

# Browser in the Box Terminal Server Safe surfing in terminal server environments

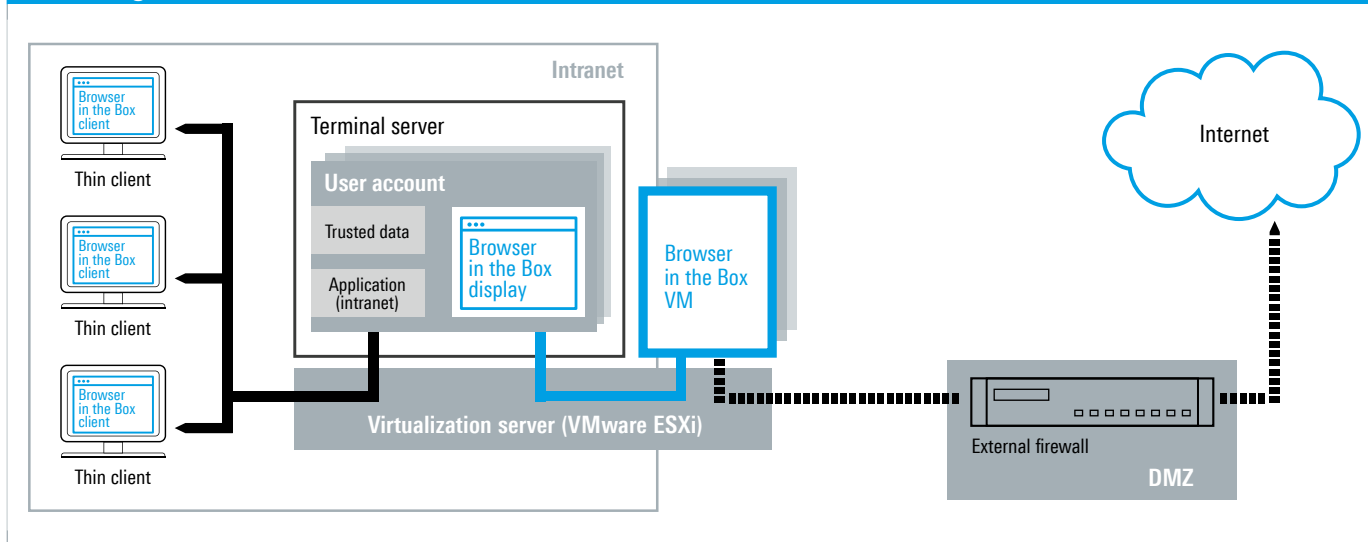
Browser in the Box for Terminal Server makes the tested and proven security concept of Browser in the Box available for terminal server environments. Users can work in their browsers as usual, while all sensitive data is protected.

Browser in the Box, a virtual surfing environment developed in cooperation with the German Federal Office for Information Security (BSI), offers a new approach for secure and comfortable web surfing. The technology was initially designed for the highest security requirements of federal authorities, Browser in the Box for Terminal Server is now also available for terminal server and thin clients.

In terminal server infrastructures, a Windows Server usually runs in a virtualized environment of the type provided by Citrix, VMware and Microsoft. The Windows Server provides a desktop session to each user, with the thin client only displaying the session. With Browser in the Box for Terminal Server, the browser does not run in the Windows Server desktop session, but on a separate virtual machine. Only the browser interface is transmitted to the desktop session for display. This allows for a reliable isolation of the intranet from the Internet. Thanks to this flexible architecture, Browser in the Box for Terminal Server can be integrated into existing virtual infrastructures. It is no longer necessary to use dedicated terminal server (which have high administrative overhead and lack the desired level of security) as a surfing alternative. Central management makes it easy to implement security policies and configurations as well as to generate, certify and distribute the necessary guest images.



## Block diagram of Browser in the Box – Terminal Server



### New security mechanism

Users are provided a virtual machine which is separated from the computer's operating system. This virtual machine has a hardened operating system running a web browser. Thanks to the separation of the Internet and the internal network, malware cannot infiltrate the company network, but is isolated in the virtual environment outside of the company network. Every time the virtual machine is restarted, it is reset to factory settings and cleared of any potential infections providing cost-efficient and care-free surfing at full performance.

### An innovative solution

Unlike the basic sandboxing method used in standard browsers, Browser in the Box for Terminal Server completely separates all browser activities from the company network by isolating the entire guest operating system. There is only one folder in the base operating system that is accessible to a specific user account. This is where the browser's persistent configuration data (bookmarks etc.) is saved. Downloaded data is saved in this folder, scanned for malware and only then moved to the regular downloads folder. This technology also prevents users from accidentally uploading documents to the internet. This way, companies can ensure that their confidential data is not leaving the internal network.

### Enterprise solution with central management

Browser in the Box for Terminal Server offers a comfortable central management for the professional use in centrally managed IT environments. It enables the comfortable management of security regulations and configurations as well as the generation, signature and distribution of guest images. The browser VMs are directly connected to an external network. From this network, only the Internet or a proxy can be accessed. Intranet portals can be accessed with any other browser. A configurable browser sniffing ensures that the correct browser is opened automatically, thereby implementing a two browser strategy that is both secure and easy to use. Browser in the Box thereby makes surfing the web cost-efficient, carefree and comfortable.

**Rohde & Schwarz Cybersecurity GmbH**  
Muehldorfstrasse 15 | 81671 Munich, Germany  
Info: +49 30 65884-223  
Email: [cybersecurity@rohde-schwarz.com](mailto:cybersecurity@rohde-schwarz.com)  
[www.cybersecurity.rohde-schwarz.com](http://www.cybersecurity.rohde-schwarz.com)

**Rohde & Schwarz GmbH & Co. KG**  
[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG  
Trade names are trademarks of the owners  
PD 3607.5719.32 | Version 02.00 | January 2018 (sch)  
Browser in the Box Terminal Server  
Data without tolerance limits is not binding | Subject to change  
© 2016 - 2018 Rohde & Schwarz Cybersecurity GmbH | 81671 Munich, Germany



3607571932