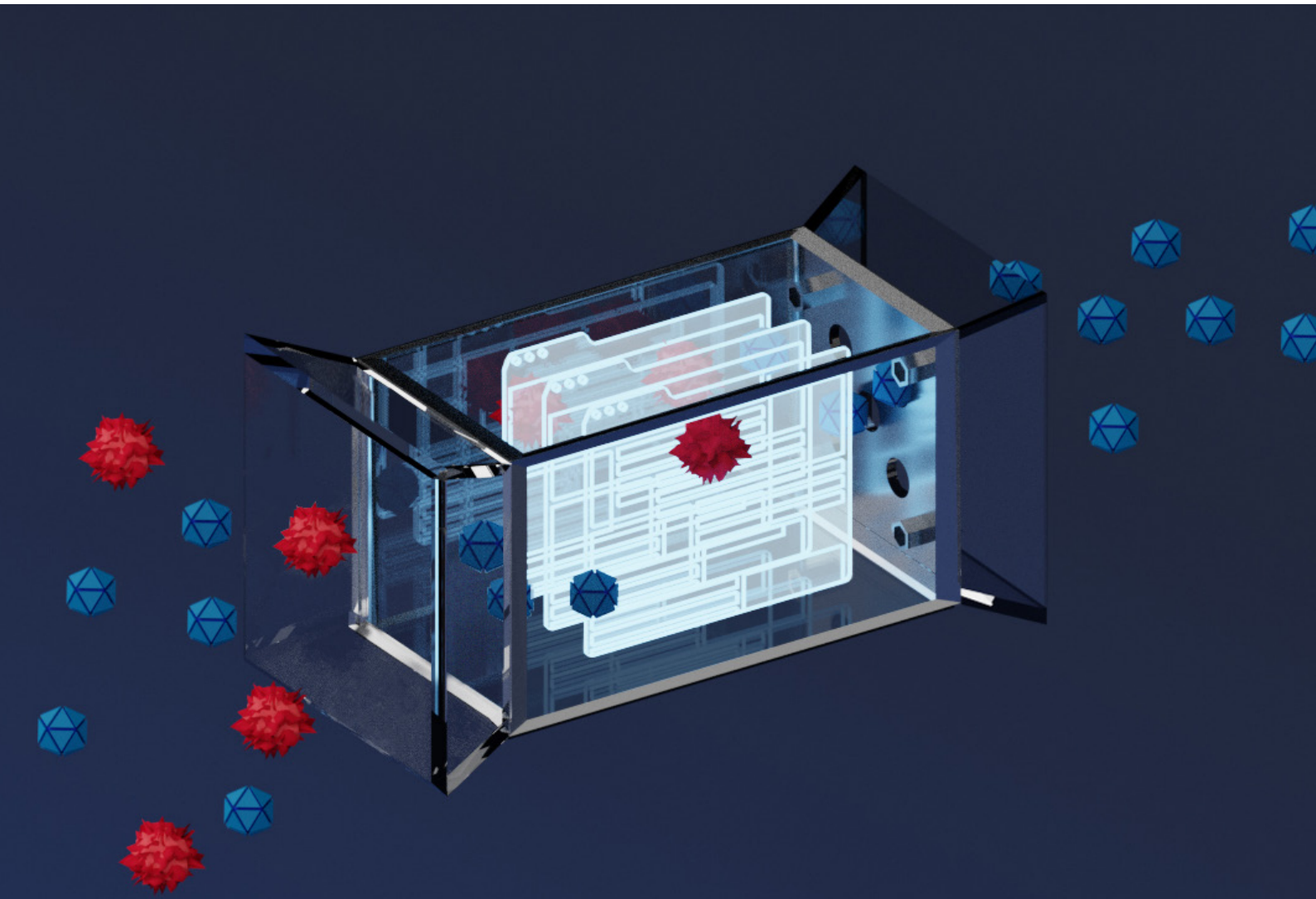
secunet
safe surfer

Unrestricted and secure access to the Internet.



secunet.com

Cyber attacks are steadily increasing in quality and quantity and, if successful, usually lead directly to the execution and propagation of malicious codes across trusted enterprise networks.

Sensitive data leaks away unnoticed or is encrypted. There is a risk of massive productivity restrictions, data loss and damage to the company's image. The greatest threat still comes from Internet use at the workplace and cannot be reliably contained with classic protective measures such as virus scanners, firewalls or content filters. **The solution is isolation.**

The principle of secunet safe surfer

Even the world's most secure browser does not offer sufficient protection if it is not also embedded in the most secure overall architecture. secunet safe surfer separates workstation systems from the Internet at the physical level.

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

Benefits

- Maximum security through physical separation of the work-station from the Internet
- High level of user convenience – no functional restriction
- Various operating modes
- Flexible licensing model
- High degree of automation
- Configurable and integrable in the default application
- Central management

Each browser session is executed in a compartmentalized environment within a specially hardened Linux system, which in turn runs in a separate network segment (DMZ) on so-called isolation systems. The browser is remotely controlled from the workstation via a secure channel. Only image and sound are transmitted.

The majority of attacks that target Windows-based vulnerabilities are already successfully fended off in the Linux environment. Additional security mechanisms and zones in the overall architecture still reliably protect against attacks even if the browser has been compromised.

The physical separation of the workstation and the browser system also protects against hardware-related attacks such as Spectre, Meltdown, and ZombieLoad. In addition, all isolation systems are regularly restored to their original state in a tamper-proof manner. Any malicious code that may be present is effectively destroyed.

The user's workstation remains disconnected from the Internet at all times. The user is thus additionally protected against malicious codes from infected documents that have been downloaded to the workstation, e.g., via e-mail attachments or USB sticks.

secunet safe surfer offers protection against

- Novel and unknown attacks (zero-day exploits)
- Targeted attacks (APT, Advanced persistent threats)
- Browser vulnerabilities
- Infectious websites and e-mail attachments
- Ransomware, Trojans, viruses, worms, drive-by downloads

Simple and comfortable without compromises

Security technologies can only be rolled out successfully if users are not restricted in their daily work. Ideally, they will not even notice any difference. For this reason, the usability of our solutions is always a key focus of development.

The user uses secunet safe surfer like a native browser with all the comfort functions:

- Personal favorites/bookmarks
- Password-free login
- Display of all content with multimedia support
- File download and upload
- Copy & paste of texts in both directions

If functions are administratively restricted - e.g. no upload allowed - the user is informed via corresponding notifications. The user does not have to worry about the use of a local browser for sensitive intranet web applications. A conveniently managed browser switch allows the user to select the appropriate browser fully automatically.

Simple administration

The secunet safe surfer overall system is ready for use in a short time, offers a high degree of automation and can be managed centrally.

Users are conveniently managed via existing directory services and are assigned the appropriate authorizations for the secunet safe surfer functions via role assignment. A configurable data lock, including a quarantine area, ensures secure data transfer. Reports on the system status or in the event of detected irregularities can be sent proactively to the administrator by e-mail.

Standardised and yet flexible

Every IT infrastructure is different, requirements change over time. Do you want to connect existing IT services? Do you use Citrix or have distributed locations? Are you interested in secunet safe surfer "as a service"? Are you already using secunet SINA workstations?

You would like to expand the system during operation? No problem, because secunet safe surfer also fulfils many individual wishes as a standard product:

- Various interfaces (SMTP, WebDAV, SSH, LDAP, etc.)
- Citrix support
- Isolation system virtualised or natively executable
- Cluster management (LoadBalancing) included-Failover
- Scalable during operation
- Transparent and growing licensing model
- Geographically distributed terminal server clusters
- Terminal server as SINA guest system
- Parallel operation and central management across all variants
- Ready „as a service"

secunet safe surfer at a glance

More than just a secure browser – simply all-round protection on the Internet

- Effective prevention of
  - Data loss and espionage
  - Productivity restrictions and downtime of business-critical services
  - High costs due to recovery measures or ransom payments
  - Image damage
- Increased employee productivity through greater flexibility in Internet use
- Reduction of IT workload through automation and seamless integration.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

More information:
secunet.com/en/safesurfer

secunet_safe surfer_EN_01/2021