

**Innominate**

# mGuard

The innovative security solution for all POS/POI terminals



Cashless payment systems have grown enormously in popularity. But in addition to EC and credit card terminals, there are many other systems that handle monetary transactions: supermarket computer cash registers, lottery terminals in stationery shops, subway station ticket machines – as well as cash card systems in company cafeterias. Networked automated machines are regularly being added to the list: slot machines, cigarette machines, vending machines, information terminals (i.e. kiosk systems), package vending machines at post offices – and the list is ever growing.

### What are the advantages of networking?

Customers receive better and faster service and more convenience. Companies become more flexible, increase their planning reliability and save on costs. Credit card companies can confirm payments immediately. At the press of a button, supermarket chains can access regularly updated information on their flow of goods and automatically control re-orders and warehousing.

In Germany, lottery administration departments accept lottery coupons as late as Saturday afternoon, because the coupons have already been recorded at the kiosk and transmitted to the lottery center via Internet. Ticket machines, like vending machines, can be monitored remotely. Regular local inspections are no longer required, thus reducing operating expenditure. A technician only has to be sent to refill the machine or if it should malfunction. In addition, an increasing number of these vending machines can be used with EC debit cards. Cash card systems, often used in company cafeterias, enable pass-by cashless payment, decreasing the time spent waiting in line for customers. Finally, entertainment systems can offer significantly higher prizes, regardless of the actual cash stock. What's more, several players can join the game at different locations, either individually or in teams. This increases the fun and is a major incentive to players, while raising profits for the operator.



### The disadvantage: high security risks

All of these networked POS/POI terminals have two things in common: an integrated computer (including operating system and application software) and a network connection – usually via the Internet. Likewise, they all come with a similar problem: seldom are they adequately protected, making them open to attack. Each individual machine represents a dangerous security hole in the central corporate network. An additional aspect that should be considered: data in the system is, in principle, often accessible to every employee. In order to protect internal company information, access rights need to be limited.

### Not just older systems are at risk

Scores of computers in POS/POI terminals work with older processor technologies (e.g. Intel 386 or 486) as well as older versions of operating systems. This does offer some advantages – such as operation without fans and a compact form, as well as the robustness, high reliability and lower costs associated with the system. But it also comes with disadvantages – not the least of which is the reduced performance and lack of support for upgrades or software-based security solutions.

Even standard PCs that run on Windows systems have their own problems. Microsoft's security holes – even for its latest product, Windows XP – have been widely documented. Even more acute are the security risks for older Windows operating systems, as Microsoft no longer supports these versions with security updates.

Similar problems exist for PCs running on the operating systems from other manufacturers. Often, older versions are no longer supported and security holes can no longer be closed through patches.

### Why conventional security technology is of little use

There is a wide range of security technology that can be used in conjunction with POS/POI terminals, but almost all of it comes with considerable drawbacks in this segment. Nearly all of these solutions – regardless of whether hardware or software-based – have the same drawback: both implementation and configuration are complex processes, requiring modifications to the system. This can only be accomplished by a technician working locally, which not only eats up time but usually costs a lot of money.

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 ensure unproblematic data transfer via Internet connection.

Unfortunately, software-based solutions (personal firewalls, anti-virus software) have other limitations: namely, they cannot run on some proprietary operating systems, due to lack of compatibility. Moreover, they often can't be integrated into systems which use 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 and again through newly detected security holes. Yet such updates are complex, requiring extensive resources in manpower and capital.

## **mGuard technology protects all POS/POI terminals: simply, reliably and economically**

The drawbacks of other forms of security technology are solved with Innominate's mGuard technology in a uniquely simple, reliable and economical manner. For mGuard components are quick and easy to install and require neither modification to the computer configuration nor any software updates. Moreover, mGuard runs independently of the processor technology and operating system used.

## **Highest level of security, gateway-independent**

With the mGuard system, every computer-based automated system – from ATMs to slot machines – can be 100% eliminated as a source of network danger. With mGuard devices, you can assign every system – at a local level – its own security components: with individual levels of security and specifically configured access rights, as well as numerous other unique advantages. Larger installations, i.e. those necessary for a large number of credit card terminals, ticket machines or entertainment systems, can be configured and administered centrally using the Innominate Security Configuration Manager.



## **Effortless integration, quick installation**

mGuard is an independent system which is directly attached to the automated machine in question before the network cable or integrated as a PCI card, as desired. The computer system does not have to be reconfigured and no driver units or other software have to be installed. What's more, the operating system never has to be updated again using security patches. With the Innominate Stealth Mode, the network does not even have to be modified. It doesn't matter which operating system or hardware platform the POS/POI terminal runs with. mGuard technology is compatible with all systems and can be installed by any system operator – quickly and effortlessly.

For manufactures that offer special solutions, Innominate offers mGuard Core, a circuit board that can be individually customized for special requirements and integrated directly into the POS/POI terminals.

## **Primary functions of mGuard**

mGuard, the "device attached security" solution from Innominate, unites all functions, reliably protecting IP connections:

- VPN for secure data transmission via open networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Configurable firewall – protects the system from unauthorized access from "outside". The packet filter filters data packets based on the originating and target address, blocking undesired data traffic – also from "inside".
- Integrated optional Kaspersky virus protection supporting 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 individual mGuard device, even in Stealth Mode, to special security requirements: for example, requirements concerning the network connection. With cost-saving X-DSL connections, for example, which are increasingly being used, accesses can be limited for open standard ports in a targeted manner.

### 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 (XP 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 or driver installation, never any updates.
- Reactionless network integration with 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

Configuration, roll-out and administration of the mGuard devices is supported centrally through the Innominate Security Configuration Manager. It is based on tried and tested technology from the Solsoft Policy Server. Using a graphic network model, the security settings 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 group and activated immediately. In addition, the VPN connections between mGuard devices, both between one another and with the gateways of other manufacturers, are 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.