



Security Laptop cyber-top

Facts & Features



Definition:

The compact cyber-top security laptop allows personnel the convenience of being able to work in high security networks and at the same time use e-mail or office applications in other areas – without a security risk. This is achieved by a separation system, which creates two working environments on the laptop. One is equipped with conventional Windows or Linux applications like browser, e-mail program etc. The second working environment is exclusively used to process sensitive data. Both working environments are strictly separated, so that the sensitive data is well protected. Access to sensitive company networks via Internet is enabled by an integrated VPN. Furthermore the complete hard drive of the cyber-top is reliably encrypted. Thus employees can safely work with sensitive data everywhere – in the office, home office or on the road.

Typical Use:

Connecting personnel to sensitive networks of companies

Customer Service:

- Customer service directly from the manufacturer
- Security system management
- Hotline service / update service

Reasons to Choose cyber-top:

- High security through strictly separated working environments
- The compact laptop with “standard” applications is easy to use
- Secure connections for mobile users
- VPN technology made in Germany
- Reliable hard drive encryption
- Central administration via management station

Reasons to Choose genua:

- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations



Firewall

Stateful packet filter	State of the art firewall for manageable rulesets
Network Address Translation (NAT)	Masquerade networks behind one address
Network bridging	Bridging compartment into the local area network without losing packet filter capability
Filter criteria	Filtering decision can be based on IP address, network protocol, port, interface, flags and state
Filter action	Choice of packet handling: pass, block, drop
Spoofing protection	Block forged packets
Packet normalisation	Reassemble fragmented packets, generate random IP identification, enforce IP header settings such as TTL and MSS
Management	Centrally managed by the administrator with management station genucenter

Virtual Private Network

General	
IPsec VPN	Operated and enforced by separation layer
Authentication	
RSA	De facto public-key standard
Elliptic curves	Fast key exchange
IKEv1 and IKEv2 authentication	Authentication with keys or certificates using a PKI
Smartcard	Key handling via smartcard

Networking

Uplinks	
Ethernet	10/100/1000 Mbit/s Base-T
WLAN	802.11a/b/g
LTE/UMTS/GPRS	Integrated modem
Friendly Net Detection	Different access profiles depending on location of laptop



Separation

Compartments	Two separate compartments
Network	Separate network connections for each compartment
Graphics performance	Native 3D graphics acceleration in primary compartment
Sound	Sound is available in one compartment
Smartcard	Available for VPN connections and user compartments

Central Management with genucenter

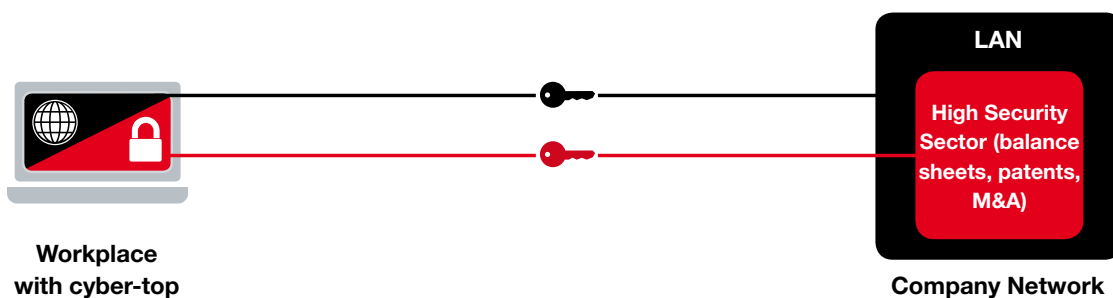
General	
Configuration	Easy management of several (thousand) systems
Monitoring	See the health of your systems at a glance
Logging	Easily collect and analyse logs
Software (patches/update)	Distribute the latest software revision
Rollout management	Freely define when to update/upgrade which system
Web GUI	Powerful web-based user interface secured with TLS/SSL (HTTPS)
Online help	Instant help in the user interface
Patch Management	
GUI	Get and install patches via GUI
Automatic updates	Automate the process of fetching updates for the appliance
Logging	
Local cache	For short term logs
Central	Use genucenter to concentrate the logs on one system



Application Examples

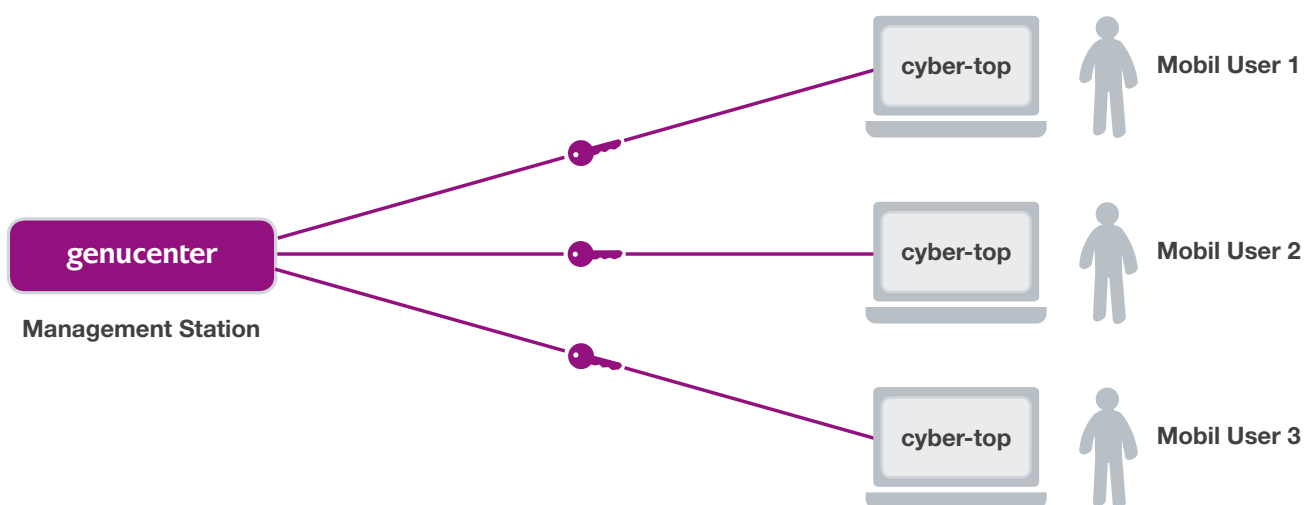
Secure and Mobile Working in Separated Networks

Employees can access sensitive data in high security networks, edit and store the data on the laptop – and at the same time they can use other applications in the company’s LAN, browse the Internet, work with e-mails etc. All this is performed comfortably and securely, because the compact cyber-top provides strictly separated working environments. The connections to the LAN and the high security network as well as the hard drive of the cyber-top are strongly encrypted, so that the sensitive data cannot be stolen or manipulated by attackers.



Central Administration from a Management Station

The cyber-top security laptop is centrally administered using the management station genucenter. This means that you can keep an eye on a number of users’ laptops from a central location and modify the configuration or install updates at any time. Thus you can ensure consequent implementation of your security policy and achieve a high level of mobile security in practice.



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