VNUG 2014
Access Rights on NonStop Guardian and OSS

Computer Security Products Inc.

About CSP

- Based in Toronto, Canada with Partners, Agents and Distributors worldwide
- NonStop® Alliance One Partner since 1987.
- Develop, Support and Distribute Security, Compliance and Audit Solutions for the HP NonStop® Market.
- Large number of Customers and over 1000+ licenses World Wide
- Customers include:
  - Largest Banks
  - Major Stock Exchanges
  - Defense and Healthcare organizations
  - Telecommunications
  - Manufacturers

Integrity Ready Partner hp invent

Business Partner hp invent

CSP

Computer Security Products Inc.

Access Rights Management (ARM)

- Access Rights are the part of Access Governance concerned with discretionary access controls: file permissions and ACLs.
- Distinct from:
  - Identity management and authentication
  - Role Based Access Controls
  - User session and command control

ARM – why does it matter?

- Effective ARM is the cornerstone of system security
- Compliance with enterprise policy
- Required for PCI, SOX, HIPAA compliance

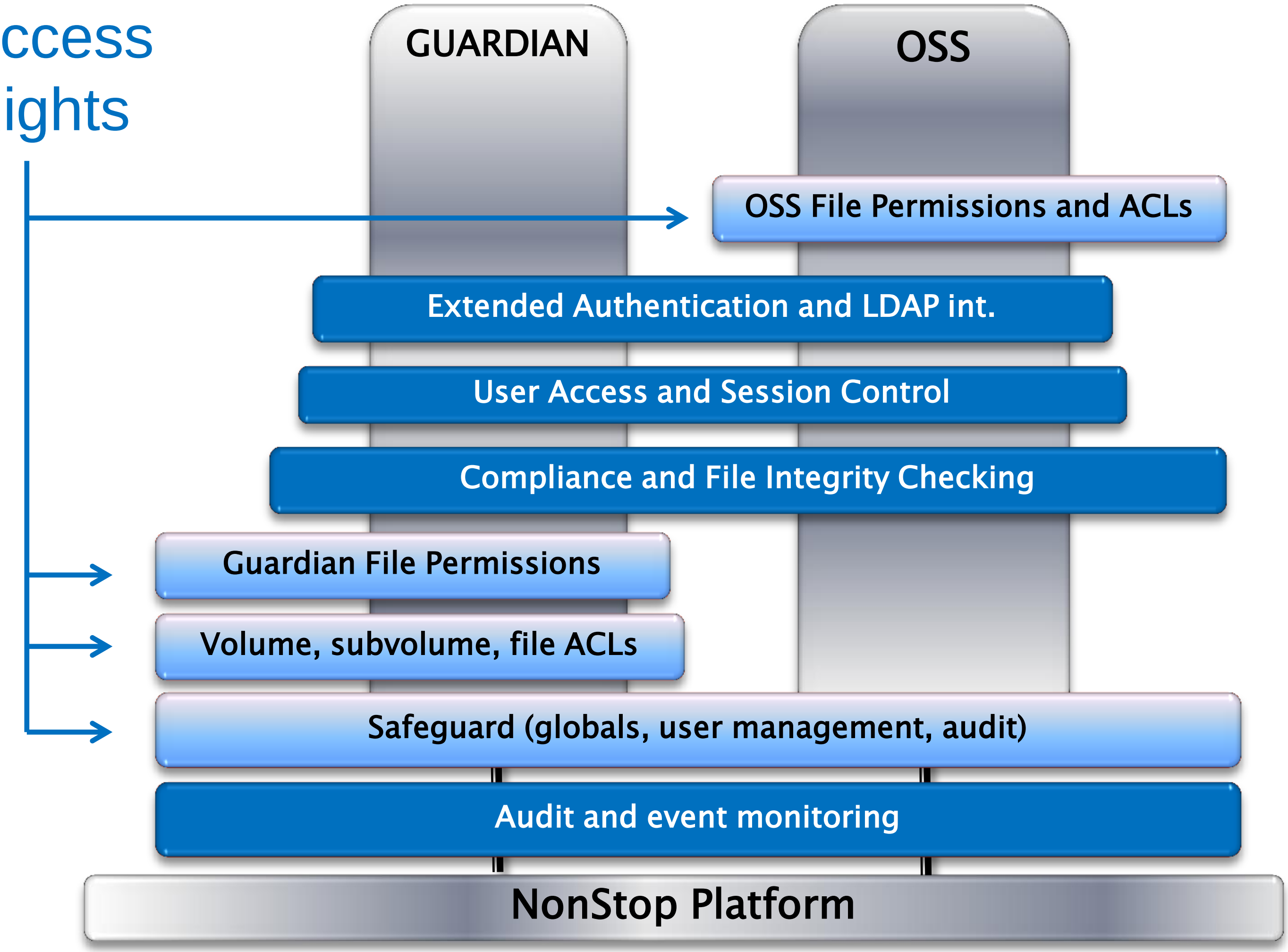
Access Rights – basic principles

- Only grant least privilege
- Change system defaults!
- Know what you have.
- Be able to prove it to auditors.

Access Rights for Nonstop

- Implemented with:
  - Guardian file permissions
  - Safeguard ACLs and object security
  - Basic OSS file permissions
  - OSS Extended ACLs

Access Rights


GUARDIAN

OSS

OSS File Permissions and ACLs

Extended Authentication and LDAP int.

User Access and Session Control

Compliance and File Integrity Checking

Guardian File Permissions

Volume, subvolume, file ACLs

Safeguard (globals, user management, audit)

Audit and event monitoring

NonStop Platform

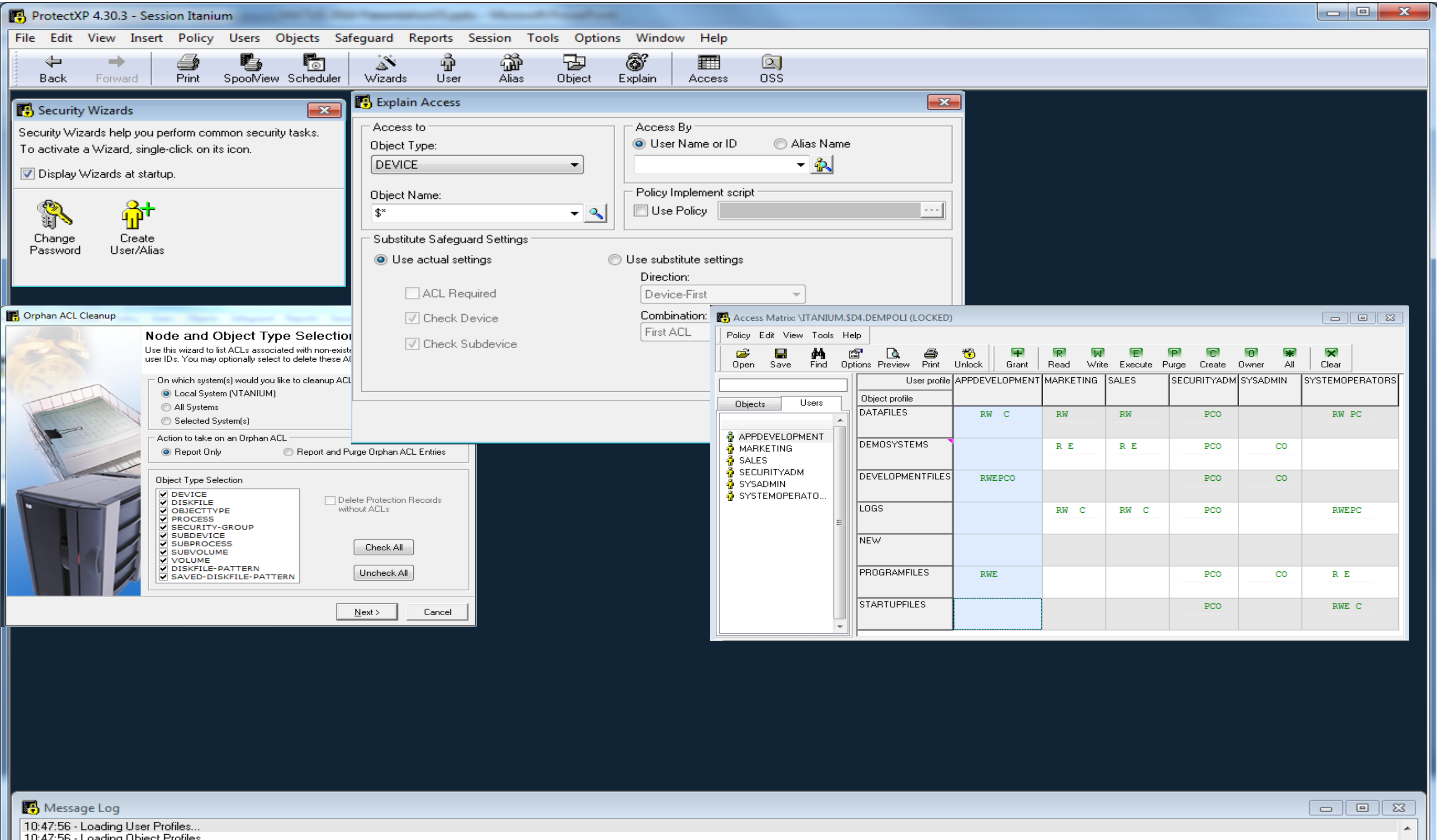
Access Rights for Guardian files

- Two challenges:
  - How do you review, analyze and manage your basic Guardian file permissions?
  - How do you manage your Safeguard volume, subvolume and diskfile ACLs?

CSP Solutions for Guardian ARM

- ProtectXP:
  - Interactive permissions analysis
  - Standard and custom reports
  - Tools for Orphan file cleanup, ownership issues etc.
  - Access Rights policy for Safeguard rules using access matrix tool.
- CRM/FIC:
  - Historical database of all report results
  - Matches rules against PCI etc.
  - Integrity checks for file content and access rights changes

ProtectXP



Security Wizards

Security Wizards help you perform common security tasks.
To activate a Wizard, single-click on its icon.

☑ Display Wizards at startup.

Explain Access

Access to

Object Type: DEVICE

Object Name: $*

Access By

● User Name or ID ○ Alias Name

Policy Implement script

□ Use Policy

Substitute Safeguard Settings

● Use actual settings ○ Use substitute settings

□ ACL Required

☑ Check Device

☑ Check Subdevice

Direction: Device-First

Combination: First ACL

Orphan ACL Cleanup

Node and Object Type Selection

Use this wizard to list ACLs associated with non-existe
user IDs. You may optionally select to delete these AC

On which system(s) would you like to cleanup ACL

● Local System (\ITANIUM)
○ All Systems
○ Selected System(s)

Action to take on an Orphan ACL

● Report Only ○ Report and Purge Orphan ACL Entries

Object Type Selection

☑ DEVICE
☑ DISKFILE
☑ OBJECTTYPE
☑ PROCESS
☑ SECURITY-GROUP
☑ SUBDEVICE
☑ SUBPROCESS
☑ SUBVOLUME
☑ VOLUME
☑ DISKFILE-PATTERN
☑ SAVED-DISKFILE-PATTERN

□ Delete Protection Records without ACLs

Check All Uncheck All

Next > Cancel

Access Matrix: \ITANIUM.$D4.DEMPOLI (LOCKED)

APPDEVELOPMENT
MARKETING
SALES
SECURITYADM
SYSADMIN
SYSTEMOPERATO...

User profile / Object profile	APPDEVELOPMENT	MARKETING	SALES	SECURITYADM	SYSADMIN	SYSTEMOPERATORS
DATAFILES	RW C	RW	RW	PCO		RW PC
DEMOSYSTEMS		R E	R E	PCO	CO	
DEVELOPMENTFILES	RWEPCO			PCO	CO	
LOGS		RW C	RW C	PCO		RWEPC
NEW						
PROGRAMFILES	RWE			PCO	CO	R E
STARTUPFILES				PCO		RWE C

Message Log

```
10:47:56 - Loading User Profiles...
10:47:56 - Loading Object Profiles...
```

Access Rights for OSS

- OSS uses the Unix format (owner/group/world)
- Common issues (just like Guardian):
  - Orphan Files
  - Excessive Privileges for applications
  - Files made accessible to all users for “emergency” purposes
- Challenges in reviewing, setting and monitoring permissions using command line utilities.
- How are you checking yours?

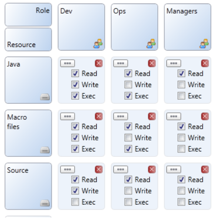
OSS Extended ACLs

- Improve granularity and control.
- Allow a specific permission to be added for a specific user or group (e.g. fred + write)
- Awkward to set and to read.
- Just like Safeguard ACLs, these can get messy very quickly…

Introducing Protect-UX

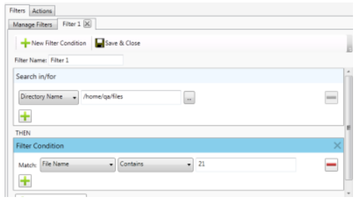
Protect-UX clients can manage 100’s of systems.

Policy controls multiple systems.



Role / Resource	Dev	Ops	Managers
Java	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Macro files	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Source	☑ Read ☑ Write ☐ Exec	☑ Read ☐ Write ☐ Exec	☑ Read ☐ Write ☐ Exec

Fileset Macros discover & correct common issues.



Filter Name: Filter 1

Search in/for

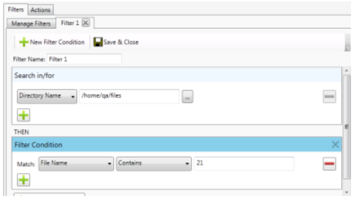
Directory Name /home/qa/files

THEN

Filter Condition

Match: File Name Contains 21

Permissions templates enforce standards



Filter Name: Filter 1

Search in/for

Directory Name /home/qa/files

THEN

Filter Condition

Match: File Name Contains 21

HP NonStop OSS systems

Platforms also include:

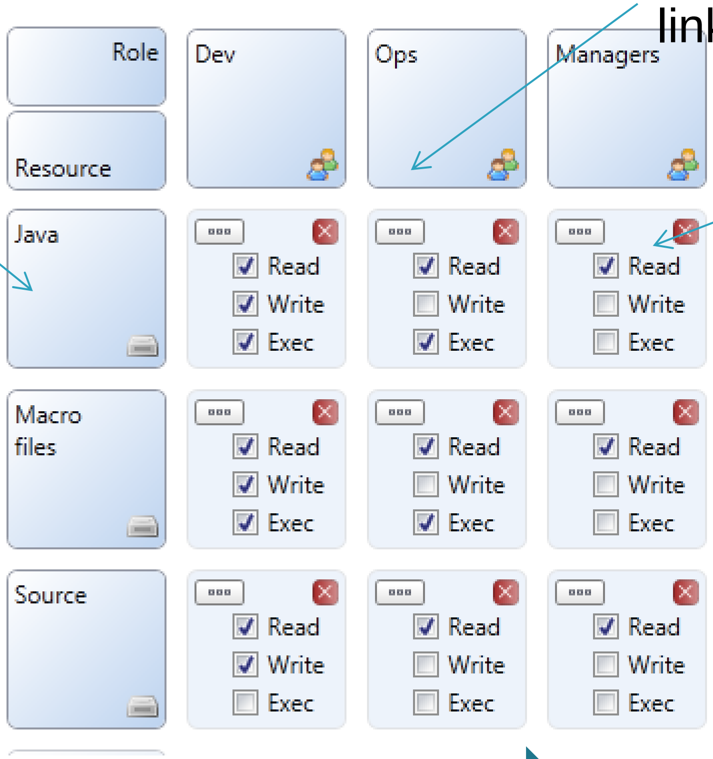
- Red Hat
- SuSE
- Ubuntu
- Solaris

Protect-UX Policy Access Matrix

1. Resources are linked to files

2. Roles are linked to users

3. Set ACLs in the cells

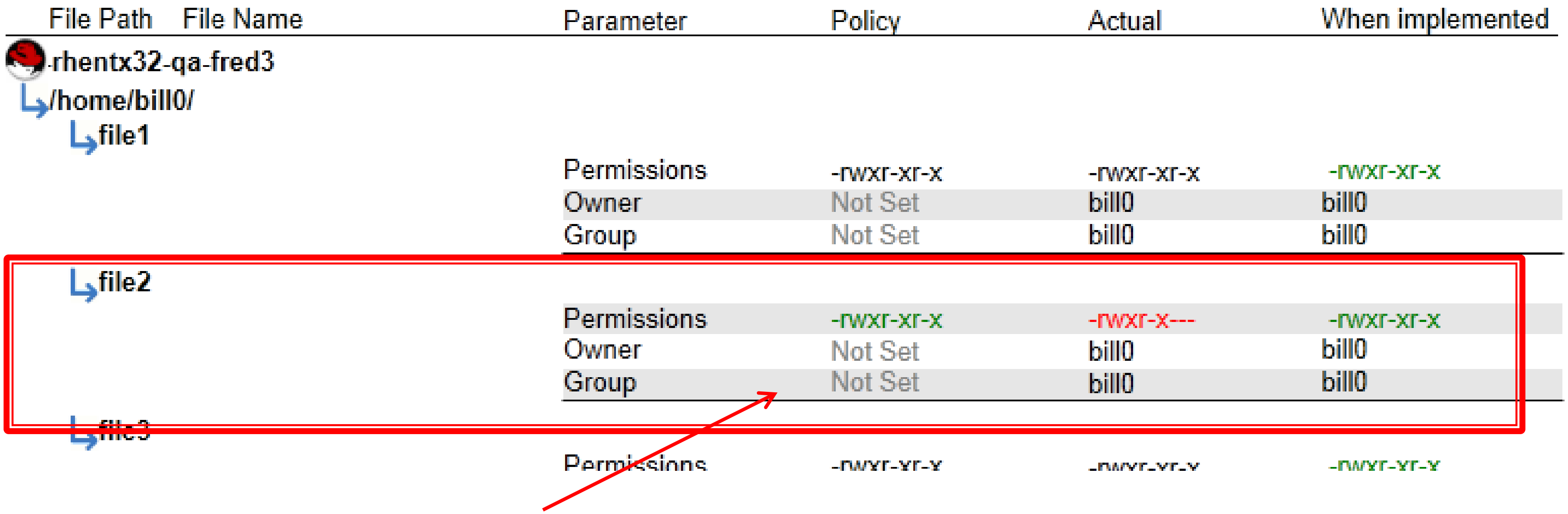


Role Resource	Dev	Ops	Managers
Java	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Macro files	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Source	☑ Read ☑ Write ☐ Exec	☑ Read ☐ Write ☐ Exec	☑ Read ☐ Write ☐ Exec

4. Implementation

Resolves access matrix and applies permissions to files.

Protect-UX Validation Reports

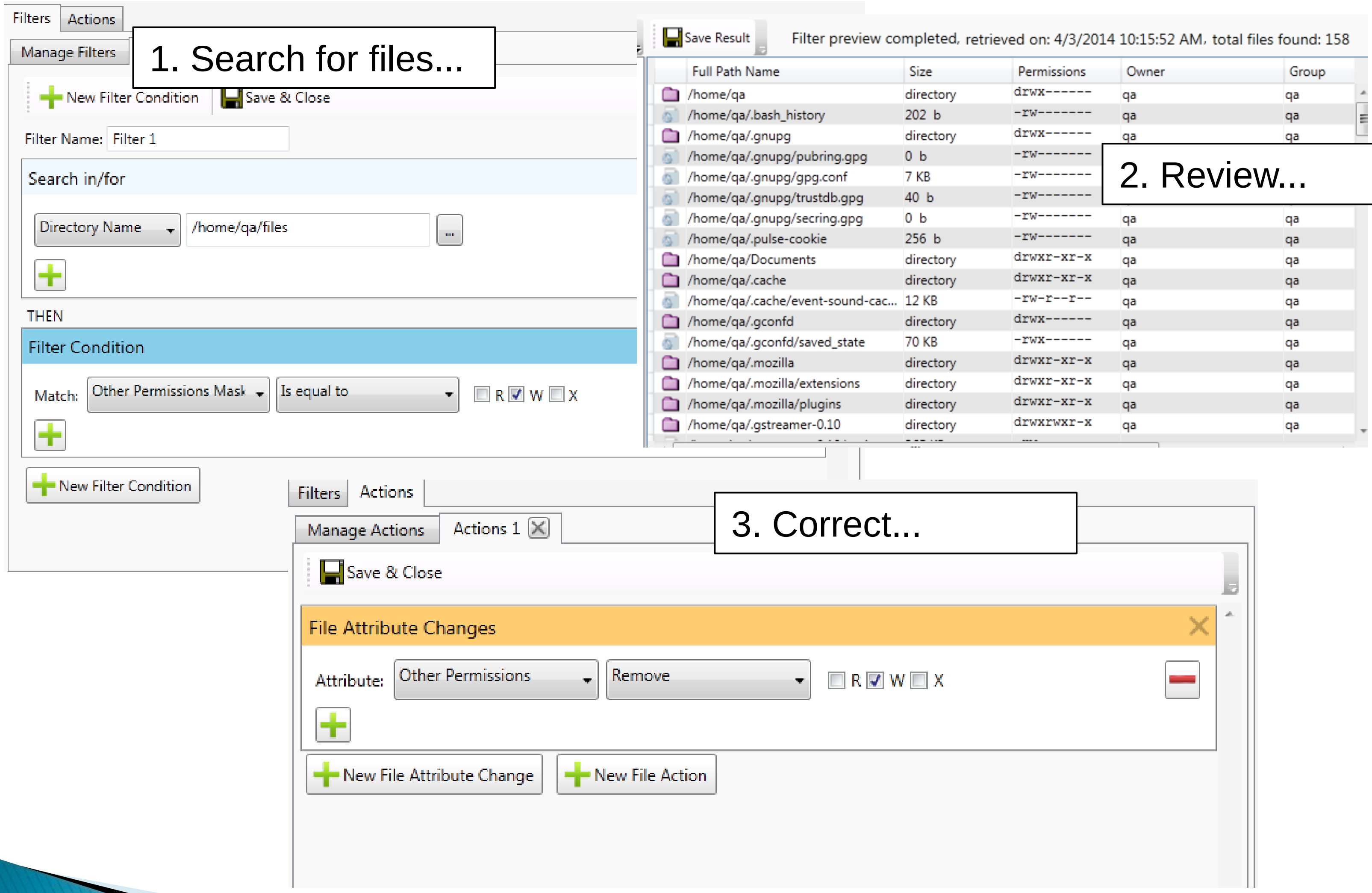


File Path	File Name	Parameter	Policy	Actual	When implemented
rhentx32-qa-fred3					
/home/bill0/					
	file1				
		Permissions	-rwxr-xr-x	-rwxr-xr-x	-rwxr-xr-x
		Owner	Not Set	bill0	bill0
		Group	Not Set	bill0	bill0
	file2				
		Permissions	-rwxr-xr-x	-rwxr-x---	-rwxr-xr-x
		Owner	Not Set	bill0	bill0
		Group	Not Set	bill0	bill0
	file3				
		Permissions	-rwxr-xr-x	-rwxr-xr-x	-rwxr-xr-x

Protect-UX compares your policy with your actual settings and flags differences.

Computer Security Products Inc.

Protect-UX Fileset Macro



1. Search for files...

Filter Name: Filter 1

Search in/for

Directory Name: /home/qa/files

THEN

Filter Condition

Match: Other Permissions Mask | Is equal to | □ R ☑ W □ X

2. Review...

Filter preview completed, retrieved on: 4/3/2014 10:15:52 AM, total files found: 158

Full Path Name	Size	Permissions	Owner	Group
/home/qa	directory	drwx------	qa	qa
/home/qa/.bash_history	202 b	-rw-------	qa	qa
/home/qa/.gnupg	directory	drwx------	qa	qa
/home/qa/.gnupg/pubring.gpg	0 b	-rw-------		
/home/qa/.gnupg/gpg.conf	7 KB	-rw-------		
/home/qa/.gnupg/trustdb.gpg	40 b	-rw-------		
/home/qa/.gnupg/secring.gpg	0 b	-rw-------	qa	qa
/home/qa/.pulse-cookie	256 b	-rw-------	qa	qa
/home/qa/Documents	directory	drwxr-xr-x	qa	qa
/home/qa/.cache	directory	drwxr-xr-x	qa	qa
/home/qa/.cache/event-sound-cac...	12 KB	-rw-r--r--	qa	qa
/home/qa/.gconfd	directory	drwx------	qa	qa
/home/qa/.gconfd/saved_state	70 KB	-rwx------	qa	qa
/home/qa/.mozilla	directory	drwxr-xr-x	qa	qa
/home/qa/.mozilla/extensions	directory	drwxr-xr-x	qa	qa
/home/qa/.mozilla/plugins	directory	drwxr-xr-x	qa	qa
/home/qa/.gstreamer-0.10	directory	drwxrwxr-x	qa	qa

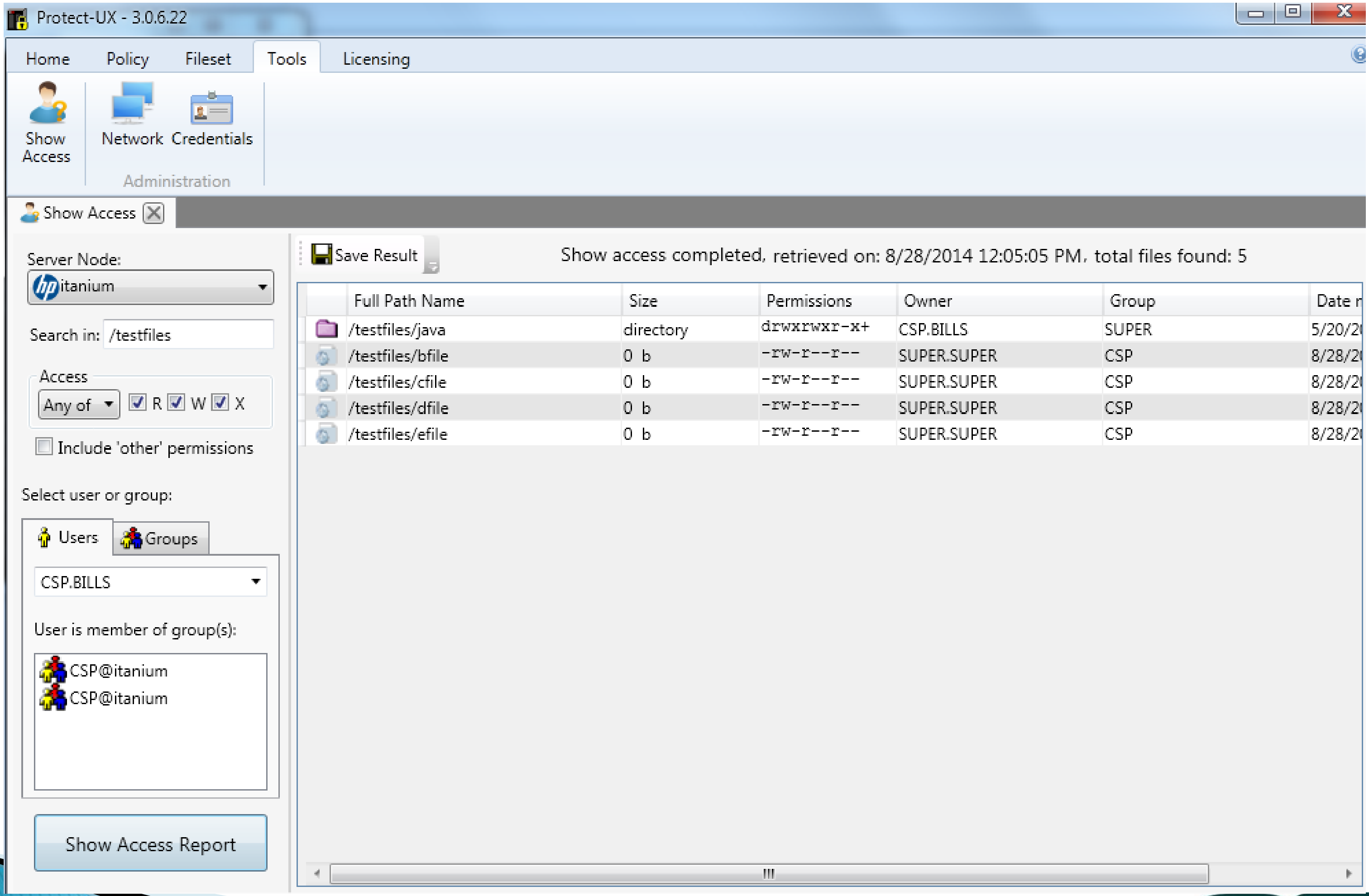
3. Correct...

File Attribute Changes

Attribute: Other Permissions | Remove | □ R ☑ W □ X

Computer Security Products Inc.

Interactive Permissions Analysis



Server Node: itanium

Search in: /testfiles

Access

Any of ☑ R ☑ W ☑ X

□ Include 'other' permissions

Select user or group:

CSP.BILLS

User is member of group(s):

CSP@itanium
CSP@itanium

Show access completed, retrieved on: 8/28/2014 12:05:05 PM, total files found: 5

Full Path Name	Size	Permissions	Owner	Group	Date r
/testfiles/java	directory	drwxrwxr-x+	CSP.BILLS	SUPER	5/20/2
/testfiles/bfile	0 b	-rw-r--r--	SUPER.SUPER	CSP	8/28/2
/testfiles/cfile	0 b	-rw-r--r--	SUPER.SUPER	CSP	8/28/2
/testfiles/dfile	0 b	-rw-r--r--	SUPER.SUPER	CSP	8/28/2
/testfiles/efile	0 b	-rw-r--r--	SUPER.SUPER	CSP	8/28/2

Computer Security Products Inc.

Permissions templates

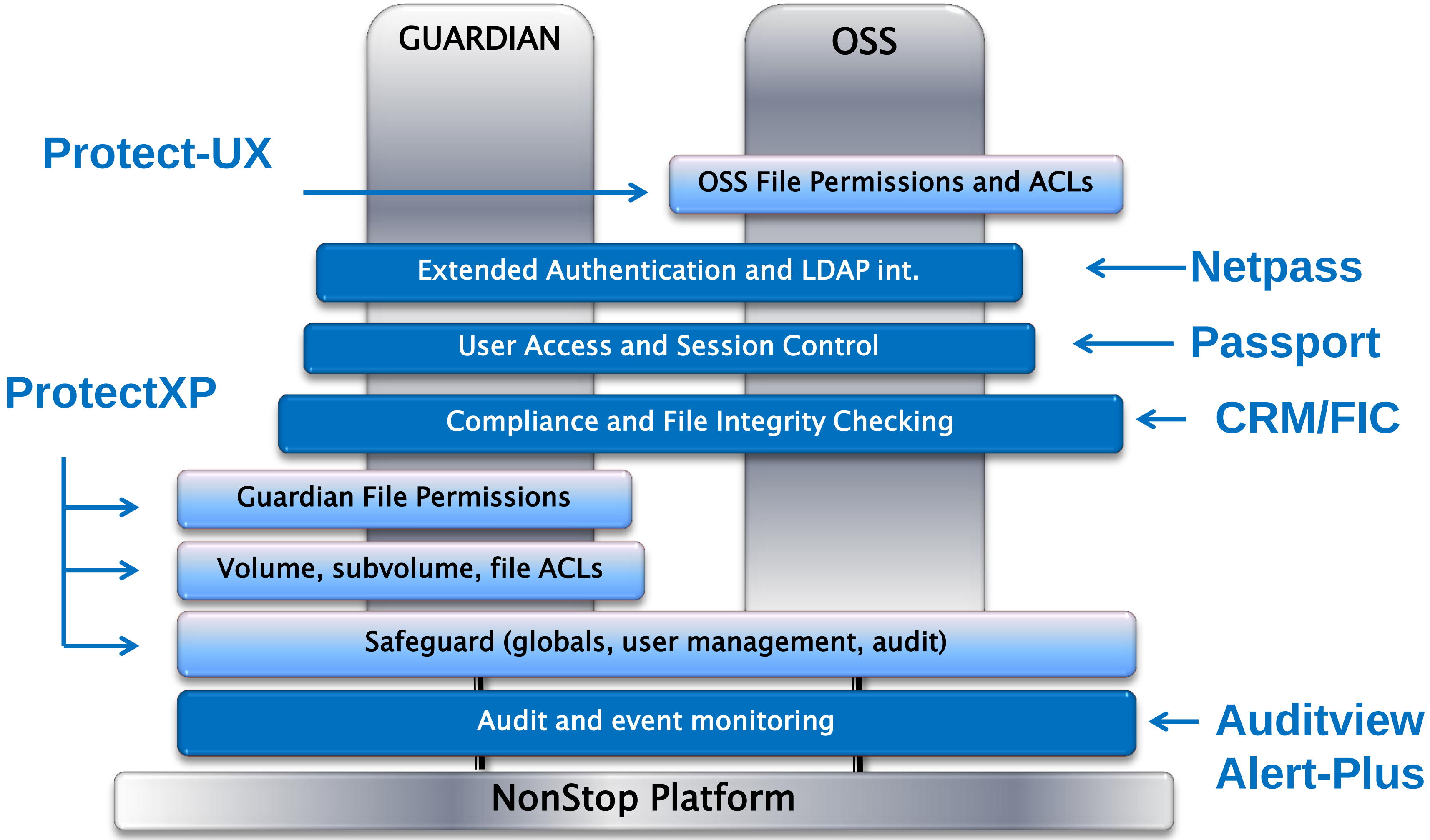
- Apply standard permissions to your system.
- Compare your current settings against standard permissions.
- Templates bring your systems in line with standard industry practice, and support compliance.

Protect-UX

- Cost-effective solution to managing access rights on HP OSS.
  - Policy tools support compliance and security.
  - Fileset Macros provide visibility and simplify common tasks.
  - Permissions templates formalise and standardize your permissions settings.

CSP solutions include:

- Audit reporting – Auditview
- Alert-Plus – real-time event monitoring and merging
- CRM/FIC – compliance and integrity reporting
- Passport – user session and command control
- CSP solutions are tightly integrated to deliver comprehensive access governance, change control and compliance



GUARDIAN

OSS

Protect-UX

OSS File Permissions and ACLs

Extended Authentication and LDAP int.

Netpass

User Access and Session Control

Passport

ProtectXP

Compliance and File Integrity Checking

CRM/FIC

Guardian File Permissions

Volume, subvolume, file ACLs

Safeguard (globals, user management, audit)

Audit and event monitoring

Auditview
Alert-Plus

NonStop Platform

Thank you!