Rocket® software

Securing Your Mainframe Access Through Consolidation

Contents

Introduction

Despite a massive shift toward cloud-native solutions, mainframes and other core backend systems still serve as foundational infrastructure for highly regulated industries. If you work in finance, healthcare, energy, or government, these systems handle your most critical operations. They house high-value data – like PII, PHI, and PCI – and naturally draw intense regulatory scrutiny.

However, organizations often overlook a crucial piece of the mainframe security puzzle. Terminal emulation connects your users to host environments, but many companies let these tools grow without a clear strategy. This leads to a fragmented patchwork of emulators scattered across different departments, business units, and acquired companies.

When you rely on disconnected tools, you introduce operational inefficiencies, complicate your compliance efforts, and leave the door open for security vulnerabilities. Consolidating your terminal emulation onto a secure, unified platform offers a straightforward way to reduce risk and improve productivity.

Mainframe access is only as secure as the tools that connect to it.

Consolidating terminal emulation reduces hidden risk while improving productivity.

The current state of terminal emulation

If you look closely at mainframe access within a large enterprise, you'll likely see a reflection of the organization's complex history. You might find dozens of different terminal emulator products running simultaneously across various geographic locations and acquired entities.

This sprawl happens for a few common reasons. Mission-critical legacy applications often demand specific emulators or unique configurations to function properly. When mergers and acquisitions occur, newly acquired organizations bring their own preferred tools, and IT teams rarely harmonize them after the deal closes. Additionally, different departments frequently adopt their own solutions to solve immediate problems, leading to a tangled web of software.

For sectors under strict regulatory oversight, auditable controls and data integrity are absolutely vital. Disparate emulation tools rarely share common security features or standardized reporting. Many of these older tools don't even support modern authentication methods, leaving your systems vulnerable.

Emulator sprawl is the legacy of M&A, one-off fixes, and app dependencies

The result: inconsistent security, configs, and reporting across the enterprise.

The risks of a fragmented landscape

Relying on a patchwork of terminal emulators directly drains your IT resources. Industry data shows that organizations with fragmented environments face significantly higher support costs. IT staff often spend three to four extra hours every week just maintaining and troubleshooting these disconnected systems.

This fragmentation severely impacts productivity. Users suffer from inconsistent interfaces, redundant workflows, and unexpected downtime. A large portion of IT support tickets in hybrid mainframe environments directly relate to emulator issues. When you multiply an average resolution time of 45 minutes across thousands of users, the lost time becomes staggering. Large organizations frequently dedicate more than one full-time employee entirely to emulator patch management, which is twice the workload of a consolidated environment.

Fragmented emulators quietly drain time and amplify compliance exposure

Extra weekly IT hours, recurring tickets, patch overhead, and audit gaps add up fast.

Compliance creates another major hurdle. The financial penalties for non-compliance in regulated sectors are immense. Healthcare organizations face massive fines for HIPAA violations, while card brands impose heavy monthly penalties for PCI DSS shortcomings. Incomplete access logs can lead to millions of dollars in fines under SOX regulations. Electric utilities face similar risks under NERC CIP for inadequate logging and access control.

When you use disparate emulators, you cannot consistently enforce access controls, logging, or reporting. You face audit gaps because your log collection remains incomplete or incompatible. Most importantly, outdated software versions create security vulnerabilities. Without centralized monitoring and modern policy enforcement, you cannot easily roll out enterprise-wide standards like multi-factor authentication or encryption.

The clear case for consolidation

Enterprises that transition to a single, secure terminal emulation platform experience immediate relief. They typically see a massive reduction in support tickets and significant cost savings in software licensing and maintenance during the first 12 months.

Consolidation transforms your security posture. A unified platform streamlines user provisioning, deprovisioning, and access reviews. You can easily demonstrate compliance during audits because you track all logs and activity in one central location. By reducing the number of tools you need to patch and monitor, you shrink your attack surface. A consolidated approach also allows you to consistently apply modern security controls, including end-to-end encryption, single sign-on, and multi-factor authentication.

Beyond security, your entire operation becomes more efficient. A unified user experience reduces the learning curve for new employees and improves overall satisfaction. Your IT team only needs to deploy, patch, and update a single platform. This streamlined approach lowers your licensing and support overhead, giving your organization the agility it needs to respond to regulatory changes and emerging threats.

One secure platform = fewer tools to patch, one place to audit, and consistent controls

Consolidation simplifies access reviews and enables MFA, SSO, and encryption at scale.

Building your modernization strategy

Security leaders need a modern mainframe access platform that delivers specific capabilities. You should look for end-to-end encryption that protects all data in transit. You need centralized management for unified policy enforcement and simple access provisioning. The right solution must support your existing identity providers and offer robust auditing with granular session capture. It should also support both legacy and emerging mainframe protocols while allowing for rapid deployment.

To justify this consolidation, you can clearly quantify the return on investment. A typical enterprise supporting five different terminal emulators spends heavily on direct IT labor and indirect costs related to downtime. Consolidation can reclaim thousands of labor hours annually while de-risking your future audits.

Start by taking a thorough inventory of your existing emulators. Identify what tools you use, who uses them, and which applications depend on them. Engage your IT, security, and business leaders to understand their specific pain points. When you are ready, plan a phased migration. Pilot the new solution with high-risk departments first, measure your gains, and then expand across the organization.

Modernization starts with the basics: inventory, standardize, migrate in phases

Prioritize encryption, centralized policy, IdP integration, and granular auditing/session capture.

Real-world success stories

We see the power of consolidation across various industries.

A national bank recently struggled with mounting PCI DSS and SOX audit findings. They decided to standardize their access on a consolidated, secure terminal emulator. This move streamlined their log management and allowed them to apply access controls consistently. They ultimately achieved a successful audit outcome with zero major findings.

A prominent healthcare network previously juggled five different terminal emulators. By unifying their access, the IT team successfully rolled out encrypted sessions and multi-factor authentication across the entire enterprise. This upgrade enabled rapid breach investigation and ensured they met strict HIPAA audit requirements.

Similarly, an electric utility company subject to strict NERC CIP regulations deployed a single, enterprise-grade emulator solution. This transition provided comprehensive session monitoring and real-time alerting. They significantly reduced their regulatory risk and bolstered their incident management protocols.

How Rocket® Secure Host Access™ can help

We understand the responsibility you carry when managing mission-critical IT environments. Your modernization journey is too important to be disrupted by fragmented tools and security vulnerabilities. Rocket Secure Host Access provides the industry's leading secure terminal emulation platform, specifically designed for highly regulated, mainframe-centric organizations.

Rocket Secure Host Access seamlessly integrates with your existing enterprise security infrastructure. We provide robust auditing and centralized management capabilities that help you reduce risk, control costs, and confidently meet regulatory demands.

Let us partner with you to find the fastest wins and build a secure, unified foundation for your organization's future.

Talk to an expert

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-17758_WP_Consolidation_V2