TAMUNIO
POWERED BY COMFORTE

Fact Sheet

TAMUNIO Assure: Quantum-Ready Security and Automated Key Management for HPE Nonstop

Modernize HPE Nonstop SSH and SSL/TLS security, centralize keys and secrets, and automate certificate lifecycles without rewriting critical applications or disrupting transaction systems.

25+

years of HPE Nonstop security expertise

3

critical capabilities in one HPE Nonstop-native solution

0

application rewrites required to modernize SSH & SSL/TLS

The Challenge

HPE Nonstop environments run some of the world's most critical transaction systems. As cryptographic expectations evolve, teams need a modern way to strengthen security, simplify compliance, and prepare for the post-quantum transition without disrupting stable core systems.

Scattered keys, certificates, and secrets

Private keys, credentials, certificates, and secrets often reside across files, scripts, application configurations, and local system stores. This creates unnecessary exposure, inconsistent governance, and audit gaps.

Manual certificate and key operations

Certificate renewals, key rotation, and lifecycle tasks are often handled manually. That increases operational effort and raises the risk of missed expirations, emergency changes, outages, and compliance findings.

Legacy SSL and SSH modernization pressure

HPE Nonstop teams need stronger cryptographic controls, but migrations can create application risk, downtime concerns, and operational resistance.

Post-quantum urgency

"Harvest now, decrypt later" threats mean encrypted traffic captured today may become vulnerable in the future. Organizations that process long-lived sensitive data need a credible path to quantum-ready protection.

The Solution

TAMUNIO Assure is purpose-built to modernize cryptographic security for HPE Nonstop without compromising uptime, stability, or operational control.

It brings together post-quantum-ready transport security, centralized key and secrets governance, and automated certificate lifecycle management in one solution designed for mission-critical HPE Nonstop environments.

- **Post-quantum-ready SSH and SSL/TLS modernization**

  Enhance legacy HPE Nonstop SSH and SSL/TLS protection and strengthen cryptographic security without requiring application rewrites.

- **Centralized key and secrets governance**

  Bring keys, credentials, certificates, and secrets under centralized, policy-driven control instead of relying on local files, scripts, and fragmented configurations.

- **Automated certificate and key lifecycle management**

  Replace manual certificate renewal, key rotation, and lifecycle tasks with automated workflows that reduce operational effort, improve consistency, and support compliance readiness.

Core Capabilities

- PQC upgrade for SSH & SSL/TLS
- Centralized key and secrets management
- Certificate lifecycle automation
- Key rotation and lifecycle automation
- Extensible crypto control
- Drop-in deployment model
- No application rewrites required

What HPE Nonstop Teams Gain

Lower outage risk

Reduce the chance of service disruption caused by expired certificates, manual errors, or emergency cryptographic changes.

Stronger protection for keys and secrets

Move cryptographic material out of scattered files and unmanaged locations into centralized, governed control.

Modernization without application rewrites

Strengthen SSH and SSL/TLS security, including post-quantum readiness, while preserving existing application behavior and operational stability.

Simpler compliance readiness

Give security, infrastructure, and compliance teams clearer control over cryptographic assets, lifecycle processes, and audit evidence.

Greater operational efficiency

Reduce the manual workload of managing certificates, keys, and secrets across HPE Nonstop systems.

Protection for existing HPE Nonstop investments

Improve cryptographic resilience while preserving the applications, infrastructure, and operational models your business already depends on.

Use Cases

- **Modernize HPE Nonstop SSH and SSL/TLS security** with post-quantum-ready protection.
- **Centralize governance** for keys, secrets, certificates, and credentials across HPE Nonstop environments.
- **Automate certificate renewal and key rotation** to reduce expiration-driven outages and emergency changes.
- **Protect long-lived sensitive data in transit**, including payment, customer, and operational data.
- **Strengthen compliance readiness** for PCI DSS and other cryptographic control requirements.
- **Reduce operational complexity** in mission-critical transaction environments.

Why TAMUNIO Assure for HPE Nonstop?

Purpose-built for HPE Nonstop

TAMUNIO Assure is designed for environments where uptime, application stability, and operational control are non-negotiable.

Security modernization without disruption

Teams can improve cryptographic protection without rewriting applications, redesigning workflows, or introducing unnecessary risk to critical systems.

A unified approach to cryptographic control

Instead of treating SSH, SSL/TLS, keys, secrets, and certificates as separate operational problems, TAMUNIO Assure brings them together in one purpose-built solution.

Deep HPE Nonstop expertise

comforte brings more than 25 years of experience securing HPE Nonstop environments that support high-volume, mission-critical business transactions.

Get started

Begin with an HPE Nonstop crypto posture consultation to identify modernization priorities, quantify operational risk and cost, and build a clear path to quantum-ready cryptographic security.

Request an assessment