Security Laptop vs-top

Providing High Security Access for Mobile Users Connecting to Classified Networks

Employees on the road frequently must connect to their company network to access and modify data, use internal applications online etc. In addition, easy connections via all sorts of protocols and methods are needed. These user requirements raise a very important question indeed: How can reliable IT security be implemented for teleworking? Very serious security issues need to be addressed, such as the download of sensitive data to employee laptops via the Internet, as well as access to your LAN and all sorts of confidential information. It is therefore essential that third parties cannot read or manipulate the data being transferred, nor misuse access to your LAN.

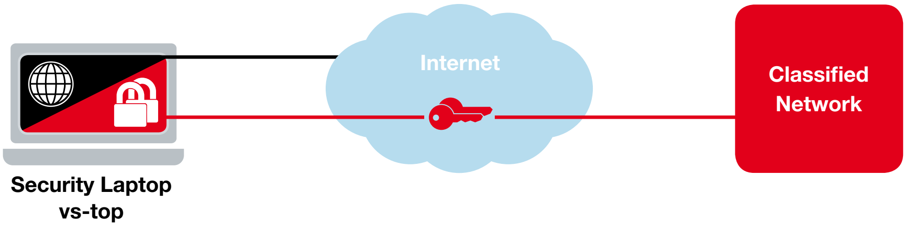
Simple to Operate

The vs-top security laptop ensures that mobile personnel are able to connect safely to sensitive company and official networks. It achieves this through two separate working environments being built into the laptop: One is equipped with conventional Windows or Linux applications, which the user can use to browse the Internet, work with e-mails and texts, etc. The second working environment is exclusively used to process sensitive data. Encrypted connections from this environment to your network are made via cell network, mobile phone, WLAN or Ethernet using an integrated VPN (Virtual Private Network) solution, made in Germany. This design means that the vs-top can enable your users to work anywhere – comfortably and securely.

High Security through Strict Separation

The key to the vs-top's high level of security is the strict separation between the internal compartments behind the working environments. This is because applications such as e-mail programs or browsers are sources of weakness. If, for example, an attacker or malicious software should manage to corrupt the browser, they must be stopped from accessing the working environment for confidential information or, even worse, from accessing your network via VPN. The strict separation in the vs-top is made possible by the L4 separation system, which runs in the background, unnoticed by the user.

genua
A
Bundesdruckerei
Company



No Way through for Attackers or Malicious Software

The L4 separation system used on the high security vs-top creates strictly isolated compartments for each working environment: The browser, mail and office applications are locked in one compartment, the working environment for sensitive information in a second. In addition, the security systems for the VPN gateway and firewall are locked in a third compartment. Each compartment comes complete with its own operating system and is therefore fully independent of the others. This consequent separation means that attackers or malicious software cannot break out from one working environment into the next or into the security systems. The L4 system is programmed to minimize code size, even though it carries out key tasks on the vs-top: It consists of merely 38.000 lines of code. This low complexity prevents errors and is an important security feature. Through its use of internal separation, the vs-top provides a level of security that up till now could only be achieved with the use of additional hardware units. In addition, the complete hard drive of the vs-top has been reliably encrypted and the key saved on a smartcard. Even if the laptop is lost, no one will be able to access your data.

vs-top at a Glance:

- Secure connections for mobile users
- Two strictly separated working environments on one laptop
- The compact laptop with „standard“ applications is simple to use
- High security VPN connections via cell network, WLAN and Ethernet
- VPN technology – Made in Germany
- Reliable hard drive encryption
- Approval for classification levels German VS-NfD, NATO and EU RESTRICTED
- Comfortable administration by management station
- Customer service direct from the manufacturer

Further information:
www.genua.eu/vs-top

www.genua.eu

Central Administration from a Management Station

The vs-top security components are managed by the Management Station genucenter. Central management enables configuring mobile users, performing modifications and updates at any time, and strictly maintaining your security policy. This in turn means that you can achieve a very high level of mobile security in practice.

Approved for Classification Level RESTRICTED

vs-top has been approved by the German Federal Office for Information Security (BSI) as meeting the requirements of the German VS-NfD, the NATO and EU RESTRICTED classifications. This allows employees to use the mobile device to work with classified data.

About genua

genua is a German company specializing in IT security. It has been securing networks and developing sophisticated security solutions since the company was founded in 1992. Our business activities range from securing sensitive interfaces in public authorities and industry to networking highly critical infrastructure, reliably encrypting data communication over the Internet, remote maintenance solutions and providing remote access for mobile users and home offices. Our solutions are developed and produced in Germany. Many companies and public authorities rely on solutions from genua to protect their IT. genua is a member of the Bundesdruckerei Group.

SecurITy made in Germany

genua gmbh, Domagkstrasse 7, 85551 Kirchheim, Germany
tel +49 89 991950-0, info@genua.eu