Enterprise-Grade Access Management for HPE Nonstop, IBM, and UNIX

Standardize secure access for Windows users across different host environments

Why TAMUNIO Access?

As enterprises modernize HPE Nonstop environments, legacy access methods often remain fragmented and insecure, creating operational inefficiencies and compliance gaps. The same challenges extend across connected IBM and UNIX systems, where legacy terminal protocols still underpin daily operations. Without proper control and visibility, organizations face risks of unauthorized access, misconfigurations, and other rising security vulnerabilities.

TAMUNIO Access delivers a unified access layer for administrators and users that standardizes secure terminal/GUI access, centralizes governance, and consolidates audit without disrupting core HPE Nonstop workloads.

» Standardize secure access and session handling
» Simplify governance and visibility
» Modernize safely while keeping proven workflows

How It Works

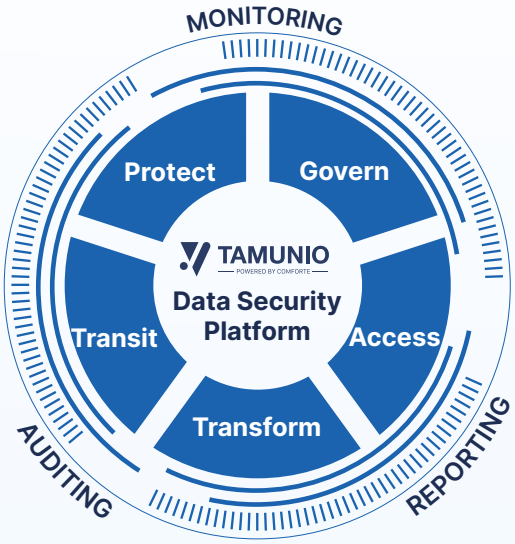
Through an integrated access layer, TAMUNIO unifies terminal emulation, Windows-based operational tools, and centralized oversight.

It functions across three core domains aligned with the overall TAMUNIO framework:

» **Connect:** Secure, encrypted sessions for terminal and file access (SSH/TLS, SSO).
» **Control:** Operator security profiles, policy-based restrictions, and role-aware tooling.
» **Capture:** Command auditing, change logs, and SIEM-ready evidence for privileged sessions.

Key Benefits

- ☑ **Standardize Secure Access:** Unify terminal and GUI access to HPE Nonstop with strong encryption, centralized controls, and consistent operator experiences.
- ☑ **Reduce Human Error and Downtime:** Replace complex command-line steps with intuitive interfaces and workflows that speed operations and reduce mistakes.
- ☑ **Modernize Without Disruption:** Introduce secure SSH/TLS, SSO, and policy-driven access while preserving established tools and procedures.
- ☑ **Streamline Compliance:** Strengthen authentication, auditing, and least-privilege enforcement for PCI and internal controls, with SIEM-ready evidence.



REDUCE RISK
STREAMLINE COMPLIANCE
ENABLE INNOVATION

Core Capabilities

Secure Terminal Access
Field-proven emulation with multiple concurrent sessions, robust security (SSH/SSL/TLS), and Kerberos-based SSO.

Unified GUI for Multi-Host Operations
Intuitive Windows interface for HPE Nonstop, IBM, and UNIX environments under one secure management view.

Operator Security Profiles & Policy Controls
Role-based profiles restrict access and enforce consistent, least-privilege operations.

Command Auditing & Change Logging
Comprehensive logging for system audit purposes captures what changed, by whom, and when.

Encrypted Sessions & File Transfers
Secure terminal sessions (SSH/TLS) plus SFTP/FTP-TLS for file movement between Nonstop and Windows.

Integrated File & Code Tools
Edit, compile, and compare Guardian/OSS files with syntax support for major languages.

Centralized Deployment
Citrix XenApp and Windows Terminal Server support for simplified rollout and admin across large user bases.

Use Cases

Modernize Access

Standardize SSH/TLS, SSO, and operator profiles while keeping familiar MR-Win6530 workflows.

Harden Privileged Operations

Apply role-based controls and log all changes/commands for audit and forensics.

Secure File Movement

Standardize SFTP/ FTP-TLS between HPE Nonstop and Windows with integrated tooling and central oversight.

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**