White Paper

InfoConnect® Desktop
Reflection® Desktop
Rumba+ Desktop
Host Access Management and Security Server

Top 3 Reasons to Make Terminal Emulation Part of Your Security Strategy

Top 3 Reasons to Make Terminal Emulation Part of Your Security Strategy

You may not think of them this way, but your host applications are the lifeblood of your company. After all, they house the critical data underlying everything your business does. And they've been housing it for decades, long before the word *internet* entered our collective vocabulary.

Over the decades, the landscape around your host applications has changed. In our digital world, they are no longer safe on the famously secure mainframe. But what's a corporate IT department to do? The process of updating your priceless host applications is inherently complicated, expensive, and riddled with risk. At least that's what everyone has always thought.

But what if the tool that you use to access your host applications could also be used to protect them? This paper supports the power and logic of that solution. By the time you're done reading, you'll know why it's time to elevate the status of your terminal emulation software—letting it play a strategic role in your IT security strategy.

A Powerful, Logical Solution

Here are the top three reasons to revise your thinking about terminal emulation and give it a more strategic role in your enterprise:

1. **Terminal Emulation Software Is the Tool Used to Access Your Most Valuable Data.**
   Terminal emulation software is the gateway to your most valuable corporate jewels—your customer data, your intellectual property, your cutting-edge designs. Yet terminal emulators are generally viewed as basic commodities with no greater value than any other desktop application.

   Let's apply an analogy to this topic. Consider the game-changing television. Moving black-and-white images in two or three dimensions, with sound! People were amazed. Time brought color images, stereo sound, and bigger screens—but it was still a TV. Today, TVs have an expanded role. Many people, though not all, use them to surf the internet, Skype with friends, project slideshows, and more.

   The first terminal emulator was a game changer, too. People cleared those dumb terminals off their desks and began accessing host applications with their amazing new PCs. With time came more terminal types, printing, graphics, automations, and more. But you still had a basic terminal emulator. That was true until the last ten years, when terminal emulators became as easy to use as Windows apps, and just as easy to manage. They also became so secure that they can now facilitate compliance with even the most stringent security mandates.

2. **Advances in Terminal Emulation Technology Qualify It to Play a Leading Security Role.**
   The security offered by today's terminal emulator bears no resemblance to what came before it. Here's what the modern emulator can provide:

   - **Military-strength encryption**
     Today's terminal emulation solutions provide military-strength encryption for data in motion and at rest. Built to support the highest U.S. government security standards (FIPS 140-2 and DoD PKI), they provide TLS 1.2 encryption and SHA-256/RSA-2048 digital signatures. It's easy to configure your security controls and then update them as needed. This high level of security helps companies safeguard their information assets while meeting regulatory requirements.
   - **Strong mainframe passwords**
     If you have an older emulator, a simple eight-character, case-insensitive password is all that stands between a malicious

hacker and your precious host data. Today's terminal emulators can use your corporate Identity and Access Management (IAM) system to authenticate users all the way to the mainframe application. No more risky passwords to remember. No more password-reset headaches. Without recoding, you can facilitate compliance with today's highest-level security mandates—even for mainframe access.

- **Multifactor authentication for mainframe sessions**
  When you rely solely on usernames and weak passwords, you're practically handing hackers the keys to your kingdom. But reengineering mainframe applications to work with strong complex passwords is risky, difficult, and expensive. So what can you do?

  The good news is that you can do something. Modern terminal emulation solutions are built to provide the strongest possible authentication for your mainframe systems. Some solutions can support up to 14 different authentication methods—from smart cards and mobile text-based verification codes to fingerprint and retina scans. From this range of options, you can pick the ones that are easiest for your organization and partners to adopt.
- **Security proxy for the mainframe**
  Some terminal emulation solutions use a security proxy to build a virtual wall of protection around the mainframe. Using new security technology, the proxy ensures that only authorized users can get to the door of the mainframe (logon screen). This extra layer of security helps you control access and prove that you are compliant with regulatory requirements.
- **Information privacy and data masking**
  PCI DSS Requirement 3 of the PCI DSS standard calls for hiding cardholder data when it's displayed in a payment system. Not all terminal emulation solutions address this mandate. But some products give you the ability to easily mask any type of data on host screens—credit card numbers, contact information, social security numbers, birthdays, account balances, and other private information. You can even redact data as it is being typed into host sessions and prevent data from being stolen via screen or host printing. These capabilities place another barrier in the way of insider fraud and human error.

3. If You Don't Tend Your Terminal Emulation Garden, You Will Quickly Lose Control.
Companies have been using terminal emulation software for thirty-plus years. In that time, the products have changed dramatically along with everything around them. Like any garden left untended, this environment has likely cultivated lots of weeds and pests that need to be dealt with:

- **Old versions**
  If you think *my terminal emulators work, so why update them*, here's why: With security breaches and insider fraud on the rise, organizations must tightly protect their sensitive systems and data. If you don't update your emulators accordingly, you may be jeopardizing your networks, host systems, host data, and host-dependent business processes. You also risk being out of compliance with new government regulations and standards—including PCI-DSS, USGCB, FDCC, ENISA, and FIPS 140-2. Modern terminal emulators are equipped to facilitate compliance. Older versions are not.
- **User settings**
  Terminal emulation clients typically allow users to record macros and change settings to streamline work processes. But when users share their macros and unintentionally weaken security settings, they introduce risk to the enterprise. You need to know who owns the macros in your enterprise, who's using them, where they are stored, and what they do. You need to be able to customize and control settings for users and groups. Secure terminal emulators provide the granular controls to help you do that.

In large organizations with 1000s of desktops across 100s of locations, strong security isn't possible without strong management. With todays' terminal emulation solutions, you can manage your host-access operation centrally. In other words, from a central server you can easily lock down desktops to prevent the use of rogue macros and changes to security settings. You can grant or deny access based on group or role via your IAM system. You can make post-install adjustments on the fly. Users typically receive their updates when they launch a session.

Put Your Garden in Order

When assessing the security of your host systems, applications, and data, don't forget to also assess the tools they work with—specifically, your terminal emulators. Just because your emulators have always worked smoothly, that doesn't mean they always will. In the last five to ten years, some of them have made notable advancements—advancements that will change the way you think about terminal emulation.

For more than 30 years, Micro Focus has developed highly secure terminal emulation products and helped customers seamlessly move to more secure solutions. We focus our development efforts on staying ahead of what's going on around your terminal emulator. That means our solutions are always equipped with the latest security technologies, and they're always ready to help you navigate the ever-changing IT security landscape. For that reason, they must play a key role in your overarching IT security strategy.

☎

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com

MICRO® FOCUS