Advantages of a Native Hardened Tomcat Server Over Citrix or Microsoft RDS in a clinical environment

A white paper

DANNY LIEBERMAN

Dec 3, 2024

Abstract

Using a native hardened Tomcat server for remote access to clinical systems offers significant advantages over Citrix or Microsoft RDS. Tomcat minimizes attack surfaces, simplifies compliance, enhances security customization, and reduces resource consumption. Its browser-based access eliminates client-side software vulnerabilities, offering a cost-effective, secure, and high-performance solution tailored to clinical environments.

In-depth discussion

Reduced Attack Surface: A native hardened Tomcat server is tailored to serve specific web applications, minimizing unnecessary services and ports. This reduces the potential entry points for attackers compared to Citrix or Microsoft RDS, which are complex systems offering a wide range of services and functionalities.

Fewer Known Vulnerabilities: Citrix has a substantial number of CVE records (over 310), indicating known vulnerabilities that could be exploited if not properly managed. While Apache Tomcat also has vulnerabilities, a hardened and well-maintained Tomcat server can mitigate these risks more effectively due to its simpler architecture and focused functionality.

RDP (the underlying protocol layer of Windows RDS) has 148 vulnerabilities including Sensitive information disclosure reported in the past 3 months.

Browser-Based Access Minimizes Client Risks: By providing access via standard web browsers, the Tomcat solution eliminates the need for additional client-side software installations required by Citrix or RDS. This reduces the risk associated with client-side vulnerabilities and simplifies updates and patch management on the client side.

Enhanced Security Customization: A native Tomcat server allows for granular security configurations. Administrators can implement specific security policies, encryption standards, and authentication mechanisms that align closely with the organization's compliance requirements, something that may be more restrictive or complex to implement in Citrix or RDS environments.

Simplified Compliance Management: Managing compliance is more straightforward with a dedicated application server. The Tomcat server can be configured to meet specific standards such as HIPAA or GDPR by focusing on the web application's security, whereas Citrix or RDS environments might require comprehensive policies covering a broader system scope.

Isolation of Application Environment: The Tomcat server runs the web application in an isolated environment, reducing the risk of cross-application vulnerabilities and data leakage. Citrix and RDS provide access to a full desktop environment or multiple applications, increasing the potential for unauthorized access to other system areas. This places additional load on IT operations.

Efficient Patch Management: Keeping the Tomcat server updated is a more streamlined process due to its singular focus. In contrast, Citrix and RDS environments are more complex, potentially delaying critical updates and patches, which can leave vulnerabilities exposed for longer periods.

Lower Resource Consumption: A hardened Tomcat server typically requires fewer system resources than Citrix or RDS solutions. This not only reduces costs but also limits the potential impact of Denial-of-Service (DoS) attacks that exploit resource-intensive services.

Improved Audit and Logging Capabilities: With a focused application server, logging and monitoring can be tailored specifically to the clinical application's activities, enhancing the ability to detect and respond to security incidents promptly. Citrix and RDS environments generate extensive log records that are not integrated with the clinical application, making incident impact analysis on the clinical data and systems more difficult.

Reduced Dependency on Third-Party Software: Relying on Citrix or RDS introduces dependencies on third-party platforms, which may have their own security vulnerabilities and compliance issues. A native solution from the clinical system vendor reduces this dependency, allowing the organization to maintain greater control over its security posture.

Flexibility in Security Protocols: The Tomcat server can be configured to use the latest security protocols and ciphers, ensuring encrypted communication meets current standards. This flexibility might be limited in Citrix or RDS environments due to compatibility requirements with client software.

Cost-Effective Security Measures: Implementing security controls on a native Tomcat server can be more cost-effective, allowing for investment in additional security tools such as web application firewalls (WAFs) or intrusion detection systems (IDS) specifically designed for web applications.

Performance: The performance of a Web application server depends on several factors, including network latency, request processing time, and resource allocation. When you add layers, such as Citrix or Windows Remote Desktop Services (RDS), you're effectively adding intermediaries that can impact throughput, either positively or negatively.

Conclusion

Choosing a native hardened Tomcat server for remote web access offers significant cost of ownership and security and privacy compliance advantages over Citrix or Microsoft RDS solutions. By minimizing complexity, reducing the attack surface, and allowing for tailored security configurations, organizations

can better protect sensitive data and meet stringent compliance requirements. Additionally, the reduced number of known vulnerabilities and the ability to efficiently manage patches and updates make the Tomcat solution a more secure and manageable option for laboratories handling critical imaging and analysis data.

About the author

Danny Lieberman is a cybersecurity and healthcare technology executive currently serving as the WHO European region's cybersecurity and privacy advisor. As founder and CEO of FlaskData.io (acquired 2024), he led the Digital CRO to support 70+ clinical trials and 5 FDA approvals. Previously, at Open Solutions, he developed an innovative threat analysis methodology for medical devices, serving Israeli medical device vendors and large US organizations like Dignity Health and Johnson & Johnson companies. With expertise spanning clinical data technologies and cybersecurity, Danny has a unique perspective on implementing robust real-world solutions for clinical applications.

Danny Lieberman can be reached at dl@dannylieberman.com, @dannylieberman (LinkedIn), and @flaskdata (X).