

NonStop PCI Compliance. Ticking the checkbox.



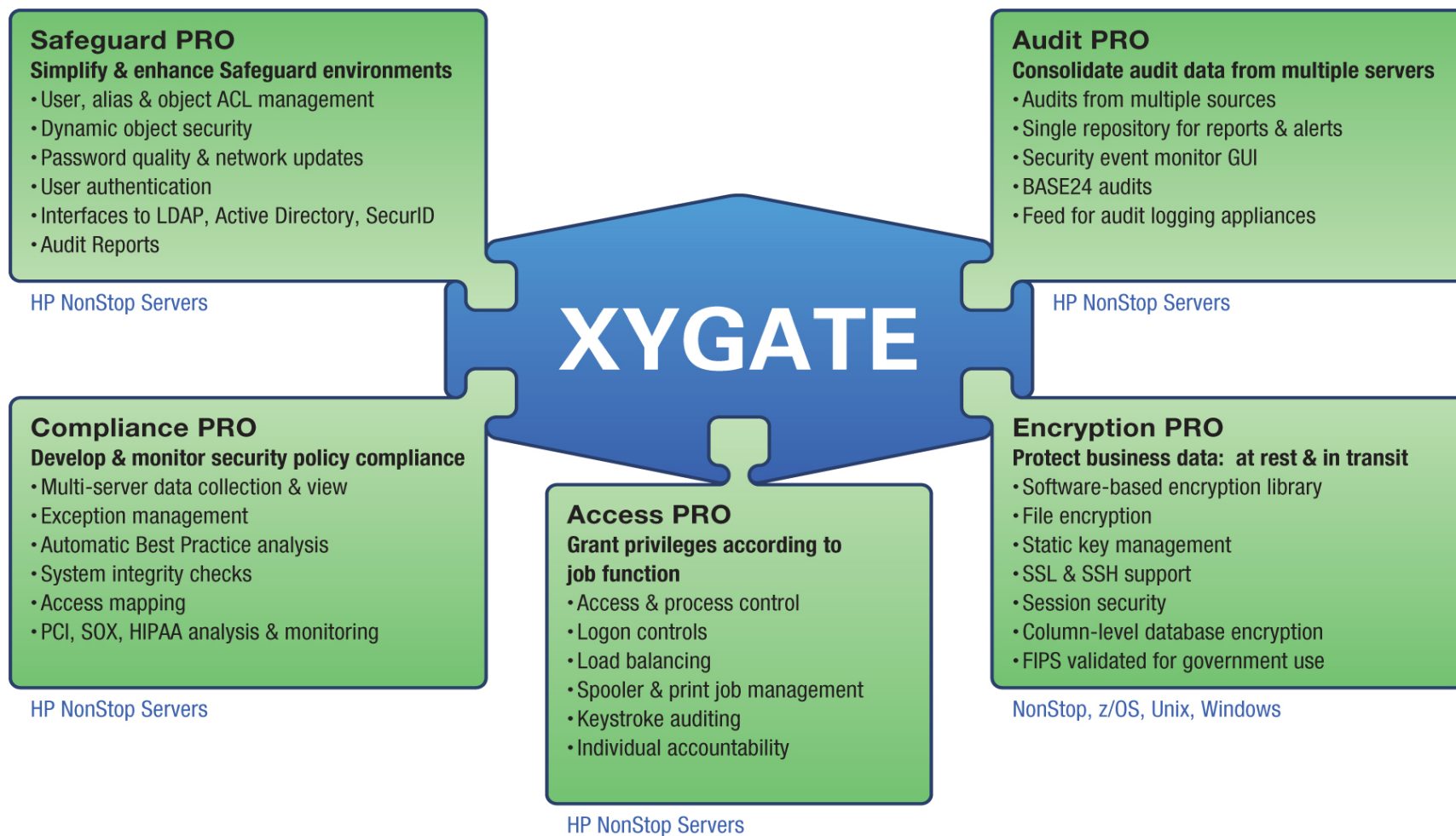
Presenter: Sean Bicknell



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)

XYGATE: The Suite



welcome to xypro technology corporation

Welcome to **XYPRO**

No ComPROmise Compliance

[>> Learn More](#)



XYPRO CALENDAR OF EVENTS - [CLICK HERE](#)

DOWNLOAD FREE

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

Specializing in HP NonStop server software since 1983, XYPRO provides the tools to achieve security compliance in a NonStop environment. XYGATE security modules include Access Control, User Authentication, Authorization and Password Quality to Automated Compliance and Audit Reporting, Integrity Checking and FIPS Validated Encryption.

XYPRO. Exceeding your NonStop security, compliance and encryption needs for more than 25 years.

> XYPRO News & Events

May 2010 - Centricity Enterprise Users: Simplify and Automate Database Management for your HP NonStop Servers

MAY 2010 - Nonstop Security Webinar

MAY 2010 - XYPRO & Tandemworld Announce Partnership

NOV 2009 - XYPRO® Announces Strategic Reseller Relationship with Merlon

OCT 2009 - XYPRO 2010 Training Dates!

SEP 2009 - XYPRO releases of XYGATE EM (XEM) version 1.20

JUL 2009 - Compliance PRO Demo - Available Online!

Securing HP NonStop Servers in an Open Systems World



The Reviews are in!



5.0 out of 5 stars, Excellent HP NonStop reference guide!!

Get your copy today!

Contact a Security Specialist!

What others say about XYPRO!

"Security was an integral part from the very beginning in 2000, and XYPRO was there to make it happen."

Follow XYPRO on:



facebook

Linked in

blog.xypro.com

Requirement	Guidance
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.

- Safeguard
 - Allows you to limit repeated logons

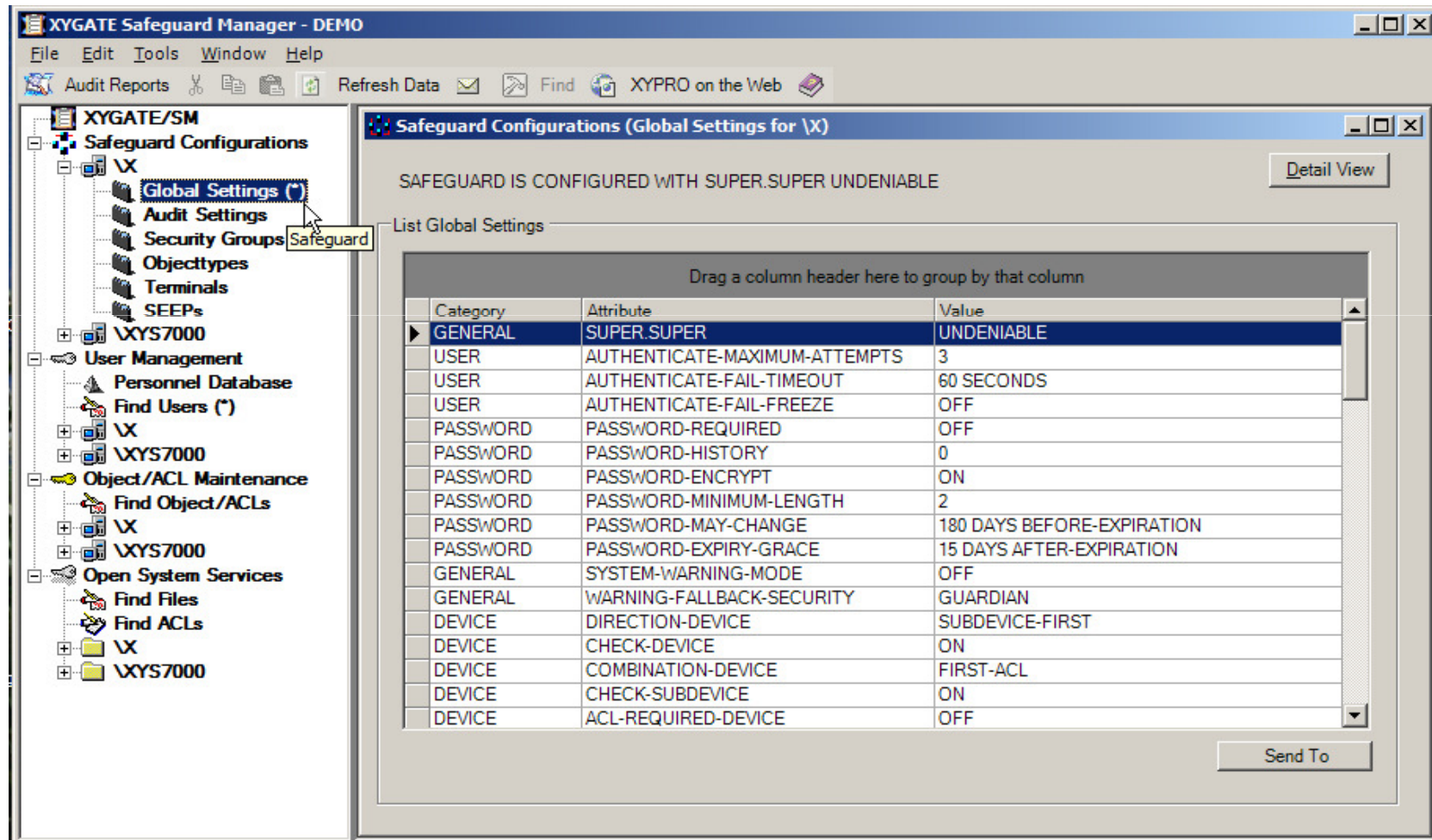


Requirement	Guidance
<p>8.5.4 Immediately revoke access for any terminated users.</p>	<p>If an employee has left the company, and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur. This access could happen from the former employee or from a malicious user who exploits the older and/or unused account. Consider implementing a process with HR for immediate notification when an employee is terminated so that the user account can be quickly deactivated.</p>

- Safeguard
 - Userid's can be deleted on a individual node basis
- XYGATE Safeguard Manager
 - Delete multiple users from multiple nodes simultaneously



XYGATE Safeguard Manager (XSM)



The screenshot displays the XYGATE Safeguard Manager (XSM) interface. The left pane shows a tree view of the system configuration, with 'Global Settings' selected under 'Safeguard Configurations'. The right pane shows the 'Safeguard Configurations (Global Settings for \X)' window. The status bar indicates 'SAFEGUARD IS CONFIGURED WITH SUPER.SUPER UNDENIABLE'. Below this, a table lists global settings.

SAFEGUARD IS CONFIGURED WITH SUPER.SUPER UNDENIABLE

List Global Settings

Category	Attribute	Value
GENERAL	SUPER.SUPER	UNDENIABLE
USER	AUTHENTICATE-MAXIMUM-ATTEMPTS	3
USER	AUTHENTICATE-FAIL-TIMEOUT	60 SECONDS
USER	AUTHENTICATE-FAIL-FREEZE	OFF
PASSWORD	PASSWORD-REQUIRED	OFF
PASSWORD	PASSWORD-HISTORY	0
PASSWORD	PASSWORD-ENCRYPT	ON
PASSWORD	PASSWORD-MINIMUM-LENGTH	2
PASSWORD	PASSWORD-MAY-CHANGE	180 DAYS BEFORE-EXPIRATION
PASSWORD	PASSWORD-EXPIRY-GRACE	15 DAYS AFTER-EXPIRATION
GENERAL	SYSTEM-WARNING-MODE	OFF
GENERAL	WARNING-FALLBACK-SECURITY	GUARDIAN
DEVICE	DIRECTION-DEVICE	SUBDEVICE-FIRST
DEVICE	CHECK-DEVICE	ON
DEVICE	COMBINATION-DEVICE	FIRST-ACL
DEVICE	CHECK-SUBDEVICE	ON
DEVICE	ACL-REQUIRED-DEVICE	OFF

Send To

Added value: XYGATE Safeguard Manager (XSM)

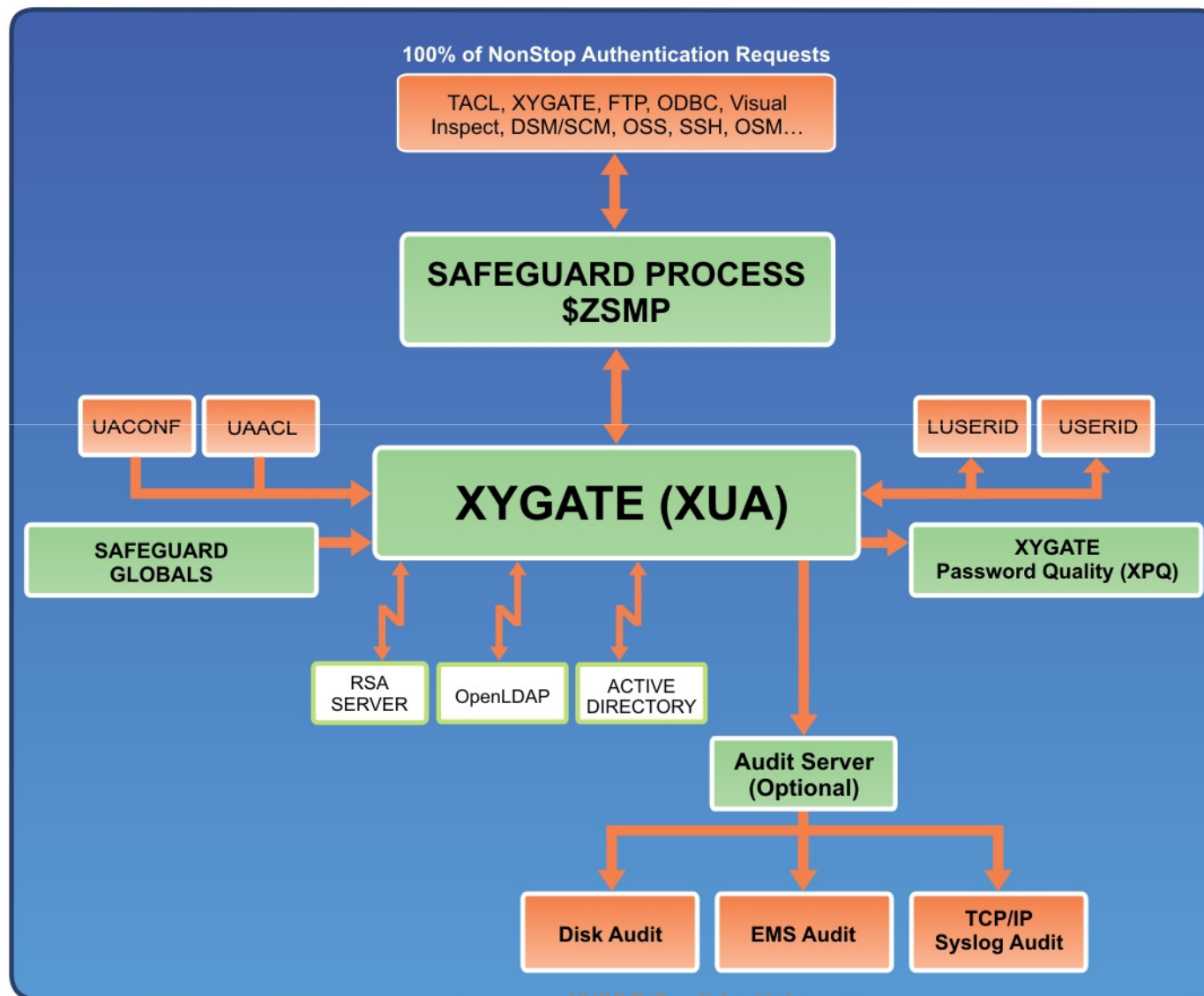
- Enhanced research and reporting makes it easy to:
 - Create multi-node lists of protection records that include obsolete userIDs and remove the user entries with one click
 - Compare global parameters, userID/alias configuration, or object protection records across nodes
 - Create multi-node lists of frozen or expired userIDs
 - Create multi-node lists of userIDs that have not logged on within a given period of time
 - Create multi-node lists of userIDs or passwords that will expire within a selected number of days
- XSM provides a Personnel Database that allows the customer to link NonStop userIDs to an actual person, as well as storing the user's phone numbers, address, department, shift, supervisor name, and other customizable information

Requirement	Guidance
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	These requirements are intended to prevent malicious individuals from accessing the organization's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an external untrusted server in an untrusted network).

- There is no native control for logon access to the HP NonStop using IP addresses.
- XYGATE User Authentication (XUA) enables logon controls via IP address



XYGATE User Authentication (XUA)



XUA Functional Highlights

- Node conditional processing
- Granular logon control
 - Authenticate_fail_freeze (this can be permanent or temporary)
- Restrictions can be configured by IP, requestor, others.....
- LDAP Setup
 - Bring NonStop into enterprise SSO
- Dynamically map existing Guardian users
 - Regular Expressions means very little configuration
 - no need to maintain additional USER id database
- Very granular audit
- Reporting

Requirement

Guidance

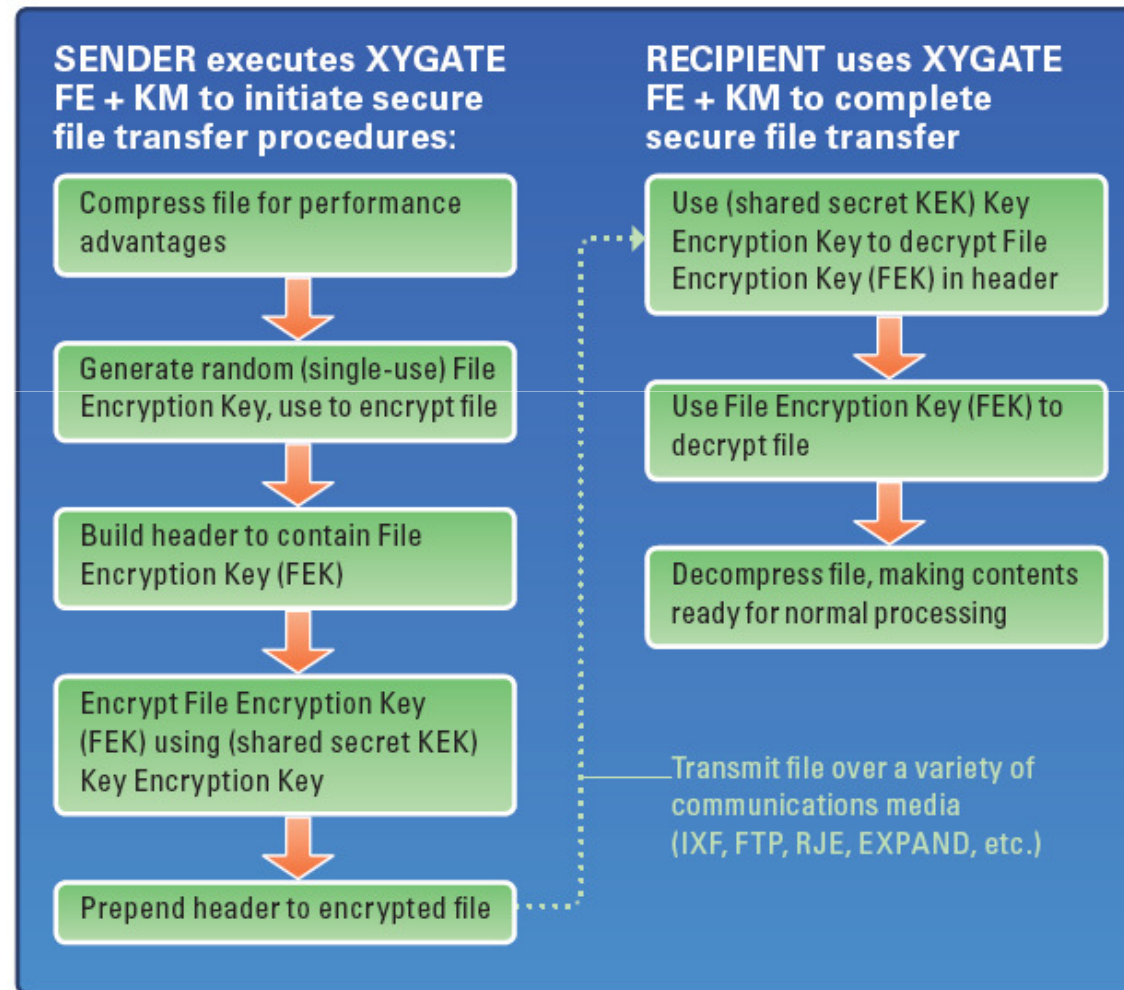
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches:

Lack of protection of PANs can allow malicious individuals to view or download this data. PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. Damage from theft or loss of backup tapes during transport can be reduced by ensuring PANs are rendered unreadable via encryption, truncation, or hashing. Since audit, troubleshooting, and exception logs have to be retained, you can prevent disclosure of data in logs by rendering PANs unreadable (or removing or masking them) in logs. Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of “strong cryptography”

- There is no encryption capability shipped with every NonStop server.
- XYGATE File Encryption (XFE) and XYGATE Encryption Library (XEL) both enable strong encryption for data stored on the HP Nonstop

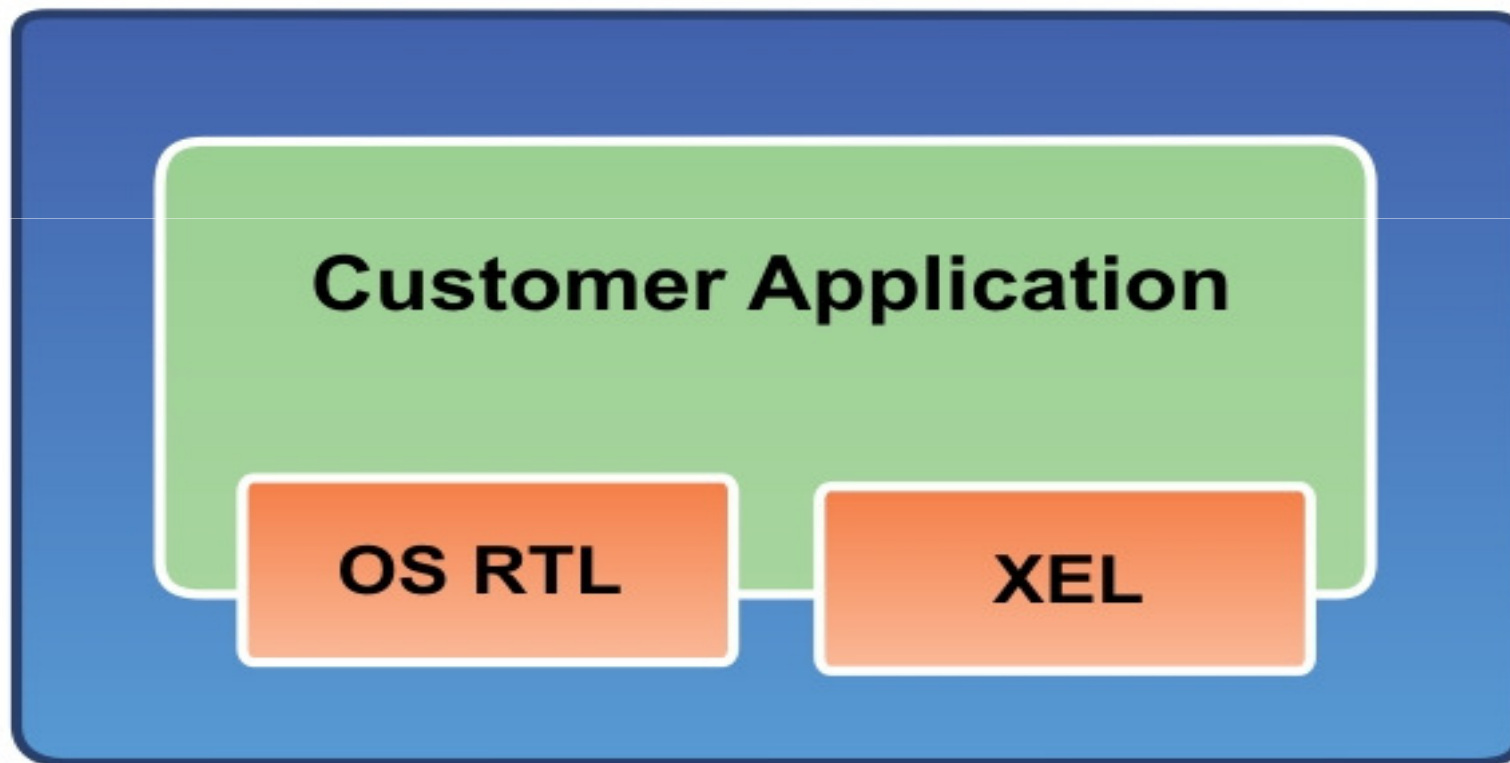


File Encryption with Optional Static Key Management



XYGATE Encryption Library

XYGATE (XEL)



XYGATE Encryption

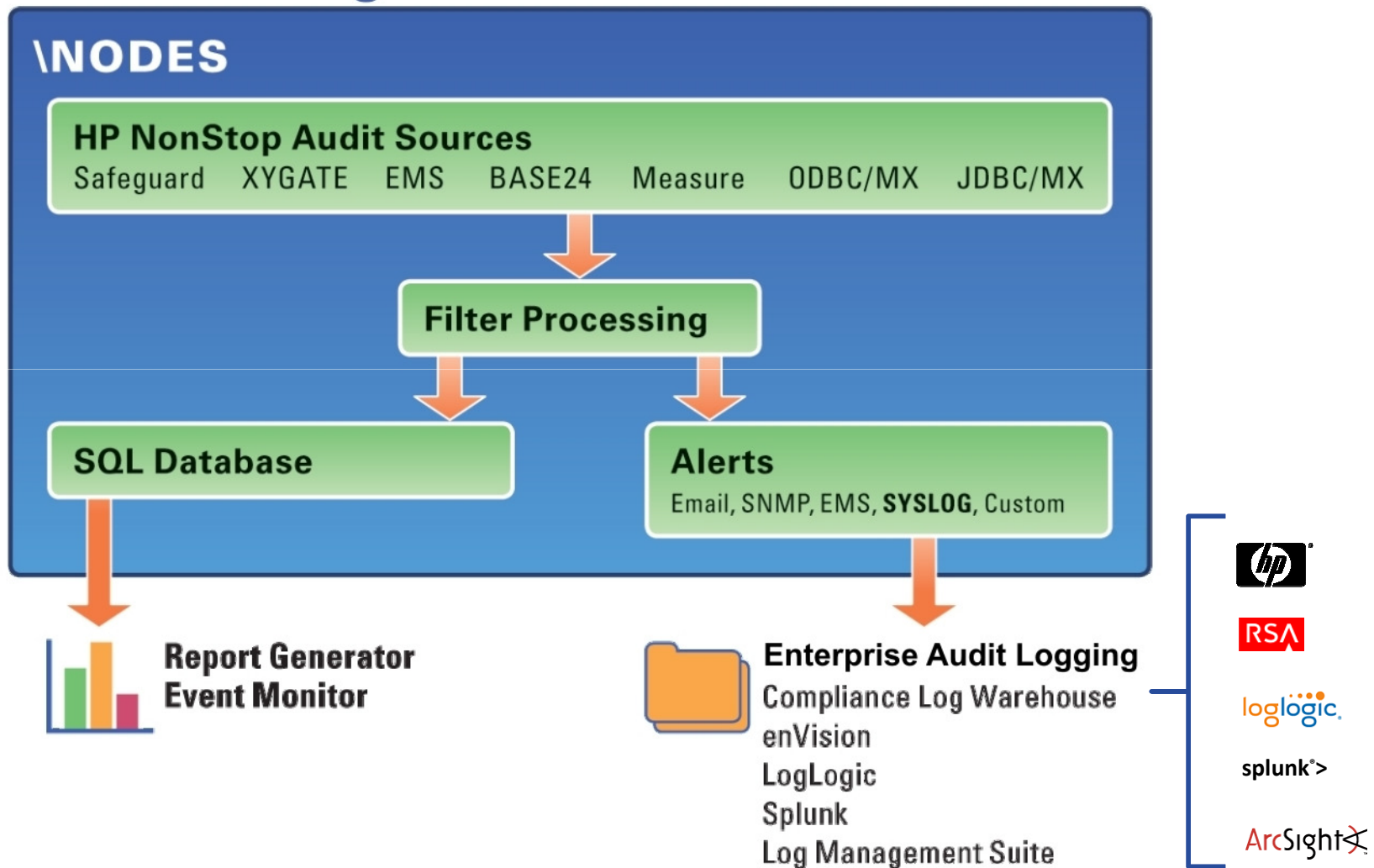
- Added Benefits
 - XYGATE Encryption is NIST validated to the FIPS 140-2 standard
 - Used by VISA, a PCI-DSS founding organisation!
 - Column level encryption is secure on disk, on backup media, and in transit.

Requirement	Guidance
<p>10.5.5 Use file-integrity monitoring and change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).</p>	<p>File-integrity monitoring systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise. For log files (which do change frequently) what should be monitored are, for example, when a log file is deleted, suddenly grows or shrinks significantly, and any other indicators that a malicious individual has tampered with a log file. There are both off-the-shelf and open source tools available for file-integrity monitoring.</p>

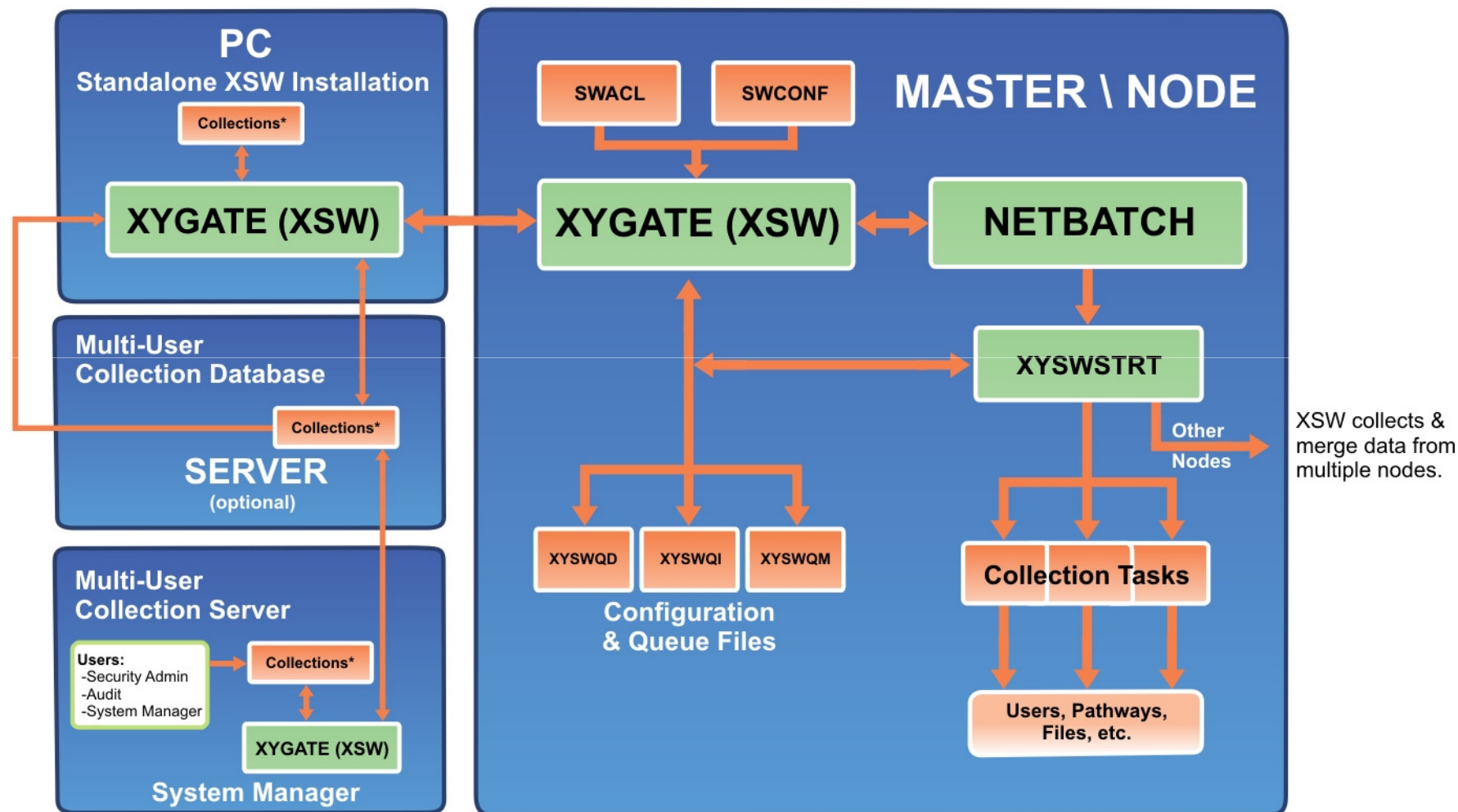
- Native file-integrity monitoring or change-detection software does not exist for the HP NonStop
- XYGATE Merged Audit (XMA) will monitor events and create alerts.
- XYGATE Security Compliance Wizard (XSW) will monitor file integrity and report differences



XYGATE Merged Audit (XMA)

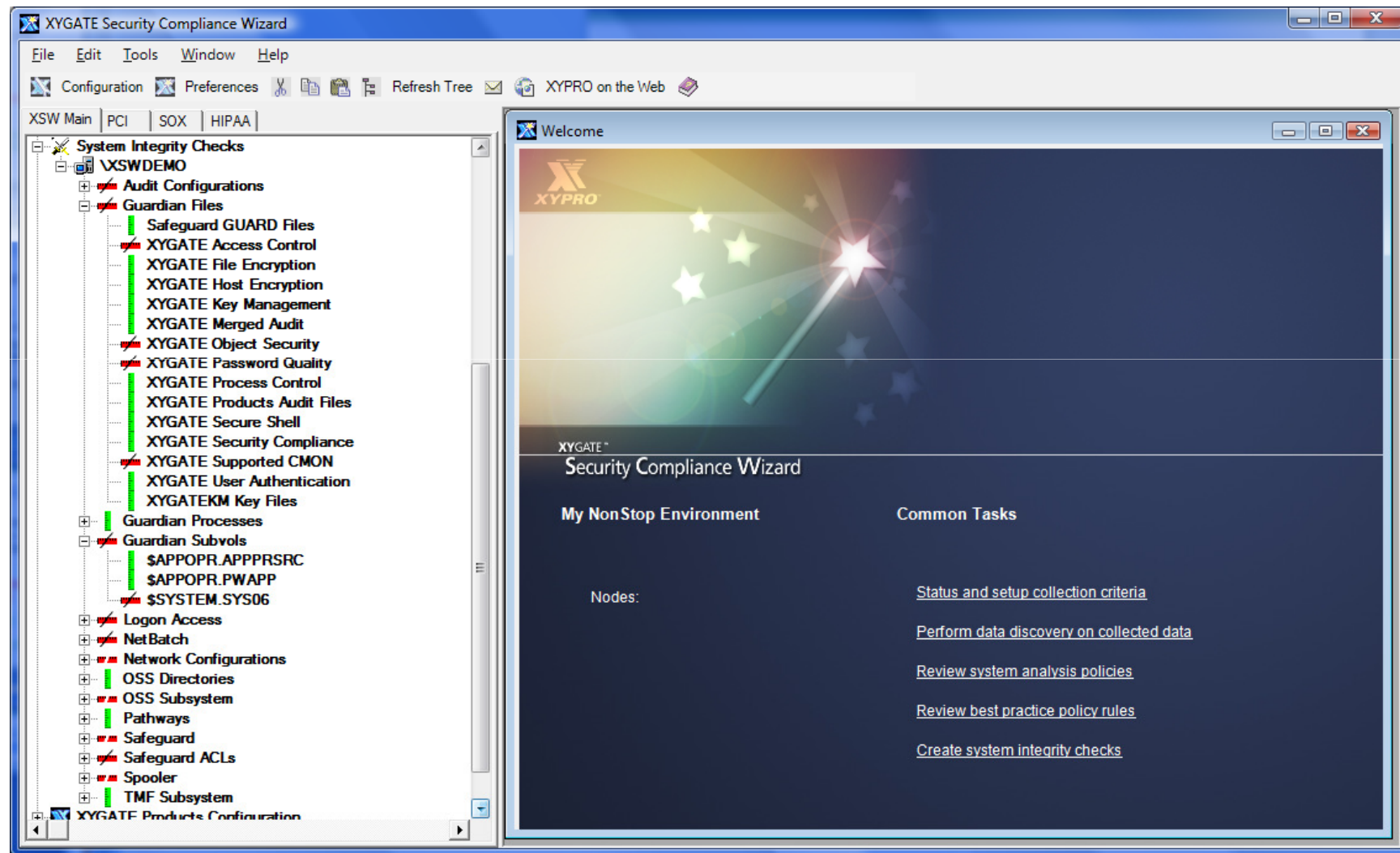


XYGATE Security Compliance Wizard (XSW)



*Collections will reside either on the PC or on a SERVER

XYGATE Security Compliance Wizard (XSW)



PCI compliance is achievable

- Native tools can tick many of the check boxes
- XYGATE tools tick the boxes that native tools can't
- XYGATE tools add functionality, reduce workload. Allow you to work smarter!



PCI Minimum Requirements

Paper out soon!!

- Please leave a business card at our booth to register your interest
- Maybe win an iPod





XYPRO

www.xypro.com

Sean.Bicknell@xypro.co.uk