The Perils of Aging Terminal Emulators: Why Older Emulators Present a High Security Risk
The Perils of Aging Terminal Emulators

Data on host systems is often the most sensitive on the network. Terminal emulators on the desktop provide access to these systems, but many organizations are still using older products, deployed using best practices from many years ago.

Older terminal emulators often don’t allow organizations to comply with current security standards, and they don’t give IT administrators the customization control they need to properly secure their network. Yet many companies are unaware of the inherent risks of staying with older products.

Does your terminal emulation client conform to modern security standards? Is your key business and customer information secure? Because security breaches and insider fraud are on the rise, organizations must protect their sensitive data more tightly and comply with new government regulations and standards such as PCI-DSS, USGCB, FDCC, and FIPS 140, which are designed to strengthen desktop deployment and data security.

Staying on an older emulator can put your networks and your sensitive data in a vulnerable position. But modernizing your terminal emulation deployment can keep you compliant and protect against threats.

Here are five reasons why you should consider updating your terminal emulation product:


If you’re using an older terminal emulator, the product’s SSL/TLS and SSH encryption and authentication technology probably isn’t secure.

Although most emulators include SSL/TLS and SSH technologies, which provide secure authentication to host systems and encrypt transmission of sensitive corporate data, hackers expose new vulnerabilities in these protocols nearly every month.

With terminal emulation products, fixes to these vulnerabilities aren’t automatically pushed to customers; instead, they’re addressed in product updates. If you’re not using the latest version of your product, you’re likely exposed to a number of vulnerabilities in your SSL/TLS and SSH protocols.

In older emulation products, these protocols aren’t lacking just important security fixes. They’re also missing new capabilities that have been added over the years, particularly on the authentication side, to better secure your connections to host systems. These additional safeguards aren’t available until you upgrade your terminal emulator.

To provide truly secure host connectivity, your emulator should contain military-strength SSH and SSL and be certified with the latest standards.


Do you know where your macros are in the enterprise? What do they do? If you don’t know the answers to these questions, you’re exposed to a large, unknown risk.

All terminal emulation clients allow end users to record macros to automate their daily tasks. Most terminal emulators allow customers to build sophisticated macros using tools like Visual Basic for Applications (VBA). These advanced macros might allow users to record everything typed into a host system, including sign-on credentials. Or they might allow repetitive crawling through screens to extract or update data on the host. Not only that, deployment practices from years ago allow users to easily share risky macros like these via email and sneaker-net.

Do you have any of these macros in the enterprise? If so, who owns them? Can they be easily shared?
To effectively manage macros and other automated tasks, your emulation client should allow administrators to deploy terminal emulation with granular controls, so that only trusted macros can be executed.

3) Tracing Features Allow the Capture of Sensitive Corporate Data.
Most older terminal emulation deployments include a tracing feature that allows end users to record to an unencrypted file all data visible during a host session. Once in a file, this sensitive information could easily leave the PC—and your enterprise—via email or portable media.

All terminal emulators provide a tracing facility; however, your product should allow you to disable or prevent access by end-users. The easiest way to do so is through the use of the User Account Control Elevation feature on Windows 7. This feature gives administrators granular control over the facilities an end-user can access.

4) Older Terminal Emulation Clients Don’t Mask Data.
Sensitive data is just a CTRL-C away from leaving most terminal emulators. Most older emulators allow users to email a host screen using the installed email system. This lack of data masking makes it easy for end-users to share sensitive information with other applications.

A modern terminal emulator should provide advanced features like privacy filters, which allow administrators to prevent certain patterns of data from leaving the application. For example, sensitive data such as credit card numbers, social security numbers, and other personal information can be prevented from reaching the clipboard, Word documents, and Outlook emails—and also from being printed. Through pattern matching technology, the information is redacted as it leaves the host application.

5) It Starts with a Secure Development Lifecycle.
Your terminal emulation vendor should utilize a well-documented Secure Development Lifecycle that will help protect you from security threats. Your vendor should make security the number-one priority for each new release or update, and should have a dedicated security team that oversees the development and certification of its security technologies. Security features should not be simple check-box items; instead, intensive security testing and threat modeling needs to be performed in order to help maintain the integrity of your business applications.

For more than 30 years, Micro Focus® has developed highly secure terminal emulation products and helped customers seamlessly upgrade from less secure products. Through our deep experience, which includes dedication to a Secure Development Lifecycle, we can help you to address crucial security risks—and gain control of your terminal emulation desktops.