TAMUNIO
POWERED BY COMFORTE

Ebook

How to Achieve PCI DSS Compliance with TAMUNIO

A Guide for HPE Nonstop Users

This eBook was produced by:

comforte AG
Abraham-Lincoln-Strasse 22
65189 Wiesbaden
Germany

www.comforte.com

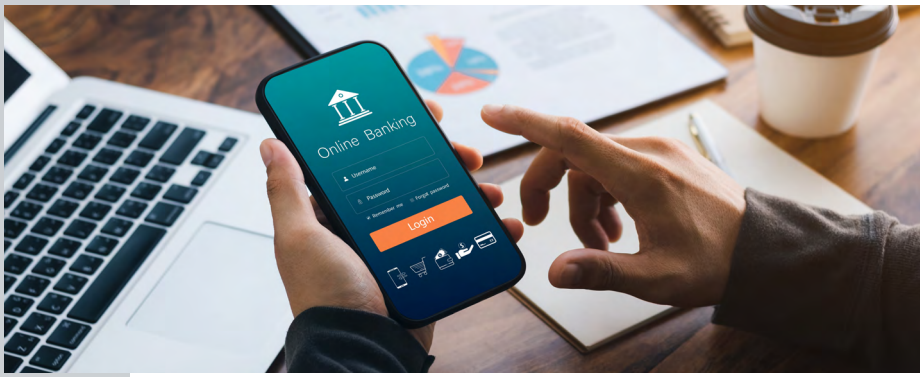
Document History: Document version 5.0
Issued November 2025

How to Achieve PCI DSS Compliance with TAMUNIO

A Guide for HPE Nonstop Users

This eBook provides an up-to-date view of PCI DSS v4.0 requirements and how they relate to HPE Nonstop environments. It explains which rules apply on HPE Nonstop, why, and how to turn them into practical action items. It then examines the most pressing challenges organizations face when implementing PCI DSS on HPE Nonstop and presents strategies to make these initiatives successful. Finally, it shows how TAMUNIO data security platform provides a unified way to deliver the controls and audit evidence HPE Nonstop teams need.

Table of Contents



Introduction to PCI DSS 4.0

The Payment Card Industry Data Security Standard (PCI DSS) governs the processing, storage, and transmission of cardholder data across merchants, processors, acquirers, issuers, and service providers. **PCI DSS v4.0** became fully effective in early 2025. The standard emphasizes continuous security, broader multi-factor authentication (MFA) across access into and within the cardholder data environment (CDE), annual scope confirmation, and rigorous cryptographic key lifecycle management.

Account data includes cardholder data (CHD), such as the primary account number (PAN), cardholder name, expiration date, and service code, and sensitive authentication data (SAD), including full track data, card verification data, and PIN/PIN block information. SAD must never be stored after authorization; if retained before authorization (e.g., in issuer flows), it must be strongly protected and tightly controlled.

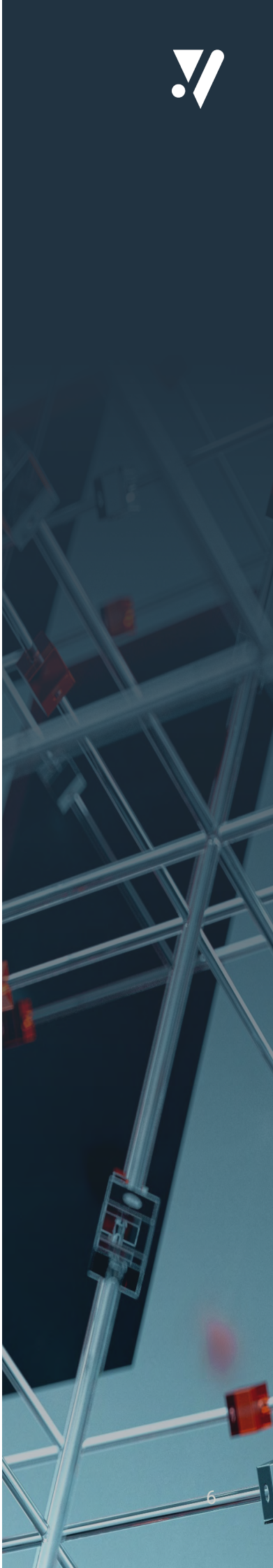
This eBook interprets those expectations for HPE Nonstop and shows how **TAMUNIO** provides a uniform way to implement controls and produce assessor-ready evidence.

Preface

Overview: How to read this eBook

This eBook presents a detailed view of how best to address PCI DSS requirements on the HPE Nonstop platform. It is organized into the following chapters:

Chapter	Contents
Executive Summary	If you don't have time to read more than a single page, this is for you.
Part 1: PCI requirements in HPE Nonstop environments	This section looks at the PCI DSS document, its 12 requirements, and how they specifically apply to the HPE Nonstop platform. It finishes with a list of 'action items' for a PCI compliant typical HPE Nonstop installation.
Part 2: Addressing action items in an HPE Nonstop environment	This chapter discusses each action item from the previous chapter and how it can be implemented on the HPE Nonstop platform.
Part 3: How TAMUNIO can help	This is the only part of this eBook which is not vendor-agnostic. It describes how various capabilities of the TAMUNIO platform can address the action items outlined in Part 1.
About comforte	A brief introduction to comforte, the company.



Executive Summary

Over the past few years, cybercriminals have created an entire industry around the theft of credit card information. These criminals are well organized, very sophisticated and highly effective, to the extent that now there are groups focused on specific aspects, such as the theft, sale, or use of sensitive cardholder information.

The growing market for stolen card numbers has put the industry on high alert, and the PCI standard represents an effort to curb crimes involving credit cards. While PCI DSS may seem challenging to implement, it does represent best practices in information security and, as such, is a very useful guideline in improving the security of payment data.

The HPE Nonstop platform has always been and still is a secure platform by nature and is not known for the type of security issues that affect other platforms, such as viruses or malware. Putting effort into those areas of PCI DSS that do pertain to HPE Nonstop environments, such as the topics discussed in this eBook, can help ensure that HPE Nonstop systems not only pass PCI audits but also achieve the highest possible level of security.

In comforte's experience, the following steps should be taken, in the order below, to help achieve PCI compliance:

- Identify all files containing Account Data (CHD/SAD)
- Encrypt network traffic using strong, standardized cryptography
- Implement secure coding practices appropriate to your stack
- Manage access control and auditing (least privilege, SSO and MFA, centralized logs/FIM)
- Encrypt backup tapes and sensitive files
- Render PAN unreadable in databases (tokenization/FPE, key management)

The rationale for this list and order can be found in Part 1 of this eBook, considerations on how to proceed in general in Part 2 and specific TAMUNIO support is summarized in Part 3. Please note that your PCI auditor might have a different view on steps to be taken and its priorities – so please do talk with your auditor about this.

Part 3 is the only part of this eBook that is not vendor-agnostic.

Part 1: PCI Requirements in HPE Nonstop Environments

The ongoing challenge of PCI

The Payment Card Industry Data Security Standard (PCI DSS) is by no means new. However, the process of being audited and achieving compliance still represents a significant challenge for many organizations today. Initially unveiled in late 2004, PCI represented the first common security standard under which all the individual security policies of credit card issuers would be aligned - meaning that merchants, processors, and financial institutions would be assessed according to a single standard.

PCI compliance remains an important priority for many organizations today. Studies show that initiatives for achieving PCI compliance are not trivial, with costs that can reach as much as several million dollars. What's more, most organizations launch such an initiative with entirely different expectations in terms of cost than they experience during execution. This is often because these PCI initiatives are the first made by an organization, which can make accurate planning and budgeting difficult.

This discrepancy is also partly due to some fundamental challenges organizations encounter when applying some of the 12 PCI standards.

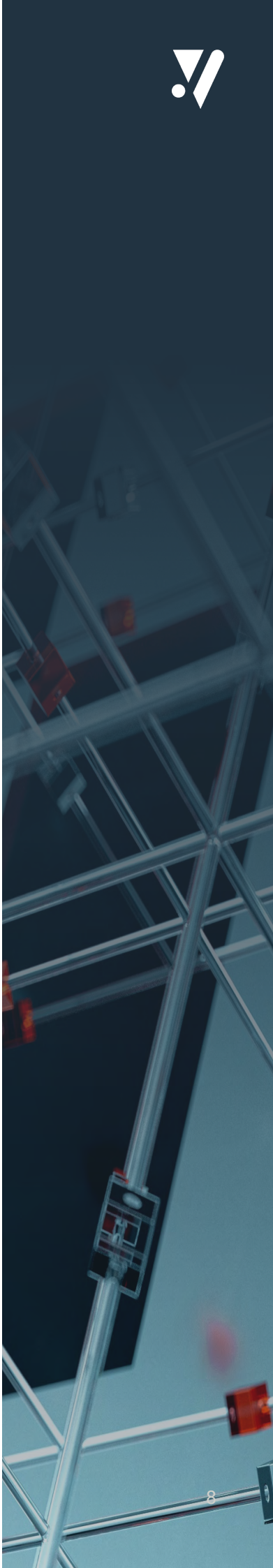
The nature of the PCI auditing process

PCI is not a one-time project with a long list of 'check-box' items, which all need to be addressed, checked off, and forgotten. It's a repeatable process that must reflect new threats, systems, and data flows. Budgets and timelines often slip because scope and evidence are underestimated. The renowned security expert Bruce Schneier[1] states, 'Security is a process, not a product' and this applies to the PCI auditing process as well:

- The audits will be repeated annually.
- Unfinished items from this year will be back on the table next year.
- Many requirements go beyond deploying a single product or security measure and instead demand ongoing operational attention, such as maintaining logs, file integrity monitoring (FIM), cryptographic key rotation, and regular access reviews.

Therefore, the PCI DSS requirements should be treated as an ongoing process to continuously improve your security posture. The PCI DSS document includes a section 'Best Practices for Implementing PCI DSS into 'Business-as-usual Processes' (BAU), which outlines specific activities that should become part of daily operations.

[1] See http://en.wikipedia.org/wiki/Bruce_schneier



How PCI relates to HPE Nonstop environments

Getting started: Where is my critical data?

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card data processing - including merchants, processors, acquirers, issuers, and other service providers.

Account data includes:

- **Cardholder data (CHD)** – Primary Account Number (PAN), cardholder name, expiration date, and service code.
- **Sensitive authentication data (SAD)** - Full track data (magnetic-stripe or equivalent on a chip), card verification code (CVC/CVV), and PIN or PIN block.

The 'Scope of PCI DSS Requirements' section within the PCI DSS Document describes an initial scoping of the audit. This includes finding all relevant network devices, servers, computing devices, virtual components, cloud components, and software.

The following excerpts from the PCI DSS describe the expectations for scoping and annual scope confirmation under Requirement 12.5.2:

> *The first step in preparing for a PCI DSS assessment is for the entity to accurately **determine the scope of the review**. The assessed entity must confirm the accuracy of their PCI DSS scope according to PCI DSS Requirement 12.5.2 by **identifying all locations and flows of account data**, and identifying all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers, remote access servers, logging servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered during the scoping process, including backup/recovery sites and fail-over systems.*

> *The minimum steps for an entity to confirm the accuracy of its PCI DSS scope are **specified in PCI DSS Requirement 12.5.2.** The entity is expected to retain documentation to show how PCI DSS scope was determined. The documentation is retained for assessor review and reference during the entity's next PCI DSS scope confirmation activity. For each PCI DSS assessment, the assessor validates that the entity accurately defined and documented the scope of the assessment.*

Note: *This annual confirmation of PCI DSS scope is defined at PCI DSS Requirement 12.5.2 and is an activity expected to be performed by the entity. This activity is not the same as, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the assessment.*

Consequently, the very first step of a PCI project should be a **'data discovery'** phase that clarifies exactly where critical data resides on your HPE Nonstop systems. The output should be a complete list of static as well as temporary files containing account data.

The 12 requirements of PCI – an overview

The PCI standard represents a comprehensive picture of all the facets required to secure payment information. Falling short in any of these areas can present significant and sometimes severe consequences. So, in that sense, all these requirements are essential, especially when it comes to enterprise-wide security measures.

However, the standard consists of about 250 'line items' and for this reason, we will prioritize and categorize the sections here. The following table lists each of the 12 sections and adds two extra columns as follows:

The "Applicability" column describes relevance to the HPE Nonstop environment from comforte's perspective:

- **[non-Nonstop]**

Those rules marked with [non-Nonstop] are relevant to HPE Nonstop environments but are typically controlled by different parts of the organization rather than by the Nonstop group. A good example for this group is the requirement for firewalls: they are critical to properly secure the HPE Nonstop platform but typically 'owned' by the networking group.

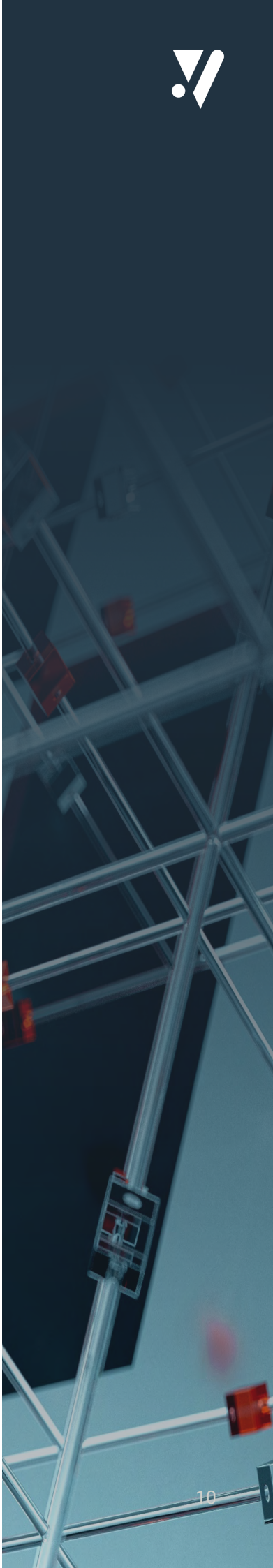
- **[FocusArea]**

The requirements marked with [FocusArea] are relevant and controlled by the HPE Nonstop group and thus will be the focus of this paper.

- **[n/a]**

Those rules marked with [n/a] generally don't apply directly to HPE Nonstop platforms.

The 'Milestone' column summarizes the information from the document *PCI Security Standards Prioritized Approach for PCI DSS 4.0* – available at: https://www.pcisecuritystandards.org/document_library.



This document gives some guidance as to which of the 250 line items should be addressed in which order/priority.[2]

Requirement	Applicability to Nonstop platform	Milestones according to PCI council (1=early, 6 =late)
1: Install and maintain network security controls	**[non-Nonstop]**	1 (network and data-flow diagram) 2 (network security controls configured and maintained, network access to/from CDE is restricted) 6 (security policies, roles and responsibilities)
2: Apply secure configurations to all system components	**[FocusArea]**	2 (system components configured and managed securely) 6 (processes and mechanisms for secure configurations)
3: Protect stored account data	**[FocusArea]**	1 (minimize storage of account data; SAD not stored after authorization) 5 (PAN is rendered unreadable anywhere it is stored; strong cryptography, e.g. tokens) 6 (processes and mechanisms for protecting stored account data)
4: Protect cardholder data with strong cryptography during transmission over open, public networks	**[FocusArea]**	2 (PAN is protected with strong cryptography during transmission) 6 (security policies, roles and responsibilities)
5: Protect all systems and networks from malicious software	**[n/a]**	2 (prevent, detect, address malware; protect against phishing attacks) 6 (security policies, roles and responsibilities)
6: Develop and maintain secure systems and software	**[FocusArea]**	3 (develop bespoke and custom software securely - secure coding) 6 (security policies, roles and responsibilities)
7: Restrict access to system components and cardholder data by business need to know	**[FocusArea]**	4 (Define/assign access to system components and data; manage access via access control system) 6 (security policies, roles and responsibilities)
8: Identify users and authenticate access to system components.	**[FocusArea]**	2 (manage user ID and accounts throughout an account's lifecycle; strong authentication for users and administrators; use multi-factor authentication (MFA) to secure access into the CDE)) 4 (strictly manage use of application and system accounts and auth factors; protect passwords/passphrases against misuse)
9: Restrict physical access to cardholder data	**[non-Nonstop]**	1 (destroy hard-copy and electronic media materials with cardholder data) 2 (restrict physical access to CDE) 5 (authorize/manage physical access for personnel and visitors)
10: Log and monitor all access to system components and cardholder data	**[FocusArea]**	4 (use audit logs to detect anomalies and suspicious activity
11: Test security systems and networks regularly	**[FocusArea]**	2 (network scans, penetration testing, IDS) 4 (File integrity monitoring, detection of unauthorized WANs)
12: Support information security with organizational policies and programs	**[non-Nonstop]**	1 (document PCI DSS scope annually) 2 (identify/analyse risks to the CDE; document /validate PCI DSS scope) 6 (establish/maintain overall information security policy; roles and responsibilities; manage PCI DSS compliance)

[2] However, it should be noted that eventually, all items from the standard will need to be addressed – the prioritized approach was made available to help get started with any PCI project. For full details of the Prioritised Approach, please refer to the 'Prioritized approach for PCI DSS 4.0' document.

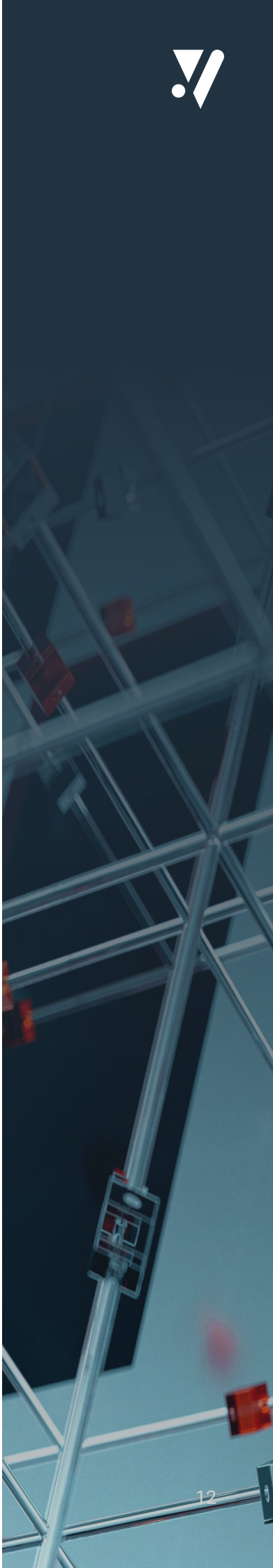
Translating the PCI DSS requirements into action items

For security administrators of HPE Nonstop environments, the challenges of adhering to the PCI DSS requirements outlined in the previous sections can be grouped into the following six action areas:

1. Identify all files containing PAN data
2. Encrypt network traffic
3. Secure coding
4. Manage access control and auditing
5. Encrypt backup tapes
6. Encrypt database data

Please note that your PCI auditor might have a different view on the steps to be taken and priorities - so please talk to your auditor about this.

This white paper will explore each of these areas in detail, outlining the relevant PCI standards, how they apply to HPE Nonstop environments, and why they are important or sometimes challenging to implement.



Part 2: Addressing Action Items in HPE Nonstop Environments

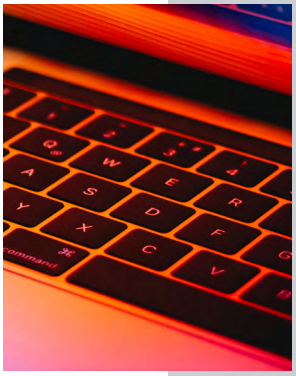
Identifying files with PAN data

At first glance, this may seem like a straightforward task: simply creating a list of all critical files. However, deeper investigation quickly reveals that the process is far from simple.

- If a **manual process** is used (based on knowledge about the system and the applications on it), the following issues arise:
  - An auditor may require formal proof beyond statements such as "We know our system" to confirm that the file inventory is complete.
  - Batch processes or system administrators may create file copies for various operational reasons. If these copies are not deleted, sensitive data could remain on the system in unsecured locations.

- Attempting to **automate the discovery process** through a global search also poses challenges:
  - The search pattern for PANs must be flexible enough to detect all valid formats while minimizing false positives.
  - Any search operation must be non-intrusive and must not negatively impact CPU utilization or system performance.
  - The output of the search must be masked or sanitized; otherwise, the search results themselves could expose sensitive data and become a compliance issue.

- PAN data can also exist in unexpected places such as SCF trace files or transaction logs that have been copied for troubleshooting or support. In some cases, even production files are copied onto development systems (which is in clear violation of PCI DSS).



Encrypting non-console admin access and protecting sensitive authentication data (SAD)

PCI DSS requires that all **non-console administrative access** be secured using **strong encryption**, and that any sensitive authentication data (SAD) transmitted or stored before authorization be protected to prevent unauthorized disclosure.

In practice, this means that Telnet, FTP, or any other protocol that sends credentials or data in clear text must not be used on HPE Nonstop systems. All such connections must use secure, strongly encrypted protocols such as **SSH, TLS, or other mechanisms** that meet PCI DSS requirements for strong cryptography. Likewise, any sensitive data must be protected using **strong encryption** or approved techniques such as **format-preserving tokenization**, supported by secure generation, storage, rotation, and retirement of the cryptographic keys that protect it **(Requirement 3.7).**

PCI 4.0 Requirement	Description	Mechanism	TAMUNIO Capabilities
2.2.7	All non-console admin access is encrypted using strong cryptography	Use TAMUNIO to secure all non-console connections with TLS or SSH. Client and emulator software must also support secure protocols. Certificate and key lifecycle management are handled centrally by TAMUNIO's Nonstop KMS.	TAMUNIO (Network Encryption & Access Management) and Nonstop KMS
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	Use TAMUNIO data protection services to safeguard all sensitive data through format-preserving tokenization. Archived or backup data can be secured using file or tape encryption.	TAMUNIO (Data Protection Services)
3.3.3	Additional requirement for issuers and companies that support issuing services and store sensitive authentication data. Any storage of sensitive authentication data is minimal and protected with strong encryption.	Apply TAMUNIO tokenization or encryption to protect stored SAD. Ensure encryption keys are rotated and managed centrally under TAMUNIO's Nonstop KMS, and retention policies enforce timely deletion after authorization.	TAMUNIO (Data Protection Services)

Implementing encryption for **Telnet, file transfer**, or **middleware traffic** is generally straightforward in HPE Nonstop environments. It comes down to selecting among several commercial products available and putting one of them into production.

There are two widely used encryption protocols for securing network traffic:

- **TLS (Transport Layer Security)** is a widely deployed protocol that evolved from **SSL (Secure Sockets Layer)**, originally developed to secure HTTP traffic on the web. It has been in broad use since the early 2000s for encrypted file transfers and secure transactions. TLS is a natural fit for file transfer with IBM mainframes, 6530 Telnet, and protocols such as ODBC or EXPAND.
- Having its origins in development in UNIX environments, **SSH (Secure Shell)** is a natural fit for communication with UNIX systems, which usually have OpenSSH installed by defualt. Furthermore, there are several commercial products available for SSH. SSH was chosen by HPE as the standard for HPE Nonstop Console Telnet/FTP encryption.

Deciding on which of the two protocols to choose is not a trivial issue. Both are undoubtedly effective and, depending on corporate security policies and environment specifics in place, some administrators opt to implement both.

The following are some questions to help in making this decision:

- Is there a corporate security policy in place recommending one over the other?
- Which other systems in the data center does the HPE Nonstop system need to communicate with? Which protocol is supported on these systems?
- For Telnet: Which emulation client(s) are in use? Which protocol does it support?
- Do you want to utilize Kerberos to leverage your domain authentication as part of your HPE Nonstop authentication? If so, SSH is typically preferred.
- Do you need PKI certificate-based authentication? If so, TLS is normally the preferred choice.

Encrypting ATM and POS network traffic can be more complex than securing Telnet because of high connection volumes and transaction rates. TLS 1.2 or higher is the standard protocol for such environments in most deployments. These channels are protected in transit by TLS, while any card data written to files or databases remains encrypted or tokenized at rest.

Secure coding

The part of the PCI standard that talks about secure coding **(Requirement 6)** keeps in mind applications that face the internet, use a web server, and use SQL as a database engine. In many instances, this will not apply to your HPE Nonstop environment, but we recommend that some thought is given to 'secure coding best practices'. The topic of secure coding goes well beyond the scope and intent of this eBook, however, here is a quick summary of what secure coding is about and how it may be implemented:

- The risks of not following best practices include but are not limited to:
  - Application crashes or excessive resource use when given malformed or malicious input.
  - Unauthorized access to or deletion of application data due to invalid or malicious input (e.g., SQL injection attacks).

- Secure coding is best achieved through **developer training, code review**, and **ongoing awareness**. Specialized products can also support **code quality assessment, vulnerability scanning,** and **penetration testing** for existing applications.

Managing Access Control and Auditing

As shown in the following table, access control and auditing are addressed in several areas of the PCI standard:

Requirement	Description of action items
7	Restrict access to system components and cardholder data by business need to know.
8	Identify users and authenticate access to system components.
10	Log and monitor all access to system components and cardholder data.
11	Implement file integrity monitoring (FIM) and intrusion detection.
12	Maintain an information security policy.

These requirements comprise a whole range of technologies that need to be implemented; therefore, there is no product available that will easily implement all requirements set forth by the standard.

However, there is a range of commercial products available which can be grouped into the following categories:

- **Safeguard (delivered as part of the operating system by HPE)**

  Safeguard implements several vital functions such as password rules, password expiration, the configuration of ACLs (Access Control Lists), and the creation of audit logs. For J and L-Series systems Safeguard is part of the core Operating System at no extra cost.

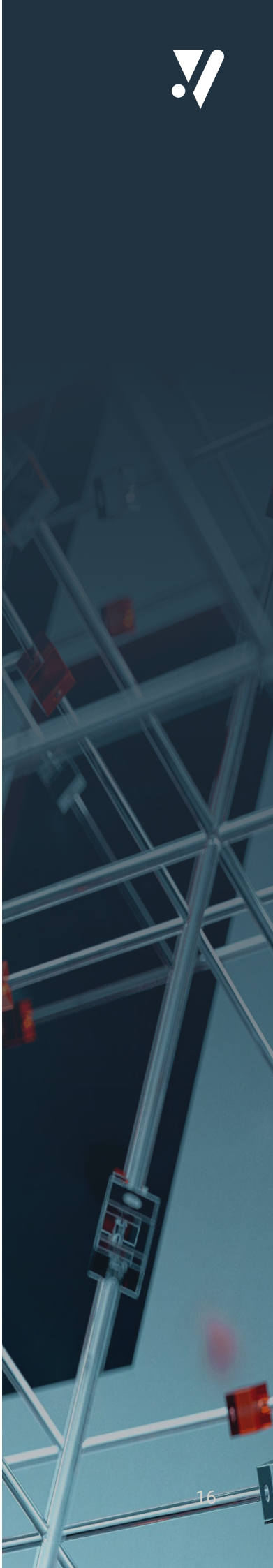
- **Configuration and management tools**

  Tools, which will process the Safeguard audit trails, provide real-time alerting, and send the logs to a central SIEM (security information and event management) device.

- **File integrity monitoring (FIM) tools**

  Tools, which provide more granular access control than TACL and Safeguard. Using the right combination of products[3] will go a long way towards achieving compliance.

[3] As mentioned earlier, 'using' should not be misread as only purchasing and implementing a product; typically, the product needs to be used on an ongoing basis to improve security.



Encrypting Data on Backup Tapes

There will be very few HPE Nonstop users who do not regularly run backup jobs. As mentioned above, **Requirement 3.5** applies to wherever account information is stored, including backup media.

The loss of backup tapes represented some of the more high-profile breaches in recent years. This is a very significant exposure, particularly because there are inexpensive, readily available hardware devices that can be used to read data on tapes, even those used on HPE Nonstop systems. As a result, if backup tapes contain payment data, they must be encrypted. This is especially true if tapes are ever transported outside of an organization's offices.

Several vendors offer products that are straightforward to deploy. At a high level, there are two types of solutions available for encrypting backup media: hardware- and software-based solutions. The following is an overview of the strengths these two options offer:

- **Hardware-based solutions** operate transparently within existing environments, with minimal impact on backup or restore performance. They store encryption keys securely on the appliance itself, offering stronger protection than software solutions that keep keys on the same system as the database.
- **Software-based solutions** have the benefit of being easy to install, test, and maintain as there isn't the requirement of adding a new hardware appliance to the infrastructure. In addition, they tend to be less expensive than hardware-based alternatives.

Database Encryption

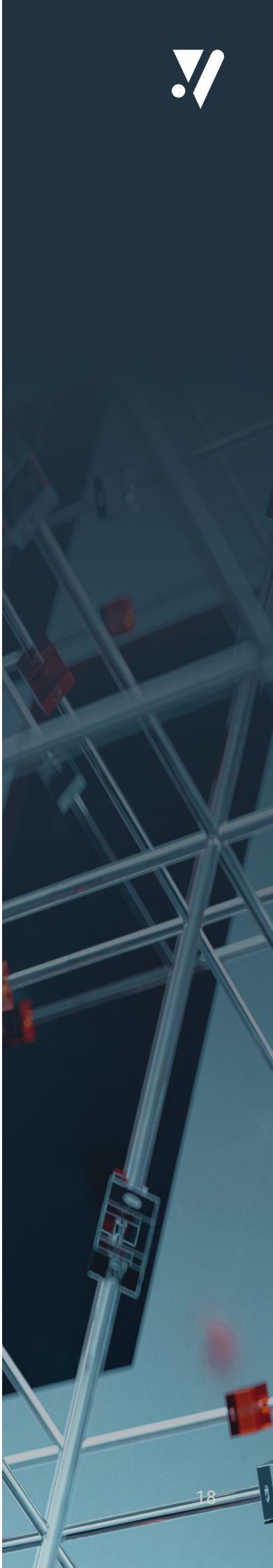
In virtually every enterprise, databases represent a critical aggregation pool of sensitive information. This also holds true in HPE Nonstop environments. Many of the PCI DSS requirements seek to address this crucial aspect within the infrastructure, specifying what can be stored in databases, what cannot be stored, and what needs to be protected when stored.

The following table is taken directly from the PCI standard. It classifies which data can be stored and how. Some data elements (such as the full magnetic stripe) simply cannot be stored at all, and hence encryption becomes a non-issue. Some other data elements (such as the cardholder name) may be saved but do not need to be protected by encryption. However, the primary account number (PAN) always has to be protected by encryption mechanisms.

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.5.1
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No (unless stored with PAN)
		Service Code	Yes	No (unless stored with PAN)
		Expiration Date	Yes	No (unless stored with PAN)
	Sensitive Authentication Data	Full Track Data (Magnetic Stripe or Chip)	No	Must never be stored per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Must never be stored per Requirement 3.2
		PIN/PIN Block	No	Must never be stored per Requirement 3.2

As shown in the following table, Access Control and Auditing are addressed in several places within the PCI DSS document:

PCI DSS Rule	PCI Text
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: ▶ One-way hashes based on strong cryptography of the entire PAN. ▶ Truncation (hashing cannot be used to replace the truncated segment of PAN) • If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. ▶ Index tokens. ▶ Strong cryptography with associated key-management processes and procedures.
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.



While encryption in databases can be challenging in any environment, it is particularly so in HPE Nonstop environments. Here are two key reasons why:

- **Database and application complexity**. In the HPE Nonstop environment, there are three databases available: ENSCRIBE, SQL/MP, and SQL/MX. Each of these databases may be accessed by a range of applications and any number of programming languages. This complexity presents inherent challenges in terms of how encryption is implemented. For example, many solutions that work for one programming language or application may not work for another.
- **SQL/MP and older versions of SQL/MX** lack such features as triggers, views, and C-based user functions that enable users or vendors to make encryption transparent to applications. For many organizations, this creates downstream implications: any associated applications accessing the database ultimately need to be retrofitted to accommodate encrypted data.

In addition to that, several challenges pertain to database encryption in just about any environment, and those also apply to HPE Nonstop servers. The following are just a few examples:

- **Key management:** PCI rules include the requirement for ongoing key rotation, secure key storage, the revocation of compromised keys, and more. For many organizations – especially those with multiple, disparate repositories of cryptographic keys – taking care of these requirements is extraordinarily complicated and time-consuming.
- **Searchability**: Another issue is that once account numbers are encrypted, how can users search for that information? Without the proper capabilities, this would require an entire database file to get decrypted, then searched, and then the data would need to be encrypted again. This is an unworkable scenario for most organizations.
- **Application architecture:** Very often, the application has been written a long time ago and does not provide a 'database access layer' where encryption/decryption functionality can be added easily.

In designing a strategy for database encryption in HPE Nonstop environments, here are some key points to consider:

- Start with a simple **assessment of associated applications**: How many applications need to be converted? How many database APIs are in use?
- Several vendors provide packages which help to encrypt and decrypt a field by a simple API call, rather than a lengthy programming project. Note that the real quality of a **cryptographic API** is in how the product protects keys, handles key management, and cross-platform requirements.
    - When looking at a product that implements an encryption API, one major factor to consider is whether key management has to be managed by the application using the API or whether the product itself allows key management without the application being aware of it. The latter approach is much preferable.
- If an application already has a **'database access layer'**, only a few code changes may be required. If not, administrators may want to consider providing a 'crypto service'. This would take the form of an internal library or PATHWAY server, which then should be leveraged by all associated applications.
- Finally, it may be worthwhile obtaining some help from **companies specializing in database encryption**. These companies should have proven experience in dealing with the challenges mentioned above.

Part 3: How TAMUNIO Can Help

Overview

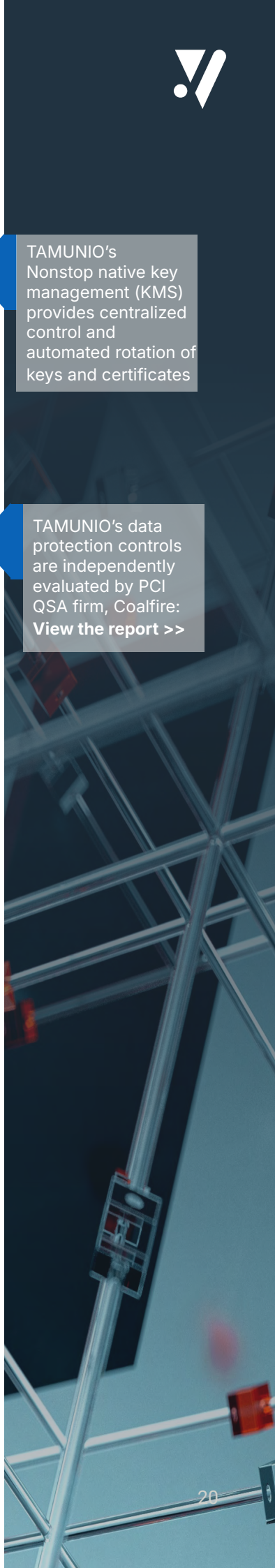
TAMUNIO offers a broad range of capabilities that may help organizations to ensure that all sensitive payment data is protected, both **in transit** and **at rest,** with **centralized key management** ensuring consistent encryption policy enforcement across all components. The following provides an overview of TAMUNIO packages which will be addressed in more detail later in this section, organized by the same grouping of functionality as used in Part 2 of this eBook.

TAMUNIO's Nonstop native key management (KMS) provides centralized control and automated rotation of keys and certificates

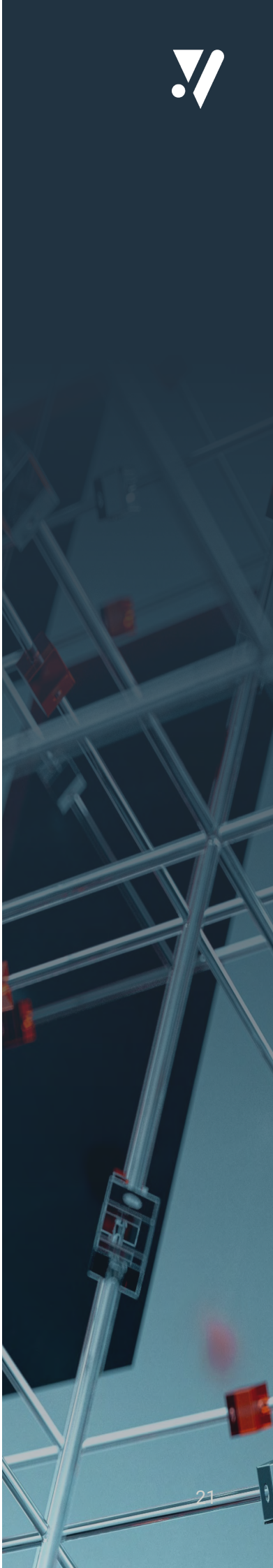
Package Name	Brief Description
TAMUNIO Protect	Secures data at rest through format-preserving tokenization, and file or tape encryption for Enscribe, SQL/MP, and SQL/MX.
TAMUNIO Govern	Centralizes monitoring, audit logging, and privileged activity tracking for full visibility and simplified PCI DSS reporting.
TAMUNIO Transit	Protects data in motion using TLS-based encryption for middleware, APIs, and client/server traffic, ideal for ATM, POS, and other payment networks.
TAMUNIO Transform	Extends secure integration and encryption to HPE Nonstop APIs and services, keeping modernized workloads compliant across hybrid environments.
TAMUNIO Access	Provides secure, centrally managed terminal and console access for HPE Nonstop, with TLS-encrypted sessions, operator oversight, and detailed session logging for compliance.

TAMUNIO's data protection controls are independently evaluated by PCI QSA firm, Coalfire: **View the report >>**

Third-party independent assessment found that TAMUNIO's **data protection and discovery** controls align with PCI DSS v4.0 expectations for protecting stored account data, logging, and scope validation, helping reduce compliance risk while streamlining reporting.



PCI 4.0 Requirement	Description	Mechanism	TAMUNIO Package
1.3.1, 1.4.2	Restrict inbound traffic from untrusted networks.	Use HPE Nonstop firewalls and ACLs for inbound traffic control. TAMUNIO enforces TLS/SSH policies and can act as a security gateway for encrypted session termination.	Transit, Access
2.2.7	All non-console admin access is encrypted using strong cryptography.	TAMUNIO supports securing HPE NonStop administrative and terminal sessions with industry-standard TLS 1.2/1.3 and SSH v2, integrating with enterprise SSO and MFA to provide authenticated, encrypted access across GUI and terminal interfaces.	Access
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	TAMUNIO protects all sensitive data using format-preserving tokenization. It also protects archived data stored on tape.	Protect
3.3.3	Additional requirement for issuers storing authentication data, must remain minimal and protected with strong encryption.	TAMUNIO protects all sensitive data using format-preserving tokenization.	Protect
3.4	Access to displays of full Primary account numbers (PAN) and ability to copy PAN is restricted.	Use TAMUNIO for tokenization and role-based masking of PAN data. Discover and classify PANs using integrated discovery tools within the platform.	Protect
3.5	PAN is secured wherever it is stored.	TAMUNIO protects all sensitive data using format-preserving tokenisation. Masking and role-dependent display can be configured. Can also protect data as it is archived.	Protect
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	Use TAMUNIO to enforce TLS/SSH for all non-console connections. Ensure corresponding clients/ emulators support secure protocols. Manage certificates/keys centrally with Nonstop-native KMS (auto-renewal, inventory).	Transit



PCI 4.0 Requirement	Description	Mechanism	TAMUNIO Packages
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	TAMUNIO's Unified Monitoring & Auditing can run file-integrity monitoring (FIM) on key files and capture post-change evidence/ reports.	Govern
7.3	Access to system components and data is managed via an access control system(s).	TAMUNIO enforces fine-grained, role-based access to SAD and ensure that all access events are captured through combined auditing for full traceability.	Govern + Protect
8	Identify Users and Authenticate Access to System Components	Integrate SSO + MFA through TAMUNIO with HPE Nonstop access patterns (e.g., SSH/Pathway).	Govern
8.4, 8.5	Use MFA as an additional layer of authentication.	Implement TAMUNIO MFA for all access into/within the CDE; store one-time password secrets and related keys in the HPE Nonstop-native KMS.	Govern + HPE Nonstop-native KMS / MFA
10	Log and Monitor All Access to System Components and Cardholder Data	TAMUNIO aggregates logs from HPE NonStop sources (Safeguard, SSH, TLS services, consoles etc.) and forwards them to an enterprise SIEM for centralized analysis and alerting.	Govern (with Unified Monitoring & Auditing)
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools).	Use TAMUNIO's FIM to track and detect changes in critical files and log stores, with alerting and retention.	Govern (with Unified Monitoring & Auditing)

Obtaining a list of all files containing PAN data

As mentioned in Chapter 'Part 2: Addressing Action Items in HPE Nonstop Environments', obtaining this information is non-trivial when done manually, and doing an automatic search is not easy either.

Discovery of unmasked or unencrypted PAN data on HPE Nonstop can be performed using platform-specific discovery tools. These findings can be incorporated into TAMUNIO's broader compliance processes to support PCI DSS scope confirmation and ongoing evidence collection.

Encrypting telnet, file transfer, middleware traffic, or ATM/POS traffic

To find out which best fits your environment, please visit the comforte website or contact a comforte representative.

TAMUNIO provides a unified set of capabilities that make complying with these PCI DSS rules straightforward and cost-effective while significantly strengthening the security of non-console administrative access in HPE Nonstop environments.

- All HPE Nonstop file transfers and session traffic are secured using industry-standard TLS and SSH protocols.
- File transfers are protected through built-in SFTP/SSH and TLS/SSL options, ensuring that data exchanged with HPE Nonstop systems remains encrypted end-to-end.
- Middleware and application traffic are encrypted transparently, extending TLS/SSL protection to client/server communications and Telnet (TN6530) sessions between emulators and TELSERV processes.
- Terminal and console access are hardened through secure Telnet and SSH connections that combine authentication, access control, and encryption in a unified framework.
- Existing TCP/IP socket applications can be TLS-enabled with minimal change, making this approach ideal for protecting ATM and POS network traffic.

In addition, TAMUNIO generates detailed audit log information for tracking and verifying system access. These logs support the evidence requirements in **Section 10** of the PCI DSS.

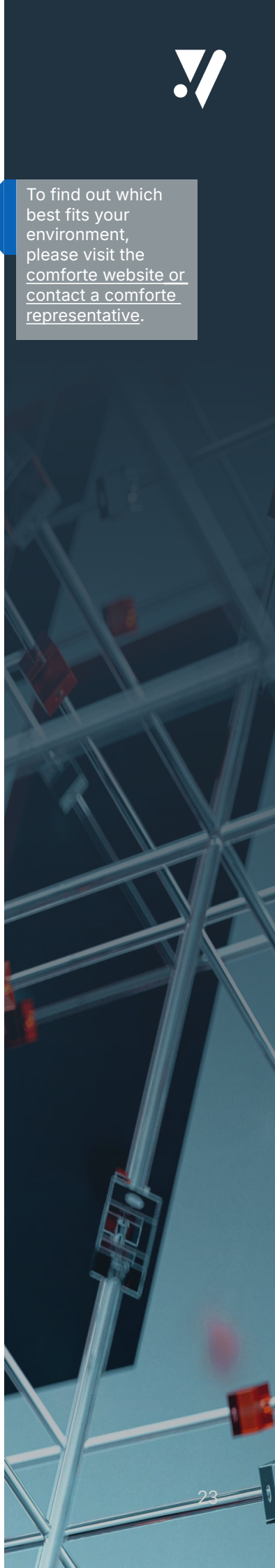
Secure coding

As briefly discussed in Part 2 of this eBook, this matter is more of an educational issue. Comforte has no products in the area of 'application penetration testing'.

Managing security configuration, access control, and auditing

TAMUNIO provides an intuitive, centralized interface that enables administrators to manage Safeguard security and other HPE Nonstop security subsystems more efficiently and effectively. Administrators gain a single solution for managing, monitoring, and reporting on multiple HPE Nonstop systems, delivering significant time and cost savings.

TAMUNIO's Unified Monitoring & Auditing allows administrators to configure alarms that are triggered based on a wide range of security and operational events. These events can originate from Safeguard, BOSS, EMS, OSS, and client systems. You can forward this data to central SIEM platforms for real-time alerting and audit correlation. Integrated keystroke logging enables the monitoring and reporting of commands entered by users, providing transparent accountability and helping address key requirements in Section 10 of the PCI standard.



Single sign-on and multi-factor authentication (MFA)

TAMUNIO provides full integration of the HPE Nonstop platform with enterprise identity providers, such as Microsoft Active Directory, through industry-standard authentication protocols.

Once deployed, users authenticated on their Windows desktop or enterprise SSO environment can access the HPE Nonstop platform without separate credentials.
This eliminates local password management, streamlines administration, and ensures that Nonstop is fully integrated into corporate identity workflows.

In addition, TAMUNIO's MFA capability enables compliance with PCI DSS v4.0 **Requirement 8** by enforcing robust multi-factor authentication across access points including SSH, Pathway, and console sessions.

Secure telnet and terminal access

Beyond encrypting Telnet traffic, TAMUNIO Transit provides advanced authentication and auditing for terminal and emulator connections. When paired with compliant emulators, Transit can log detailed session metadata, such as:

- Logged-in Windows username
- Workstation name
- Local IP address, even behind NAT (Network Address Translation)

Encrypting data on backup tapes

In nearly every HPE Nonstop environment, administrators regularly run backup jobs. PCI DSS requires that any media containing account data (including physical tapes and virtual tape archives) be protected with strong encryption and managed under a controlled key-management process to ensure that cardholder information remains unreadable and secure.

With TAMUNIO, organizations gain a robust tokenization/encryption solution that effectively secures data at rest on HPE Nonstop backup tapes and virtual tape systems.

Key benefits include:

- **Robust security**
  Encryption keys are managed and stored centrally in a HPE Nonstop-native KMS with split knowledge and dual control. Keys are never exposed in plaintext, and rotation policies are automatically enforced. Support for industry-standard strong encryption algorithms such as AES-256 is provided with options for legacy cipher compatibility where required by existing environments.
- **Ease of use and installation**
  Protect integrates seamlessly with existing BACKUP and RESTORE processes and virtual tape systems (e.g., TapeLabs). Administrators can configure policies through simple commands or via the TAMUNIO console.
- **Cost efficiency**
  As a software-based solution, TAMUNIO eliminates the need for dedicated hardware encryption devices, lowering costs while maintaining enterprise-grade security.
- **Disaster-recovery readiness**
  The same encryption mechanisms also apply to disaster recovery processes. When production data is protected, encrypted copies flow naturally through existing replication or DR tooling without any special handling.

Encrypting data in databases

PCI DSS requires that organizations render primary account numbers (PAN) unreadable anywhere they are stored, including in databases.

This remains one of the most challenging areas of compliance for HPE Nonstop users due to the platform's mix of Enscribe, SQL/MP, and SQL/MX databases and legacy applications.

TAMUNIO simplifies this process through **format-preserving tokenization.**

For applications that cannot easily be modified, TAMUNIO transparently intercepts read/write calls, tokenizing and detokenizing data on the fly so applications continue to function normally without code changes.

Key capabilities:

- Protects PAN and sensitive data in all supported HPE Nonstop database formats.
- Maintains field length and format, ensuring legacy compatibility.
- Stores only tokenized data in Enscribe and database files.
- Centralizes key and token management in TAMUNIO's Nonstop-native KMS, enforcing proper rotation, dual control, and audit logging.

In addition to protecting data stored in Enscribe or database files, the platform can also encrypt temporary or staging files the moment they are created. This ensures that intermediate data generated during batch processing, ETL workflows, or database update cycles never appears in plaintext on disk.

In Summary

TAMUNIO consolidates multiple data security and compliance functions into a cohesive, integrated platform for HPE Nonstop environments.

- **Govern** manages access, SSO, MFA, and audit evidence.
- **Transit** secures Telnet, file transfer, and middleware traffic.
- **Protect** encrypts data at rest, in databases, files, and backups.
- **Transform** enables secure integration and data flow modernization.
- **Access** provides secure, authenticated console and emulator connectivity.
- **TAMUNIO's core services** deliver HPE Nonstop-native key management (KMS), MFA and Unified Monitoring & Auditing for consistent security and compliance across all modules..

Together, they bring HPE Nonstop systems in line with the latest **PCI DSS v4.0** expectations, securely, efficiently, and with full audit visibility.

PCI DSS continues to evolve as threats and technologies change, and early indications for v4.1 suggest refinements around AI use, post-quantum readiness, cloud security, and modern encryption guidance. While most updates are expected to be clarifications rather than new requirements, organizations can be reassured that our platform already aligns with these directions.

About comforte

Comforte is a global leader in the HPE Nonstop solutions market, offering customers a comprehensive suite of proven and innovative middleware, connectivity, and security technologies.

Organizations across industries rely on comforte to protect mission-critical workloads and to maximize the value of their investment in HPE Nonstop systems. In 2023, comforte celebrated its twenty-fifth year of business, and in 2025 we launched the TAMUNIO platform – our next-generation security foundation for HPE Nonstop and enterprise environments.

While the TAMUNIO launch marks a new era, comforte's HPE Nonstop heritage reaches back much further. Our management and development teams bring decades of Tandem/HPE Nonstop expertise, and since our founding we have remained steadfast in our mission to serve and strengthen the HPE Nonstop community.

Comforte's first product, MR-Win6530, became the leading terminal emulation package for HPE Nonstop. Over the years, we expanded into secure connectivity, application modernization, and cross-platform integration for business-critical workloads.

Today, TAMUNIO unifies all aspects of HPE Nonstop security, data in transit, data at rest, access control, Safeguard administration, alerting, reporting, and single sign-on (SSO). The platform aligns more closely than ever with enterprise security practices with the same identities, the same keys, the same telemetry, and the same audit evidence used across the organization, without requiring risky changes.

Explore the full enterprise platform that protects data, strengthens compliance, and drives secure growth. **TAMUNIO >>**

With comforte, organizations can:

Connect HPE Nonstop platforms with the systems, applications, users, and initiatives required to meet their business and technical objectives.

- **Protect mission-critical data** as it is stored in and exchanged with HPE Nonstop environments.
- **Transform their environmen**t by seamlessly integrating HPE Nonstop with enterprise APIs, web services and modern application architectures.

Throughout its history, comforte has earned the trust of its customers and partners. The partnership with HPE remains close and successful, built on decades of collaboration around the HPE Nonstop platform.

In 2007, after an extensive evaluation of emulation technologies, HPE selected comforte's solution as the standard offering bundled with the HPE Nonstop System Console. Comforte technology also underpins several secure connectivity components within the HPE Nonstop Operating System, which incorporate comforte's protection and secure communication capabilities to secure management and application traffic across HPE NonStop environments.

Today, more than 300 customers around the world rely on comforte products to manage access to mission-critical HPE Nonstop server applications and data.

For general information about comforte, please visit http://www.comforte.com, to contact comforte please send an email to info@comforte.com.

Disclaimer

Contact us:

https://www.comforte.com/contact

comforte AG, Germany
phone +49 (0) 611 93199-00

comforte, Inc., USA
phone +1 646 438 5716

comforte Asia Pte. Ltd., Singapore
phone +65 6808 5507

comforte Pty Ltd, Australia
phone +61 2 8197 0272

SECURE YOUR GROWTH