XYGATE Compliance PRO
Now available through the HP NonStop division

Customer Product Education Series

Karen Copeland
April 14th, 2011
XYGATE Compliance PRO

Agenda

• Security Today
• XYGATE Compliance PRO
  • What does it do?
  • Preview the look and feel of the product
• Support, Licensing and Services
• Questions?
Security Issues facing customers

• When security is breached, companies face:
  – Fines
  – Lost productivity
  – Customer loss/dissatisfaction
  – Government probes
  – Bad press
  – Ruined reputations

• Around the world there are 20,000 security regulations that businesses must meet and more emerge locally every year.

<table>
<thead>
<tr>
<th>Security Breach</th>
<th>User records Impacted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartland Payment Systems</td>
<td>100,000,000+</td>
</tr>
<tr>
<td>TJ Maxx retail stores</td>
<td>45,700,000</td>
</tr>
<tr>
<td>Dai Nippon Printing</td>
<td>9,000,000</td>
</tr>
<tr>
<td>Johns Hopkins University and Hospital</td>
<td>1,200,000</td>
</tr>
<tr>
<td>State of Ohio</td>
<td>860,000</td>
</tr>
</tbody>
</table>

Source: [http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP](http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP)
Compliance is no longer optional

- Security compliance affects businesses worldwide
- Today compliance regulations exist for nearly all industries
  - Financial, Retail, Telco, Healthcare
- Regulations get stricter each year with stronger penalties for failure
  - PCI/DSS, HIPAA, Sarbanes-Oxley, etc
- Laws continue to emerge that govern what actions a company must take when a breach occurs
  - 45 states, Washington D.C., Puerto Rico and the Virgin Islands all have legislation in this area.
Cost of Non-Compliance
Not doing anything is dangerous to your business

Fines are real! Governments can **and do** levy fines for non-compliance:

**Cignet Health** (Feb. 2011) received a $4.3 Million dollar HIPAA fine for not protecting its customers’ personal information – levied by the US Dept. of Health and Human Services

Processing delays are real!

Being “demoted” in the payment processing tier structure for not being PCI compliant can cost millions every month while your competitor’s transactions are handled ahead of yours.

The risk of breach increases and if it does occur, the company suffers:
- Financial impact of whatever is actually stolen
- Loss of IP and Corporate Confidential information such as trade secrets, time to market
- Loss of customer confidence due to inability to protect customer’s private information
- Ruined company reputation and brand
So what goes wrong?
Verizon Data Breach Investigations Report

WHAT COMMONALITIES EXIST?

- 98% of all data breached came from servers (-1%)
- 85% of attacks were not considered highly difficult (+2%)
- 61% were discovered by a third party (-8%)
- 86% of victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls (+9%)
- 79% of victims subject to PCI DSS had not achieved compliance
So what goes wrong?
Verizon Data Breach Investigations Report

WHAT COMMONALITIES EXIST?

98% of all data breached came from servers (-1%)

85% of attacks were not considered highly difficult (+2%)

61% were discovered by a third party (-8%)

86% of victims had evidence of the breach in their log files

96% of breaches were avoidable through simple or intermediate controls (+9%)

79% of victims subject to PCI DSS had not achieved compliance
Managing all aspects of Security
A daunting effort

• To gather and review security settings for all parts of the system can quickly mount into 1000s or even millions of data items to review.

• By the time data collection has been completed, it’s often already out of date.

• To manually do this requires a highly trained NonStop staff with deep TACL skills, available around the clock, who never make mistakes.

Effective management of the system’s security settings can close issues that a seasoned criminal would happily exploit.
XYGATE Compliance PRO

What is it?

XYGATE Compliance PRO is a sophisticated and powerful tool specifically designed for the NonStop platform to help customers:

- analyze system security settings and configurations
- automate the extensive system data collection to compare changes in the system from different points in time
- track and audit their security settings to improve and maintain protection and of their system
- have confidence about monitoring compliance with documented evidence
Focus on Compliance Options for Customers

Security policies can be verified to be working and compliance regulations can be proven to be in place.

New Offering!
XYGATE Compliance PRO

- An independent product
- Helps customers to verify current system security settings for compliance and system protection
- Available J Series, H Series and G Series

Offered as of fall 2010
XYGATE Merged Audit

- Part of OS Security Update bundle
- Provided on all new systems
- Helps customers to review audit data for security events on their NonStop system
- Available for J Series & H Series through OS Security Update bundle
- Available for G Series as independent product
XYGATE Compliance PRO

How is the system secured?

- Compare system configuration & security settings against:
  - Regulations
  - PCI, SOX, HIPAA, ETC.,
  - Best Practices
  - Internal Security Policy

- Integrity Checking
  - Compare Files
  - Compare entire systems
  - MD5 Hashing

- Access Mapping
  - What can users access?
  - Compare access across systems

- Extensive Reporting
  - Prove compliance to an Auditor & Senior Management

XYGATE Merged Audit

What is happening on the system?

- Consolidated Audit Logs
  - Multiple NonStop Audit Sources
  - From across the entire NonStop Network
  - Filtered to include only what you want/need.
  - Detailed canned and highly customizable reports

- Alerts
  - EMS
  - EMAIL
  - Pager
  - Security Event Display includes visual and auditory alerts

- Enterprise Security
  - Deliver NonStop Audit to any SIEM (ArcSight)
  - Integrates NonStop into the Enterprise Security Architecture
Compliance PRO
Look and feel
Lisa Partridge and Barry Forbes
XYGATE Compliance PRO

Product Features

• Enables easy investigation of NonStop security with comprehensive system examination and evaluation:
  • Provides data about security standards adherence for use with compliance auditors
  • Verifies general and specific system integrity across any area of the system of interest

• Supports security data collection
  • Dramatically improves data collection time and efforts
  • Integrates with NetBatch to automate cyclical collections and monitoring
  • Uses consistent collection metrics for each cycle
  • Offers an “open platform” for sharing of data collections
  • Captures data from multiple NonStop systems into a single repository for reporting
XYGATE Compliance PRO
Product Features

• Supports security policies
  • Provides a robust set of baseline policies and recommendations
  • Allows users to define and establish their own security policies
  • Provides automatic tracking of security policies
  • Notifies customer by email when policy failures are detected
  • Provides the foundation for custom policies to achieve PCI, SOX or HIPAA requirements

• Supports PCI, SOX and HIPAA requirements
  • Maps regulations and regulation compliance to monitor compliance status
  • Meets the PCI, SOX and HIPAA requirement for “active monitoring”
  • Provides active archives for audit requirements
  • Regular updates keep you up to date with the latest policies for PCI, SOX and HIPAA
XYGATE Compliance PRO
Product Architecture

*Collections will reside either on the PC or on a SERVER
A Customer Use Case Example

“I don’t know if we are PCI compliant – how do I find out?”

If I can’t **track** and **prove** compliance:

- I can’t answer an auditor’s questions
- I can’t answer my manager’s questions
- My company probably won’t pass an audit*
- My company could be fined or worse……
- My own job is in jeopardy

*Not passing PCI audits cost one client $1M per month until they implemented XYGATE Compliance PRO software.

Real concerns expressed by a Compliance PRO user prior to purchasing the software
XYGATE Compliance PRO
PCI Reporting – Reports maps to the exact PCI Data Security Standard

PCI regulations have a series of Data Standards numbered 1 – 12.
XYGATE Compliance PRO
PCI Reporting – Violations appear in RED

Looking at the next level reveals “in red” where a problem in the configuration exists which might be flagged by an auditor.
XYGATE Compliance PRO

PCI Reporting – Details can be viewed by clicking further

Requirement is explained as to how it applies to the NonStop platform
XYGATE Compliance PRO – Best Practice Policy

The image shows a screenshot of the XYGATE Security Compliance Wizard. The screenshot includes a tree view of available collections, rules, and policies. There is a focus on the Best Practice Policy Analyzer for 'Users/Aliases--SUPER'. The policy details include:

- **Node Name**: [ ]
- **Category**: Users/Aliases–SUPER

The O/S Release is H06.19.00, and it was updated on 07/12/2009 4:18:21 PM.

The policy description states: The Best Practice items associated with this category and their verified value as compared to the desired value.

The table shows the following columns:

- **Check_Attribute**
- **Check_Modifier**
- **OSS_FullPath**
- **Recommended_Value**
- **Discovered_Value**
- **Status**
- **Referer**

The policy items and their statuses are as follows:

<table>
<thead>
<tr>
<th>Check_Attribute</th>
<th>Check_Modifier</th>
<th>OSS_FullPath</th>
<th>Recommended_Value</th>
<th>Discovered_Value</th>
<th>Status</th>
<th>Referer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password-Must-Change</td>
<td></td>
<td></td>
<td>30</td>
<td>0</td>
<td>FAIL</td>
<td></td>
</tr>
<tr>
<td>AUDIT-AUTHENTICATE-FAIL</td>
<td></td>
<td></td>
<td>ALL</td>
<td>NONE</td>
<td>FAIL</td>
<td>Vol 1, F</td>
</tr>
<tr>
<td>AUDIT-MANAGE-FAIL</td>
<td></td>
<td></td>
<td>ALL</td>
<td>NONE</td>
<td>FAIL</td>
<td>Vol 1, F</td>
</tr>
<tr>
<td>AUDIT-MANAGE-PASS</td>
<td></td>
<td></td>
<td>ALL</td>
<td>NONE</td>
<td>FAIL</td>
<td>Vol 1, F</td>
</tr>
<tr>
<td>AUDIT-USER-ACTION-FAIL</td>
<td></td>
<td></td>
<td>ALL</td>
<td>NONE</td>
<td>FAIL</td>
<td>Vol 1, F</td>
</tr>
</tbody>
</table>

The policy analysis provides a detailed view of compliance with specific attributes and their statuses.
XYGATE Compliance PRO – Best Practice Policy

Tree View of Available Collections, Rules and Policies
XYGATE Compliance PRO – Best Practice Policy
XYGATE Compliance PRO – Best Practice Policy
XYGATE Compliance PRO – Policy Checking
XYGATE Compliance PRO – Policy Checking
XYGATE Compliance PRO – Policy Checking
XYGATE Compliance PRO – Policy Checking
XYGATE Compliance PRO – Policy Checking

![XYGATE Security Compliance Wizard](image)

**System Policy Analyzer (Last Logon over 90 days)**

Policy Analysis by Collection: XSV Demo Collection; XSV_DEMO

**Status = Failed**

- **Policy Class:** User and Alias Policies
- **Policy Name:** Last Logon over 90 days
- **Predicate on:** Users/Aliases
- **Entity:** [Last Logon more than 90 days old]

**Policy Description:**
User’s last logon was over 90 days ago and should be considered for removal.

### Recent (0) Failed (11) Exclusions (0) Resolved (0) Log Entries Properties

<table>
<thead>
<tr>
<th>Tracking_No</th>
<th>Resolution</th>
<th>Current_Status</th>
<th>Node_Name</th>
<th>Group_id</th>
<th>User_Id</th>
<th>Alias</th>
<th>Group_Name</th>
<th>User_Name</th>
<th>Alias_Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>3</td>
<td>N</td>
<td></td>
<td>XYGATEP</td>
<td>TEST1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>1</td>
<td>N</td>
<td></td>
<td>PQTEST</td>
<td>USER002</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>N</td>
<td></td>
<td>PQTEST</td>
<td>USER04</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>5</td>
<td>Y</td>
<td>PQTEST</td>
<td>USER005</td>
<td>pg24-005</td>
</tr>
<tr>
<td>5</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>6</td>
<td>N</td>
<td>PQTEST</td>
<td>USER006</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>8</td>
<td>N</td>
<td>PQTEST</td>
<td>USER008</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>8</td>
<td>Y</td>
<td>PQTEST</td>
<td>USER008</td>
<td>pg24-008</td>
</tr>
<tr>
<td>8</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>9</td>
<td>N</td>
<td>PQTEST</td>
<td>USER009</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>171</td>
<td>N</td>
<td>PQTEST</td>
<td>USER171</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td>245</td>
<td>Y</td>
<td>PQTEST</td>
<td>RON</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Failed</td>
<td></td>
<td>XSVDEMO</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>xsr-alias</td>
</tr>
</tbody>
</table>
XYGATE Compliance PRO – Integrity Checking
XYGATE Compliance PRO – Integrity Checking
XYGATE Compliance PRO – Access Mapping
XYGATE Compliance PRO – Access Mapping
XYGATE Compliance PRO – Access Mapping
XYGATE Compliance PRO – Automated Reporting
XYGATE Compliance PRO – Automated Reporting

XYGATE/Security Wizard Policy Report

System Policy Summary Report by Policy Class

<table>
<thead>
<tr>
<th>Policy Class Name</th>
<th>Policy Name</th>
<th>Collection Name</th>
<th>Dataset Name</th>
<th>Current Status</th>
<th>Policy Predicate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guardian Policies</td>
<td>Audit File Owner</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>354 Recent; 354 Failed; 0 Excluded; 0 Resolved</td>
<td>(User File Cid=134 OR S41 OR S47 OR S41) AND (Owner NOT = 2252255) WHERE (Info.File_Name Not Like &quot;ZZEVPY&quot; OR Info.File_Name Like &quot;ZZEVPY&quot;) AND (Info.Security &lt;&gt; &quot;NULU&quot;) AND (Info.Security &lt;&gt; &quot;****&quot;)</td>
</tr>
<tr>
<td></td>
<td>ENS Audit Logs</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>56 Recent; 56 Failed; 0 Excluded; 0 Resolved</td>
<td>WHERE (Info.Sub.Volume = &quot;MBM&quot; AND Info.File_Name Not Like &quot;LDWVR&quot;) AND (Info.Security &lt;&gt; &quot;NULU&quot;) AND (Info.Security &lt;&gt; &quot;****&quot;)</td>
</tr>
<tr>
<td></td>
<td>Licensed Files</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>111 Recent; 111 Failed; 0 Excluded; 0 Resolved</td>
<td>WHERE (Info.Sub.Volume = &quot;MBM&quot; AND Info.File_Name Not Like &quot;LDWVR&quot;) AND (Info.Security &lt;&gt; &quot;NULU&quot;) AND (Info.Security &lt;&gt; &quot;****&quot;)</td>
</tr>
<tr>
<td></td>
<td>NetAgent Logs</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>202 Recent; 202 Failed; 0 Excluded; 0 Resolved</td>
<td>(Licensed) AND (Owner NOT = 2252255)</td>
</tr>
<tr>
<td></td>
<td>Pidogi Files for SUPER</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>29 Recent; 29 Failed; 0 Excluded; 0 Resolved</td>
<td>(Pogodi AND (Owner = 2252255)) AND (Pogodi AND (Licensed) AND Volume.Name NOT = &quot;SYSTEM&quot;) AND (File.Name NOT LIKE &quot;%SYS%&quot;) AND (File.Name NOT LIKE &quot;%XYGATE%&quot;)</td>
</tr>
<tr>
<td></td>
<td>Pidogi Licensed Not On $SYSTEM</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>17 Recent; 17 Failed; 0 Excluded; 0 Resolved</td>
<td>(Pogodi AND (Owner = 2252255)) AND (Pogodi AND (Licensed) AND Volume.Name NOT = &quot;SYSTEM&quot;) AND (File.Name NOT LIKE &quot;%SYS%&quot;) AND (File.Name NOT LIKE &quot;%XYGATE%&quot;)</td>
</tr>
<tr>
<td></td>
<td>Suspected Duplicated Objects</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>0 Recent; 0 Failed; 0 Excluded; 0 Resolved</td>
<td>(Duplicate FileShare Timestamp &quot;INVALID&quot;)</td>
</tr>
<tr>
<td>Orphan Policies</td>
<td>Orphan FS Members</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>13 Recent; 13 Failed; 0 Excluded; 0 Resolved</td>
<td>(Orphaned FileSecurity Members)</td>
</tr>
<tr>
<td></td>
<td>Orphan OSS File Owners</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>0 Recent; 0 Failed; 0 Excluded; 0 Resolved</td>
<td>(Orphaned OSS Owners)</td>
</tr>
<tr>
<td></td>
<td>Orphan OSS Group List</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>0 Recent; 0 Failed; 0 Excluded; 0 Resolved</td>
<td>(Orphaned OSS Groups)</td>
</tr>
<tr>
<td></td>
<td>Orphaned Safeguard ACL List</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>0 Recent; 0 Failed; 0 Excluded; 0 Resolved</td>
<td>(Orphaned Safeguard-ACL List)</td>
</tr>
<tr>
<td></td>
<td>Orphaned Safeguard ACL Owners</td>
<td>X Full Collection</td>
<td>BP_20110412_0026</td>
<td>0 Recent; 0 Failed; 0 Excluded; 0 Resolved</td>
<td>(Orphaned Safeguard-ACL Owners)</td>
</tr>
</tbody>
</table>
Compliance is a Continuous Process

- Evaluate Current Compliance
- Implement Policies and Procedures to meet goals
- Create Auditing to Document Current Environment
- Produce Reports for Use in Next Round of Evaluation
XYGATE Compliance PRO
Licensing and Product Support

• As an independent product, XYGATE Compliance PRO requires a license file to run on your system
• On J Series and H Series the product is sold “per CPU”
• On G Series the product is sold “per SYSTEM”
• If you are gathering data from multiple systems using Compliance PRO, a license must be purchased for each system.

• All product versions are supported by HP through the GCSC.
• Customers who’ve ordered the XYGATE Software Compliance Wizard from XYPRO directly in the past, need to work out support contract situations with the partner.
• HP is not a party to contracts held between customers and XYPRO.
XYGATE Compliance PRO
Security Services

We strongly recommend that customers who are new to Compliance PRO purchase a Service from HP to install, configure and train your staff on how to make best use of the product.

- Alternatively, if you’d rather not invest in Compliance PRO at this time, but need help around your server’s compliance status, a service can be provided that:
  - Uses Compliance PRO to analyze your system for compliance and security soundness
  - Provides you with a report and set of recommendations as to actions you should take to secure your NonStop server
XYGATE Compliance PRO

• Provides comparison with regulations (PCI, SOX, HIPAA) and best practices against your current NonStop Server environment

• Helps to assure consistency across multiple nodes

• Keeps you up to date with latest compliance regulation requirements

• Closes the loop
XYGATE Compliance PRO

More information

• A data sheet and more information about XYGATE Compliance PRO is now on our NonStop Security Compliance web page:

• Contact your sales rep for a quote

• Karen Copeland is the HP Product Manager for Compliance PRO.
  • [Karen.Copeland@hp.com](mailto:Karen.Copeland@hp.com)
Outcomes that matter.