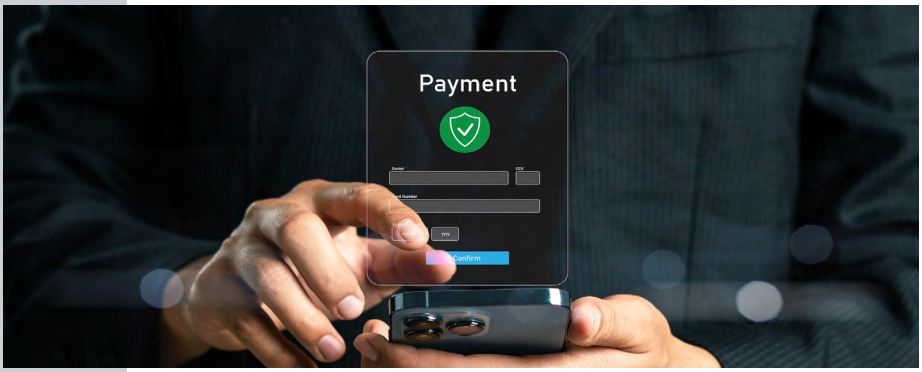
TAMUNIO
POWERED BY COMFORTE

Guide

TAMUNIO Protect for HPE Nonstop Payment Environments

Evaluate Data-Centric Protection for PCI DSS 4.0 Compliance and Payment Processing

Table of Contents



Introduction

Beyond storage encryption. Beyond feature checklists. Built for operational core of the payment switch.

Payment switches on HPE Nonstop sit at the center of highly regulated, always-on transaction environments handling extensive volumes of sensitive payment data. To combat security risks in payment switches, PCI DSS 4.0 sets a much higher bar than “encrypt the files and move on.” The decisive issue is whether sensitive payment data is protected at the application layer and whether access to cleartext data, protection keys, tokenization secrets, and de-protection services is governed effectively against audit standards.

With higher evaluation parameters, buyers must look beyond crypto labels and ask whether the solution can authenticate and authorize consuming workloads at a granular level, enforce separation of duties, eliminate plaintext secrets and unmanaged key files, generate usable audit evidence, and close gaps across files, transfers, backups, and operational tooling. Shortcuts taken here may look acceptable during early project phases, but they often reappear later as audit findings, remediation projects, operational workarounds, or expensive redesigns when the switch is already live.

TAMUNIO Protect is built to meet these critical standards. It combines transparent application-level protection for sensitive data in HPE Nonstop payment environments with file encryption for disk-resident artifacts, integrated key and secret governance through the Nonstop-native Key Management Service - KMS, and operational controls designed for mission-critical systems. The result is a practical path to reducing exposure, strengthening PCI DSS 4.0 readiness, and modernizing without disrupting the switch.

What Payment Leaders Should Evaluate

The strongest evaluation starts with the control model, not the crypto label. Thus, payments leaders must address a range of questions that move beyond a surface-level fix to a solution that will hold up in production and under audit.

1. Protection must happen at the application layer, not only at the storage layer

Encrypting storage is useful. It helps protect backups, exports, reports, refresh files, and other sequential artifacts. But for PCI-level protection in payment switches, storage encryption alone does not answer the harder question: which workloads can ever access cleartext PAN and other sensitive payment data elements inside real operations?

That is the key difference between field-level protection and database file encryption. A transparent database encryption approach protects the Enscribe file or a SQL table as a stored object. It does not intelligently locate sensitive fields inside the record, message, token, or segment structures used by the application. It also does not by itself create a granular control model around which workloads are allowed to access clear values inside operational processing. In contrast, application-level field protection locates the sensitive elements themselves and protects them where they actually matter.

PCI DSS 4.0 effectively pushes the market beyond storage-centric shortcuts. In payment switch environments, protection must hold where sensitive data is actually consumed—inside live application paths, service interactions, utilities, batch jobs, and operational tooling. If cleartext data can still be exposed broadly inside the application environment, or if de-protection depends on loosely governed keys or secrets, the control model may not hold up under deeper audit scrutiny.

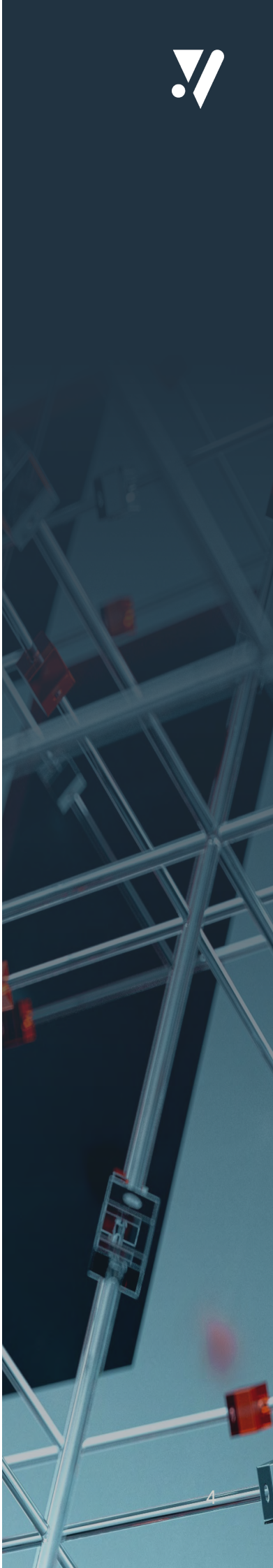
TAMUNIO Protect addresses that challenge at the application layer. It transparently protects sensitive data in live HPE Nonstop payment environments while preserving existing schemas, formats, and workflows. That makes it possible to strengthen protection without broad rewrite projects or disruptive architectural changes.

2. Workload authorization must be granular and auditable

A serious evaluation must go beyond “the data is encrypted.” Payment operators need to know:

- Which processes can invoke protection or reveal functions?
- Which workloads can access cleartext data?
- How are those permissions enforced?
- What audit evidence exists when protected data is accessed or transformed?

This is one of the most important implications of PCI DSS 4.0. It is no longer enough to rely mainly on broad operating-system access or coarse server-level trust assumptions. Access to application-level protection services and the secrets behind them must be controlled with much greater precision.



TAMUNIO Protect is designed around process-level control. It supports granular policies tied to application and operational context so that access to cleartext data, protection services, and sensitive secrets can be restricted to explicitly authorized workloads. Just as important, those interactions can be audited in a way that supports both compliance review and forensic investigation.

A mature solution also needs versatile field-location intelligence. In real payment switches, sensitive values do not only appear at one fixed offset in a simple record. They appear at variable offsets and inside complex structures such as ISO8583 messages that vary by network schema, BASE24 metadata tokens, transaction data elements, Connex segments, TRACK2 content, and PANs represented in different encodings and formats. That is where basic field-level approaches often reveal gaps.

3. Key and secret protection must be part of the solution

In payment environments, protecting the PAN is only part of the problem. Tokenization seeds, encryption keys, TLS keys, SSH keys, MFA secrets, certificates, and configuration secrets all need the same level of operational rigor.

This is where traditional approaches break down. If protection keys, tokenization secrets, passwords, or private keys are left in plaintext files, embedded in scripts, tied to broad OS identities, or handled outside a governed trust model, the organization may close one compliance gap only to create another. Those gaps can be especially painful because they often surface late during audit or production hardening—when they are hardest to fix cleanly and result in costly manual remediation efforts.

TAMUNIO includes an advanced Nonstop-native Key Management Service as part of its core platform. It centralizes the control of keys and secrets, supports strong governance practices such as split knowledge and dual control, uses process-based authorization for secret retrieval, and helps eliminate insecure operational patterns such as storing plaintext secrets or unmanaged key material on disk.

An additional strength is support for HSM-backed protection. TAMUNIO's Nonstop KMS can protect tokenization seeds with strong encryption and be deployed with optional HSM backing. The underlying Nonstop security stack also supports integration with external hardware security modules, which is important for customers that require a hardware root of trust for key custody.

High-quality randomness is part of the same story. In payment environments, the quality of random generation is not just a detail—it is foundational to strong key generation, secret protection, OTP security, and cryptographic trust overall. A hardware-backed key and secret architecture strengthens that foundation giving buyers an additional layer of assurance beyond software-only approaches.

Just as important, customers increasingly need a credible path to post-quantum readiness. Long-lived protected data creates a special challenge: if a protection method must be replaced later, large-scale migration can become costly and disruptive. TAMUNIO's direction explicitly includes post-quantum-safe tokenization and format-preserving encryption across supported platforms. That matters because stable, long-lived tokens are a major operational advantage. A quantum-ready tokenization approach helps customers reduce the risk of future re-protection projects simply to remain cryptographically current.

4. Architecture matters as much as features

Many solutions can show that a field is tokenized or encrypted. Far fewer can prove that the architecture will hold up under real payment switch conditions.

This is where architectural choices become decisive. In an intercept-based protection model, every relevant I/O involving sensitive data creates inter-process communication between the consuming workload and the process performing protection or de-protection. That means the runtime communication model directly affects transaction cost, latency, scalability, security, and auditability.

Buyers should therefore evaluate:

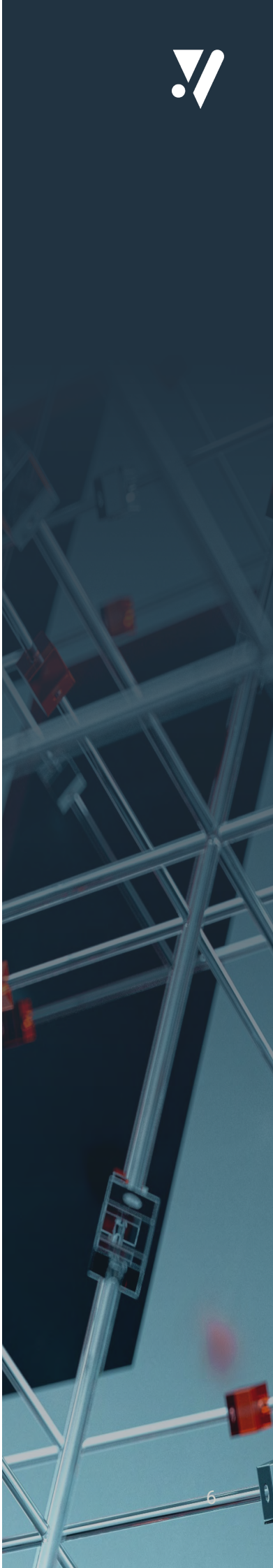
- Runtime latency and CPU overhead
- Behavior under high parallel load
- Batch and bulk-processing efficiency
- Failover characteristics
- Ability to authenticate the original consuming workload
- Operational simplicity and maintainability

Some competing architectures rely on Nonstop TS/MP, also known as PATHWAY or Pathsend, as the core communication layer between intercept components and the protection engine—which introduces real trade-offs. A Pathsend request does not go straight from the requester to the server. Even under favorable conditions it passes through a Redirector, and under load it can also involve Process Brokers, Pathmon, and TSMSGIP, creating extra hops, extra processing, and additional tuning burden.

That matters operationally. A TS/MP-centric design adds overhead to every protection request and becomes especially expensive when large numbers of records, rows, or fields with sensitive data must be processed in a short period of time. In online payment paths, that can increase latency and CPU consumption. In batch, migration, and high-volume transfer scenarios, it can extend runtime materially and make processing windows harder to meet.

It also matters from a security and PCI DSS 4.0 perspective. With a TS/MP-based model, securely identifying and authorizing the original consuming workload becomes more complex because the protection engine does not interact as directly with the true requester. That can leave the control model too dependent on broad operating-system identity unless additional mechanisms are layered on top. The result is an architectural dilemma: either accept weaker native requester authentication or add compensating mechanisms that further increase runtime cost and complexity.

TAMUNIO Protect is built differently. Its direct IPC-based model uses manager processes on each CPU and automatic failover in the intercept layer, with the same-CPU communication by default for optimal performance. This helps avoid unnecessary message hops and helps preserve both throughput and control over which application processes are actually authorized to use protection and de-protection functions.



5. Coverage must extend beyond online records

Real payment environments create more than online database rows. Sensitive data also appears in:

- Extract and refresh files
- Import and export files
- Reports and audit files
- Transfer and exchange files
- Temporary and intermediate files
- Backups and retention artifacts

TAMUNIO Protect supports application-level protection for selected fields or entire file records. Tape encryption capabilities are also part of the TAMUNIO suite, extending transparent protection to backups and tape-oriented retention scenarios.

This breadth matters because buyers often underestimate the difference between versatile field-level protection and simpler approaches that only work in limited record layouts. TAMUNIO Protect is designed to locate and protect sensitive values across the complex formats common in payment switching, including variable-position fields, repeating structures, schema-driven ISO8583 content, BASE24 token and TDE constructs, Connex segments, and PAN-related content in multiple field formats.

6. The solution must fit a broader enterprise security strategy

Nonstop is mission-critical, but it should not remain an isolated security island. Payment organizations increasingly need consistent policies across Nonstop, open systems, cloud, analytics, and AI initiatives.

TAMUNIO gives customers a path from Nonstop point protection to a broader enterprise data protection model, with consistent controls for keys, secrets, access, protection, and auditability.

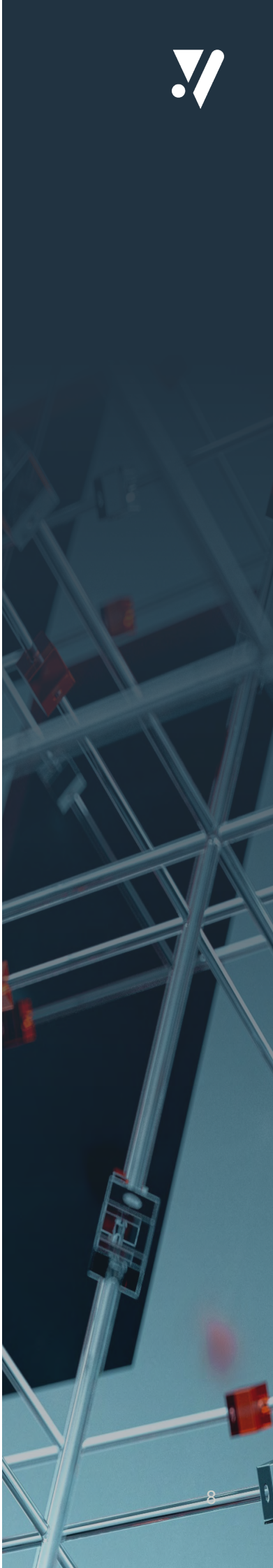
What Production-Grade Looks Like in a Payment Switch

A production-grade approach for HPE Nonstop payment environments should deliver all of the following:

- Application-level protection of sensitive elements
- Support for tokenization, format-preserving protection, and encryption where each fit best
- Granular workload authorization for reveal functions and secret access
- Integrated key and secret governance
- Optional HSM-backed and strong randomness for critical key material
- A credible path to post-quantum-ready tokenization and format-preserving protection
- Low-risk deployment that preserves formats and minimizes application disruption
- Strong coverage for files, transfers, backups, and intermediate artifacts
- Performance suitable for both online and batch workloads
- Failover-aware runtime behavior
- Practical migration support from unprotected to protected state
- Operational maturity for long-term support

Just as important, the design should reduce the risk of unpleasant surprises later. A solution that looks simpler at the start can become far more expensive if it leaves unresolved gaps in workload authorization, audit evidence, key governance, transfer-file handling, or operational tooling. In payment-switch environments, those are not minor follow-up items. They are the kinds of issues that can trigger audit findings, delay sign-off, force compensating controls, or require redesign when change windows are limited and the business is already committed.

This is the standard that payment operators should set.



How TAMUNIO Protect Meets that Standard

Transparent protection without broad application rewrites

TAMUNIO Protect is built to layer controls into existing HPE Nonstop payment environments without forcing wholesale redesign. It applies protection that fits established schemas and workflows, helping customers reduce risk without breaking what already works.

Field-level protection, not just encrypted database files

There is a fundamental difference between encrypting an Enscribe database file and protecting the sensitive fields inside it. A database-file encryption approach protects the file as an object at rest. TAMUNIO Protect works at the field level, locating PANs and other sensitive data within live records and protecting those elements transparently during read, write, and keyed-access processing. That is far closer to the actual PCI DSS 4.0 control problem in a payment switch.

Versatile intelligence for real payment-switch data formats

TAMUNIO Protect is designed for the complexity of real payment environments, not only for simple fixed-position fields. It can work with variable offsets, repeating structures, and schema-driven message formats used across payment networks and switch platforms. That is critical for environments that rely on ISO8583 schemas, BASE24 metadata tokens, transaction data elements, Connex segments, TRACK2 content, and PAN-related values represented in different field formats.

Online migration without breaking keyed application logic

Migration is not just a data conversion exercise. In many payment switch files, the protected field is also part of an Enscribe key used for record lookup. A mature solution must support online migration in a way that allows a mixed protected and unprotected state during transition without breaking the application. TAMUNIO Protect is built with migration mechanisms for exactly this challenge, helping customers move to protected state with less disruption and lower implementation risk.

Column-level and column-subfield protection for SQL/MP and SQL/MX

TAMUNIO Protect is not limited to Enscribe records. It also supports transparent protection for Nonstop SQL/MP and SQL/MX environments. That matters for customers that need consistent application-level protection across mixed Nonstop data stores and for modernization paths that increasingly involve SQL-based access patterns.

Stronger control over who can access clear data

Instead of treating every system with operating-system access as effectively trusted, TAMUNIO Protect enables a more disciplined model. Only explicitly authorized workloads should be able to access clear data, keys, or reveal services.

Integrated KMS-backed trust model

TAMUNIO's Nonstop-native KMS provides a unified foundation for tokenization seeds, file-encryption keys, TLS and SSH credentials, MFA-related secrets, and other sensitive materials. This reduces operational sprawl and strengthens compliance posture.

Where customers require an additional hardware-backed protection layer, TAMUNIO also supports HSM-backed deployment patterns. That strengthens key custody, supports stronger assurance around key handling, and is especially relevant for organizations that want a hardware-enforced trust anchor and high-quality entropy for critical cryptographic material.

The same trust model supports a longer-term cryptographic strategy. TAMUNIO is positioned to deliver post-quantum readiness, including quantum-safe tokenization and format-preserving protection. For payment environments, this is not just a future-technology talking point. Stable tokens often remain in production for many years and replacing them later can result in large-scale migration work. A post-quantum-ready tokenization strategy helps protect customers from that future disruption.

Designed for operational reality

Payment leaders cannot afford fragile solutions that look acceptable in a demo but create friction and weaken velocity in production. TAMUNIO Protect is designed for high-value, high-availability environments where performance, resilience, and maintainability matter as much as protection itself.

That is especially important when comparing architectural choices. A TS/MP-based approach may appear convenient because PATHWAY is already familiar in Nonstop environments. However, that convenience can become misleading. The extra routing, broker, monitor, and cross-CPU messaging behavior of a PATHWAY-centric design adds cost to every protection request, increases sensitivity to tuning, and can turn batch or migration windows into a performance problem. More importantly, it complicates the secure identification of the original consuming workload at exactly the layer PCI DSS 4.0 expects buyers to scrutinize.

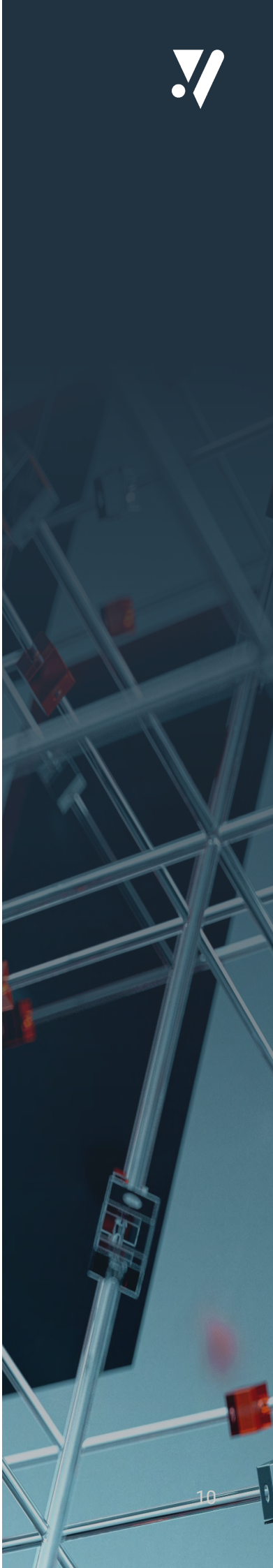
TAMUNIO Protect avoids that trap with a leaner architecture designed specifically for transparent application-level protection under production conditions.

Broader protection for the full operational surface

TAMUNIO Protect is not limited to protecting individual fields. It also addresses exports, transfers, backups, and other files that routinely become blind spots during compliance projects.

Built for modernization, not just containment

The goal is not only to reduce breach impact. It is also to help payment organizations modernize safely: enable analytics, API-led integration, secure partner connectivity, and broader enterprise alignment without expanding exposure.



Questions Every Payment Operator Should Ask Vendors

Use these questions to expose hidden architectural, compliance, and operational gaps early in the evaluation process:

- Does the solution protect sensitive data at the application layer, or only encrypt storage?
- How are consuming workloads authenticated and authorized?
- Can the vendor demonstrate granular controls over reveal functions and key access?
- Is key and secret management integrated, or left to separate tooling and manual processes?
- What is the runtime architecture, and what does it do to latency and CPU cost?
- How does the solution behave under high parallel load and batch processing?
- How are extract, backup, transfer, and intermediate-file scenarios handled?
- Can the solution preserve existing formats and workflows without broad application changes?
- Is there a practical migration path from unprotected to protected state?
- Does the vendor have the experience, support model, and ecosystem validation required for a mission-critical switch deployment?

Why Vendor Credibility Matters in this Decision

A payment switch protection project is not a commodity software purchase. It is a change in the operational heart of the payment environment.

That means buyers are not only selecting a feature set. They are selecting a partner that must be able to:

- Understand payment-switch realities
- Execute with low disruption
- Support the environment globally over time
- Stand behind the architecture under production pressure

Comforte brings that level of credibility:

- More than 20 years in the HPE Nonstop market
- More than 25 years protecting mission-critical systems
- More than 500 enterprises worldwide relying on comforte solutions
- Long-standing payment-sector experience with continuous product evolution
- Global footprint and follow-the-sun support suited to international payment operations

For a head of payments, that matters. A lower-cost option can look attractive on paper, but if it lacks validation, operational maturity, or architectural depth, the hidden cost shows up later in project delays, audit friction, performance problems, operational workarounds, and personal accountability when things go wrong.

Market Validation that Reduces Decision Risk

TAMUNIO Protect is not an unproven theory.

Comforte has established strong validation in the payments market through its relationship with ACI Worldwide. Following extensive compatibility testing with ACI's payment solutions, ACI selected comforte to protect BASE24 payment switch environments operating on both HPE Nonstop and open systems. Today, ACI uses comforte's data-centric security solutions to help secure sensitive payment data for customers while supporting PCI DSS 4.0 compliance requirements across mission-critical payment processing environments.

Comforte's technology is also trusted by leading global payment organizations and major card-network participants. For customers, the implication is straightforward: this is an approach that has already been validated in environments where failure is least acceptable.

That does not remove the need for diligence. But it materially reduces the risk of betting your payment core on an immature or unvalidated approach.

The comforte Point of View

The wrong way to evaluate this market is to ask, "which product can encrypt or tokenize a field?".

The right way is to ask, **"which solution can protect sensitive payment data where it is actually exposed, govern who can access clear data and secrets, cover the full operational surface, and hold up in the real-world conditions of a mission-critical HPE Nonstop payment switch?"**

PCI DSS 4.0 raises that bar materially. It pushes buyers to evaluate not just whether data is protected somewhere, but whether the full control model around applications, workloads, keys, secrets, and auditability is strong enough to survive scrutiny. A shortcut that looks cheaper or faster early in the process can become the most expensive option later if it produces audit exceptions or architectural gaps that are hard to remediate without disruption.

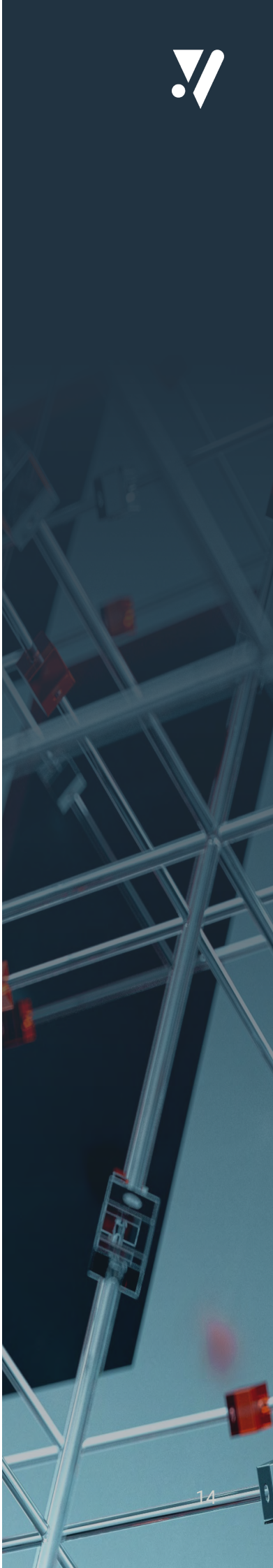
That is the problem TAMUNIO Protect was built to solve.

Why Payments Organizations Choose TAMUNIO Protect

They want to:

- Reduce PCI exposure without destabilizing the switch
- Protect sensitive data in place without broad rewrites
- Close gaps across exports, transfers, backups, and intermediate files
- Govern keys and secrets through one trust model
- Add hardware-backed protection and stronger entropy where required
- Avoid future disruption through a credible path to post-quantum-ready tokenization
- Modernize Nonstop security without creating enterprise exceptions
- Work with a vendor that has real payment-sector credibility and operational maturity

TAMUNIO Protect delivers that combination.



For HPE Nonstop payment environments, the decision is bigger than just storage encryption or a feature checklist—it is a decision about operational trust.

TAMUNIO Protect delivers that combination by delivering a stateless, vaultless tokenization solution that eliminates the need for centralized token vaults while ensuring high performance, scalability, and resilience. By applying protection directly within the data flow, TAMUNIO Protect secures sensitive information across HPE Nonstop systems as well as broader enterprise environments—covering data at rest, in transit, and in use. This unified approach allows organizations to seamlessly extend protection beyond core systems to modern applications, enabling secure data utilization in cloud platforms, analytics, AI, and fraud detection use cases.

The result is consistent, high-speed data protection that preserves format and usability, empowering businesses to innovate without compromising security or operational efficiency.

Contact

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