



SINA Virtual Desktop

SOLUTION



SINA Virtual Desktop enables the secure integration of an autonomous SINA platform in a Windows operating system environment. Your familiar operating system environment remains unchanged. The integrated SINA VPN Gateway inside the SINA Virtual Desktop enables access to SINA-secured network domains. The SINA Virtual Desktop encrypts and encapsulates the classified data and therefore separates them from the "insecure" workplace system by means of virtualisation.

About SINA Virtual Desktop

System requirements include a PC or notebook (Intel-compatible) with at least 1.5 GB main memory and Windows 2000, XP or Vista as a host operating system. SINA Virtual Desktop is installed on this system and provides full SINA Thin Client functionality inside. An additional operating system (Windows or Linux) can be installed in SINA Virtual Desktop. You can now use your Office applications such as Word or Internet Explorer in this guest operating system. Access to SINA Virtual Desktop is protected by means of a smart card or a USB smart card token and PIN.

Your advantages:

- Secure processing, transfer and storage of classified data in a Windows or Linux environment
- Can be installed on any MS Windows-based workstation
- Sensitive data is securely encapsulated in the Windows environment

With the SINA Virtual Desktop you can start a file download from the Internet in the host operating system and, at the same time, work on your classified data. Both areas are completely separated. If there should be malware on the PC (resulting, for instance, from the download), your classified data remains protected. This data is encapsulated by means of a specially developed virtualisation solution and separated from the "insecure" workplace system. Of course, malware cannot leak into the classified network even when the online connection is open.

For you as a user this means: You can process your classified data in a secure way, online and offline. The information can be transferred to other, classified SINA networks or stored on the local machine. The required level of confidentiality is always ensured. Your staff can continue to work with their familiar processes even outside of a secure IT environment. It is no longer necessary to switch from computer to computer for "classified" and "non-classified" jobs. And if your computer is lost or stolen, hard disk encryption still provides maximum security: Your data is always protected.

The technology: Virtualisation + SINA

SINA Virtual Desktop contains two Virtual Machines (VMs) which are securely linked and which represent an encapsulated security subsystem within a Windows operating system environment. The first VM implements the VPN and CFS (Crypto File System) functionality and makes Thin Client applications available. The second VM contains a Windows or LINUX guest operating system. This, in turn, accesses the VPN and CFS services of the first VM.

This security subsystem is comparable to a "good Trojan" within the Windows host which protects its own data and functions from access by the host.

The type of virtualisation used is not simply a driver or an application, but a mechanism that runs a complete operating system (guest operating system) inside of another operating system (host operating system). This means that the virtualisation layer must have full control over the system, because the guest operating system assumes it has this full control itself. The combination of the two Virtual Machines in SINA Virtual Desktop achieves an unparalleled security level for a software-based security application on a Windows PC.

secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Approval

The evaluation is underway. Aim of the evaluation: RESTRICTED.

Sources of supply

You can purchase SINA directly through secunet or through authorised SINA distributors. A SINA Business version is available for customers from the private sector.

PC hardware	
Basic requirements	Intel-compatible hardware Intel Core-2 Duo processor > 1.6 GHz
Host operating system requirements	
	Windows 2000 or Windows XP 40 MByte hard disk plus guest operating system images 256 MB RAM plus guest operating system
Cryptographic methods	
Symmetric:	AES, 3DES, (HMAC-) SHA1, (HMAC-) RIPEMD 160
Asymmetric:	RSA, EC-GDSA, Diffie-Hellman (MODP und ECP)
Standards	
	RFC 2104 (HMAC), RFC 2367 (PFKey), RFC 2401-2412 (IPsec), RFC 2459 (X509v3), RFC 2510/2511 (CMP), ISO/IEC 15946-2 (EC-GDSA)
	IP v4
On request:	IP v6, v4/v6- und v6/v4-Tunnelling
NAT	NAT-T support for IPsec (RFC 3947 for some)
QoS	
	DiffServ Codepoints Bandwidth management per security association

Editor:

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany
Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-mail: info@secunet.com
www.secunet.com