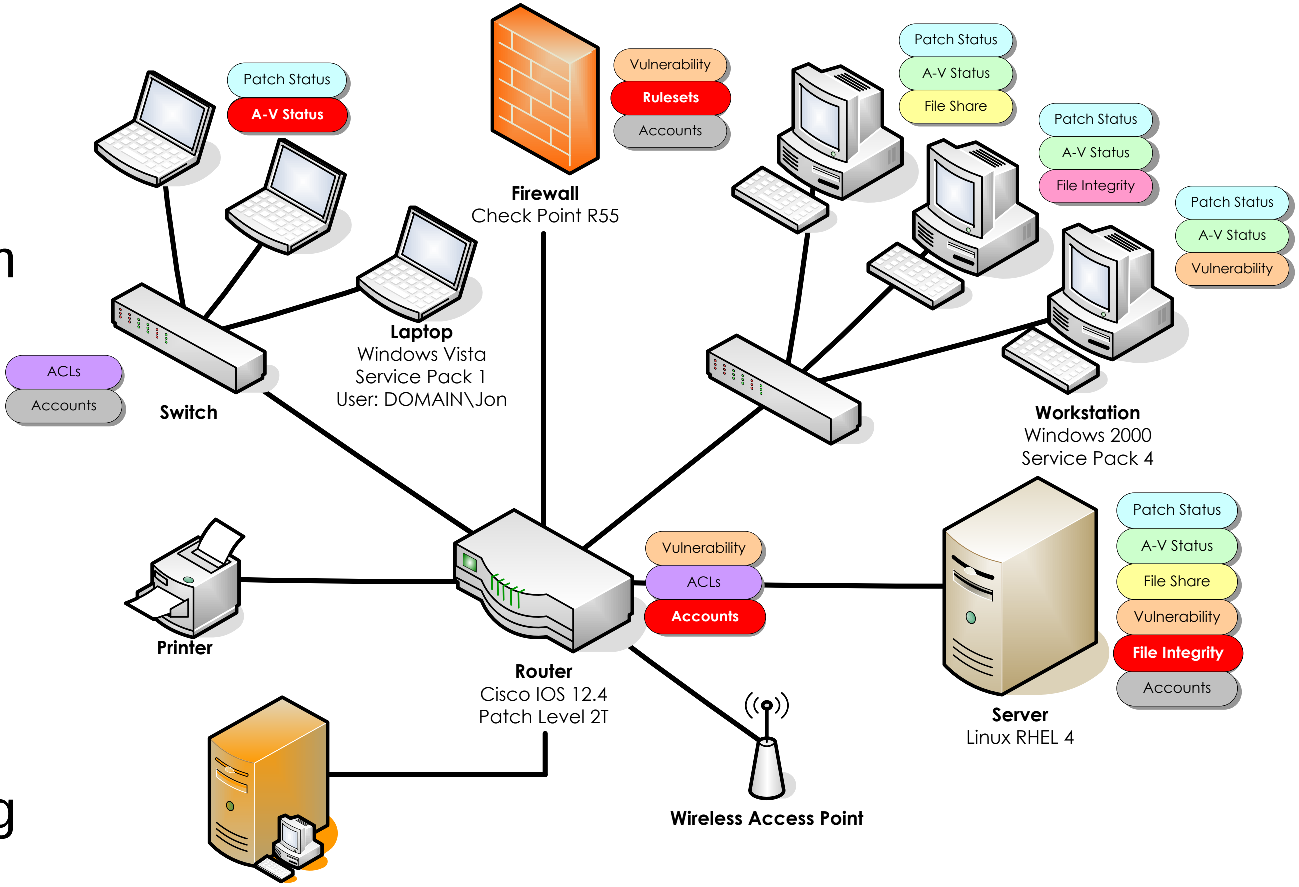
nCircle
Proactive Network Security

2. Detail Each System's Configuration



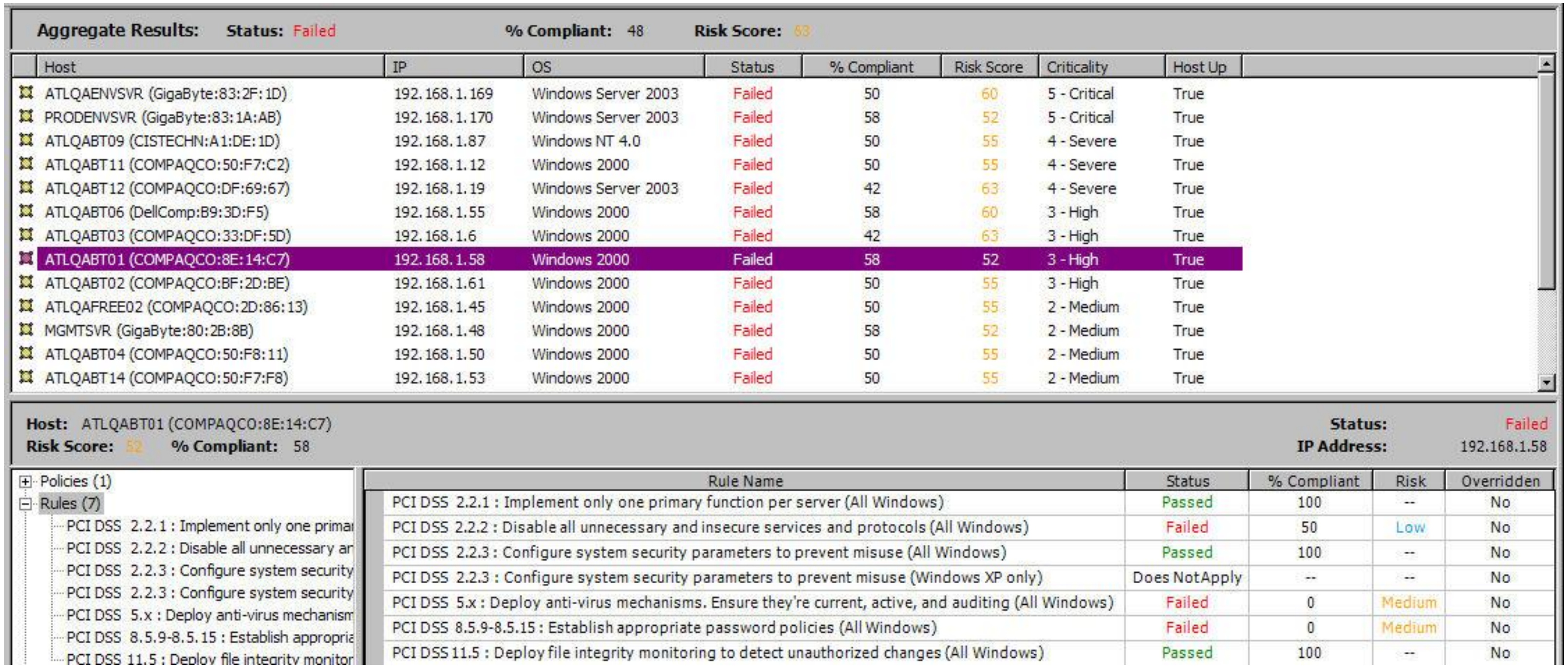
3. Enumerate Configuration Changes

- Continuous detection of changes in system files and asset configurations
- All changes recorded in database
- Change events drive alerts and follow-on scanning



nCircle
Proactive Network Security

4. Evaluate Configuration Against Policy



Aggregate Results: **Status:** Failed **% Compliant:** 48 **Risk Score:** 63

	Host	IP	OS	Status	% Compliant	Risk Score	Criticality	Host Up
	ATLQAENVSVR (GigaByte:83:2F:1D)	192.168.1.169	Windows Server 2003	Failed	50	60	5 - Critical	True
	PRODENVSVR (GigaByte:83:1A:AB)	192.168.1.170	Windows Server 2003	Failed	58	52	5 - Critical	True
	ATLQABT09 (CISTECHN:A1:DE:1D)	192.168.1.87	Windows NT 4.0	Failed	50	55	4 - Severe	True
	ATLQABT11 (COMPAQCO:50:F7:C2)	192.168.1.12	Windows 2000	Failed	50	55	4 - Severe	True
	ATLQABT12 (COMPAQCO:DF:69:67)	192.168.1.19	Windows Server 2003	Failed	42	63	4 - Severe	True
	ATLQABT06 (DellComp:B9:3D:F5)	192.168.1.55	Windows 2000	Failed	58	60	3 - High	True
	ATLQABT03 (COMPAQCO:33:DF:5D)	192.168.1.6	Windows 2000	Failed	42	63	3 - High	True
	ATLQABT01 (COMPAQCO:8E:14:C7)	192.168.1.58	Windows 2000	Failed	58	52	3 - High	True
	ATLQABT02 (COMPAQCO:BF:2D:BE)	192.168.1.61	Windows 2000	Failed	50	55	3 - High	True
	ATLQAFREE02 (COMPAQCO:2D:86:13)	192.168.1.45	Windows 2000	Failed	50	55	2 - Medium	True
	MGMTSVR (GigaByte:80:2B:8B)	192.168.1.48	Windows 2000	Failed	58	52	2 - Medium	True
	ATLQABT04 (COMPAQCO:50:F8:11)	192.168.1.50	Windows 2000	Failed	50	55	2 - Medium	True
	ATLQABT14 (COMPAQCO:50:F7:F8)	192.168.1.53	Windows 2000	Failed	50	55	2 - Medium	True

Host: ATLQABT01 (COMPAQCO:8E:14:C7) **Status:** Failed
Risk Score: 52 **% Compliant:** 58 **IP Address:** 192.168.1.58

⊞ Policies (1)
⊟ Rules (7)
PCI DSS 2.2.1 : Implement only one primar
PCI DSS 2.2.2 : Disable all unnecessary ar
PCI DSS 2.2.3 : Configure system security
PCI DSS 2.2.3 : Configure system security
PCI DSS 5.x : Deploy anti-virus mechanism
PCI DSS 8.5.9-8.5.15 : Establish appropria
PCI DSS 11.5 : Deploy file integrity monitor

Rule Name	Status	% Compliant	Risk	Overridden
PCI DSS 2.2.1 : Implement only one primary function per server (All Windows)	Passed	100	--	No
PCI DSS 2.2.2 : Disable all unnecessary and insecure services and protocols (All Windows)	Failed	50	Low	No
PCI DSS 2.2.3 : Configure system security parameters to prevent misuse (All Windows)	Passed	100	--	No
PCI DSS 2.2.3 : Configure system security parameters to prevent misuse (Windows XP only)	Does Not Apply	--	--	No
PCI DSS 5.x : Deploy anti-virus mechanisms. Ensure they're current, active, and auditing (All Windows)	Failed	0	Medium	No
PCI DSS 8.5.9-8.5.15 : Establish appropriate password policies (All Windows)	Failed	0	Medium	No
PCI DSS 11.5 : Deploy file integrity monitoring to detect unauthorized changes (All Windows)	Passed	100	--	No

- Configuration of “gold image”
- Rich library of policies from a variety of sources
  - Prescriptive policies from CIS, NIST, and Microsoft
  - Regulatory policies such as PCI, HIPAA, and SOX
  - Emerging policies like Federal Desktop Core Configuration

CERTIFIED BY the CENTER for INTERNET SECURITY

nCircle
Proactive Network Security

Agentless Configuration Auditing

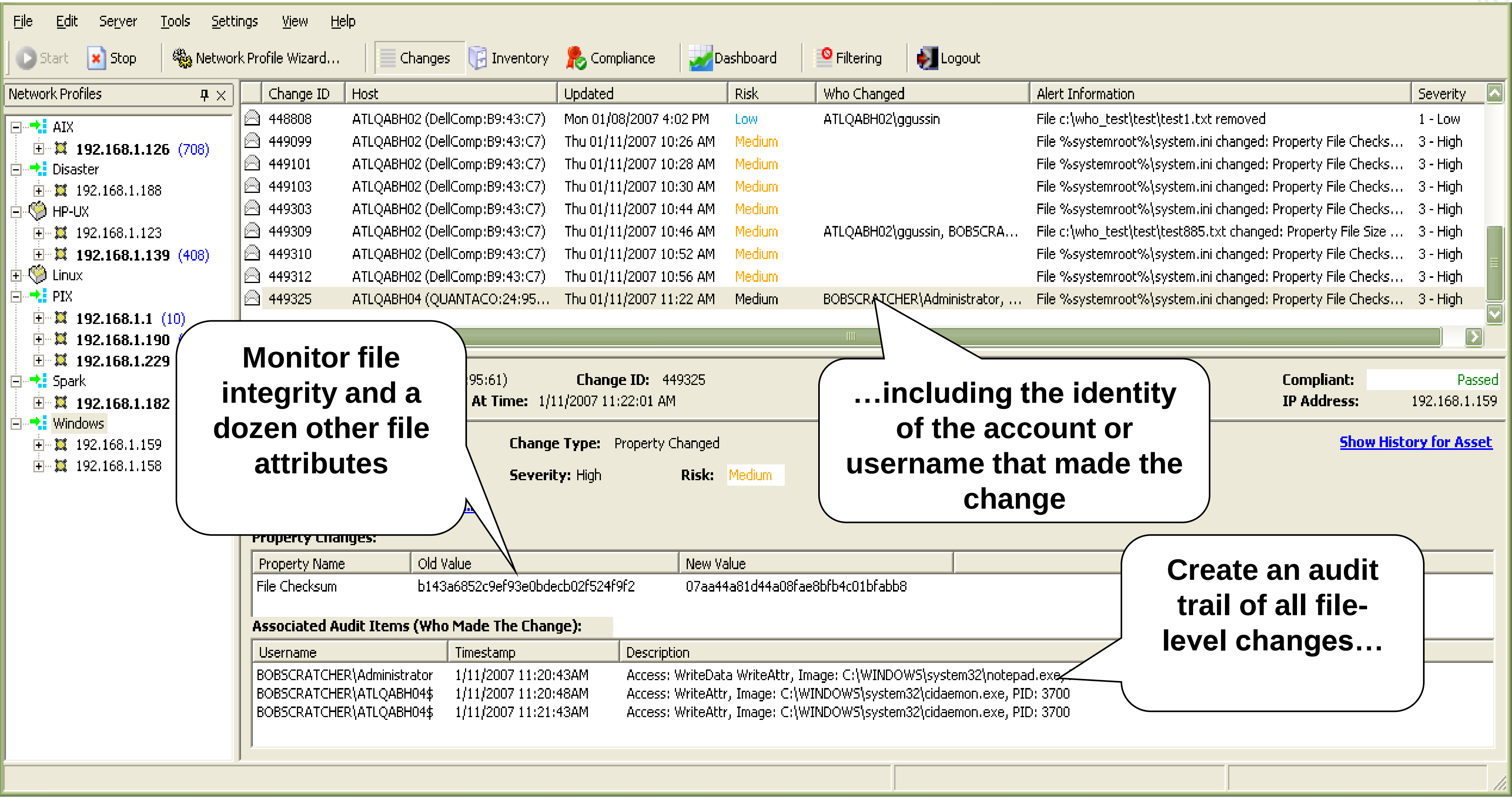
- Identity Management has enabled organizations to audit system configurations on a network-wide basis
  - No agents to install on endpoints
  - Agentless auditing provides complete coverage of all networked systems, not just major operating systems (unmanaged devices, infrastructure, IP phones, etc.)
  - Greatly reduced political issues compared to installing agents on systems managed by others

File Integrity Monitoring

Identity Management enables file integrity monitoring to be implemented on all applicable systems, at a reasonable cost

- Monitor files for security and compliance purposes
  - Monitor file integrity and attributes for protection against trojans, etc.
  - Monitor file contents for compliance purposes – personal information, confidential information, etc.
- Provides an audit trail of all file-level changes, including the identity of the account or username that made the change

File Integrity Monitoring in Action



Change ID	Host	Updated	Risk	Who Changed	Alert Information	Severity
448808	ATLQABH02 (DellComp:B9:43:C7)	Mon 01/08/2007 4:02 PM	Low	ATLQABH02\ggussin	File c:\who_test\test\test1.txt removed	1 - Low
449099	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:26 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449101	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:28 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449103	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:30 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449303	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:44 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449309	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:46 AM	Medium	ATLQABH02\ggussin, BOBSCRA...	File c:\who_test\test\test885.txt changed: Property File Size ...	3 - High
449310	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:52 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449312	ATLQABH02 (DellComp:B9:43:C7)	Thu 01/11/2007 10:56 AM	Medium		File %systemroot%\system.ini changed: Property File Checks...	3 - High
449325	ATLQABH04 (QUANTACO:24:95...	Thu 01/11/2007 11:22 AM	Medium	BOBSCRATCHER\Administrator, ...	File %systemroot%\system.ini changed: Property File Checks...	3 - High

95:61) **Change ID:** 449325

At Time: 1/11/2007 11:22:01 AM

Compliant: Passed

IP Address: 192.168.1.159

Show History for Asset

Change Type: Property Changed

Severity: High **Risk:** Medium

Property Changes:

Property Name	Old Value	New Value
File Checksum	b143a6852c9ef93e0bdecb02f524f9f2	07aa44a81d44a08fae8bfb4c01bfabb8

Associated Audit Items (Who Made The Change):

Username	Timestamp	Description
BOBSCRATCHER\Administrator	1/11/2007 11:20:43AM	Access: WriteData WriteAttr, Image: C:\WINDOWS\system32\notepad.exe,
BOBSCRATCHER\ATLQABH04$	1/11/2007 11:20:48AM	Access: WriteAttr, Image: C:\WINDOWS\system32\cidaemon.exe, PID: 3700
BOBSCRATCHER\ATLQABH04$	1/11/2007 11:21:43AM	Access: WriteAttr, Image: C:\WINDOWS\system32\cidaemon.exe, PID: 3700

Monitor file integrity and a dozen other file attributes

…including the identity of the account or username that made the change

Create an audit trail of all file-level changes…

nCircle
Proactive Network Security

Why is the Enablement of Agentless Technology Important?

Intelligence

- Discovery
- Coverage
- Network Context

Operations

- Deployment speed
- Internal politics
- System impact

Business

- Cost of ownership
- Third-party system monitoring

- Discover and identify all

- Minimal resources required to be operational
- Assessing all networked systems within hours

- Lower acquisition cost and easier to maintain and support
- Ability to monitor externally-owned systems on the network (e.g. contractors)

Summary

- Identity Management has evolved over the past decade into a de-facto solution

- The evolution of IDM has had cascading effects throughout IT, including security and compliance

- The transition of IDM from a monolithic, proprietary, agent-based system to an agentless system based on standards has both enabled and modeled a similar transition in other IT systems

- The result is improved visibility and significantly reduced overhead required to collect data about systems on the network

Questions?