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
2. Reliance on Internet Explorer
3. Exposed unaudited macros
4. Threatened IAM integration
5. No access audit trail
6. VPN-dependent encryption
7. Exposed 3270 fields

Find out how Virtel Web Access solves these problems.

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 notorious for its vulnerability 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 maintenance effort required, 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 through the internet.

2. Reliance on Internet Explorer

Modern browsers have deprecated the Java plugins that some legacy TN3270 emulators rely upon. Internet Explorer (IE) is the only browser to still support this now-outdated technology, and Microsoft is in the process of retiring IE. Most organizations would like to migrate from IE to a modern browser, but they can't because of their TN3270 emulator.

To take advantage of modern web-browsing technology and to avoid relying on an unsupported browser after Microsoft pulls the IE plug, a web-based 3270 terminal emulation such as Virtel Web Access should be deployed.

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.

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

4. Threatened IAM Integration

Identity and Access Management systems – typically referred to as IAMs - are 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.

IAMs are now following the same track that browsers did a few 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 in the near future, TN3270 emulators that rely on code components running on the user's device will likely no longer be able to access IAMs for authentication and authorization.

5. No Access Audit Trail

Legacy TN3270 emulators do not log the origin – more specifically, the end-user identification – of 3270 application accesses. 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. VPN-Dependent Encryption

Telnet connections have been encryptable for years. However, many organizations still 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 corporate applications. But VPNs can have high licensing costs, high support requirements, and slow response times.

Migrating to a web-based 3270 TE solution such as Virtel Web Access that leverages IBM AT-TLS cryptography software or an ICSF cryptographic card results in SSL-encrypted 3270 TE connections that are both FIPS 140.2 and TLS 1.2/1.3 compliant. It is no longer necessary to license, deploy, and support a VPN to encrypt data exchanged over the internet.

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 the 3270 field settings on the host itself, behind the host firewall. Virtel doesn't send hidden fields over the internet and it terminates the terminal emulation 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*.