Browser in the Box
Effective protection against attacks from the Internet

Safe web surfing through isolating the Internet from the intranet

Protection against malware, zero-day exploits and APT

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 as well as Web 2.0 are not simply advances in functionality. They are first and foremost a series of battles in the ongoing war against different attack scenarios. Programming languages like JavaScript, Java, ActiveX and VBScript include techniques for accessing the user's PC, e.g. the file system. Trojan horses and viruses can exploit these new and powerful capabilities to access confidential data.

New approach with Browser in the Box

The Browser in the Box solution was initially developed by Sirrix on behalf of the German Federal Office for Informa-tion Security (BSI). It uses a totally new secure approach to protect against threats from the Internet. It enables users to safely surf the Internet despite the usual warnings to the contrary – even when using convenient, state-of-the-art web technologies.

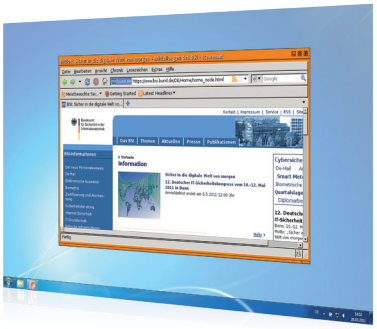
Browser in the Box provides a virtual machine with a hardened operating system and an encapsulated web browser. Malware cannot penetrate the host operating system, and any damage to the separate virtual machine (VM) disappears when the browser restarts since the VM returns to a certified starting state. All of this takes place transparently for the user. This innovative concept ensures continuous protection – even against new and unknown types of attacks. The level of protection does not increase and decrease with the malware detection rate as is the case with signature- and behavior-based approaches.

Protection against malware and data loss

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 a malware scan has beenperformed. In addition to monitoring downloads, Browser in the Box also monitors uploading of files to the Internet, effectively preventing critical data from reaching third parties via an unintentional upload.

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 secure surfing environment – without any loss of convenience. It is no longer necessary to use the dedicated terminal server (a costly approach with high administrative overhead) as a secure surfing alternative. The performance im-



Browser in the Box

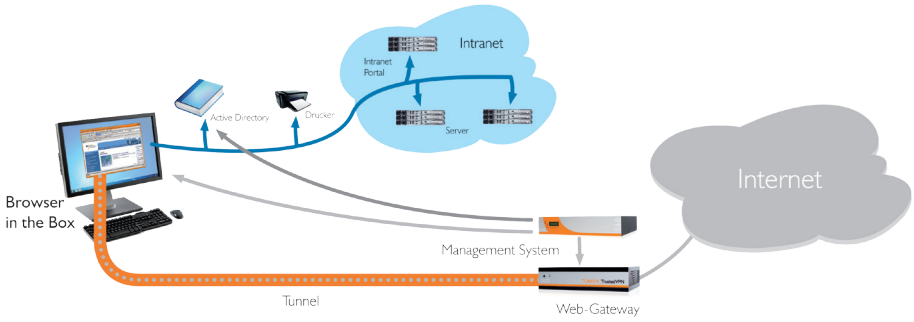
pact is minimal for today's computer architectures.

This innovative concept ensures continuous protection – even against new and unknown types of attacks such as zero-day exploits and advanced persistent threats (APT). The level of protection does not increase and decrease with the malware detection rate as is the case with signature- and behavior-based approaches.

Browser in the Box Enterprise with directory service support and central management

Browser in the Box Enterprise with directory service support and central management

Browser in the Box Enterprise provides central management for professional applications in managed IT environments. Central management makes it easy to implement security policies and configurations as well as to generate, certify and distribute the necessary guest images. A tunnel is transparently integrated between Browser in the Box and a central Internet gateway to reliably isolate the Internet from the intranet. While other applications on the client can only access the internal corporate network, Browser in the Box has a tunnel to the outside and is the only application that can access the Internet – isolated from other client applications.



The enhanced version, Browser in the Box Enterprise, completely isolates the workstation and its host operating system from the Internet. Only the virtual machine with its encapsulated browser is connected to the Internet via a tunnel.

Features

Basic characteristics

- Supported operating systems: Windows XP, Windows 7, Windows 8
- Supplied components: VirtualBox, Firefox or Chrome (selectable)

Security

- Browser runs exclusively on an isolated virtual machine with its own operating system
- Internet downloads are first scanned and then made available
- Secure printing of Internet content via client
- Secure cut & paste, configurable via policy
- Prevention of file uploads (optional)
- Resets to certified start image when browser is restarted
- Browser configuration data can be stored persistently and retained after reset

Convenience

- Transparent use just like normal browser
- Easy installation – no special knowledge required

Central management with TrustedObjects Manager

- Convenient management system for security policies, configurations and images
- LDAP and Active Directory integration
- Isolation of intranet from Internet via a tunnel between Browser in the Box and Internet gateway

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