comforte

COMFORTE EBOOK

THE SUCCESSFUL WAY TO ACHIEVE PCI DSS COMPLIANCE - UPDATE FOR PCI DSS 4.0

This eBook was produced by:

comforte AG
Abraham-Lincoln-Strasse 22
65189 Wiesbaden
Germany

www.comforte.com

Document History: Document version 4.0
Issued September 2023

The successful way to achieve PCI DSS compliance

A guide for HPE NonStop users

This eBook provides an overview of the changes in the newly released PCI DSS 4.0 standard and describes how the PCI DSS requirements relate to the HPE NonStop platform – detailing which rules apply, which do not, and why. The eBook then looks in detail at the most pressing challenges organizations face in their efforts to adhere to PCI in HPE NonStop server environments, and it reveals strategies and solutions HPE NonStop users can employ to make their PCI initiatives a success. Finally, it presents products by comforte, which can help achieve PCI compliance more easily.

Table of Contents

Introduction to PCI DSS 4.0

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards and policies that govern the processing, storage, and transmission of cardholder data to protect against credit card fraud. The main goal is to protect cardholders' data. The standard is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC), a global organization made up of major card brands such as Visa, Mastercard, American Express, and Discover.

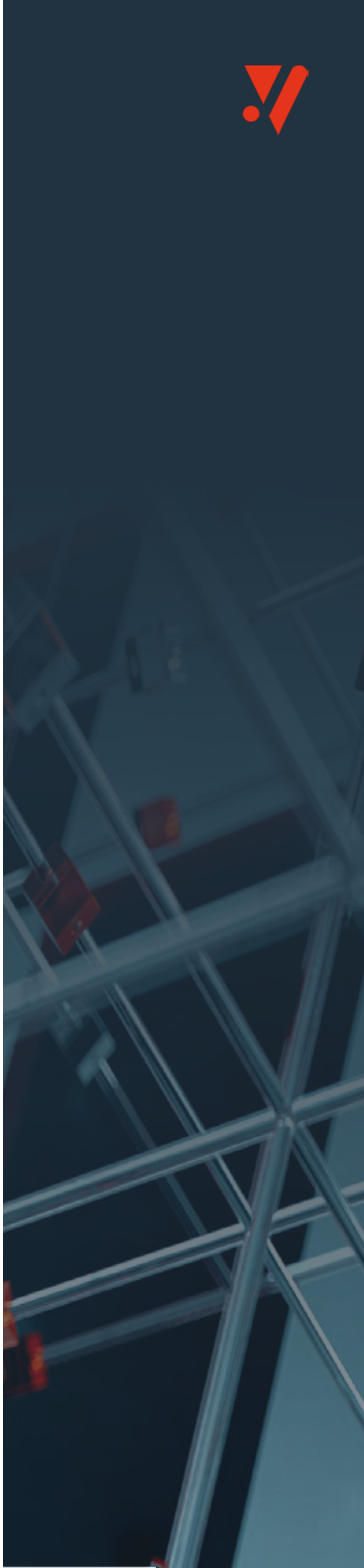
The latest version of the standard, PCI DSS 4.0, is set to take effect on March 31, 2024, and has 63 new requirements. Some requirements are effective immediately, but most aren't effective until March 31, 2025, giving businesses a year-long transition period to implement the more challenging requirements. The new version aims to address emerging threats and ensure that organizations are better equipped to protect themselves and their customers' sensitive information from increasingly sophisticated cyber-attacks.

One of the main changes in PCI DSS 4.0 is a focus on the security lifecycle of payment systems. This means that the standard will emphasise the importance of ongoing monitoring and testing, as well as the need for regular updates and maintenance of security controls.

PCI DSS 4.0 will bring several changes and a renewed focus to the security lifecycle of payment systems. Going forward, organizations will need to place a stronger emphasis and importance on a variety of factors like new authentication requirements, ongoing monitoring and testing, scope measurement, data classification policies, encryption requirements, as well as the need for regular updates, maintenance, and penetration testing around security controls and processes.

Overall, PCI DSS 4.0 aims to provide a more robust and comprehensive set of security standards to help organizations protect against cyber threats and ensure the safe and secure handling of cardholder data. As with previous versions of the standard, compliance with PCI DSS 4.0 will be mandatory for any organization that processes, stores or transmits payment card information.

PCI DSS 4.0 includes a broader definition of account data and includes cardholder data (PANs, cardholder name, expiration date, service code) and sensitive authentication data (full track data, card verification code, PINs/PIN blocks).

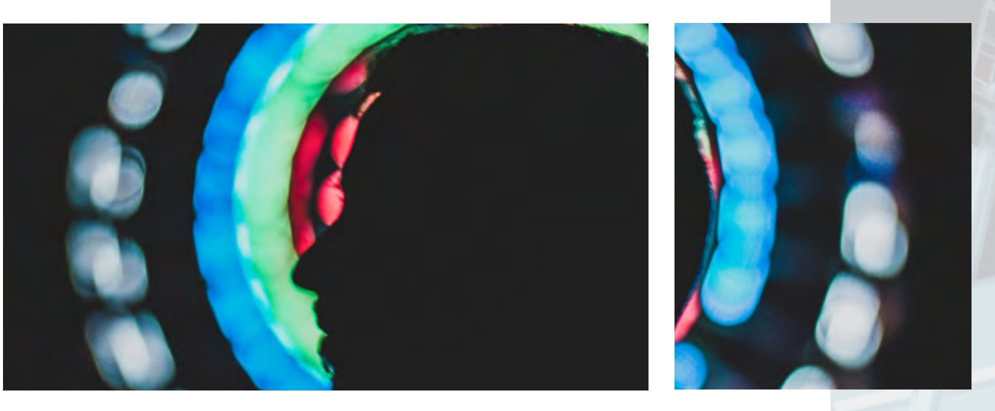


Preface

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 organised 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 chapter 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', which the PCI DSS standard requires for a typical 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 comforte products can help	This is the only part of this eBook, which is not vendor agnostic. It describes how various products from comforte 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 credit card information.

The growing market for stolen credit card numbers has put the industry on red alert, and the PCI DSS standard is an effort to put an end to crimes involving credit cards. While the PCI DSS standard may seem challenging to implement, it does represent best practices in computer 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 rather secure platform by nature and is not plagued by 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 achieve the highest possible level of security.

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

- Obtaining a list of all files containing Account Data
- Encrypting Network Traffic
- Implementing Secure Coding Practices (might not be relevant to you, see below in the eBook)
- Managing Access Control and Auditing (are you running HPE Safeguard and are you using MFA already?)
- Encrypting Backup Tapes
- Encrypting data in Databases

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 comforte product recommendations 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

Introduction: 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. Certainly, this is in part because often these PCI initiatives are the first for any given 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 standards.

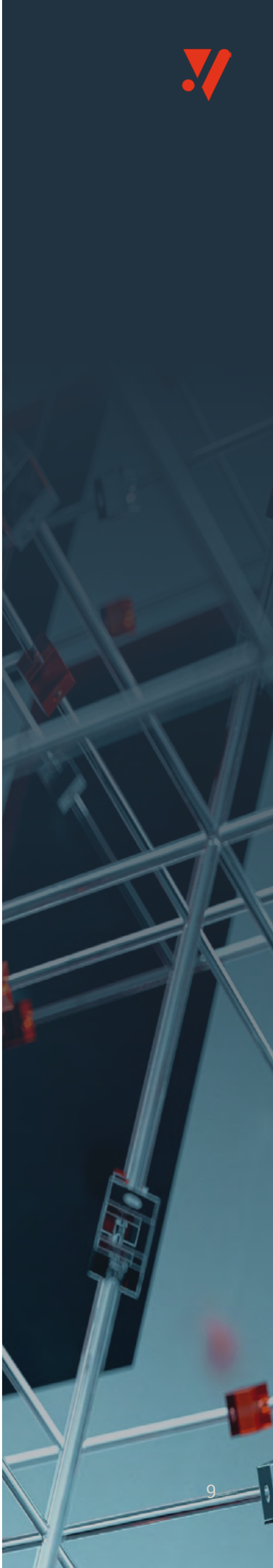
The nature of the PCI auditing process

The PCI standard should not be understood as a long list of 'check-box' items, which all need to be addressed, checked off and forgotten. 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.
- Things which cannot be finished this year will be back on the table next year.
- Many requirements within the standard go well beyond installing a single product or security measure but require constant attention on how to properly secure your systems.

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

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



PCI and how it 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 account processing - including merchants, processors, acquirers, issuers, and other service providers.

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE.

The Account Data includes:

- CARDHOLDER DATA – Primary Account. Number (PAN), Cardholder Name, Expiration Date, Service Code
- SENSITIVE AUTHENTICATION DATA - Full Track Data (Magnetic-Stripe Or Equivalent On A Chip), Card Verification Code (CVC), Pins/PIN Block

The section '4 Scope of PCI DSS Requirements' within the PCI DSS Document describes an initial scoping of the PCI DSS audit. This includes finding all relevant network devices, servers, computing devices, virtual components, cloud components, and software.

Quoting from there:

> *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 at 12.5.2 and is an activity expected to be performed by the entity. This activity is not the same, 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 DSS 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 dire 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 of the standard here. The following table lists each of the 12 sections and adds two extra columns as follows:
The column 'Applicability' describes the applicability to the HPE NonStop environment in comforte's view as follows:

▶ **[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.

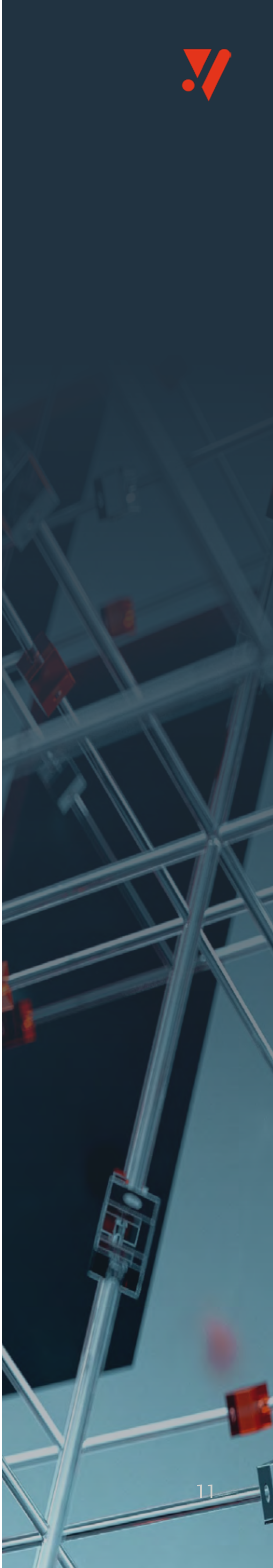
▶ **[FocusArea]**

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: Regularly test security systems and networks	**[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)

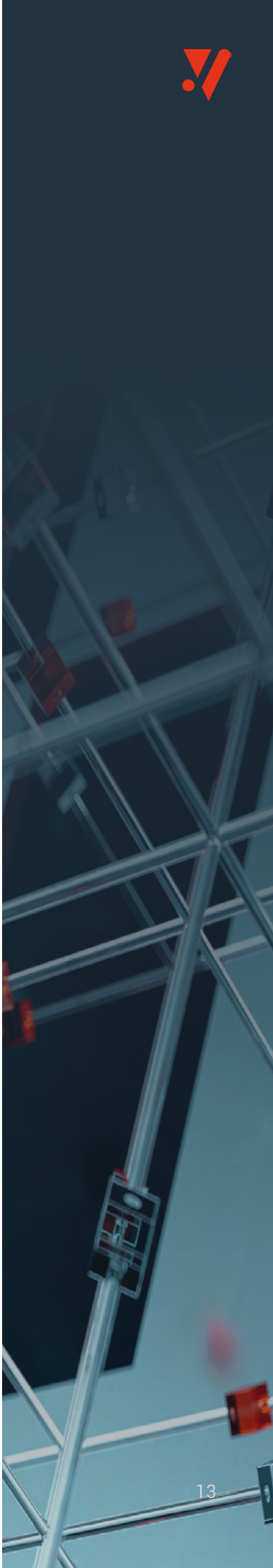
[2] However, it should be noted that eventually, all items from the standard will need to be addressed – the prioritized approach was made available to help get started with any PCI project. For full details of the Prioritised Approach, please refer to the 'Prioritized approach for PCI DSS 4.0' document.

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 categories (the number in brackets indicates priorities according to the PCI Milestones discussed earlier with 1 being high):

- Obtaining a list of all files containing PAN data (1)
- Encrypting network traffic (2)
- Secure Coding (3)
- Managing Access Control and Auditing (4)
- Encrypting Backup Tapes (5)
- Encrypting Data in Databases (5)

Please note that your PCI auditor might have a different view on steps to be taken and priorities - so please talk to your auditor about this. This white paper will explore each of these areas, detailing specific PCI DSS standards, how they apply to HPE NonStop environments, and why they are important or challenging to comply with.



Part 2: Addressing action items in HPE NonStop environments

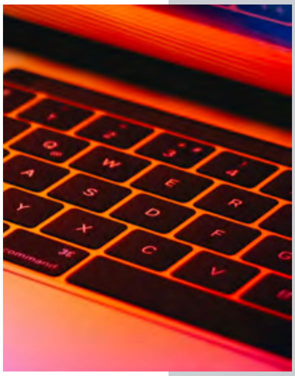
Obtaining a list of all files containing PAN data

This sounds nearly trivial at first and seems only to require creating a list of the critical files. However, some investigation shows that the task is not as easy as it may sound:

- If a manual process (based on knowledge about the system and the applications on it) is used, the following applies:
  - An auditor might require more formal proof than 'We know our system' to ensure that the list is complete.
  - Batch processes and system administrators may create copies of files, often for various reasons. If these files are not deleted, files containing critical data will be left on the systems.

- Trying to automate the process via a 'global search of all files' is not easy either:
  - A search pattern for PANs needs to be flexible enough to both catch all PANs but also not create too many false positives
  - Any search operation must run in the background and must not impact CPU utilization in a negative way
  - The output of the search operation must be masked; otherwise, the result of the search would be a critical file itself

- PAN data often exists in unexpected locations such as SCF trace files or Transaction logs that have been copied to locations outside of the application for support purposes. Perhaps even production files have been copied onto development systems (which is in clear violation of the PCI DSS standard).



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

The following table lists specific sections of the PCI DSS standard that mandate the encryption of 'non-console administrative access', and Sensitive Authentication Data (SAD), Simply put, HPE NonStop organizations can't use Telnet, FTP, or any other protocol that transmits passwords in the clear without strong encryption. It is recommended to protect all sensitive data using format-preserving encryption.

PCI 4.0 Requirement	Description	Mechanism	comforte Products
2.2.7	All non-console admin access is encrypted using strong cryptography	Use SecurLib/SSL, SecurLib/SSL-AT, SecurCS, HPE NonStop SSL, HPE NonStop SSH to protect traffic using either TLS or SSH. Any corresponding client software must also be capable of supporting such traffic, for example MR-Win530, TOP, SafePoint.	SecurLib/SSL, SecurLib/SSL-AT, SecurCS
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation. SecurTape can be used to protect archived data stored on tape.	SecurDPS, SecurTape
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.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation.	SecurDPS

Implementing encryption for Telnet, file transfer, or middleware traffic is rather 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 dominant encryption standards for network traffic:

- TLS/SSL is a widely deployed technology that evolved through the Internet, (SSL was originally developed to carry http traffic for the web) and has been in broad usage for PC file transfers and transactions since 2001. This 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 is a natural fit for communication with UNIX systems, which usually have OpenSSH installed. 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. 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 NonStop authentication? If so, prefer SSH.
- Do you need PKI certificate-based authentication? If so, prefer TLS.

Encrypting ATM/POS network traffic can be more challenging than encrypting Telnet as typically one is dealing with a large number of concurrent connections and a high transaction rate. In principle, the TLS/SSL protocol is best suited for this as it is supported by most ATM vendors.

Secure coding

The part of the PCI DSS 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:
    - Your application crashes or consumes significant system resources when deliberately being fed invalid or certain maliciously constructed data
    - An attacker gaining access to and/or deleting application data by entering invalid manipulated input into your data entry fields ('SQL insertion attacks')
- Secure Coding is best implemented by proper training and code review; however, some products may be used for quality control and penetration testing of existing applications.

Managing Access Control and Auditing

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

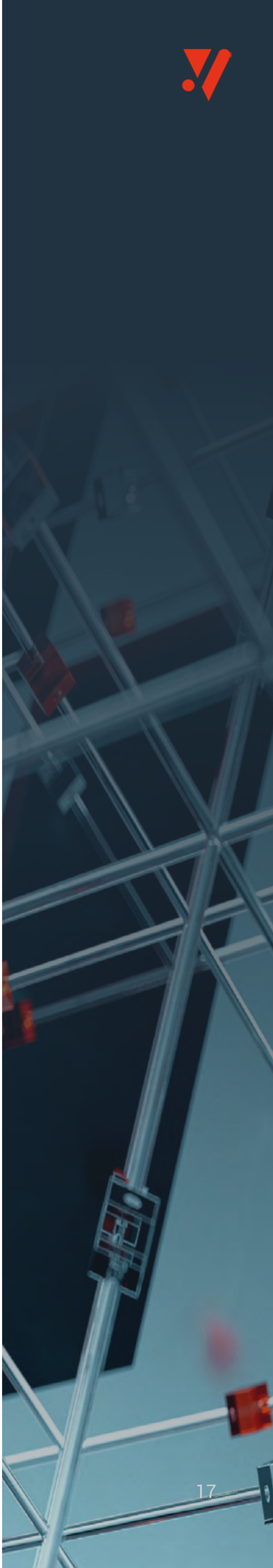
Requirement #	Description of action items
10	Log and Monitor All Access to System Components and Cardholder Data
7	Restrict Access to System Components and Cardholder Data by Business Need to Know
8	Identify Users and Authenticate Access to System Components
12	Maintain an information security policy
11	File Integrity Monitoring (FIM), Intrusion Detection

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 is a product 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.
- Tools, which ease Safeguard configuration and management.
- 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 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 rather 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 are transparent to the existing environment, they have virtually no performance impact on backup and restore, and they safely store keys on the appliance, which is generally more secure than having the keys reside on the same machine as the database, which is typical for most software solutions.
- Software 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

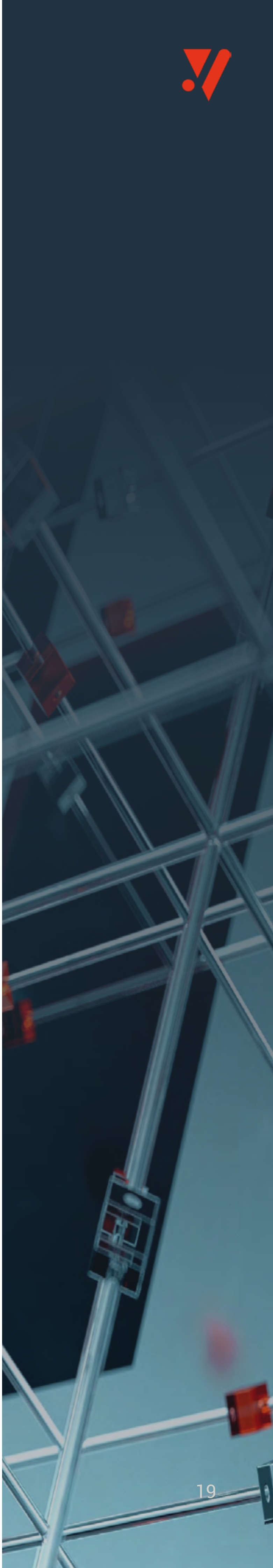
In virtually every enterprise, databases represent a critical aggregation pool of sensitive information. This also holds true in HPE NonStop environments. Many of the PCI DSS standards seek to address this crucial aspect within the infrastructure, specifying what can be stored in databases, what cannot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

The following table is taken directly from the PCI DSS 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, some of which are detailed in the table below.

		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
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data2	Full Track Data3	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID4	No	Cannot store per Requirement 3.2
		PIN/PIN Block5	No	Cannot store per Requirement 3.2

As shown in the following table, Access Control and Auditing are addressed in several places within the PCI DSS standard 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. Furthermore, 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. 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.
- Searching. 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.
- 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 plotting 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 key to evaluate 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.

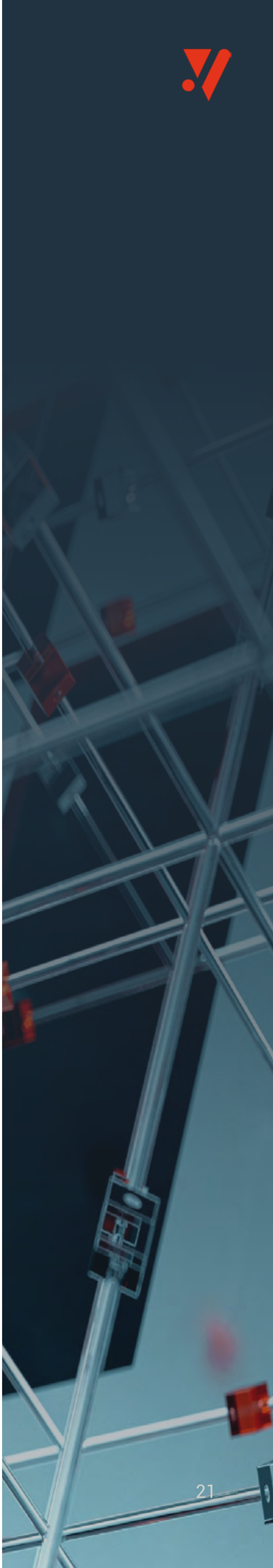
Part 3: How comforte products can help

Overview

Comforte offers a broad range of security products that may help organizations to ensure that all sensitive payment data is protected, both in transit and at rest.

The following table provides an overview of products 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:

PCI 4.0 Requirement	Description	Mechanism	comforte Products
1.3.1,1.4.2	Restrict inbound traffic from untrusted networks	Use HPE iptables, managed in TOP. Use CONNECT_FROM in SecurCS SecurSH and HPE NonStop SSH. Use ALLOWIP in SecurCS SWAP and HPE NonStop SSL.	TOP, SecurCS
2.2.7	All non-console admin access is encrypted using strong cryptography	Use SecurLib/SSL, SecurLib/SSL-AT, SecurCS, HPE NonStop SSL, HPE NonStop SSH to protect traffic using either TLS or SSH. Any corresponding client software must also be capable of supporting such traffic, for example MR-Win530, TOP, SafePoint.	SecurLib/SSL, SecurLib/SSL-AT, SecurCS
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation. SecurTape can be used to protect archived data stored on tape.	SecurDPS, SecurTape
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.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation.	SecurDPS
3.4	Access to displays of full PAN and ability to copy PAN is restricted.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation. Masking and role-dependent displays can be configured. Use SecurDPS Discover & Classify to find PAN and account data.	SecurDPS SecurDPS Discover & Classify
3.5	Primary account number (PAN) is secured wherever it is stored.	Use SecurDPS to protect all sensitive data using format-preserving tokenisation. Masking and role-dependent display can be configured. SecurTape can be used to protect data as it is archived.	SecurDPS



PCI 4.0 Requirement	Description	Mechanism	comforte Products
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Use SecurLib/SSL, SecurLib/SSL-AT, SecurCS, HPE NonStop SSL, HPE NonStop SSH to protect traffic using either TLS or SSH. Any corresponding client software must also be capable of supporting such traffic, for example MR-Win530.	SecurLib/SSL, SecurLib/SSL-AT, SecurCS
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.	Use SafePoint FIM to track/detect changes in key files.	SafePoint
7.3	Access to system components and data is managed via an access control system(s).	Use SecurDPS to protect access to SAD with fine granularity for role-based protection.	SecurDPS
8	Identify Users and Authenticate Access to System Components	Use SecurSSO in co-operation with HPE NonStop SSH or SecurSH to supplement any conventional NonStop authentication with any domain authentication.	SecurSSO
10	Log and Monitor All Access to System Components and Cardholder Data	Use SafePoint to collect and analyse logging and auditing from HPE NonStop SSH, HPE NonStop SSL, Safeguard, TOP, optionally processing with a corporate SIEM.	SafePoint
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools)	Use SafePoint Logstream to track and detect changes in all log files to facilitate threat analysis and security compliance.	SafePoint Logstream

Obtaining a list of all files containing PAN data

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

SecurDPS Discover & Classify was developed with precisely this problem in mind. It searches HPE NonStop systems for unmasked/unencrypted payment card data and provides a comprehensive report that can be used either as a starting point for a PCI audit or as proof of ongoing compliance during repeated audits.

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

Comforte offers several products that help make complying with these PCI DSS rules straightforward and cost-effective [4], while significantly strengthening the security of non-console administrative access in NonStop server environments.

- SecurFTP/SSH, which uses the SFTP/SSH standard to secure file transfers for HPE NonStop systems.
- SecurFTP/SSL, a product that enables secure FTP file transfer for HPE NonStop systems through the SSL/TLS protocol, both for the FTP client and server.
- SecurCS, which brings SSL/TLS encryption capabilities to client/server middleware protocols and to the Telnet data stream between standard TN6530 emulators and HPE NonStop TELSERV processes.
- SecurTN, a Telnet server that provides secure, scalable, and manageable access to applications running on HPE NonStop systems, featuring authentication, access control, and encryption capabilities
- SecurSH, an enterprise security solution that provides secure shell connectivity for HPE NonStop servers.
- SecurLib/SSL and SecurLib/SSL-AT, products to SSL-enable existing TCP/IP socket applications. These products are a perfect fit for the encryption of ATM or POS network traffic.

In addition, these comforte products can generate detailed audit log information for tracking system access, which helps to address many audit-related rules in Section 10 of the PCI standard.

To learn more and find out which is the best fit for your environment, please see the comforte website at https://www.comforte.com/hpe-nonstop-solutions/ or contact a comforte representative at https://www.comforte.com/contact/.

Secure Coding

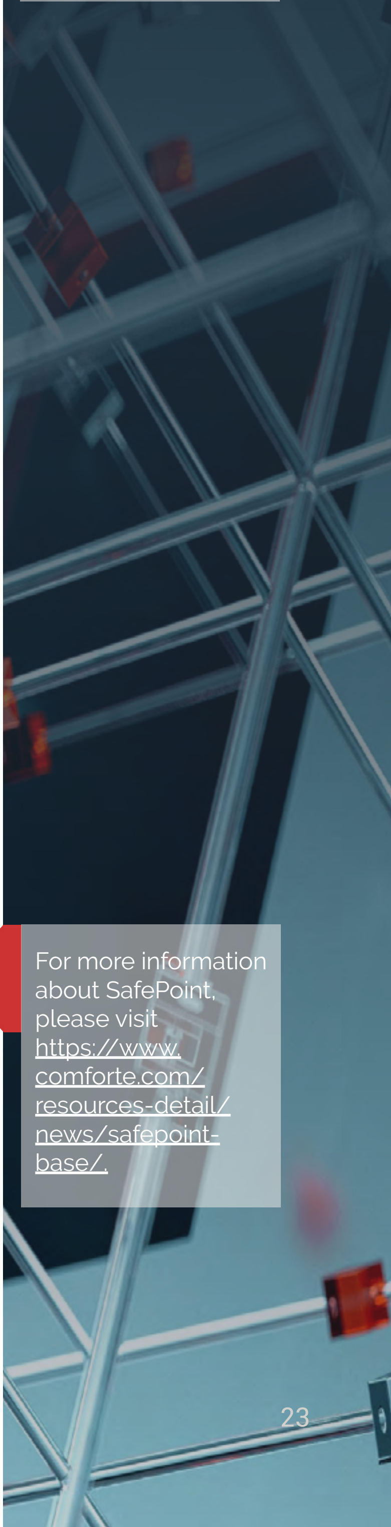
As briefly discussed in Part 2 of this eBook, this matter is more of an educational issue. comforte has no products in the area of 'application penetration testing'.

Access control and auditing

As mentioned in Part 2 of this eBook, there is no single one-size-fits-all product to address the complex requirements of Access Control and Auditing. comforte provides the following products that help organizations meet many of PCI's access control and auditing requirements.

SafePoint

SafePoint offers an intuitive, centralized interface that enables administrators to manage Safeguard security more efficiently and effectively. With SafePoint, administrators get a single solution for managing, monitoring, and reporting on multiple HPE NonStop systems – which yields significant time and cost savings. SafePoint Alarms enables administrators to configure alarms that are triggered based on an array of events. SafePoint Alarms can be generated by data from a range of systems, including Safeguard, BOSS, EMS, OSS, and clients. SafePoint Alarms also can send the content of the Safeguard Audit Trail to central SIEM systems. SafePoint/KSL allows the monitoring of and reporting against keystrokes entered by users. SafePoint Logstream for the efficient streaming of alerts and system log data to your SIM. SafePoint Logstream also handles messages from KSL and our FIM - File Integrity Monitoring solution. We provide dashboards for Splunk. Our FIM solution can now be packaged with SafePoint Logstream.



For more information about SafePoint, please visit https://www.comforte.com/resources-detail/news/safepoint-base/.

[4] Since September 2010, the comforte products SecurSH, SecurCS and SecurFTP have been part of the 'HPE NonStop OS Security Update Bundle' for J- and L-series systems.

SecurSSO

For more information about SecurSSO, please visit https://www.comforte.com/resources-detail/news/fact-sheet-securssо/.

SecurSSO leverages the Kerberos protocol to integrate login to the HPE NonStop platform with Microsoft Active Directory. After installing SecurSSO, it is no longer required to manage passwords on HPE NonStop. Instead, authentication to the HPE NonStop platform will be based on already being authenticated to the Windows desktop.

This streamlines security administration and better integrates the HPE NonStop system in the corporate environment.

SecurTN

For more information about SecurTN, please visit https://www.comforte.com/resources-detail/news/fact-sheet-securtn/.

Beyond encrypting Telnet traffic, the SecurTN product also provides advanced auditing capabilities when used with an emulation which supports querying the remote workstation for detailed information. In that case, the following details on the remote workstation connecting to the NonStop are written to an EMS collector:

- Windows user name
- Windows workstation name
- The IP address as seen on a workstation (this is different from the one seen by HPE NonStop if NAT (Network Address Translation) is used)

Encrypting data on backup tapes

In just about any HPE NonStop server environment, administrators regularly run backup jobs. Requirement 3.4 of the PCI DSS standard applies to wherever account information resides, including the tapes on which these backups are typically stored.

With comforte's SecurTape product, organizations gain a robust encryption solution that effectively secures data at rest on HPE NonStop backup tapes. SecurTape offers a range of benefits:

Robust security

With SecurTape, encryption keys are saved in a secure key store on the HPE NonStop system. That way, access can be controlled on a per-user basis and keys are never available in the clear. SecurTape supports a range of strong cyphers, including 168-bit 3DES-EDE (triple DES) and 256-bit AES-CBC (Advanced Encryption Standard).

Ease of use and installation

SecurTape is easy to install and administer, with a guided, wizard-based installation process, and an easy-to-use command-line interface for managing keys. SecurTape interacts with existing BACKUP and RESTORE processes, which helps streamline deployment.

Cost efficiency:

SecurTape is a software-based solution that costs less than hardware-based alternatives. In addition to that, because it resides on the HPE NonStop server, SecurTape eliminates any need to purchase or install new hardware, which further reduces expenditure.

Furthermore, SecurTape features support for virtual tape systems, such as those from TapeLabs, enabling organizations to enjoy the cost and performance gains these technologies deliver, while effectively securing tapes in these environments.

Encrypting data in databases

PCI DSS specifically requires that organizations encrypt credit card information, such as primary account numbers (PAN), anywhere it is stored, and that includes data held in databases. This requirement, perhaps more than any other, presents significant challenges.

SecurLib/DataEncryption

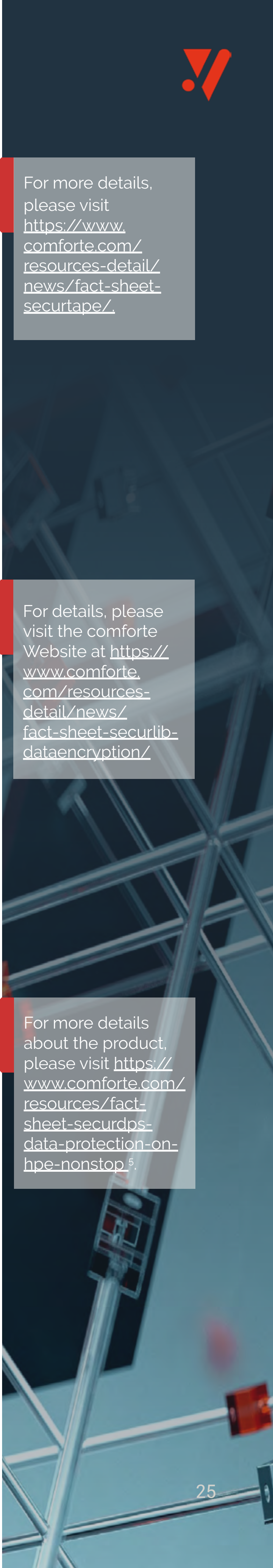
While the challenges for database encryption may seem daunting, several HPE NonStop users already have overcome these challenges and successfully employed database encryption by changing their existing application source code – with comforte's SecurLib/DataEncryption product. With SecurLib/DataEncryption, organizations can effectively and efficiently do database encryption in HPE NonStop server environments.

SecurLib/DataEncryption offers a range of robust encryption capabilities that are tailored to the HPE NonStop server environment. SecurLib/DataEncryption may be deployed in a stand-alone configuration or in conjunction with enterprise database encryption products. For details, please visit the comforte Website at https://www.comforte.com/resources-detail/news/fact-sheet-securlib-dataencryption/

SecurDPS

If customers do not want to change their application source code and if the application uses ENSCRIBE to store critical data, comforte's SecurDPS product allows encrypting the data without any code changes. In a nutshell, SecurDPS combines two technologies to make the seemingly impossible possible:

- It uses tokenization rather than encryption to protect the PAN data. Whereas the encryption of PAN data typically increases the data length, Tokenization leaves the data length unchanged and thus allows the tokenized (protected) PAN data to be stored in the same ENSCRIBE file as the PAN data.
- It uses intercept technology on the HPE NonStop platform to intercept all calls the application makes to OPEN, READ, WRITE etc. It then tokenizes and de-tokenizes data 'on the fly' with the result that:
- The ENSCRIBE files only contain tokenized data, thus complying with PCI 3.4
- The application still sees PAN-like data and therefore will still function



For more details, please visit https://www.comforte.com/resources-detail/news/fact-sheet-securtape/.

For details, please visit the comforte Website at https://www.comforte.com/resources-detail/news/fact-sheet-securlib-dataencryption/

For more details about the product, please visit https://www.comforte.com/resources/fact-sheet-securdps-data-protection-on-hpe-nonstop[5].

[5] Please see http://en.wikipedia.org/wiki/Tokenization_(data_security) for details on Tokenization.

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 products. Organizations in all industries are using comforte products to more effectively leverage their investment in HPE NonStop systems.

In 2023, comforte celebrates its twenty-fifth year of doing business – but the company's HPE NonStop heritage goes back much further. comforte's management and development teams came to the company with deep HPE NonStop/Tandem expertise, and since its foundation, the company has never wavered in its mission to serve the HPE NonStop community.

Comforte's initial product was MR-Win6530, a leading terminal emulation package. In the following years, comforte has expanded its offerings to feature solutions for securing HPE NonStop system connectivity, application modernization, and cross-platform integration of business-critical applications. Today, comforte's security solutions cover all aspects of HPE NonStop security – data in transit, data at rest, system and application access control, Safeguard administration, alerting and reporting as well as single sign-on (SSO).

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 environment by seamlessly integrating HPE NonStop with Web services and SOA initiatives.

Throughout its history, comforte has earned the trust of its customers and partners. The partnership with HPE is a very close and successful one. In early 2007, after an extensive evaluation of emulation solutions, HPE chose comforte's MR-Win6530 to be the standard emulation offering, bundling the solution with the HPE NonStop System Console. comforte's SecurLib/SSL product is being used to encrypt the TCP/IP connection for HPE's Open System Management and other protocols. Finally, since 2010 the NonStop Operating System includes HPE NonStop SSH and HPE NonStop SSL based on the comforte products SecurSH, SecurFTP and SecurCS.

Today, more than 500 customers around the world rely on comforte products to manage access to mission-critical 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

This eBook has been written with industry best practices in mind and in good faith. However, passing or failing an individual PCI audit is dependent on many factors, and comforte cannot take responsibility for the outcome of a specific PCI audit.

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