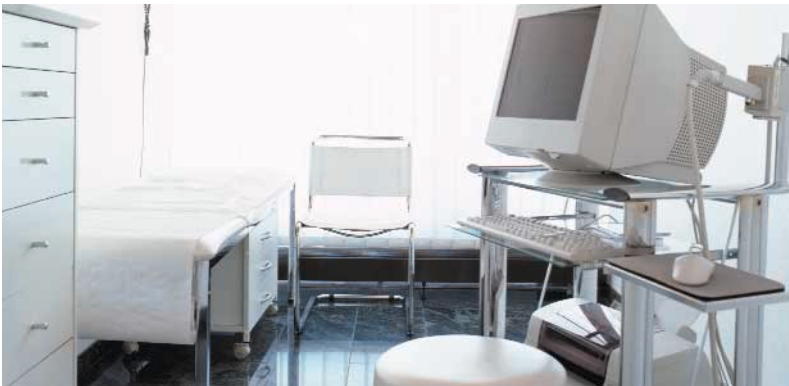


Innominate

mGuard

Innominate mGuard: the innovative solution for IT security in medical technology

Today, data exchange between various medical systems and PCs is an everyday occurrence, both within the clinic and with general practitioners or specialists. At the same time, patient data availability and security is the subject of ever increasing attention.



More technology for the patient's benefit...

The integration of information technology (IT) into medical systems is reaching increasingly complex levels. More and more, a wide range of options are becoming standards in medical diagnostics, from digital x-ray technology and full electronic analysis systems to high-tech computerized tomography. What's more, technological advances in the OP area must also be factored into the equation. Computer-controlled laser scalpels are among the latest innovative technological developments. Video recording and archiving and the new field of telemedicine – which encompasses video conferencing, i.e. between specialists located in different cities – are increasingly being used for difficult operations. Today, even routine operations require computer-controlled systems.

... with all the advantages of an efficient operating procedure

An increasing number of these medical systems have been linked up in order to save time and cut costs. This networking allows the complete range of patient data – from inpatient registration and laboratory results to OP reports – to be stored in a central location. In this way, any authorized user can access a complete range of data immediately. At the push of a button, the treating doctor is fully informed and “in the picture”.

The other main advantage: the systems' availability can be monitored remotely. In the case of an emergency, maintenance work or software updates can also be undertaken remotely, without a service technician having to work on the system locally. This also saves time and money while ensuring that the system is always up for use.



Provided that availability and security are guaranteed

One disadvantage inherent in networking is that many computer systems in the medical-technical environment are not adequately protected from attacks. Sometimes, this is due to the fact that they run on proprietary platforms. In such cases, conventional security solutions cannot be implemented, because software or hardware are not compatible. These systems often employ older processor technologies (e.g. Intel 386 or 486) or outdated operating system versions, which limit their performance. But even newer standard systems using Windows are at high risk. After all, the security holes in Windows systems have been widely documented.

In most cases, however, security gaps occur due to what is known as validation of medical-technical systems. In other words, their operators are subject by law to carry out comprehensible documentation on the unit and the system maintenance history. This means that every modification to the system, whether to software or hardware, is tied to a further expenditure in resources, both in terms of manpower and costs.

Paradoxically, it is those systems running with standards such as Windows, Ethernet, TCP/IP and HTTP – which supposedly offer advantages – that actually end up “eating up” large amounts of resources under the aspect of validation. This is due in large part to the numerous security patches that are constantly being issued by Microsoft, often creating a huge strain on budgets. For this reason, these system updates are often not even carried out. Yet many IT heads are not conscious of the fact that their computer-controlled medical technology systems are susceptible to exactly the same dangers as administrative PCs, e.g. virus attacks. With a drastic added disadvantage: malfunction or even temporary breakdown of the medical technology system could make itself felt in terms of human life.

Why conventional security technology is of little use

A range of security technology is available that can be used in conjunction with medical technology systems. However, in this application area, all these solutions – whether hardware or software-based – have one decisive disadvantage: they require the computer-controlled systems to be modified. Under the aspect of validation, large expenditures must be budgeted, in addition to the costs arising from complex implementation and configuration measures carried out locally by a technician.

Hardware-based systems (routers, bridges) have the drawback that they can always be identified in the network based on their IP – and are therefore highly susceptible to attack. Particularly due to the fact that in many systems, standard ports are left open in order to make data transfer more unproblematic.

Software-based solutions (personal firewalls, anti-virus software) have other limitations: namely, they cannot run on some proprietary operating systems. Moreover, they often can't be integrated into systems using older processor technology – because these lack the necessary performance. Blocking a virus attack would demand so much of the processor's performance that the whole system would be paralyzed. Not to mention the fact that software constantly requires updates – otherwise viruses can easily attack the operating system time through newly detected security holes. Updates are already complex to carry out on normal computers, requiring extensive resources. And for validated systems, the costs are much higher.

Protect your computer-controlled medical system simply, reliably and economically

mGuard technology is a superior, innovative security solution falling under the category "device attached security". With the mGuard components, all the well-known disadvantages of conventional security technology – particularly for validated systems – are solved in a simple, reliable and economical manner. mGuard technology requires no modifications to medical systems – either upon installation or thereafter. mGuard products are installed quickly and easily and run independently of processor technology and the operating system used. Nor do they require regular software updates. In this way, mGuard technology protects systems reliably and permanently, and as a rule, does not entail any additional validation costs. Indeed, validation costs are cut because there is no longer a need to install security updates for Windows operating systems.

Highest security level, network-independent

Computer-controlled medical technology systems are normally connected to the clinic network and therefore usually protected from exterior attacks through conventional gateway appliances, with the same security standard as office PCs. However, critical systems such as medical equipment actually require a much higher level of security. In addition, a tricky fact remains: whatever components are used to protect a network from outside, a dangerous potential still exists from within – e.g. viruses that are unknowingly transmitted into the system by way of employee laptops.



With mGuard technology, you can now assign each computer-controlled medical system its own security components – with an individual security level, specifically-configured access rights and numerous other unique advantages.

Effortless integration, quick installation

mGuard is an independent system which is either inserted between the medical system and the network cable or if desired, as a PCI card. It doesn't matter which operating system or hardware platform the system runs with, for mGuard is compatible with all systems.

Primary functions of mGuard

mGuard, the "device attached security" solution from Innominate, unites all functions, reliably protecting IP connections, e.g. for remote administration of the system or for remote access by the head physician's PC:

- VPN for secure data transmission using public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Configurable firewall protects the system from unauthorized access from the "outside". The packet filter filters data packets based on the originating and target address and also blocks undesired traffic coming from the "inside".
- Integrated optional Kaspersky virus protection supports the protocols HTTP, SMTP and POP3 (recommended exclusively for the versions enterprise and enterprise XL). Virus protection already takes place on the mGuard – assuring increased security and high performance for the secured system.

Unassailable with the Innominate Stealth Mode

mGuard, the "device attached security" system from Innominate, features the one-of-a-kind Innominate Stealth Mode. This allows the device to work absolutely transparently, requiring no IP address of its own. mGuard uses the same IP as the computer it is protecting and therefore cannot be recognized by invaders, making it unassailable to attack. To use the standard Stealth Mode setting, nothing must be reconfigured or modified on the mGuard. At the same time, it is possible to customize each mGuard, even in Stealth Mode, to specific security requirements or your company's individual security policies.

The Innominate Security Configuration Manager offers an ideal and simple means of support for configuration, roll-out and administration, as well as servicing of mGuard devices.

Maximum data throughput for the VPN and firewall

The basis of the integrated security solution is the embedded Linux configured by Innominate, running on a special network processor with XScale core by Intel (IXP 42x), with up to 533 MHz processor capacity, up to 64 Mbytes of SDRAM working memory and 16 Mbytes of Flash memory. The Intel processor features hardware-based DES, 3DES and AES encryption. This guarantees maximum data throughput for firewall (up to 99 Mbit/s) and VPN (up to 70 Mbit/s). VPN connections are also quickly and reliably established in Stealth Mode.



At a glance:

- "device attached security" system: independent of hardware platform and operating system used.
- Simplest integration: no system adaptation, driver installation, never any updates.
- Reactionless network integration when using the transparent Innominate Stealth Mode.
- Maximum data throughput using hardware-based encryption for high speed VPN/firewall.
- Highly efficient anti-virus solution based on Kaspersky technology (optional).
- Full interoperability with other standard security solutions (IPsec) within the LAN/WAN.
- Fully integrable in central management environments (SNMP).
- Convenient company-wide configuration of all security devices via drag and drop with the Innominate Security Configuration Manager (optional).

Convenient integration and administration

The platform-spanning security of mGuard devices is ideally supported by the Innominate Security Configuration Manager (ISCM), which is based on tried-and-tested technology from the Solsoft Policy Server. ISCM is a group-based platform. Using a graphic network model, the security adjustments for several mGuard systems can be quickly and conveniently configured. The defined rules are automatically verified and approved for completeness and correctness. Firewall rules, VPN configurations and NAT settings are loaded directly for all devices in a single group and activated immediately. In addition, the VPN connections between mGuard devices, both between one another and with the gateways of other manufacturers, are set up and managed. Everything is displayed conveniently on the graphic interface for easy operation via mouse click.

What was once complex, time-consuming and error-prone due to the configuration of individual systems is now quick and flawless with the Innominate Security Configuration Manager's group administration. The overwhelming benefit: operating expenses and manpower are reduced significantly.