

Enterprise-Grade Transport Security for HPE Nonstop

Standardize TLS/SSH for admin, terminal, file, and applications flows.

Why TAMUNIO Transit?

HPE Nonstop environments are mission-critical, but their security posture often reflects decades of technical evolution. The result? Inconsistent protection, non-compliance risk, and operational friction that slows modernization.

TAMUNIO Transit provides a unified transport security layer purpose-built for HPE Nonstop environments.

- » Standardize secure transport & access
- » Simplify and centralize governance, key management & visibility
- » Modernize without disruption

How It Works

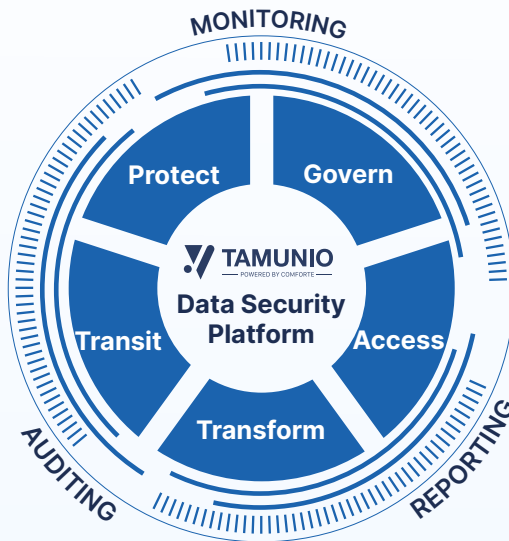
TAMUNIO Transit is a drop-in layer that standardizes TLS/SSH, centralizes access controls, and unifies audit without disrupting mission-critical workloads.

It operates across three domains:

- » **Connect:** Encrypted sessions for admin/terminal and secure file transfer.
- » **Control:** Centralize security governance for consistent enforcement.
- » **Capture:** Consolidate audit and evidence with SIEM-ready logs.

Key Benefits

- ☒ **Reduce Interception Risk:**
Replace cleartext channels and enforce authenticated, encrypted flows.
- ☒ **Lower Operational Overhead:**
Central credentials and standards-based interoperability preserve procedures and partner tools.
- ☒ **Modernize Safely:**
Upgrade legacy connectivity without disrupting existing workflows.
- ☒ **Future-Proof Against Quantum Threats:**
Use post-quantum TLS and SSH to reduce "harvest-now, decrypt-later" risk for critical data.
- ☒ **Bridge to Enterprise Standards:**
Secure file exchanges across enterprise stakeholders using SFTP/FTPS with proxy encryption for non-modern endpoints.



REDUCE RISK
STREAMLINE COMPLIANCE
ENABLE INNOVATION

Core Capabilities

Secure File Transfer

Standardize SFTP/FTPS for teams and partners with centralized credentials and complete transfer logs.

Application & Network Encryption

Add encryption to existing connections without rewrites; secure app traffic when proxies won't fit.

Existing Flow Hardening

Protect older Telnet/FTP and other TCP sessions via tunneling with minimal changes.

In-Motion Payload Protection

Tokenize or encrypt sensitive payloads during transfers to limit exposure.

Post-Quantum-Ready Transport

PQ-TLS and PQ-SSH options to protect long-lived data and align with evolving compliance.

Centralized Key & Secrets Management

One place to manage certificates, keys, and secrets with automated rotation to cut risk and effort.

Built-In MFA For Privileged Access

Strengthen admin operations with multi-factor authentication without disrupting core Nonstop settings.

Why work with us

- » **Deep HPE Nonstop Expertise:** Over 25 years pioneering security for the world's most demanding environments.
- » **End-to-End Security Stack:** Single vendor delivering transport security, data protection, access control, and governance optimized for HPE Nonstop environments.
- » **Proven Scale & Reliability:** Battle-tested components serving enterprise-class workloads with high availability and minimal performance impact.

Learn more at www.comforte.com

Use Cases



Secure & Harden File Transfers

Replace FTP with SFTP/FTPS under strong authentication & centralized keys.



Modernize Terminal & Admin Access

Encrypted, policy controlled sessions with full logging.



Protect Middleware & Service Traffic

Add application-transparent TLS where proxies or rewrites are impractical.