XYPRO Technology Corporation

Compliance, Auditing and Alerts
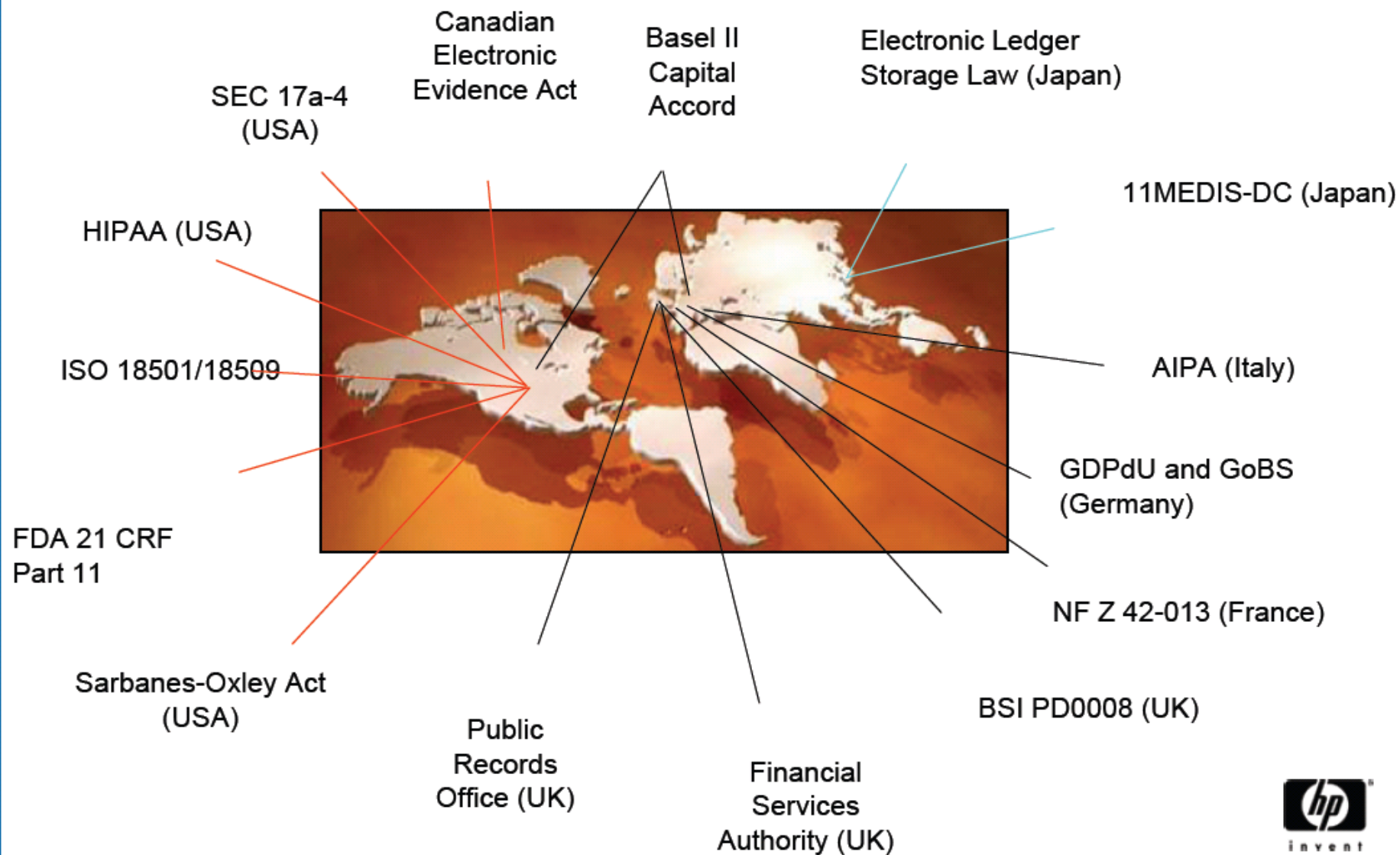
Sean Bicknell
XYPRO

Agenda

- **XYPRO Overview**
- **XYGATE Audit Pro**
  - **NonStop Audit to the Enterprise**
- **XYGATE Compliance Pro**
  - **So you think your compliant, prove it!**

ABOUT XYPRO

- **Proven Performers & Business Partners**
  - Founded in 1983
  - HP NonStop server security since 1990

- **Fast Response Team**
  - 24 x 7 Support service
  - Quality driven, growing company

- **HP / XYPRO Relationship**
  - Long-term relationship between XYPRO and HP (Tandem/Compaq)
  - HP helped publish XYPRO security handbooks
  - Used to secure HP internal systems (20+ nodes)

Regulatory compliance
The international minefield of digital information

SEC 17a-4 (USA)

Canadian Electronic Evidence Act

Basel II Capital Accord

Electronic Ledger Storage Law (Japan)

11MEDIS-DC (Japan)

HIPAA (USA)

ISO 18501/18509

AIPA (Italy)

FDA 21 CRF Part 11

GDPdU and GoBS (Germany)

NF Z 42-013 (France)

Sarbanes-Oxley Act (USA)

Public Records Office (UK)

Financial Services Authority (UK)

BSI PD0008 (UK)

https://www.xypro.com/

Google

Getting Started   Latest Headlines

xypro.com

Home | About | Jobs | Contact | Links   MAR 3, 2008

PRODUCTS   NEWS   SERVICES   USER GROUP   LOGIN   GO

welcome to xypro technology corporation

25 YEAR ANNIVERSARY XYPRO

Securing HP NonStop Server Security — A Practical Handbook

Securing HP NonStop Servers in an Open Systems World TCP/IP, OSS & SQL

The leader in HP NonStop™ server security and encryption solutions.

DOWNLOAD FREE

- ■ **Auditor's Checklist**
- ■ **PCI** Compliance Solutions Paper
- ■ **SOX** Compliance Solutions Paper
- ■ **HIPAA** Compliance Solutions Paper

⇒ XYPRO in the News

JAN 2008 - XYPRO Publishes "Auditor's Checklist" for HP NonStop Servers

NOV 2007 - XYGATE /MA adds support for BASE24 Audit

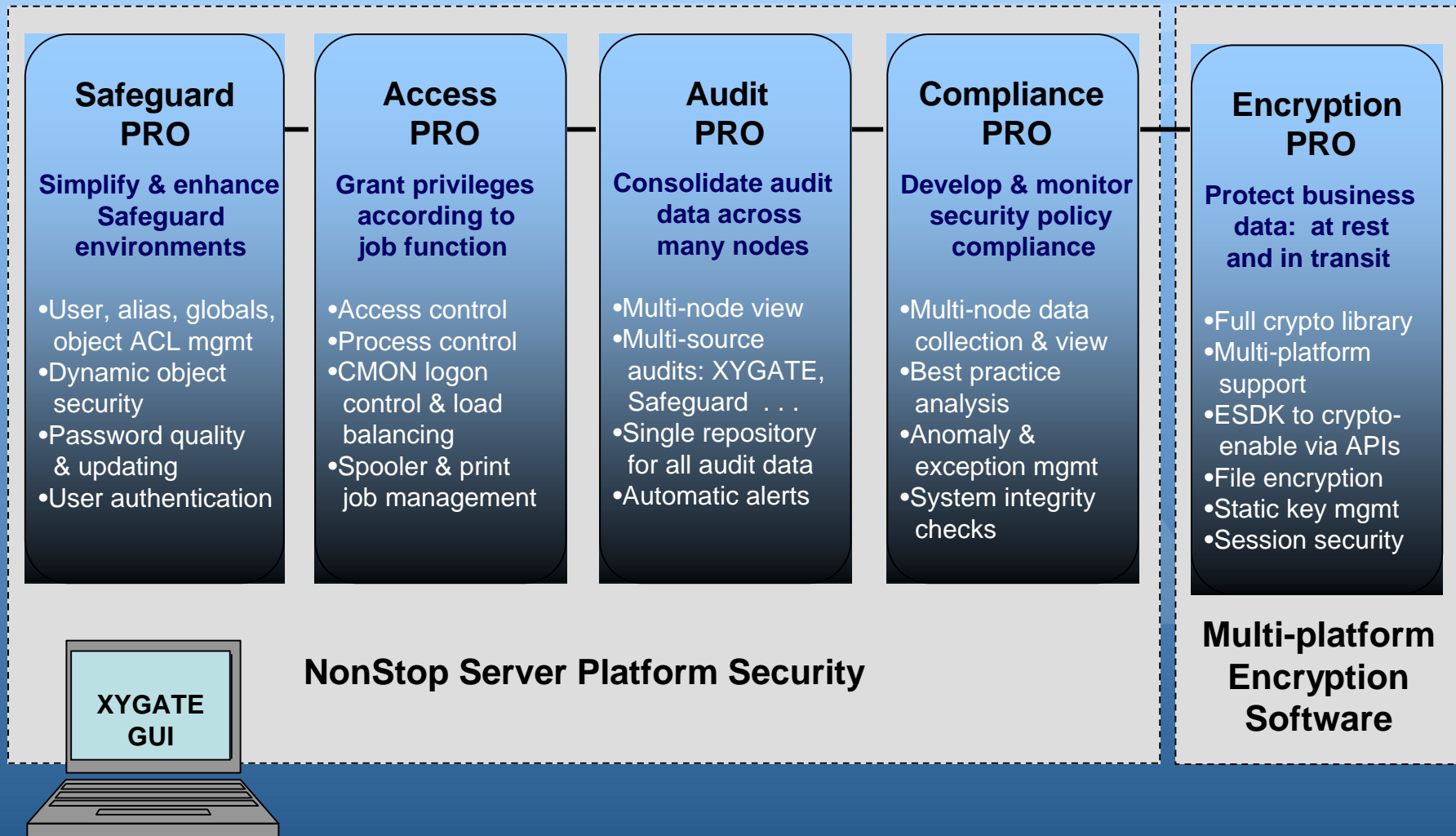OCT 2007 - XYPRO Supports Single Sign-On with LDAP

JUL 2007 - XYPRO "PCI" Solutions Paper for HP NonStop Servers

JUN 2007 - XYPRO Expanding to Meet Greater Demand for XYGATE Security Solutions
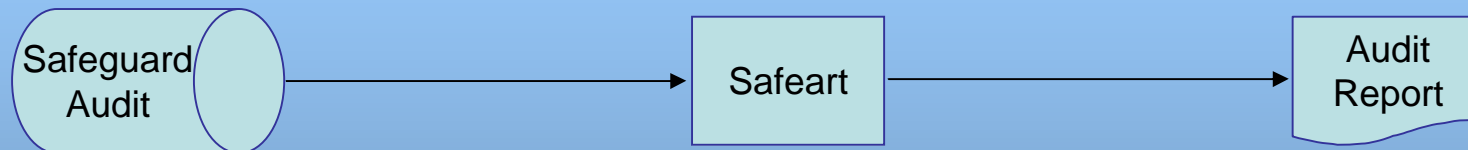
MAY 2007 - Get focused on your security by attending the HP Technology Forum and Expo 2007, June 18 – 21 in Las Vegas.

JAN 2007 - XYPRO writes the book on Security. Again.

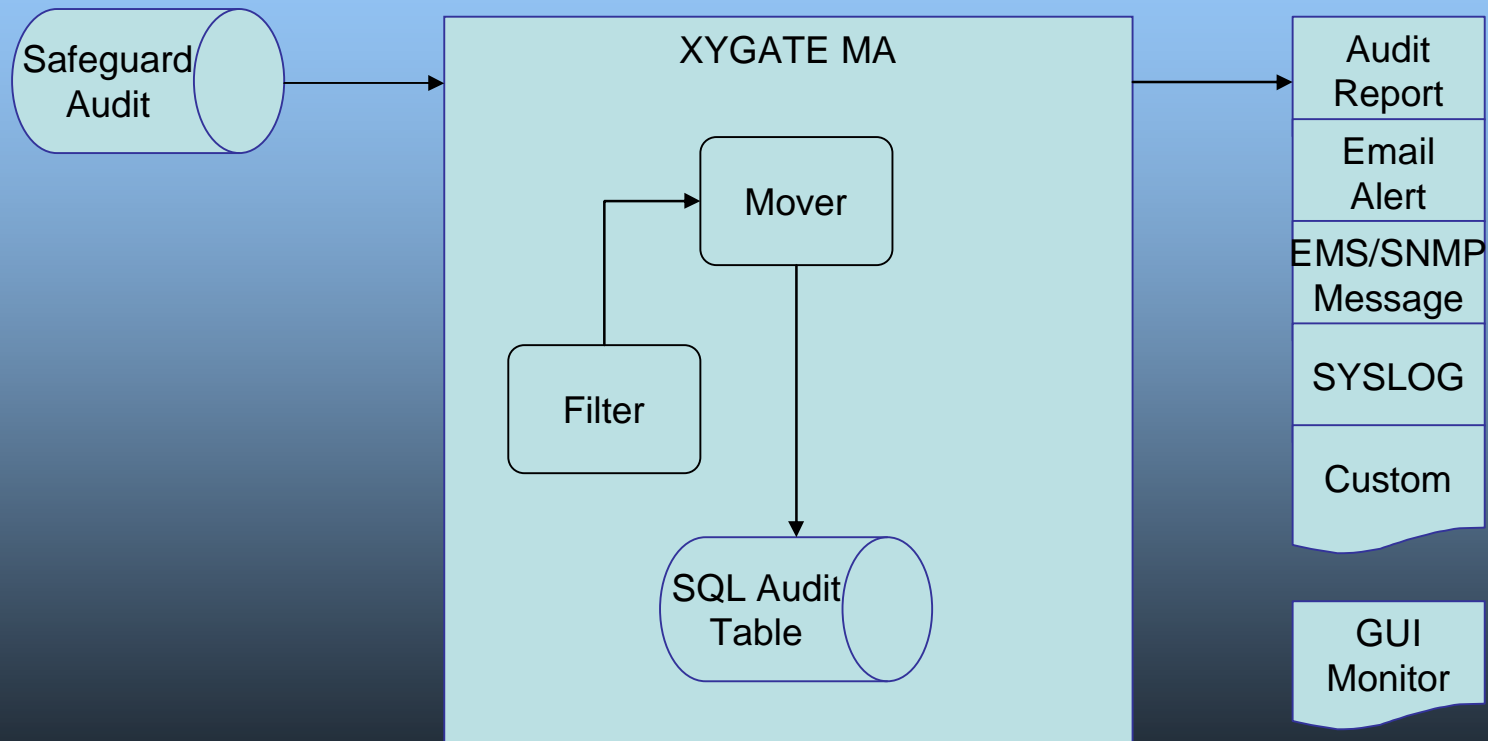Done   www.xypro.com
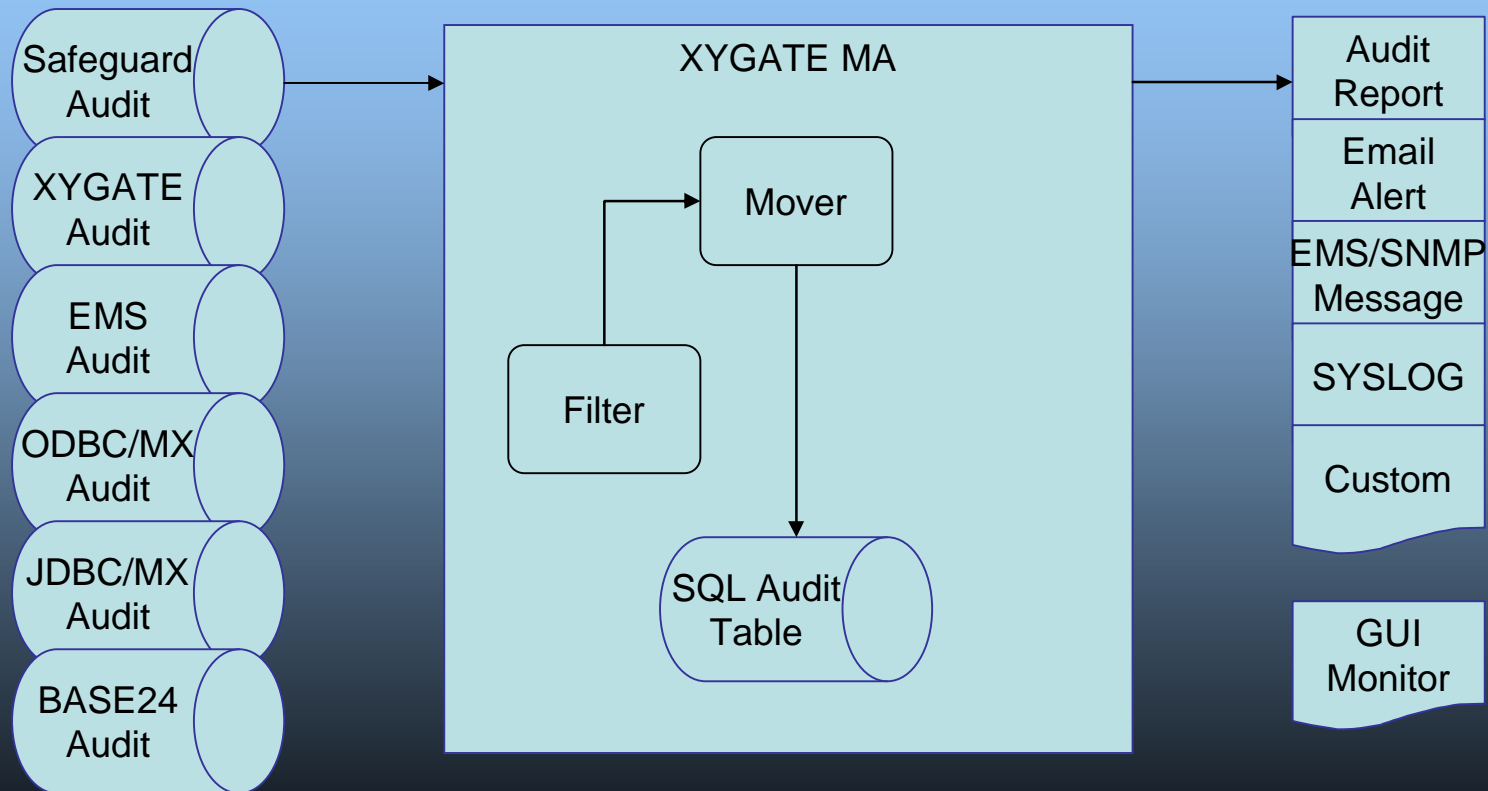
XYGATE Security Suite

Safeguard PRO

Simplify & enhance Safeguard environments

- User, alias, globals, object ACL mgmt
- Dynamic object security
- Password quality & updating
- User authentication

Access PRO

Grant privileges according to job function

- Access control
- Process control
- CMON logon control & load balancing
- Spooler & print job management

Audit PRO

Consolidate audit data across many nodes

- Multi-node view
- Multi-source audits: XYGATE, Safeguard . . .
- Single repository for all audit data
- Automatic alerts

Compliance PRO

Develop & monitor security policy compliance

- Multi-node data collection & view
- Best practice analysis
- Anomaly & exception mgmt
- System integrity checks

Encryption PRO

Protect business data: at rest and in transit

- Full crypto library
- Multi-platform support
- ESDK to crypto-enable via APIs
- File encryption
- Static key mgmt
- Session security

XYGATE GUI

NonStop Server Platform Security

Multi-platform Encryption Software

Typical Safeguard Audit

Safeguard Audit → Safeart → Audit Report

XYGATE Merged Audit
Safeguard – Single Node

```
Safeguard
Audit            ──────►    XYGATE MA

                                    Mover
                            Filter

                            SQL Audit
                            Table              ──────►    Audit
                                                          Report

                                                          Email
                                                          Alert

                                                          EMS/SNMP
                                                          Message

                                                          SYSLOG

                                                          Custom

                                                          GUI
                                                          Monitor
```

XYGATE Merged Audit
Multi-Audit – Single Node

Safeguard Audit

XYGATE Audit

EMS Audit

ODBC/MX Audit

JDBC/MX Audit

BASE24 Audit

XYGATE MA

Mover

Filter

SQL Audit Table

Audit Report

Email Alert

EMS/SNMP Message

SYSLOG

Custom

GUI Monitor

XYGATE Merged Audit
Multi-Audit – Multi-Node
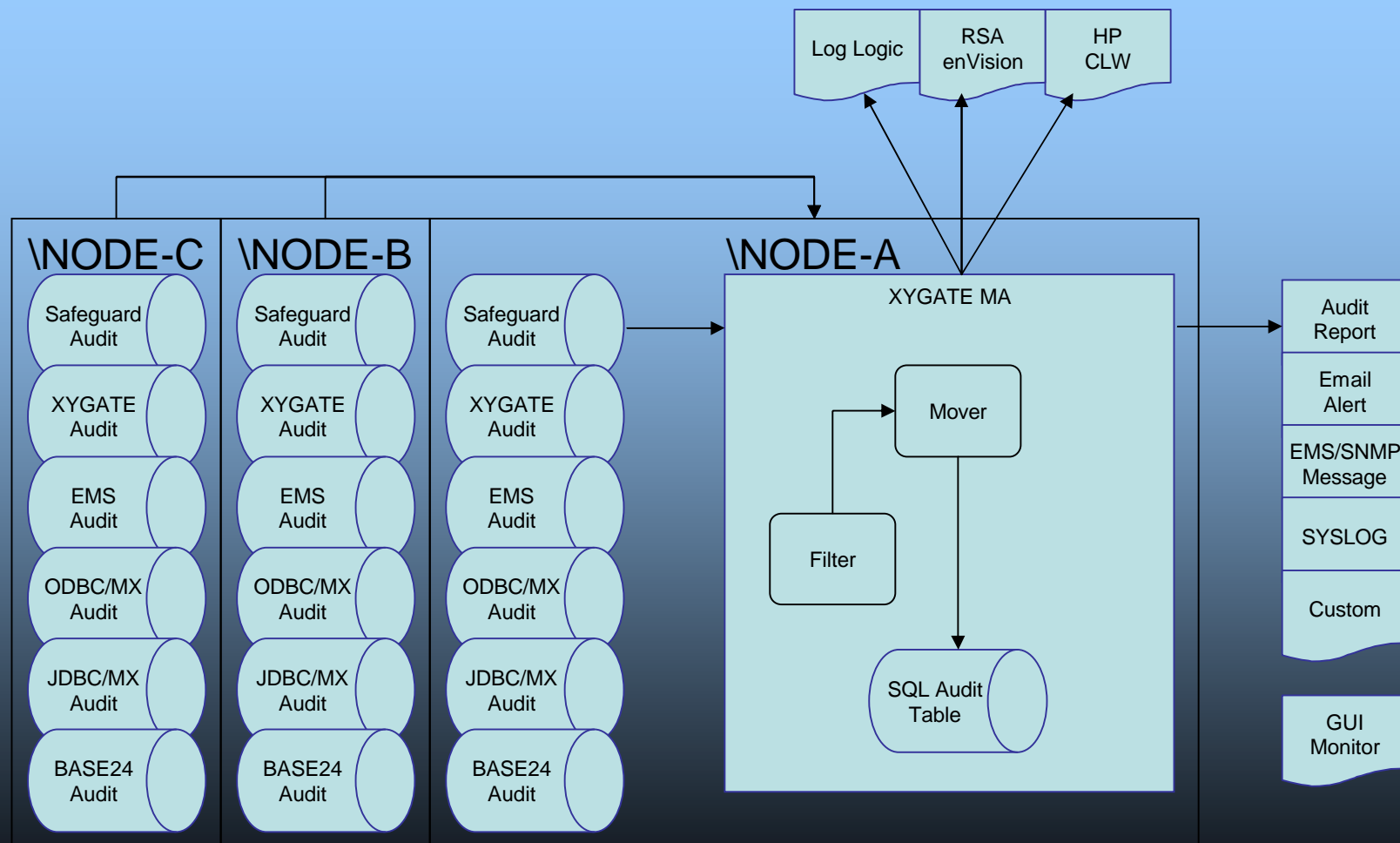
NonStop and CLW
Basic architecture

From HP

NonStop System
(S-series, NS-Integrity & NS Blade Systems)

EMS EVENTS

SAFEGUARD AUDIT TRAIL

XYGATE EVENTS

Base24 EVENTS

ODBC/MX EVENTS

XYGATE Merged Audit

Component from XYPRO

XYPRO

HP CLW

CLW Log Adapter for XYGATE

EVENT DATABASE

Report Engine

Compliance Audit Reports

The CLW comes with a Log Adapter that can process NonStop events passed by the XYGATE Merged Audit product from XYPRO

Future product plans, dates, and functionality are subject to change without notice.

XSW
Security Compliance Wizard

XSW
Security Compliance

Screen showing <u>collection</u> options;
batched or immediate
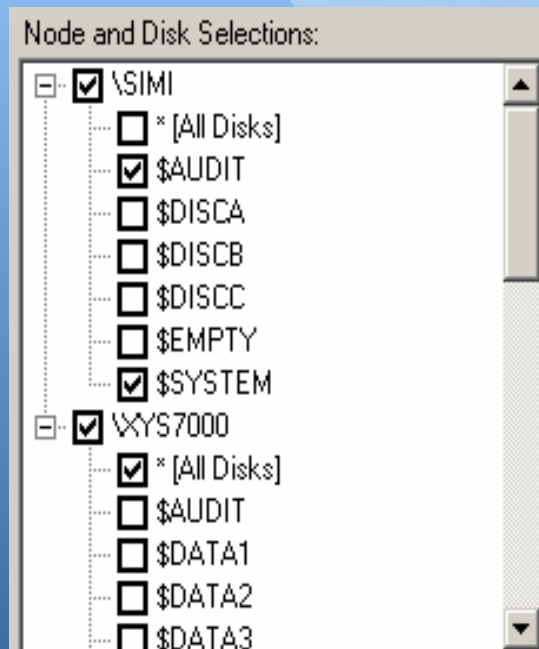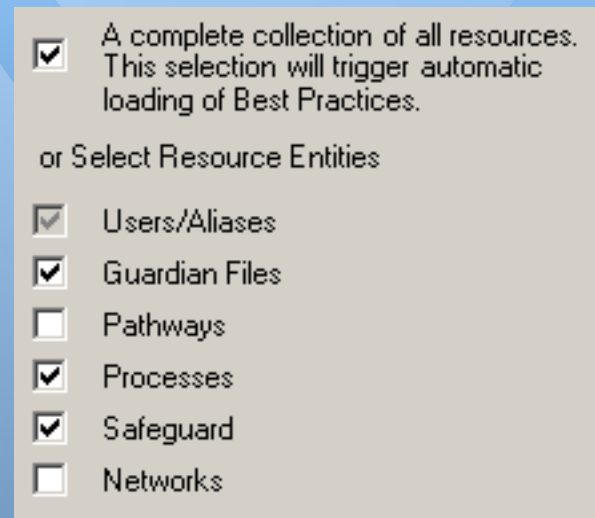
Select entities to collect

Select nodes and disks

XSW
Security Compliance

Screen showing policy results
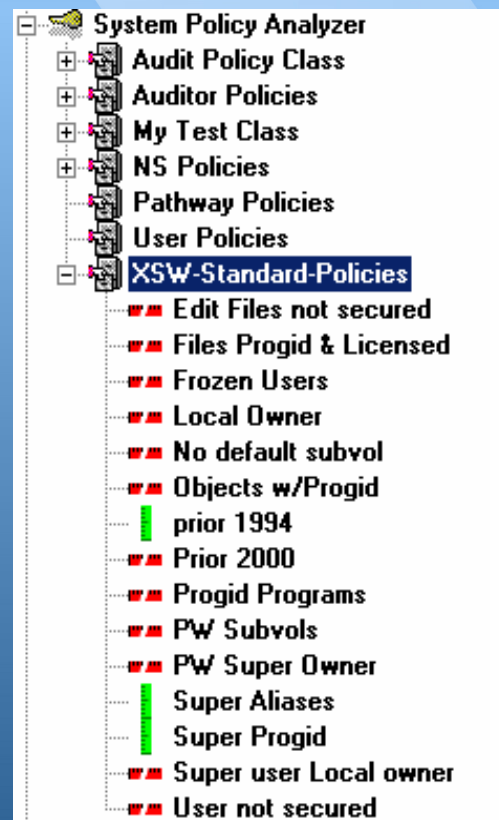
Instantly Visible!

Green ruler passed!

Red ruler failed!

14

XSW
Security Compliance

Screen showing policy results

Access Mapping

XSW
Security Compliance

- **HP NonStop Security Handbooks**
    - Alphabetic listing of system processes
    - Nuts and bolts of securing each object
    - Hundreds of programs and subsystems
    - Includes risks and Best Practice recommendations
    - Guardian and OSS
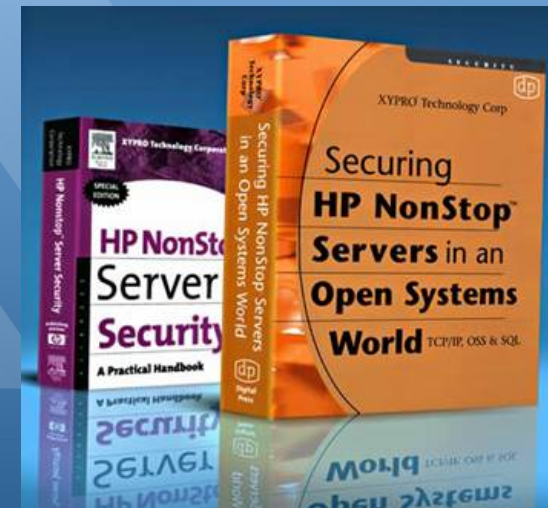
Best Practice Report

XYGATE/Security Wizard Policy Report

Best Practices Detail Report
Node Name: \XYS7000
Dataset Name: BP_20040928_0850
for Failed Policies

BP Id	Object Name	Attribute Checked	Recommended Value	Discovered Value	Reference	Best Practice Description
BP-DEVICE-OBJTYPE-02(FAIL)						
	OBJECTTYPE DEVICE	Owner	255,255	*.253,1	Vol 1, Part 5, Pg 164	The Security Administrator userid or SUPER.SUPER should be the primary owner of the DEVICE OBJECTTYPE Record. If the Security Administrator userid is not the primary owner, it must have the (O)wner privilege so that it can manage all OBJECTTYPE Records.
BP-DISK-OBJTYPE-01(FAIL)						
	OBJECTTYPE DISKFILE	Exists	YES	*NO VALUE OR OBJECT FO	Vol 1, Part 3, Pg 177	The DISKFILE OBJECTTYPE Record should be created to control who is allowed to create Protection Records for the various files on the system. If the DISKFILE OBJECTTYPE record doesn't exist, any local member of the SUPER group can add DISKFILE Records.

XYPRO Technology Corporation

XYPRO Europe

Tel: +44 (0) 1384 850133
Sean.Bicknell@XYPRO.co.uk

WWW.XYPRO.COM