

Uneingeschränkt sicher  
ins Internet



# Uneingeschränkt sicher ins Internet

Kaum ein Arbeitsplatz kommt ohne eine Verbindung zum Internet aus. Doch Internetverbindungen sind angreifbar. Erfolgreiche Angriffe führen heutzutage meist direkt zur Ausführung von schadhaftem Code im vertrauenswürdigen Unternehmensnetz. Die tägliche, massive Bedrohung über das Internet ist mit herkömmlichen reaktiven Schutzmaßnahmen wie Endpoint Security, funktionalen Einschränkungen oder dem Einsatz von Filtern kaum noch kontrollierbar.

Es gibt jedoch etablierte Technologien, die Ihnen helfen, diese Herausforderung zu meistern. Gleich zwei davon finden Einsatz im secunet safe surfer. Er separiert das vertrauenswürdige interne Netz und die Arbeitsplatz-Systeme vom potenziell gefährlichen Internet und schützt damit zuverlässig vor Online-Angriffen. Basierend auf dem Remote-Controlled Browser System (ReCoBS) Protection Profile des Bundesamtes für Sicherheit in der Informationstechnik (BSI) trennt der secunet safe surfer den Arbeitsplatz-PC sicher vom Internet. Jede Browsersession wird in einer eigens abgeschotteten und gehärteten virtuellen Umgebung ausgeführt. Zusätzlich zu dem ReCoBS-Ansatz setzt secunet safe surfer mobile auch die „Browser-in-the-Box“-Lösung des BSI um und bietet somit nicht nur ein hohes Maß an Flexibilität, sondern vor allem höchste Sicherheit.

## Vergleichen Sie selbst!

Um die für Sie optimale Lösung zum sicheren Surfen im Internet zu finden, haben wir Ihnen diesen Vergleichswegweiser zusammengestellt. Er enthält alle wesentlichen Aspekte, die Sie bei der Beschaffung, der Integration in Ihre Infrastruktur und für den reibungslosen Betrieb in ihrem Netzwerk beachten sollten.

Bei Fragen zu den einzelnen Punkten helfen wir Ihnen gerne weiter. Sprechen Sie uns an!

► [info@secunet.com](mailto:info@secunet.com)

Uneingeschränkt sicher ins Internet mit

**secunet** (safe surfer)



# Ihr Wegweiser zum sicheren Surfen

Nr.	Funktionalität	secunet (safe surfer)	Alternative Technologie
1	<p><b>Usability und User Experience</b>                      Beim Browsersystem stehen Usability und User Experience im Vordergrund. Beides bietet der secunet safe surfer: Beim Surfen sieht der Nutzer ausschließlich einen üblichen Browser (secunet safe surfer basiert auf Mozilla Firefox) und alles befindet sich am gewohnten Platz. Auch erfordert die Nutzung keinerlei Schulung. Weitere Komfortfunktionen sind:</p> <ul style="list-style-type: none"> <li>▶ Passwortlose und trotzdem kryptografisch gesicherte Anmeldung</li> <li>▶ Transparenter Druckservice</li> <li>▶ Hochsicherheits-Datenschleuse</li> <li>▶ Unterstützung des gewohnten One-Click Downloads</li> <li>▶ Seamless-Mode: Der Nutzer sieht ausschließlich den Browser und keine potenziell verwirrenden Zusatzkomponenten oder –Fenster</li> <li>▶ Intelligenter Weichendienst (URL-Handler): Steuert die Übergabe von internen und externen URLs auf Internet- und Intranet-Anwendungen</li> </ul>	<p style="text-align: center;">✓ ✓ ✓ ✓ ✓ ✓</p>	
2	<p><b>Multimediaunterstützung</b>                      Unterstützung aller gängigen Medienformate. Bei Videos besteht Synchronität zwischen Bild und Ton.</p>	<p style="text-align: center;">✓</p>	
3	<p><b>Unterstützung aktiver Komponenten: Java, JavaScript, Adobe® Flash®, HTML 5</b>                      Die Nutzung aktiver Komponenten ist gefahrlos möglich. Sicherheitslücken, auch unbekannte, können sich nicht auf das interne Netzwerk oder den Arbeitsplatz-PC auswirken.</p>	<p style="text-align: center;">✓</p>	
4	<p><b>Austausch von Text per Zwischenablage (Copy &amp; Paste)</b>                      Zwischen Browser und Arbeitsplatzrechnern können Textabschnitte sämtlicher Sprachen über die Zwischenablage ausgetauscht werden.</p>	<p style="text-align: center;">✓</p>	
5	<p><b>Drucken über vorhandene Druck-Infrastruktur</b>                      Die Druckausgabe erfolgt über übliche Mechanismen – wahlweise auf Netzwerkdrucker, lokal am Arbeitsplatzrechner angebundene Drucker oder als PDF-Datei.</p>	<p style="text-align: center;">✓</p>	
6	<p><b>Mehrsprachigkeit</b>                      Die Benutzeroberfläche ist wahlweise in Deutsch oder Englisch gehalten.</p>	<p style="text-align: center;">✓</p>	

<b>7</b>	<b>Datenschleuse: Flexibilität für Uploads und Downloads</b> Up- und Downloads können vollautomatisiert mit gruppen- oder rollenindividueller Berechtigungssteuerung erfolgen; Berechtigungssteuerung z. B. durch bestehende Verzeichnisdienste (Active Directory / LDAP) oder das Administrationssystem.	✓	
<b>8</b>	<b>Browsersynchronisation</b> Profildaten des Browsersystems - bspw. Benutzereinstellungen, Lesezeichen, Browser-Chronik oder gespeicherte Passwörter - werden im zentralen Administrationssystem synchronisiert und sind stets aktuell.	✓	

<b>Nr.</b>	<b>Installation und Administration</b>	<b>secunet (safe surfer)</b>	<b>Alternative Technologie</b>
<b>9</b>	<b>Anbindung an bestehende Verzeichnisdienste</b> Die Anbindung an bestehende Verzeichnisdienste, wie z.B. Active Directory (AD) oder LDAP-Verzeichnisse, ist ohne Aufwand möglich. Nutzer- und Rollenattribute können automatisch in das Administrationssystem importiert und dort synchronisiert werden.	✓	
<b>10</b>	<b>Installation und Inbetriebnahme</b> ▶ Lieferung als vorkonfigurierte Server.  ▶ Lieferung als bootfähige System-ISOs zur Virtualisierung im Rechenzentrum des Kunden.	✓  ✓	
<b>11</b>	<b>Unterstützung aller gängigen Virtualisierungsplattformen</b> Das Browsersystem unterstützt VMware®, Hyper-V und Xen®.	✓	
<b>12</b>	<b>Skalierbarkeit der Installation</b> Durch den virtualisierten Betrieb muss keine teure Spezialhardware angeschafft werden. Das System skaliert mit den der virtuellen Maschine zugewiesenen Ressourcen.	✓	
<b>13</b>	<b>Mitgelieferter Clusterservice</b> Die Server der Browsersysteme werden automatisch durch eine Clusterfunktionalität gemanagt. Automatische Load-Balance und Fail-Over sind möglich. Damit ist auch die Hochverfügbarkeit des Clusters umgesetzt, unterstützt durch eine redundante Netzwerkanbindung.	✓	
<b>14</b>	<b>Mitgeliefertes Monitoring-System</b> Integrierte Überwachung von Systemparametern über Web-Frontend oder SNMP.	✓	
<b>15</b>	<b>Rollout auf Arbeitsplätzen</b> Der Arbeitsplatz-Rollout erfolgt durch standardkonforme Rollout-Prozesse.	✓	
<b>16</b>	<b>Zentrale Administration</b> Die zentrale Administration verschafft Übersicht über die aktuelle Ressourcennutzung der verschiedenen Server.	✓	
<b>17</b>	<b>Benutzerverwaltung</b> Nutzeraccounts und Berechtigungen können automatisch über Active Directory / LDAP abgerufen werden und in gewohnter Umgebung ohne Mehraufwand gepflegt werden.	✓	

<b>18</b>	<b>Aktualisierungen</b> Updates werden herstellerseitig quartalsweise bereitgestellt.	✓	
<b>19</b>	<b>Datensicherung und -Wiederherstellung</b> Datensicherungen werden für alle nötigen Komponenten in regelmäßigen, konfigurierbaren Abständen erstellt. Zusätzlich werden Mechanismen zur Wiederherstellung der Systemkomponenten mitgeliefert.	✓	
<b>20</b>	<b>Bestehende Proxy-Server können weiter genutzt werden</b> Fast jedwede bestehende Proxy-Server Architektur lässt sich ohne Änderung weiter nutzen.	✓	
<b>21</b>	<b>Geringe Bandbreitenanforderung pro Nutzer</b> ▶ Flexible Wahl des Darstellungsprotokolls VNC- oder X11 / NX möglich.	✓	
	▶ X11 / NX ist deutlich bandbreiteneffizienter als VNC. Für multimediantensive Szenarien kann VNC besser geeignet sein.	✓	✗

<b>Nr.</b>	<b>Sicherheitsaspekte</b>	<b>secunet (safe surfer)</b>	<b>Alternative Technologie</b>
<b>22</b>	<b>Sicherheitsarchitektur</b> ▶ Das Browsersystem erfüllt die Sicherheitsvorgaben des BSI, festgelegt in BSI-PP-0040 ReCoBS.	✓	
	▶ Das Browsersystem bildet für mobile Nutzer den „Browser-in-the-Box“-Ansatz ab, welcher eine effizientere Bandbreitennutzung ermöglicht.	✓	
	▶ Eine Integration in die SINA Workstation-Umgebung ist möglich, was für SINA Nutzer eine höhere und effizientere Integration des „Browser-in-the-Box“-Ansatz bedeutet.	✓	✗
<b>23</b>	<b>Schutz vor Angriffen über den Internetbrowser</b> Gezielte Angriffe über Browser und Schadcode, etwa aus Drive-by-Downloads, können nicht in das interne Netzwerk gelangen.	✓	
<b>24</b>	<b>Datenschleuse: Sicherheit durch Dateitypfilter und Malware-Scan</b> Zu übertragende Up- und Downloads durchlaufen immer die mitgelieferte Dateischleuse. Diese beinhaltet einen flexibel konfigurierbaren, MIME-basierten Dateitypfilter sowie einen zusätzlichen Antivirenschanner. Zusätzlich gibt es einige konfigurierbare Komfortfunktionen – sowohl für den Nutzer (z. B. One-Click Download) als auch den Administrator (z. B. konfigurierbare max. Up-/Downloadgröße).	✓	
<b>25</b>	<b>Trennung des internen Netzes vom Internet</b> Das Browsersystem bildet den zentralen Übergang ins Internet und trennt diesen auch physikalisch vom internen Netz.	✓	

<b>26</b>	<b>Vermeidung von Datenabfluss</b> Durch die physikalische Trennung des internen Netzes vom Internet wird jeglicher Datenabfluss ins Internet unterbunden.	✓	
<b>27</b>	<b>Nächtliche Neuinstallation</b> Eine automatisierte nächtliche Neuinstallation der Terminal-Server garantiert sehr hohe Sicherheit, ein darin integrierter File-System-Integritätscheck sorgt für einen Intrusion Detection-Mechanismus.	✓	
<b>28</b>	<b>Sicherheit durch Trennung</b> Dedizierte Hardware bildet eine unabhängige Ausführungsumgebung. Angriffe auf das interne Netzwerk über den Browser werden durch das ReCoBS-Prinzip unmöglich. Gleiches gilt für den „Browser-in-the-Box“-Ansatz, bei dem eine unabhängige Ausführungsumgebung virtualisiert bereitgestellt wird.	✓	
<b>29</b>	<b>Funktionsspezifische Kommunikation</b> Das VNC-Protokoll bzw. das X11 / NX-Protokoll bewirken eine strikte Trennung vom „Internet“.	✓	

Nr.	Betriebswirtschaftliche Aspekte	secunet (safe surfer)	Alternative Technologie
<b>30</b>	<b>Lizenzmodelle</b> ▶ Es existieren verschiedene flexible Lizenzmodelle.	✓	✗
	▶ Es kann ein Pool von Lizenzen (Concurrent) vorgehalten werden, aus dem die Nutzergruppe flexibel, nicht nutzerspezifisch, schöpfen kann.	✓	
	▶ Es können nutzerspezifische Lizenzen (Named) bereitgestellt werden, mit denen sichergestellt ist, dass sich jeder Nutzer zu jeder Zeit sicher im Internet bewegen kann.	✓	
	▶ Auch Mischmodelle sind möglich, bei denen sich Nutzer einen Pool von Lizenzen teilen und VIP-Nutzer nutzerspezifische Lizenzen erhalten.	✓	
<b>31</b>	<b>Beschaffungskosten für Server</b> ▶ Durch die Virtualisierung der Serverfunktionalität ist die Serverwahl frei und vorhandene Serverkapazitäten können genutzt werden. Falls keine Kapazitäten vorhanden sind, kann die Wahl auf den Hauslieferanten fallen, sodass Hardware einheitlich in Ihrem Rechenzentrum eingesetzt werden kann.	✓	
	▶ Es kann auch eine durch den Hersteller qualifizierte Hardware geliefert werden.	✓	
<b>32</b>	<b>Unterstützung und Anpassungen an Kundeninfrastruktur</b> Umfassende Unterstützungsleistungen sind direkt vom Hersteller erhältlich. Besonderheiten in der Kundeninfrastruktur können berücksichtigt und auf Kundenwunsch schnell umgesetzt werden.	✓	