CSP & PCI DSS Compliance on HPE NonStop systems

November 01, 2019

For more information about Computer Security Products Inc., contact us at:

30 Eglinton Ave., West
Suite 804
Mississauga, Ontario, Canada L5R 3E7
Tel: 904-568-8900
Fax: 905-568-8911
www.cspsecurity.com

The following are registered trademarks or service marks of HPE:

HPE NonStop
Guardian
NonStop OSS
Safeguard

Contents

Overview

The PCI DSS standard is now well established, both as a specific requirement for organizations that wish to handle credit and debit card information, and as a more general standard for computer system security.

The fundamental goal of PCI DSS is to mandate the protection of cardholder data from being stolen, inappropriately accessed or used.

Any organization that stores, processes or transmits payment card cardholder information must comply with all PCI DSS requirements. This compliance is the result of a formal annual assessment by a Qualified Security Assessor.

A PCI DSS assessment will typically include:

- Proof of system settings or configuration
- Documentation review
- A review of the record of related activities and changes
- Analysis of network traffic

This assessment will be carried out in relation to the location (storage points, process handling, application inputs and outputs, transaction histories etc.) of cardholder data on the system in question.

For more information on PCI DSS requirements and the assessment procedures, visit www.pcisecuritystandards.org.

Preparing for PCI DSS compliance on HPE NonStop

The first phase of the work required to meet these requirements is accomplished by creating and maintaining effective documentation of the how an organization intends to implement the appropriate protections on that system.

The second phase is concerned with how these protections are actually implemented. For example, how is password quality settings applied?

The third phase is concerned with the mechanisms that will be used to prove that the protections are effective, are not changed without appropriate authorizations, and that any unauthorized or unexpected changes are detected and managed.

For the HPE NonStop platform, the following steps will be required:

1. Identification of where cardholder information exists (processed, stored or transmitted).
2. Data protection mechanisms, including data file access controls and encryption.
3. Definitions of roles and responsibilities

4. System administrators and privileged userids
5. Security audit trails

This document is not intended as a guide for this process.

Third party solutions

It is generally accepted in the HPE NonStop community that PCI DSS compliance is not possible using native controls alone; additional controls must be created and deployed.

Such controls will include encryption software, auditing and change control packages, security management tools and related utilities.

CSP is one of the leading suppliers of solutions for PCI DSS compliance on HPE NonStop systems, and this document will describe how CSP technology can help organizations achieve and maintain compliance.

About Computer Security Products (CSP)

CSP has been developing security software for the NonStop® platform since 1989. CSP's products are widely used in the banking, telecommunications, medical and financial service industries.

CSP Product Suite

- **Auditview®** meets the need for flexible, coherent, focused reports from the complex SAFEGUARD® audit trails.
- **Verify Elite** is an audit compliance tool that ensures that your NonStop system security settings meet industry standards and regulations, including PCI/DSS, SOX and HIPAA. It includes a comprehensive set of security checks, which are categorized according to requirement or functional area, which can be modified for local requirements. **Verify Elite** also monitors specified files for changes to content, size, security and other attributes.
- **Alert-Plus®** is an on-line monitor of security events. It will respond to events as they are happening, notifying the appropriate personnel of a possible attack or initiating a programmatic response to the event.
- **Protect XP®** is a full-feature front-end to SAFEGUARD® that extends SAFEGUARD® protection rules into policies that apply to multiple objects and multiple groups of users.

- **CSP PassPort®** gives full command line capture and control for sensitive users and/or actions.
- **CSP NetPass** provides a unique solution for both enforcing password quality and for managing passwords across multiple HPE NonStop systems.
- **CSP Authenticator+** is a solution for authenticating logins to NonStop systems using various primary and secondary authentication methods.
- **Protect-X** is a highly automated browser based security hardening solution for HPE NonStop, NonStop X & Linux/Unix based servers

For more information about Computer Security Products Inc., contact us at:

30 Eglinton Ave West
Suite 804
Mississauga, Ontario, Canada L5R 3E7
Tel: 904-568-8900
Fax: 905-568-8911
www.cspsecurity.com

PCI DSS Requirement 1:
Install and maintain a firewall configuration to protect cardholder data

This requirement and its sub-requirements are typically addressed using network devices and software, and is not subject to controls and mechanisms on the NonStop platform.

CSP Solution:

Not applicable

PCI DSS Requirement 2:
Do not use vendor supplied defaults for system passwords and other security parameters

HPE NonStop systems are designed to be deployed by technicians and administrators, and therefore do not have strong defaults.

In this context, managing the initial system settings to a secure level represents a significant task.

While HPE provides a range of documents to guide the administrator, and there are several publications that lay out the industry standards in this respect, the native tools for implementing and then checking these settings are command line utilities, and these may be slow and difficult to use.

CSP Solution:

CSP products can help in two key areas:

***2.1** Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.*

> Using the **CSP Protect XP** advanced Safeguard and Security management interface, the administrator can quickly and effectively make the necessary changes.

2.2 *Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

Using **Verify Elite**, the administrator can run periodic checks to ensure that the settings have not diverged from the desired state. **Verify Elite** is populated with industry standard settings for key security parameters; these can be customized to match your local policy.

PCI DSS Requirement 3: Protect stored cardholder data

This requirement is primarily concerned with encrypting cardholder data that is stored anywhere on the HPE NonStop system. A range of third party solutions are available that provide encryption on HPE NonStop systems.

However, the administrator must ensure that the underlying objects – files, processes and devices – are also protected from misuse, and that the access rules that protect them match the policy definitions for roles and responsibilities.

CSP Solution:

CSP Protect XP (for Guardian) and **CSP Protect-X** provide a comprehensive framework for managing all object access rules.

Both products feature advanced GUI interfaces that:

1. Allow the administrator to view, manage and monitor object access rules individually or in bulk.

2. Provide a powerful access matrix policy visualization that applies corporate definitions of roles and responsibilities to object access rules.

Associated reports allow the administrator and auditor to monitor and validate that the object access rules match policy.

Since object access rules can be applied to processes, devices and other objects in addition to diskfiles, they are a key part of the protection of stored cardholder data, encryption routines and keys.

Verify Elite includes a range of checks on object security. This includes PROGID and LICENSE files, various configuration and other key system files. These checks can prevent "decay" of key object access rules, and again help prevent unauthorized access to cardholder data, encryption routines and keys.

PCI DSS Requirement 4: Encrypt transmission of cardholder data across open, public networks.

This requirement is met in a wider scope, which will include other connected systems and devices and possibly other organizations. As a result, there are no HPE NonStop specific responses.

CSP Solution:

Not applicable.

PCI DSS Requirement 5: Use and regularly update anti-virus software or programs

HPE NonStop systems are not generally known targets for malware, viruses or trojan horses. However, this does not remove the possibility of an intruder or internal attacker placing modified scripts, programs and utilities on the system.

As a result, system administrators need to take steps to ensure the integrity of all programs running on the system.

CSP Solution:

Verify Elite provides a simple mechanism for detecting and reporting any changes to specified files on the HPE NonStop system. This includes changes to the content (both static and incremental) and other file attributes (last modified, file size, security attributes etc.).

By ensuring that any change to a diskfile is found and reported, Verify Elite can help detect any unauthorized copies of a script, program or utility being loaded and run on the system.

PCI DSS Requirement 6: Develop and maintain secure systems and applications

This requirement is directed towards two areas of concern:

1. Ensuring that systems and applications are updated appropriately to take account of known security vulnerabilities and issues.

2. Ensuring that applications are developed and deployed using industry best practices.

These requirements are generally met with effective policies and procedures to stay abreast of any reported vulnerabilities and to deploy patches and recommended protective measures as needed.

CSP Solution:

An important aspect of this requirement is the need to implement effective change control processes and procedures:

> ***6.4*** *Follow change control processes and procedures for all changes to system components.*

CSP products support effective change control in a number of areas:

1. **Verify Elite** detects changes to static configuration changes and security settings, and also detects changes to specified files

2. **Auditview** generates reports from audit trails (Safeguard, BASE24 OMF, Verify Elite etc.) that can show changes to objects and settings.

3. **Alert-Plus** can generate alarms on audit and other changes

By providing an audit of system changes, CSP products ensure that any unauthorized changes will be detected and addressed.

PCI DSS Requirement 7: Restrict access to cardholder data by business need to know

This requirement mandates the principle of least privilege to guide how access controls should be applied. The point of departure for applying this principle is a fully documented policy that itemizes the roles, responsibilities, related activities, and the objects to be accessed.

This would then be applied on HPE NonStop systems in the two following areas:

User Session Control and Role-Based User Access

While Safeguard provides a range of authorization and authentication controls, additional controls are required to manage how users logon to TACL and/or OSH, and what privileged userids can then be used.

At the same time, once logged on, it is important to control what activities may then be carried out.

CSP Solution:

CSP PassPort provides complete user and command control, password quality enforcement and comprehensive auditing of terminal sessions running on HPE NonStop Servers.

PassPort filters user access to systems, programs and commands according to customized user profiles, and monitors and audits all user terminal input/output operations.

CSP PassPort complements Safeguard with additional security features, and, for systems without Safeguard, greatly expands the Guardian security package.

- Provides monitoring and auditing of user sessions down to keystroke level
- Enforces password quality standards
- Time restrictions by command and program
- Restricts users, including those with powerful Ids to authorized operations
- Restricts users to specific work stations, official functions and days/hours.

User Access Privileges:

HPE NonStop systems support granular access controls both in Safeguard and OSS and user access privileges can be set up as required. However, these permissions are readily modified with resulting "privilege creep', so careful monitoring is required to ensure that the policy is maintained.

In addition, the complexity of the resulting rules can make it hard to maintain "least privilege", with competing ACLs and wild card definitions creating an unmanageable setup up.

CSP Solution:

CSP ProtectXP provides a GUI interface to Safeguard object access control, and this simplifies the task of managing and maintaining user access privileges:

1. Setup and review Safeguard global object access controls
2. View and set individual types and instances for volumes, subvolumes, diskfiles and wildcard patterns.
3. Analyze and review settings for each object or by user or group
4. Find and correct common issues (orphan records etc.)

For OSS, **CSP Protect-X** provides similar functionality, allowing the administrator to effectively develop, manage and maintain file permissions as needed. Powerful analysis tools help prevent "privilege creep" and ensure "least privilege" is applied.

Both **Protect XP** and **Protect-X** also include a powerful access matrix feature that allows the administrator to develop user access privileges in terms of roles and resources.

With powerful graphical design tools, the policy can be developed, then linked to users and objects and then implemented. Policy variances can be easily detected and corrected to prevent unwarranted changes from preventing compliance.

PCI DSS Requirement 8:
Assign a unique ID to each person with computer access

In requiring that each individual who accesses the HPE NonStop system has a unique ID, PCI DSS mandates that all activities for that individual are entirely accountable.

A key corollary is that the logon method used can be trusted to prevent anyone but that individual using their user ID.

This implies the following:

1. Effective user ID management and maintenance.
2. Password controls on quality, change, encryption etc.
3. User ID revocation procedures
4. User session controls

Safeguard provides the basic controls but must be augmented in the following areas:

1. User management
2. Two-factor authentication (for example RSA SecurID) provides enhanced protection against userid abuse
3. Password quality enhancements to create stronger passwords.
4. User Session control

CSP Solution:

User Management:

CSP Protect XP provides a user-friendly management interface for managing userIDs on HPE NonStop systems. With automatic password generation, wizards to automatically assign user parameters, and mechanisms to cleanly remove users from systems, **Protect XP** improves efficiency and prevents common errors.

Multi-factor Authentication:

CSP Authenticator+ is a solution for authenticating logins to NonStop systems using various primary and secondary authentication methods:

- SecurID (RSA) tokens
- OpenLDAP, Active Directory
- RADIUS
- OTP via Email or SMS

- Google Authenticator

Password Quality Controls:

CSP NetPass provides a solution for both enforcing password quality and for managing passwords across multiple HPE NonStop systems.

Password quality is improved above Safeguard standards with a range of configurable constraints.

User Session Control:

CSP PassPort provides complete user and command control, password quality enforcement and comprehensive auditing for terminal sessions running on HPE NonStop Servers.

PassPort filters user access to systems, programs and commands according to customized user profiles, and monitors and audits all user terminal input/output operations.

PassPort complements Safeguard with additional security features, and, for systems without Safeguard, greatly expands the Guardian security package.

- Provide monitoring and auditing of user sessions down to keystroke level
- Enforce password quality standards
- Time restrictions by command and program
- Restrict users, including those with powerful Ids to authorized operations
- Restrict users to specific work stations, official functions and days/hours

PassPort supports the mapping of individual **PassPort** userIDs to shared Guardian privileged IDs, ensuring full audit and accountability.

PCI DSS Requirement 9: Restrict physical access to cardholder data

This requirement is not applicable to HPE NonStop systems and should be addressed separately.

PCI DSS Requirement 10:
Track and monitor all access to network resources and cardholder data

Requirement 10 refers to the writing, storage, management and reporting of auditable events.

For HPE NonStop systems, this is provided by the Safeguard audit trails.

Key steps in establishing an effective audit must include:

1. Review and set the appropriate audit flags in Safeguard for objects and users.
2. Ensure that storage, retention, and roll-over parameters meet local needs.
3. Review audit events and set up audit reports as required.

While Safeguard audit trails can generate the events, the native reporting tool is inadequate.

CSP Solutions:

Configuring Audit Trails:

CSP Protect XP provides an easy to use GUI interface to set and review the Safeguard audit settings.

Reporting from Audit Trails:

CSP Auditview is the premier audit trail report generator for Safeguard . **CSP Auditview** can be used interactively to search for and show particular events, and can also be set to run at intervals to automatically create audit reports.

Centralized SIEM (Security Information and Event Management):

CSP Alert-Plus can be used to generate alarms from Safeguard audit trail events and also to forward those events to a central server (HPE Arcsight, LogRhythm etc.) using syslog.

Keystroke Logging:

For specified activities and/or userids, **CSP PassPort** can provide a complete keystroke record of the user session. This provides complete accountability, beyond what the Safeguard audit trails can provide.

PCI DSS Requirement 11: Regularly test security systems and processes

The security of HPE NonStop systems and processes should be monitored continually for unexpected or unauthorized changes from policy. This would include changes to:

1. Configuration and system files
2. Safeguard global settings
3. Safeguard object access controls
4. Application configuration and data files

CSP Solutions:

CSP products support effective scheduled testing in a number of areas:

1. **Verify Elite**: detects changes to static configuration changes and security settings, and detects changes to specified files

2. **CSP Auditview**: generates reports from audit trails (Safeguard, BASE24 OMF, Verify Elite etc.) that can show changes to objects and settings.

3. **CSP Alert-Plus** – can generate alarms on audit and other changes

4. **CSP Protect XP** – changes to object access controls in Safeguard

5. **CSP Protect-X** – changes to object access controls in OSS

By providing an audit of system changes, CSP products ensure that any unauthorized changes will be detected and addressed.

PCI DSS Requirement 12: Maintain a policy that addresses information security for employees and contractors

While this requirement is fundamentally about the development of a documented security policy, a key consideration is how that policy will be translated and then implemented on to the target system.

CSP Solution:

CSP's products are designed to accomplish this task simply and effectively as follows:

PCI DSS Req.	Description	CSP Solution
12.2	*Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.*	**CSP Protect XP** and **Protect-X** can be used to manage all aspects of security as it relates to Safeguard, Guardian and OSS. Roles and responsibilities can be created and assigned to ensure that this requirement is met.
12.3.3	*A list of all such devices and personnel with access.*	**CSP Protect XP** and **Protect-X** can provide access matrices that easily show how access is configured for one, some or all users.
12.3.8	*Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.*	**CSP PassPort** user session controls can be configured to automatically disconnect sessions based on inactivity.
12.3.9	*Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.*	**CSP PassPort** can be configured to restrict access to particular terminals and listeners, thus controlling remote access to the system. Time limits can control access to only when needed.
12.5.4	*Verify that responsibility for administering user account and authentication management is formally assigned.*	**CSP Protect XP** can be configured to limit access to its functions, so that specified users can carry out only specified commands. For example, help desk staff can be limited to access only password resets and no other Safeguard activities.

Summary

PCI DSS requirements may be readily met on HPE NonStop systems, but only in conjunction with third party tools and technologies.

CSP products have been helping organizations secure their HPE NonStop systems for over 25 years and are thus well-placed to help those same organizations achieve formal PCI DSS compliance.

PCI Requirement	CSP Solution
1. Install and maintain a firewall	Not applicable
2. Do not use vendor supplied defaults	Protect XP Protect-X Verify Elite
3. Protect stored cardholder data	Protect XP Protect-X Verify Elite
4. Encrypt transmission of cardholder data	Not applicable
5. Use anti-virus software	Verify Elite
6. Develop and maintain secure systems and applications	Verify Elite Auditview Alert-Plus
7. Restrict access to cardholder data by business need to know	PassPort Protect XP Protect-X
8. Assign a unique ID to each person with computer access	Protect XP Authenticator+ NetPass PassPort
9. Restrict physical access to cardholder data	Not applicable
10. Track and monitor all access to network resources and cardholder data	Protect XP Auditview Alert-Plus PassPort
11. Regularly test security systems and processes	Verify Elite Auditview Alert-Plus ProtectXP Protect-X
12. Maintain a policy that addresses information security for employees and contractors	PassPort Protect XP Protect-X

