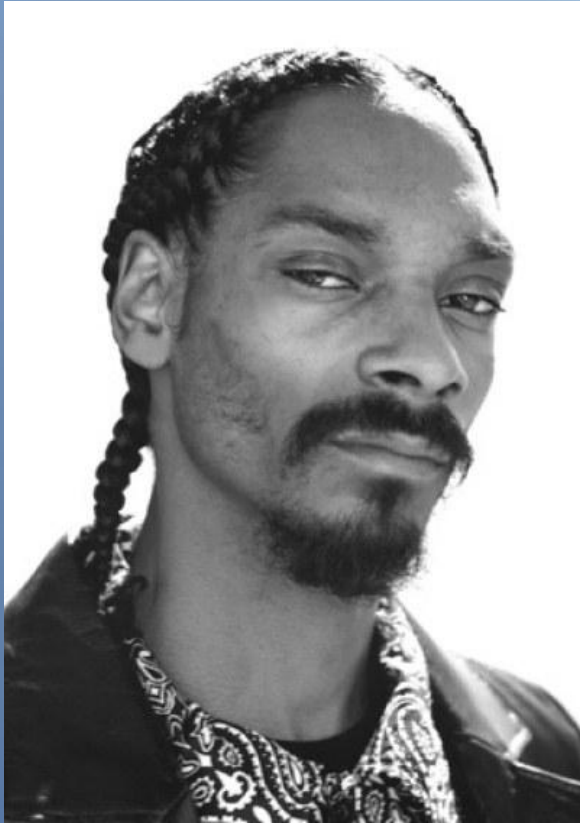


NetVision

Network Access Auditing and Security

Who has access. To what. How they got it. What they're doing with it.

Examples of Access Misuse



67% IT Pros access non-relevant information

41% abused admin passwords to snoop sensitive data

37% stumbled into network areas to which they shouldn't have access

50% work around security policies in order to get their jobs done

Cyber-Ark Trust, Security and Passwords Survey, July 2010

RSA Insider Threat Survey, October 2008

The Cost of Access Misuse

Time & cost to resolve errors

*Time & cost of risk
management*

Legal action & financial loss

Risk Management/Cleanup is costly

2,000 shared files per employee

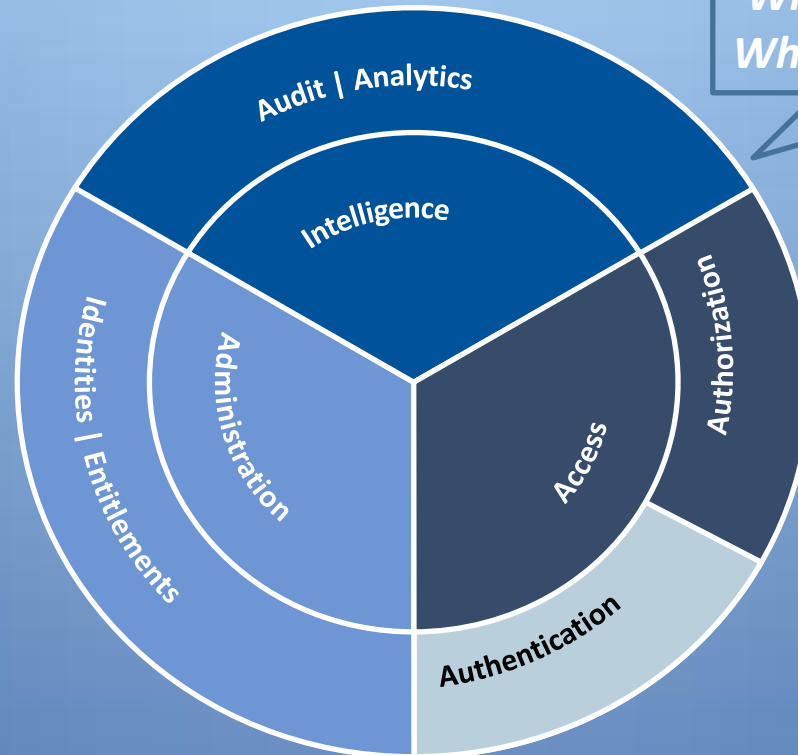
2GB shared data per employee

1 Active Directory group per employee

*20% of Accounts are enabled but
dormant*

IT Needs Access Auditing

*Who has access to what?
How did they get it?
What are they doing with it?
What needs to be cleaned up?*



Critical Elements of Identity Management

Source: Gartner Group 2011

NetVision - Easy Access Auditing



NetVision Appliance

Virtual Appliance OR Hardware

Self-Contained:

- NetVision Engine
- Database
- Reporting Engine
- Web Services

Pre-Installed and Configured

Security Hardened



NVMonitor – what is happening

The screenshot displays the NetVision Administration Console interface. On the left, the 'Policy Center' tree shows a hierarchy of policies under 'Microsoft' and 'Novell'. The 'Policies' pane on the right lists several active policies, including 'AD Group Deletions' and 'AD Group Moves or Renames of Administrator ...'. The 'Registrations' pane shows a table with one entry: 'Active Directory' with the event type 'Object Modified'. Below this, there are 'Add...' and 'Remove' buttons, and a 'Registration Filters' section with tabs for 'Domains/Servers', 'AD Context', 'AD Classes', 'AD Attributes', and 'AD ...'. The 'AD Classes' tab is selected, showing a list of classes with 'group' listed. The bottom status bar indicates the current user is 'SIMON10\Administrator'.

Event Type	Name
Active Directory	Object Modified

Classes
group

One product monitors:

- Active Directory
- eDirectory
- Windows File Sys
- NetApp Filers
- NetWare File Sys
- Novell NSS File Sys
- Microsoft Exchange

Best practice policies for each system built in

Highly configurable = necessary and sufficient information

Access Rights Inspector – who has access, how did they get it?

Effective Rights - By User/Group

Server	User	Size	Full Control	Traverse Folder / Execute File	List Folder / Read Data
2003SERVER	32BIT2003DOMAIN\Administrator	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\Administrators	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\BP (Brian P)	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\Domain Admins	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\Enterprise Admins	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\HR Admins	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\janedemo (Janedemo)	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\jimdemo (Jimdemo)	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\joedemo (Joedemo)	C:\ 4,871	+	+	+
2003SERVER	32BIT2003DOMAIN\johndemo (John)	C:\ 4,871	+	+	+

- Effective Rights for File System

- Automatically gathers indicators of Groups and files needing attention

- Visibility to delegated rights in Active Directory

- Easy visibility to Security Group memberships

- Enables automation of routine processes

NetVision Access Audit

Eliminates cost of IT investigation and cleanup

Eliminates downtime due to accidents or insider attacks

Quickly identify and correct bad behavior