Browser in the Box TS

Effective protection against malware and exploits

Support for terminal servers and virtualized server environments

Safe web surfing through isolating the Internet from the intranet

Nowadays, it's hard to imagine our daily work without the Internet. But PCs are also used to process critical and confidential information related to personnel and internal operations and the immense benefit of the Internet comes with constantly evolving threats. Recent browser developments are not simply advances in functionality and convenience. They are first and foremost a series of battles in the ongoing war against different attack scenarios.

Ever since the development of Web 2.0, when the Internet became active, the balance between threats and benefits has been lost. Today's websites could not exist without the „active content" that makes these sites more or less indis-tinguishable from full-featured native computer applications.

Programming languages like JavaScript, Java, ActiveX and VBScript include techniques for accessing the user's PC, e.g. the file system or a connected webcam. Trojan horses and viruses can exploit these new and powerful capabilities to access confidential data. Companies and authorities alike are facing a dilemma. Either they must significantly limit Internet use (by various means) or find a way of living with the threats. Existing technologies such as antivirus software are no longer capable of preventing attacks that exploit weaknesses in the browser or operating system. Even if computer systems are regularly patched, zero-day exploits can enable attackers to successfully penetrate the systems. Besides such targeted attacks, companies and authorities can suffer damages in other ways, too. Due to the large number of infected servers on the web, the risk of infection even during ordinary websurfing is sufficiently high as to entail significant costs. For example, client machines must be routinely reinstalled and reconfigured after infections occur.

An innovative solution: Browser in the Box

Initially developed by Sirrix on behalf of the German Federal Office for Information Security (BSI) for use by federal authorities in Germany, the Browser in the Box virtual surfing environment allows users to safely browse the Internet. The proactive security-by-design concept can even protect against new vulnerabilities and malware. Browser in the Box provides a virtual machine with a hardened operating system and an encapsulated web browser. Malware cannot penetrate the host operating system, and any damage to the separate virtual machine (VM) disappears when the browser restarts since the VM returns to a certified starting state. All of this takes place transparently for the user.

Protection against exploits and malware

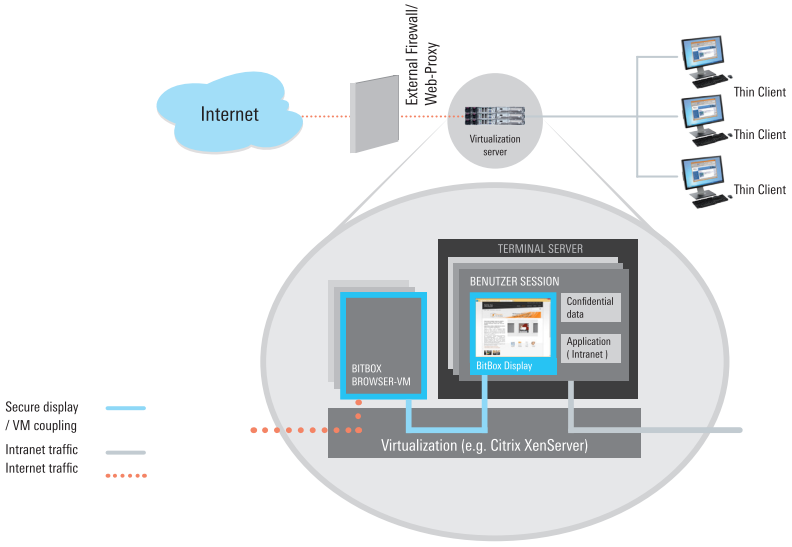
In contrast to the basic sandboxing methodology implemented in standard browsers, Browser in the Box fully isolates all browser activities from the host operating system. Only one single shared folder in the host operating system is accessible using a separate user account. All of the browser's persistent configuration data, such as favorites, is stored there. Similarly, all files downloaded from the Internet are initially stored in this folder and are only forwarded to the user's normal download folder after

Browser in the Box TS

a malware scan has been performed. When the host system is protected in this manner against attacks from the Internet, the confidentiality of critical internal information is not jeopardized by simply providing Internet access to employees. Browser in the Box provides a cost-effective and worry-free surfing environment – without any loss of convenience or performance.

Browser in the Box for Terminal Servers

The proven Browser in the Box concept is also available for centrally virtualized infrastructures with terminal servers and thin clients. In terminal server infrastructures, a Windows Server runs in a virtualized environment of the type provided by Citrix, VMware and Microsoft. The Windows Server provides a desktop session to each user. This session is displayed on the thin client. With Browser in the Box for Terminal Servers, the browser runs on a separate virtual machine instead of in the Windows Server desktop session. Only the browser display is transmitted to the desktop session for display, reliably isolating the intranet from the Internet. The flexible architecture allows Browser in the Box for Terminal Servers to be integrated into existing virtual infrastructures. It is no longer necessary to used dedicated terminal servers (which have high administrative overhead and lack the desired level of security) as a secure alternative. Central management makes it easy to implement security policies and configurations as well as to generate, certify and distribute the necessary guest images.



Features

Basic characteristics

- Supported operating systems: Windows Server 2008/2012/2012 R2 in Citrix infrastructure

Security

- Browser runs fully isolated on virtual machine with its own operating system
- Downloaded files are first scanned and then made available to user
- Secure printing of pages from Browser in the Box via client
- Secure cut & paste, configurable via policy
- Prevention of file uploads (optional)
- Browser resets to certified initial image whenever it is restarted
- Browser configuration data can be stored persistently and retained after reset
- Isolation of intranet from Internet

Convenience

- Transparent use just like normal browser
- Easy installation
- Convenient management system for security policies, configurations and images
- Active Directory integration

Rohde & Schwarz Cybersecurity
Sirrix AG
Campus Gebäude D3 2
66123 Saarbrücken Germany

Phone +49 681 959 - 860
Fax +49 681 959 86 - 500

Email cybersecurity@rohde-schwarz.com

cybersecurity.rohde-schwarz.com