secunet (safe surfer

In a nutshell: 360° internet protection

Your benefits:

- » Maximum security by physically isolating the workplace from the internet
- » Ultra-convenient for the user – no restriction of functionality
- » Various operating modes: centralised, on the go or 'as a service'
- » Flexible licence model
- » High level of automation
- » Can be configured and integrated in the standard
- » Managed centrally

Cyber attacks are constantly increasing in both quality and quantity and, when successful, usually lead directly to the execution and dissemination of malicious codes within trustworthy corporate networks. Sensitive data are siphoned off unnoticed, or are encrypted. This risks massive productivity restrictions, loss of data and damage to reputation. The biggest threat continues to come from internet use in the workplace, and cannot reliably be curbed using traditional forms of protection such as virus scanners, firewalls or content filters. The solution to the problem is isolation.

The principle behind secunet safe surfer

Even the most secure browser in the world does not offer sufficient protection if it isn't also embedded in the most secure overall architecture. secunet safe surfer separates the workplace systems from the internet at a physical level.

This principle is based on the ReCoBS architecture of the Federal Office for Information Security (BSI).

Every browser session is therefore executed in a sealed-off environment within a specially hardened Linux system that in turn runs in a separate network segment (DMZ) on terminal servers. The workplace browser is controlled remotely via video stream over a secured channel. No content is transmitted, only audio and image data. The majority of the attacks that are targeted at Windows-based security vulnerabilities are already successfully averted in the Linux environment. However, further security mechanisms and zones in the overall architecture still protect from attacks even if the browser has been compromised. The physical separation of the workplace and browser system additionally provides protection from hardware-related attacks such as Spectre, Meltdown and Zombie-Load. Moreover, all terminal servers are regularly restored to their original settings free of tampering. This ensures that any potential malicious code is effectively destroyed.

The user's workplace remains separated from the internet at all times. It is therefore also protected against reloading malicious code through infected files that have managed to get through to the computer in e-mail attachments or via USB sticks.

secunet safe surfer offers reliable protection from

- » New and unknown types of attacks (zero day exploits)
- » Targeted attacks (APT, Advanced Persistent Threats)
- » Browser vulnerabilities
- » Infected websites and e-mail attachments
- » Ransomware, Trojans, viruses, worms, drive-by downloads

Simple and convenient without compromise

Security technologies can only then be rolled out when they do not consequently restrict users from carrying out their everyday work. Ideally, users will hardly notice any change. Due to this, the operability of our solutions is always an important focus for development.

Users utilise secunet safe surfer like a native browser with all its useful features:

- Personal favourites/bookmarks
- Password-free registration
- Representation of all content with full multimedia support
- File downloads and uploads
- Copy & paste of text in both directions

Where features are restricted administratively – e.g. no uploads permitted – the user is notified via the corresponding notifications. Users also do not need to worry about compulsory use of a local browser for sensitive intranet web applications. An administratively managed browser detector automatically selects the appropriate browser for the user.

Simple administration

The secunet safe surfer overall system is ready for use in a very short amount of time, offers a high level of automation, and can be managed centrally. Users are conveniently managed via existing directory services and receive the appropriate permissions for the secunet safe surfer functions required for the role assignment. A configurable data lock, including a quarantine area, ensures that data are transferred securely. The admin can request to proactively receive reports on system status or regarding recognised anomalies.

Standardised yet flexible

Every IT infrastructure is different; requirements change over time. Would you like to connect existing IT services? Do you use Citrix or are your sites spread out? Are you interested in secunet safe surfer 'as a service'? Do you already use secunet SINA Workstations? Are you looking to expand the system during continued operation? No problem, as secunet safe surfer can also fulfil many individual requests as a standard product:

- Diverse interfaces (SMTP, WebDAV, SSH, LDAP, etc.)
- Citrix support
- Terminal server virtualised or natively executable
- Cluster management (load-balancing), including failover
- Scalable during continued operation
- Transparent licence model that grows accordingly
- Geographically spread out terminal server clusters
- Terminal server as SINA guest system
- Parallel operation and central management across all versions
- Ready 'as a service'

secunet safe surfer at a glance

More than just a secure browser – it's 360° internet protection in a nutshell

- » Effective prevention of
  - – Espionage and loss of data
  - – Productivity restrictions and failure of services critical to the company
  - – High costs due to recovery measures or ransom payments
  - – Damage to reputation
- » Higher employee productivity through greater flexibility when using the internet
- » Reduction in the IT workload through automation and seamless integration

More information:
www.secunet.com/safesurfer

secunet
secunet Security Networks AG
Essen, Germany

Phone: +49 201 5454-0
Fax: +49 201 5454-1000
E-mail: info@secunet.com
www.secunet.com