Virtel Web Access

Seven Vulnerabilities of Thick-Client TN3270 Emulators That Compromise Mainframe Resources

Security is paramount to most organizations, including those whose business relies on mainframe 3270 applications. However, accessing applications through thick-client TN3270 emulators exposes them to web attacks.

These seven vulnerabilities of thick-client TN3270 emulators can be eliminated by migrating to a thin-client, browser-based 3270 terminal emulator such as Virtel Web Access.

1. Exposed Terminal Emulation Code

Thick-client TN3270 emulators rely on code components running on user devices. Typically coded in Java, these code components require installing Java Virtual Machines on the user devices. They may be permanently installed on the devices or dynamically uploaded at login.

Java is vulnerable to cyber attacks. Periodic Java security updates must be deployed flawlessly to hundreds or thousands of remote workstations.

In addition to the complex and costly required maintenance, terminal emulation code running on a user device could be compromised and used for unauthorized access to mainframe applications. Even one compromised user device could expose your mainframe assets to a web attack.

Virtel Web Access does not use code components running on the client side that could be compromised and used for unauthorized access to mainframe assets. Instead, Virtel serves hardened terminal emulation pages to the browser, which renders them as emulated 3270 screens. Modern browsers – Edge, Chrome, Firefox, and Safari – have undergone a systematic hardening transformation in recent years.

A browser-based terminal emulation solution such as Virtel Web Access is the most secure way to access 3270 applications via the internet.

Find out how **Virtel Web Access** solves these security problems:

1 Exposed terminal emulation code
2 Reliance on outdated browsers
3 Exposed unaudited macros
4 Threatened IAM integration and SSO implementation
5 No access audit trail
6 Third-party mainframe access
7 Exposed 3270 fields

2. Reliance on Outdated Browsers

Modern browsers have deprecated the Java plugins that some legacy TN3270 emulators rely upon. Some users may still be using older browsers with outdated TN3270 software.

VWA provides modern browser-based 3270 terminal emulation, eliminating the risk of outdated browsers and device-based TN3270 terminal emulators.

3. Exposed Unaudited Macros

User-developed TN3270 emulation macros are a real security threat for mainframe assets because they are developed without consideration for mainframe asset security and without oversight from the mainframe security team. They may contain unencrypted login credentials or submit many CICS transactions from Excel sheets. It only takes one compromised TN3270 workstation hosting such user-defined macros to expose the mainframe assets to a cyber attack or runaway CPU processing.

The best way for the mainframe technical team to inventory, audit, and secure user-developed macros is to deploy a 3270 TE solution such as Virtel Web Access where macros are stored safely on the mainframe behind the firewall.

4. Threatened IAM Integration and SSO Implementation

Identity and Access Management systems, typically referred to as IAMs, and Single Sign-On (SSO) methodologies utilize a combination of active directory, multi-factor authentication, PIV, LDAP, SAML, OKTA, Shibboleth, and other such technologies. They are essential for robust resource access authentication and authorization.

Virtel integrates seamlessly with IAMs and supports modern SSO efforts.

IAMs are now following the same track that browsers did years ago. They are progressively deprecating access from code components running on the user's device and restricting access to calls issued from web browsers. This means that eventually, TN3270 emulators that rely on code components running on the user's device will likely no longer be able to access IAMs for authentication, authorization, and SSO purposes.

5. No Access Audit Trail

Some legacy TN3270 emulators do not log the origin or the end-user identification of accesses to 3270 applications. When an unauthorized access results in the loss, alteration, or theft of corporate data, the mainframe security team cannot retrieve and prove with irrefutable evidence the origin of the attack and the identity of the attacker.

A modern, web-based 3270 TE solution such as Virtel Web Access logs all 3270 application access origins in a central location, which provides security auditors the data they need to react to unauthorized access.

6. Third-Party Mainframe Access

Many organizations rely on a Virtual Private Network (VPN) to encrypt the data exchanged through 3270 TE connections, in part because the VPN is also used to access non-mainframe systems and applications. In situations where third-party (non-employee) access to certain mainframe applications is only needed, that access via TN3270 software would still require a VPN connection that might inadvertently expose other IT systems and assets to unauthorized access.

A web-based 3270 emulation solution such as Virtel Web Access leverages IBM AT-TLS cryptography software or an ICSF cryptographic card, resulting in SSL-encrypted 3270 TE connections that are FIPS 140.2 and TLS 1.2/1.3 compliant and do not require a VPN connection for third-party mainframe users.

7. Exposed 3270 Fields

Application developers can specify 3270 screen fields as hidden, unprotected, or protected. With legacy 3270 terminal emulators, those settings are enforced by the TN3270 emulation code running on the user device. If that code is compromised by a cyber attack, the attacker may be able to see the hidden fields and change the protected fields.

Virtel Web Access enforces 3270 field settings on the host itself, behind the host firewall. VWA doesn't send hidden fields over the internet and it terminates the user session if protected fields return changed from the user's device.

Control of access to mainframe assets belongs on the mainframe

Legacy TN3270 emulators are distributed solutions with code components running on hundreds or thousands of remote user devices. With this type of solution, remote user devices control access to mainframe assets. The mainframe technical team has no choice but to rely on the desktop technical team and on users to protect access to mainframe assets. This is a potentially unsecure and unreliable solution.

With Virtel Web Access, the mainframe technical team regains control of access to the assets that they are expected to protect. To fully secure mainframe resources, control mainframe access from the mainframe.

For information about Virtel Web Access, please visit sdsusa.com/vwa.

Quality Mainframe Software Since 1982

Software Diversified Services delivers comprehensive, affordable mainframe and distributed software with a focus on cybersecurity and compliance. Hundreds of organizations worldwide, including many Fortune 500 companies, rely on SDS software. Our expert development and award-winning technical support teams are based in Minneapolis, MN.