Companies have to reliably protect sensitive information from loss or espionage. To this end they often configure security zones for the areas in which the so-called crown jewels are processed: For example, corporate management has its own network, as do the specialists for acquisitions and mergers, the patent and research departments, and so on – the exact breakdown depending on the company size, the sector it is in and its focus. Access to each security zone is restricted to senior management and staff from the departments in question, while other network areas are all strictly separated from these zones to prevent unauthorized access and malicious software. This network separation is an important basis for protecting your confidential data.

**High Security Requires Consequent Separation**

In order to achieve a high level of protection, network separation must be consequently implemented down to the individual employees' workstations. This is because data in the security zones is accessed from these workstations and at the same time other network areas such as those used for e-mail and office applications – and the Internet – will be accessed as well. The applications used in these other network areas are a potential source of weakness: if attackers or malicious software should manage to reach a workstation, their next step will be into the security zone. However, you can close these security weaknesses with the cyber-top laptop: the L4 separation technology used in this compact laptop reliably keeps the applications using different security areas apart.

**No Way Through for Attackers and Malicious Software**

The L4 separation system on the high security cyber-top creates strictly isolated compartments: mail and office applications run in one compartment, in another the corporate management data can be processed. You can configure the compartments on the cyber-top as required. Each compartment comes complete with its own operating system and is therefore fully independent of the others. Attackers or malicious software cannot find their way from one compartment to another – for example, from the office compartment to the corporate management one. This consequent separation is your guarantee of high security. Furthermore the entire hard drive of the security laptop is reliably encrypted and the key stored on a smart card. Thus, nobody can access your data even if the laptop itself is lost.

---

Security Laptop cyber-top

Secure and Mobile Working in Separated Networks

**genua**

Security first.
Low Complexity as a Security Feature
The L4 technology used in the cyber-top security laptop not only protects your IT with its consequent separation of security zones – a further important feature is its low complexity. L4 is a minimally programmed microkernel operating system and has only some 38,000 lines of code. In contrast to an operating system with several million lines of code, all the source code in the L4 system can be thoroughly examined for errors. genua’s vs-top laptop, which uses the same technology as the cyber-top, is currently undergoing this process as part of the approval procedure for use up to the German classification level “Restricted” at the German Federal Office for Information Security (BSI). In doing so, the BSI is providing an independent confirmation of the high quality of our security solutions.

Central Administration from a Management Station
The cyber-top security laptop is centrally administered using the Management Station genucenter. This means that you are keep an eye on a number of users’ laptops from a central location and modify the configuration or install updates at any time. This also means that you can ensure consequent implementation of your security policy and thereby achieve a high level of security throughout your company.

About genua
genua is a German IT security specialist. Since our company was founded in 1992, we have been involved in securing networks and developing sophisticated solutions. Our products comprise firewalls certified to the international Common Criteria (CC) standard, high-security gateways and diodes for sensitive network interfaces, intelligent VPN and remote maintenance systems, mobile security solutions, and a wide range of services. Many large and medium-sized companies and authorities rely on our know-how and solutions to protect their IT. genua is a member of the Bundesdruckerei Group.

Convenient to Use Anywhere
The cyber-top is convenient to use despite its high security features: employees can work with Windows or Linux and their accustomed applications. In addition, an integrated VPN gateway (virtual private network) and a firewall run in isolated compartments, as they are critical security components. These protect from unauthorized access, and allow VPNs to be established for data transmission via, for example, the Internet. Our VPN solutions use the strongest encryption algorithms and are unbreakable with today’s technology. This means that it is safe for your personnel on the road or working from home to call up and work with sensitive data.

The cyber-top at a Glance:
- High security through strictly separated networks
- Individual configuration of separated working environments
- Secure connections for mobile users
- The compact laptop with “standard” applications is simple to use
- VPN connections via cell network, WLAN and Ethernet
- VPN technology – Made in Germany
- Reliable hard drive encryption
- Support for IPv6
- Central administration by management station
- Customer service direct from the manufacturer

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