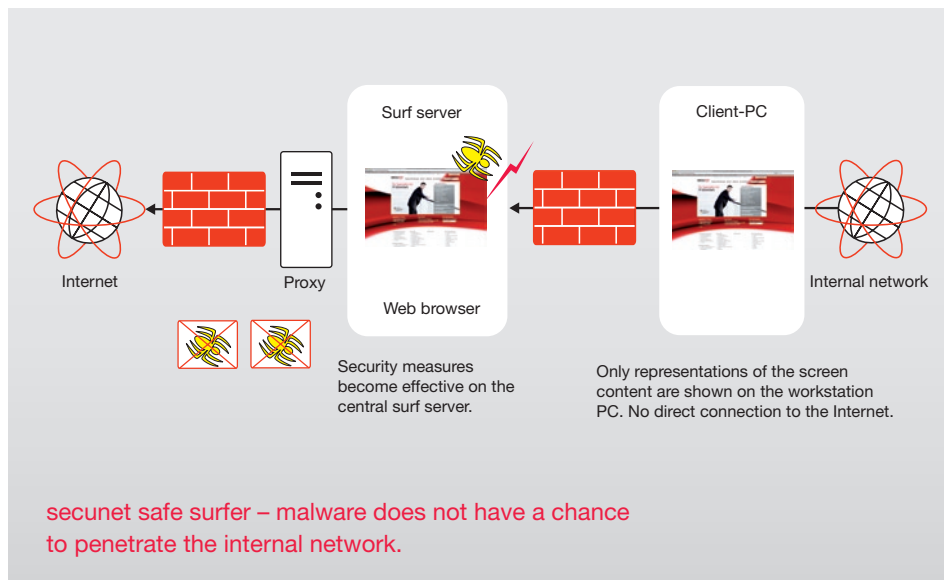


Secure Protection against Malware



Benefits:

- » Highly secure protection of the workstation PC against malware
- » Policy-compliant security as a result of central administration
- » Secure use of active content also in the classified sector

secunet safe surfer protects your systems and data against attacks from the Internet as you surf the web. Access to the Internet is via a Remote-Controlled Browser System (ReCoBS). Only screen data is displayed at the workstation. **The advantage: the workstation no longer has direct access to the Internet. Confidential data on the PC are protected against malware in a highly secure way.**

secunet safe surfer – the secure way to the Internet

It is impossible to imagine a modern workstation that does not use the Internet. However, the risk of malware gaining access to the workstation unnoticed while the user surfs the web is still high. Virus scanners are no longer able to provide 100% protection of the workstation against targeted attacks. Especially in the case of high-security environments or the processing of classified data at the workstation, Internet access is often only permitted from separate workstations. With secunet safe surfer, we have developed a solution which enables secure and convenient web surfing even from workstations with data requiring high security. Intelligent separation of the web browser and the workstation makes it impossible for malware to gain access to the workstation while the user surfs. The user's web browser is relocated to a central surf server which is specially secured vis-à-vis the Internet. The user only receives a representation on screen of the websites and has no direct access to the Internet.

Secure surfing now convenient

The secunet safe surfer was developed according to the specifications of the German Federal Office for Information Security (BSI). The solution consists of client and server components which are intelligently combined to allow secure and convenient surfing. On the main server, active content is only executed under strong restrictions. This provides better protection of sensitive data at the workstation. The following functions support convenient use of the Internet:

- E-mail transmission of downloads and printouts to the user
- E-mail transmission of PDF printouts
- Direct document printing on standard printers
- Copy & paste functions
- Image data compression

In the case of large numbers of users, the solution can be distributed across several servers for greater availability in addition to being set up redundantly.

ReCoBS-compliant security mechanisms

Separating the web browser and the workstation is not sufficient to ensure secure protection against attacks from the Internet. The ReCoBS-compliant secunet safe surfer has further security mechanisms available. The solution supports the ReCoBS Protection Profile (PP) and can be evaluated according to Common Criteria (CC). This makes it possible to use the system even in environments with very high security requirements. With the secunet safe surfer, the following security mechanisms are implemented:

Automated integrity check daily

The central surf server automatically starts from a secure boot medium and checks the integrity of the installed system against a reference database. The security officer is automatically informed of manipulations of the system. Then the entire system is reinstalled, also automatically. Re-installation deletes any malware which may have been installed while the user was surfing.

Stringent restriction of system rights

The user sessions on the surf server are assigned only minimal rights to operating system functions, ensuring that other user sessions are not jeopardised. Malware executed on the server is unable to read or change system files or sensitive data.

Centrally updated software

Users remain able to manage their own bookmarks as usual. Browser software, browser plug-ins and the operating system are updated via a central repository by simply booting from a storage medium which has been secured in terms of integrity. This approach guarantees that users always have current versions of software and browsers as well as the recommended configurations.

Pseudonymisation of user data

For security reasons, the central server stores no internal user data, e.g. internal user IDs. A proxy service hides the IP addresses of the internal network. For reasons of data protection, user profiles are pseudonymised and stored. It is impossible for third parties to make assignments to internal users from the Internet. Administrator rights are required to make these assignments.

Protected logging

The log data on events on the surf server are logged by a management server. The two servers are separated from each other by means of a packet filter. In this way, it is possible to store log data independent of the security of the surf server.

Reference Project: German Federal Chancellery

secunet safe surfer has been in use at the German Federal Chancellery since January 2007. secunet implemented an architecture with three servers operating in parallel for more than 500 employees. Feedback to date from users has been entirely positive; prior to this, access to the WWW was awkward as it was only possible via encapsulated PCs which were separated from the network. Being able to access the Internet from the workstation without risk to the internal network has improved the way staff works.

More information:
www.secunet.com/en/safesurfer