



Managing access permissions to unstructured data

Edward Wasilchin
Regional Manager
Scandinavia
+46 708 10 58 78
edward@varonis.com

Common File System Infrastructure

- Technology
 - ▶ **TB's of unstructured data**
 - ▶ **Data grows significantly**
 - ▶ **Many users, many AD groups**
 - ▶ **Many folders with unique permissions (5%)**
- Personnel
 - ▶ **Several employees managing access control (FTE equivalents)**
 - ▶ **Manual authorization workflows and permissions management**
 - ▶ **Significant time spent working with audit on access control related issues**

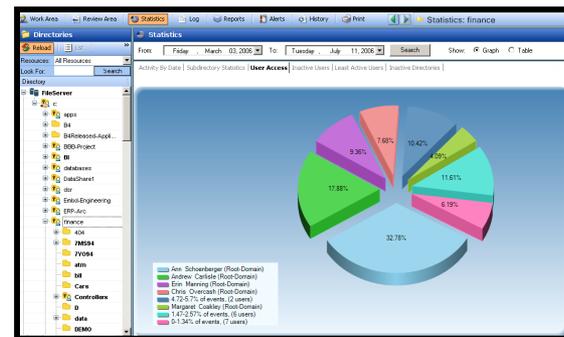


Common Infrastructure Challenges

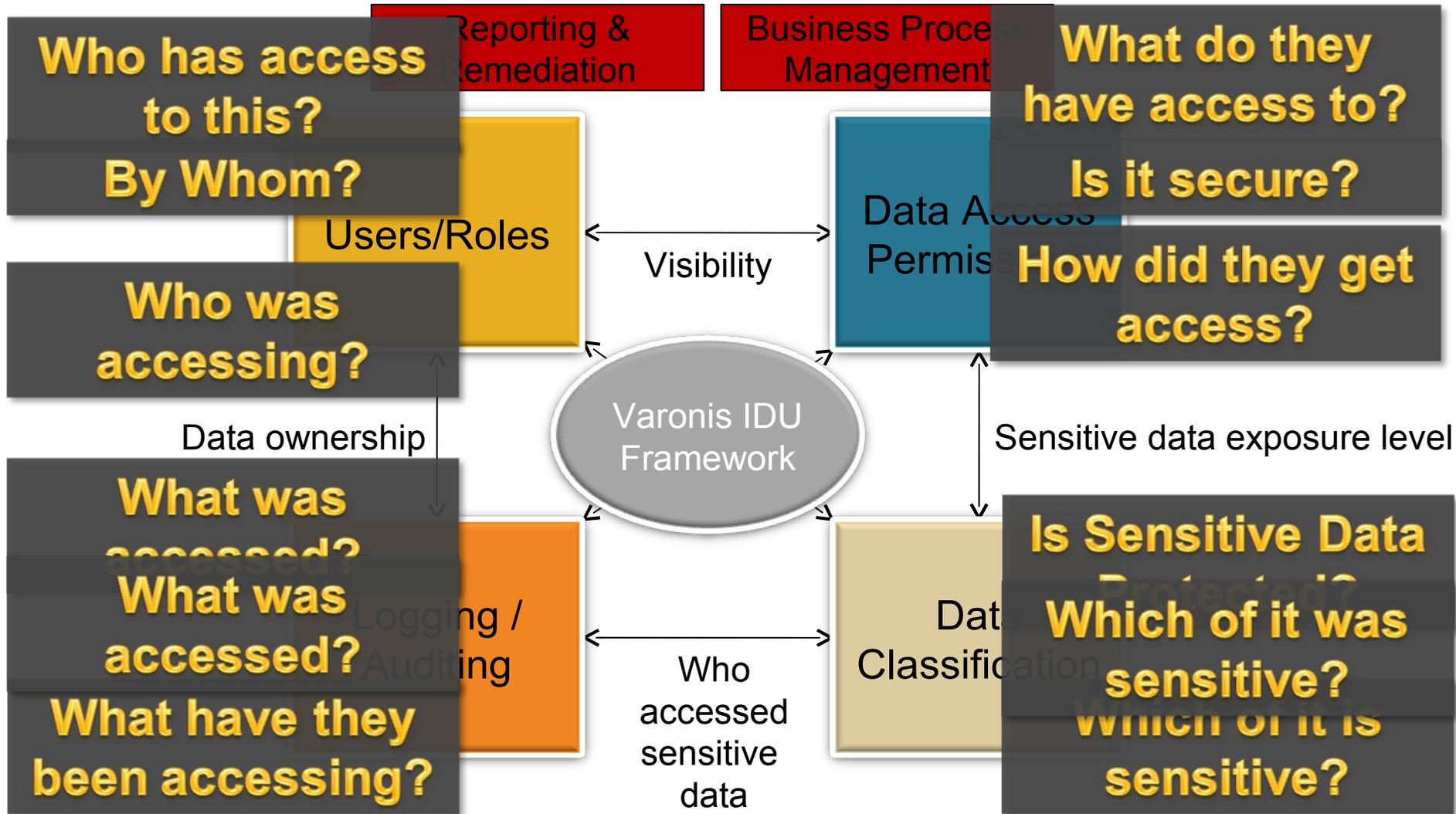
- High Risk Levels
 - ▶ **File System data is at great risk for loss, theft, and misuse**
 - ▶ **Access configuration changes are untested**
- File System Controls Gaps
 - ▶ **Many access controls are “loose,” even broken**
 - ▶ **No audit trail exists**
 - ▶ **>50% of data has no known business owner**
- Regulatory Requirements
 - ▶ **HIPAA**
 - ▶ **CMS**
 - ▶ **Sarbanes Oxley**

Varonis Solution

- Technological Breakthrough
 - ▶ **Automatically Identify and Remediate Access Control Gaps**
 - ▶ **Provide a Usable Audit Trail of Data Usage**
 - ▶ **Identify Data Owners, Inactive Data**
 - ▶ **Automate and Enforce Access Control Processes**
- Efficient, Effective Risk Reduction
- IT Data Protection Jumpstart
- Proven Operational Execution
 - ▶ **>600 customers**
 - ▶ **All Verticals**



A Complete Value Chain for Unstructured Data Protection



Common Use Cases for Varonis

- Access Control Cleanup – Identify & Remediate:
 - ▶ **“Global” Groups** -(everyone, authenticated users, etc)
 - ▶ **Redundant, Excessive Group Memberships**
 - ▶ **Orphaned SID’s, Individual User SIDS on ACL’s**
- Find Lost & Deleted Files
- Identify Anomalous Behavior
- Track Permissions & Group Changes
- Ongoing Entitlement Reviews
- Automate Access Authorization & Revocation
- Identify Inappropriate File Activity (mp3’s, etc.)
- Enhance Other Data Protection Projects

Common Use Cases for Varonis (cont'd)

- Efficient audit compliance - provide evidence of:
 - ▶ **Effective permissions (preventive controls)**
 - ▶ **Usable audit trail (detective controls)**
 - ▶ **Authorization processes**
 - ▶ **Compliance with authorization processes**
- SharePoint Migration
 - ▶ **Stale Data Identification**
 - ▶ **Data Owner Identification**

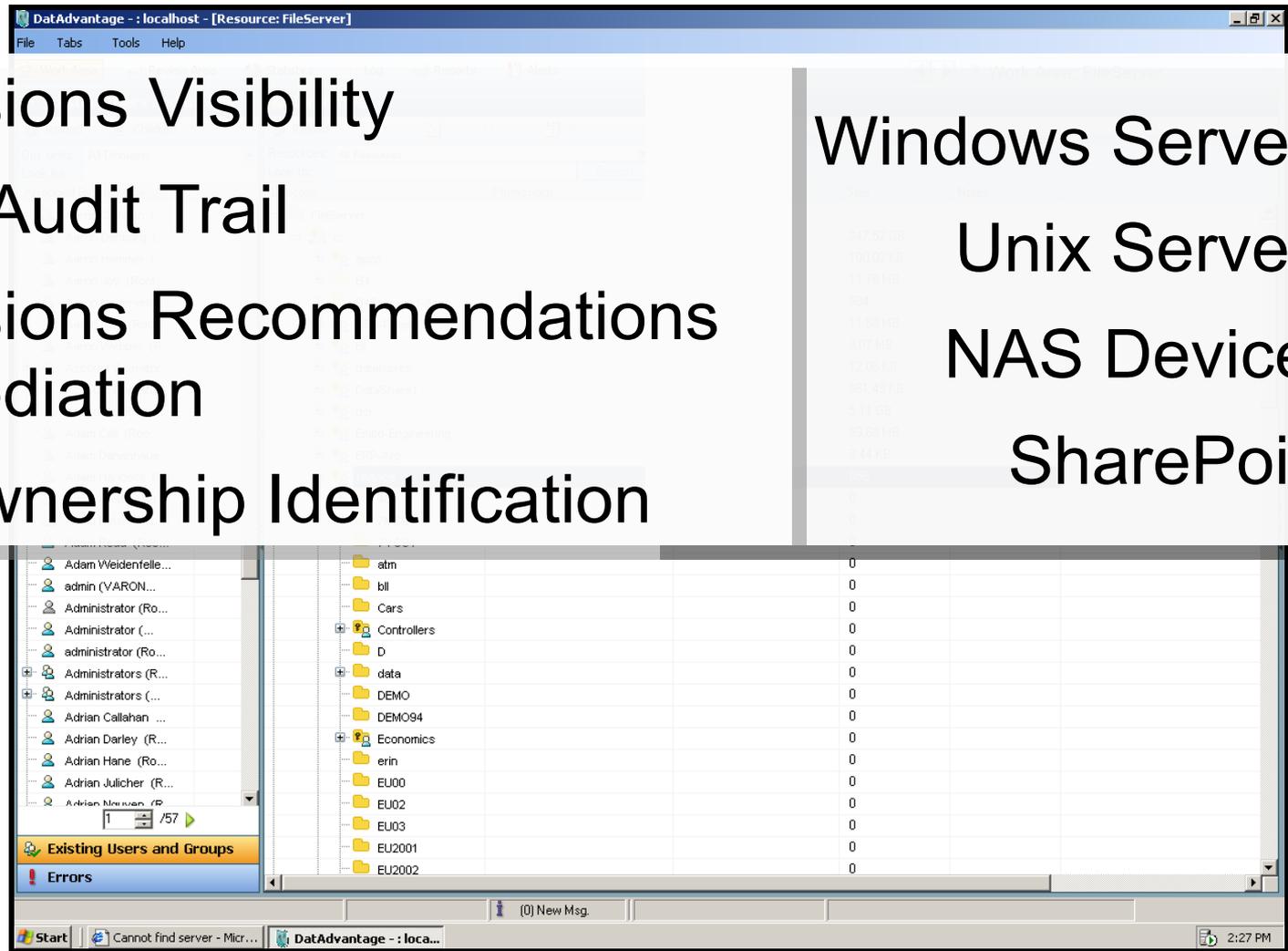
Use Case Efficiency Matrix

<u>Use Case</u>	<u>Manual Time Requirements</u>	<u>Varonis Time Requirements</u>	<u>Efficiency Gain</u>
Access Provisioning	20 min per folder	1 min per folder	20x
Creating a permissions report	30 min per folder	1 min per folder	30x
Data Owner Identification	4 hours per folder	20 minutes per folder	12x
Everyone Group Remediation	6 hours per folder	10 min per folder	36x
Entitlement Reviews	30 min per folder	2 min per folder	15x
Find lost files, Forensic Investigation	N/A	5-15 min per incident	N/A
Stale Data Identification	?	15 min – 1 time	N/A

DatAdvantage Functionality

- Permissions Visibility
- Usable Audit Trail
- Permissions Recommendations & Remediation
- Data Ownership Identification

Windows Servers
Unix Servers
NAS Devices
SharePoint



Permissions - Bi-Directional Visibility

Existing Users and Groups

Directories

Directory	Permissions	Explanations	Size
databases	M R W X L	(Inherited from "Everyone")	1
DataShare1			9 347.52 GB
dsr	F M R W X L	(Inherited from "Everyone")	5 100.02 KB
Embd-Engineering			9 11.78 MB
ERP-Arc			3 984
finance	M R W X L	(Inherited from "Group:Finance")	8 11.88 MB
404			0 3.07 MB
7MS94			0 12.06 KB
7Y094			0 961.49 KB
tm			0 5.11 GB
bill			0 93.68 MB
Cars			0 3.44 KB
Controllers			0 856
n			0 0
data			0 0
MEMO			0 0
MEM094			0 0
Economics			0 0
erin			0 0
EU00			0 0
EU02			0 0
EU03			0 0
EU200			0 0

Users/Groups...

to Users/Groups

to Data

Data...

SharePoint Visibility

Edit Permission Levels

Effective Permission Levels

Name	Description
Limited Access	
Contribute	
Aggregated Permission Level	

List Permissions

- Manage Lists
- Override Check Out
- Add Items
- Edit Items
- Delete Items
- View Items
- Approve Items
- Open Items
- View Versions
- Delete Versions
- Create Alerts
- View Application Pages

Site Permissions

- Manage Permissions
- View Usage Data
- Create Subsites
- Manage Web Site

Directories

Reload | List | Pruned Tree | Arrow Tree

sources: corpfs02, centos5, http://sharepoint

Effective Permissions

Inherited from "Everyone(Anonymous)"

Full Control [Site defines permission levels] Inherited from "Authenticated Users(Anonymous)"

Jump To... | Edit Permissions... | **Edit Permission Levels...** | Remove Protection from Site... | Manage Ownership... | Stop Monitoring... | Follow Up | Clear All Flags | Open...

Permission Levels

Unix Visibility

The image shows two overlapping windows from a Linux system administration interface. The background window is titled "Existing Users and Groups" and "Directories". In the "Existing Users and Groups" window, the "Users" tab is active, and the user "finance (centos5)" is highlighted with a red rectangle. The "Directories" window shows a tree view of the file system, with the "finance" directory under the "share" directory selected. A semi-transparent grey box with the text "POSIX ACL's" is overlaid on the "Existing Users and Groups" window.

The foreground window is titled "finance Properties" and shows the "Permissions" tab. It displays the "Access Control List (1)" for the "finance" directory. The list is divided into "Trivial access control entries" and "Extended users and groups access control entries".

Object Name	R	W	X	Effective
Mask	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
User (varonisuser(centos5))	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Group (varonis(centos5))	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Other(Abstract)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Object Name	R	W	X	Effective
finance(centos5)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Buttons at the bottom of the "finance Properties" window include "Add...", "Remove", "Remove All", "OK", "Cancel", and "Apply".

POSIX ACL's

Audit Trail

The screenshot displays the Varonis Audit Trail interface. On the left, a directory tree shows the 'finance' folder selected. The main window shows a search query: 'Date between 12/1/2008 12:00:00 AM and 1/14/2009 11:59:59 PM AND Show data from Equals 'File-system events' AND Directory Starts with 'c:\finance''. The results are grouped by 'Operation Type: Object removed (17)'. A table lists the removed objects with columns for Time, File Server / Do..., Operation On, Operation Ty..., Change Description, Operation By, File Type, and Event Count.

Time	File Server / Do...	Operation On	Operation Ty...	Change Description	Operation By	File Type	Event Count
12/4/2008 12:38:...	FileServer	c:\finance\Econo...	Object removed	Object removed	Root-Domain\Ann Schoenberger	xls	5
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	doc	6
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	doc	5
12/1/2008 4:44:0...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	DOC	5
12/1/2008 4:44:0...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	DOC	50
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	doc	60
12/2/2008 9:53:0...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Margaret Coakley	DOC	8
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	doc	50
12/2/2008 11:09:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Margaret Coakley	DOC	3
12/2/2008 11:08:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Anne Thornton	DOC	1
12/2/2008 11:52:...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Anne Thornton	DOC	1
12/1/2008 11:49...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Anne Thornton	doc	1
12/2/2008 10:53...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Anne Thornton	doc	1
12/1/2008 12:10...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Anne Thornton	DOC	2
12/2/2008 10:46...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Ann Schoenberger	xls	3
12/2/2008 4:50:0...	FileServer	c:\finance\Control...	Object removed	Object removed	Root-Domain\Erin Manning	doc	1
12/3/2008 4:15:0...	FileServer	c:\finance\Econo...	Object removed	Object removed	Root-Domain\Eric Adler	xls	1

Search, Sort, and Group

Recommendations

The screenshot displays two overlapping windows from a software application. The left window, titled 'Marc Farhat', shows a tree view of resources with a red border. A semi-transparent grey box with the text 'What if?' is overlaid on it. The right window, titled 'ERP-Arc', shows a file tree with a red border. A semi-transparent grey box with the text 'Permissions?' is overlaid on it. The background window shows a navigation menu with options like 'Reload', 'List', 'Pruned Tree', 'Arrow Tree', and 'Filters'. The right window also has a 'Permissions' table with columns M, R, W, X, L and rows for 'Christy' and another user.

What if?

Permissions?

Permissions Clean-up

The screenshot displays a file server management interface with three main panels:

- Errors Panel (Left):** Lists users with their counts. A red box highlights the list.

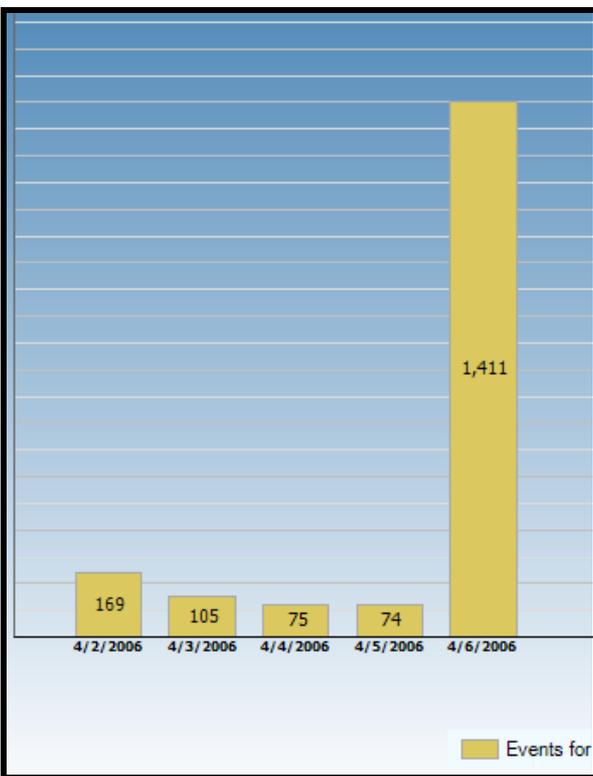
User	Count
Alice Tanner	29
Allen Weinheimer	16
Darren Parker	7
Fred Phelps	13
Melissa Cooley	13
Melissa Donovan	15
- Directories Panel (Middle):** Shows a tree view of directories. A red box highlights the 'legal' directory under 'HumanResources'.
 - ERP-Arc
 - finance
 - Fondue
 - groups
 - HR
 - HR-Private
 - HumanResources
 - legal
 - Market
 - Market_Budget
 - Market-Cost
- Recommended Users and Groups Panel (Right):** Shows a table of permissions. A red box highlights the 'Everyone (Abstract)' group with permissions F, M, R, W, X, L.

Group	Permissions
Everyone (Abstract)	F M R W X L

View Outcome

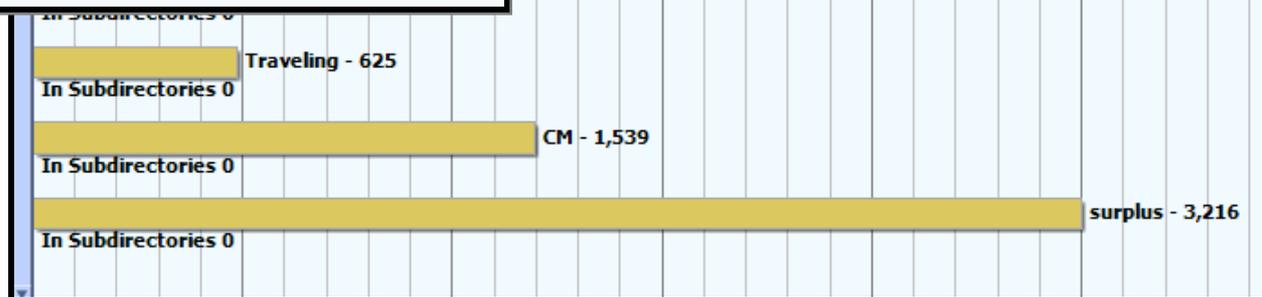
Simulate Changes

Activity Analysis



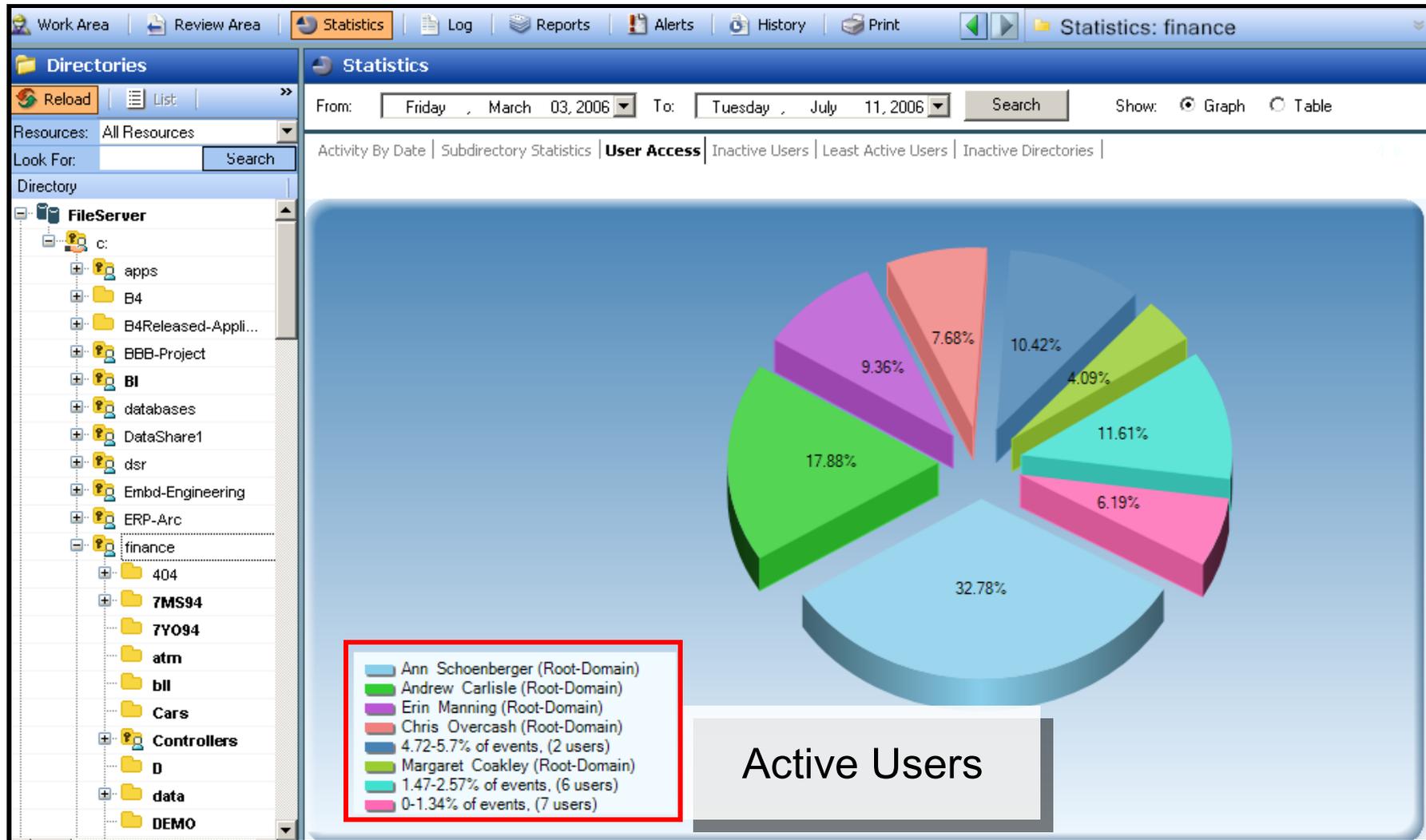
[Root-Domain] (729)
ey [Root-Domain] (786)
kley [Root-Domain] (801)

- Most/Least Active Users
- Most/Least Active Directories
- Anomalous Behavior



2)
Event Count

Data Ownership Identification



Data Ownership Assignment

Ownership Assignment

Are you sure you want to set Person Ann Schoenberger as owner for Directory finance?

Yes No

Statistics: finance[FileServer]

From: Monday, December 01, 2008 To: Wednesday, January 14, 2009

Activity By Date | Subdirectory Statistics | **User Access** | Inactive Users | Least Active Users | Inactive Directories | Activity on managed folders

Ownership Assignment Legend:

- Ann Schoenberger (Root-Domain) 32.78%
- Andrew Carlisle (Root-Domain) 10.42%
- Erin Manning (Root-Domain) 9.36%
- Chris Overcash (Root-Domain) 7.68%
- 4.72-5.7% of events, 2 users
- Margaret Coakley (Root-Domain) 6.19%
- 1.47-2.57% of events, 6 users
- 0-1.34% of events, 7 users

Right-click
Set Ownership

Jump To...
Manage Ownership...
Set Ownership...

Represents the distribution of events per user on the specified directory

Q & A

Hit "Esc" to return to Main Menu