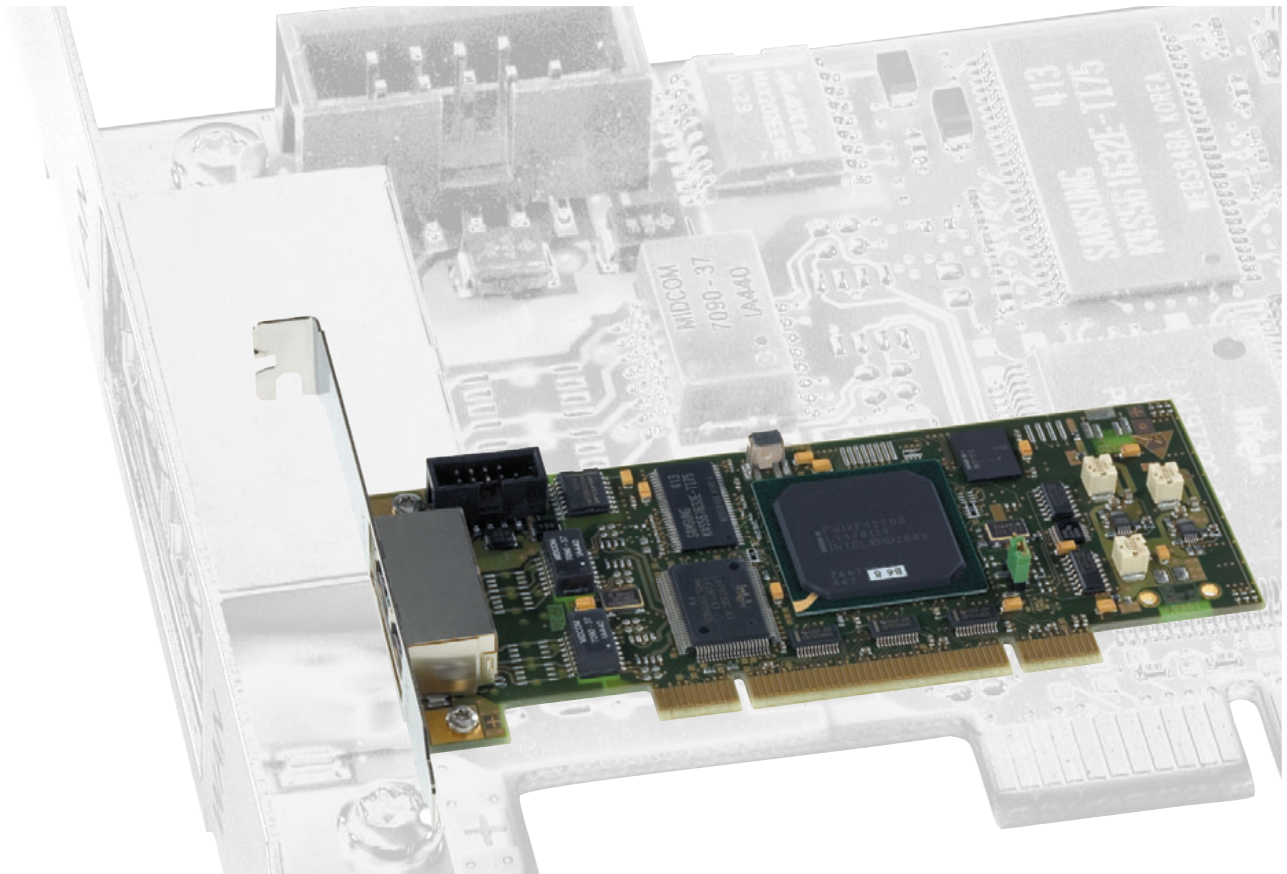


**Innominate**

# mGuard PCI

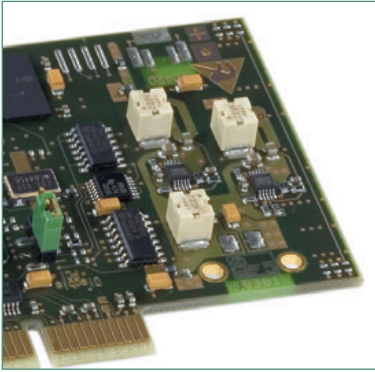
The first all-in-one security solution in PCI standard



**The mGuard PCI is available in the performance classes**

- mGuard PCI/266
- mGuard PCI/533
- mGuard PCI/266 VPN
- mGuard PCI/533 VPN

The mGuard PCI is currently the only PCI-compliant security device that unites all required security functions in a single component. It can be integrated quickly and easily, without modifications to the system settings or driver installation – regardless of the processor technology and operating system used.



## Primary functions

mGuard, the “device attached security” solution from Innominate, unites all functions to reliably protect IP connections:

- VPN (optional) for secure data transmission via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Configurable firewall – protects the system from unauthorized access from “outside”. The Stateful Inspection Firewall filters data packets based on the originating and target address, blocking undesired data traffic – also from “inside”.
- User firewall regulates access to internal or external resources via user login to the mGuard and central RADIUS server.
- Integrated anti-virus protection (optional) supporting the HTTP, FTP, SMTP and POP3 protocols. Anti-virus protection takes place outside of the system – assuring increased security for the applications and high performance for the secured system.

## How can you protect your validated or critical application systems?

With the mGuard PCI, Innominate offers the world’s first all-in-one security solution for servers in PCI standard. In addition to the integrated Stateful Inspection Firewall high-performance VPN functionality and anti-virus solution can be supplemented (optional).

Regardless of the computer platforms you use, regardless which operating systems you work with – if your systems support PCI, they can guarantee the highest integrated security standards with this unique “device attached security” solution. In every office environment, in every industry environment – and also in your company.

Conventional hardware-based security concepts always require a complicated implementation with modifications to the system configurations. In many areas, however, systems cannot be safely modified or updated. In industry environments, for example, strict security provisions for production systems require extensive testing before system modifications can be carried out. In the medical technology sector, every system change follows an extensive validation process by law. For this reason, it has always been virtually impossible to adequately protect these critical application systems from worm attacks, faulty operation or unauthorized access in a cost-effective manner.

## Quickly installed, reliably protected: the comprehensive mGuard security concept

With Innominate’s unique mGuard technology, you can guarantee the highest level of security for a complete range of systems – especially for those areas in which it was previously difficult to find a reliable – and at the same time, cost-effective – security solution.

The mGuard solution unites the advantages of hardware and software-based security concepts in a single component. All the security functions are integrated into the independent mGuard platform. It is not necessary to reconfigure the computer system being protected, nor do drivers or additional software need



to be installed. Thanks to the Innominate Stealth Mode, the mGuard PCI is also integrated completely transparently into the system. The PCI bus is only used for the power supply.

In addition, you can install the mGuard PCI in lieu of a network card, for use as a high-performance security router with interface functions.

## Innominate Device Manager

With the Innominate Device Manager (IDM) large populations encompassing several thousand mGuard appliances can be efficiently configured and managed. Due to the Innominate mGuard's template-based approach, the roll-out of numerous identically-configured appliances can be carried out quickly and conveniently.

## Maximum data throughput for the VPN and firewall

The INTEL security network 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, optional mGuard VPN-10 or mGuard VPN-250).

## At a glance:

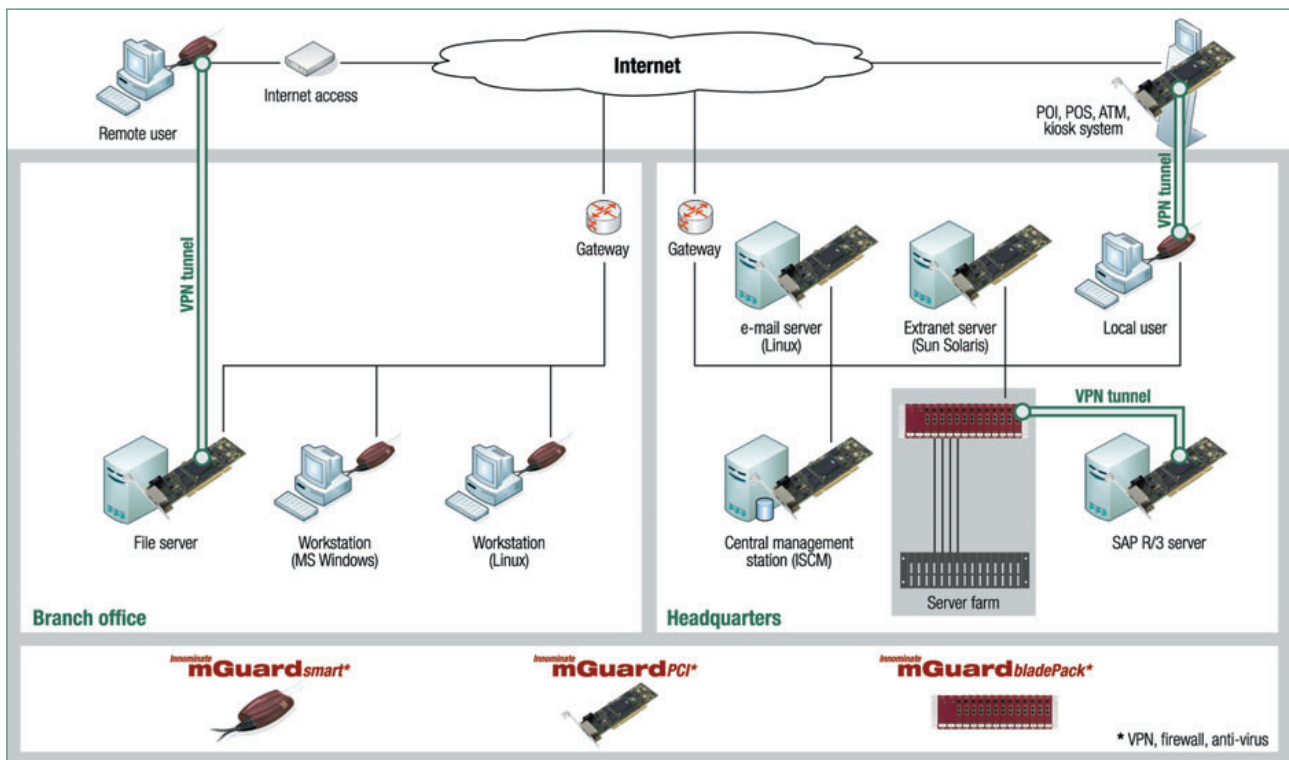
- High data throughput for VPN and firewall.
- Virtual addressing (1:1 NAT) in the VPN tunnel avoids address conflicts.
- Simple integration without configuration modifications and without installation of drivers or additional software.
- User firewall regulates access to internal or external resources via user login to the mGuard and central RADIUS server.
- Transparent Innominate Stealth Mode.
- Integrated, high-capacity anti-virus solution (optional).
- Configuration with the Innominate Device Manager (IDM).
- Via the "Simple Network Management Protocol", status changes and alarm messages are communicated to a central SNMP system.

## Unassailable with the Innominate Stealth Mode

Innominate's mGuard systems take advantage of a special function – the Stealth Mode. In this mode, the systems perform absolutely transparently and do not even require their own IP addresses. Instead, mGuard uses the same IP as the computer it is protecting and therefore cannot be recognized by invaders, making the system unassailable to attack.

## Applications for mGuard PCI

- PCI card for integration in individual machines
- Available as network card driver for Windows and Linux
- Used e.g. in panel PCs for automobile production
- Can be integrated into industry robots



Hardware performance features	mGuard PCI/266 mGuard PCI/533	mGuard PCI/266 VPN mGuard PCI/533 VPN
CPU	Intel IXP 42x with 266/533 MHz	Intel IXP 42x with 266/533 MHz
RAM / Flash	64 MB SDRAM / 16 MB Flash	64 MB SDRAM / 16 MB Flash
1 LAN / 1 WAN port	Ethernet IEEE 802.3 10 / 100 BaseTX,	Ethernet IEEE 802.3 10 / 100 BaseTX,
MAU management	RJ45, full-duplex, Auto-MDIX	RJ45, full-duplex, Auto-MDIX
	•	•
<b>Internet</b>		
Internet support	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi Stealth	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi Stealth
<b>Network services</b>		
DHCP support	Server or relay agent	Server or relay agent
DNS cache	•	•
Dyn. DNS	•	•
NTP client	•	•
LLDP (Link Layer Discovery Protocol)	•	•
VLAN (802.1Q)	•	•
Internet updates	•	•
Remote syslog logging	•	•
User based configuration profiles	•	•
Multi language	German, English and Japanese	German, English and Japanese
<b>Virtual Private Network (optional)</b>		
VPN data throughput (3DES)	-	35/70 Mbit/s
Max. number of VPN tunnels	-	10 or 250
Encryption procedure	-	DES, 3DES, AES-128, -192, -256
Hardware-based encryption	-	•
IPsec mode	-	ESP tunnel / ESP transport
Authentication	-	X.509v3 certificates with RSA or PSK
Data integrity	-	MD5, SHA-1
Internet Key Exchange (IKE)	-	Quick mode, main mode, PFS
IPsec L2TP Server	-	•
VPN in Stealth Mode	-	•
1:1 NAT in the VPN	-	•
IPsec NAT Traversal	-	•
Dead Peer Detection (RFC 3706)	-	•
Dyn. DNS VPN support	-	•
<b>System management</b>		
Web-based management (HTTPS)	•	•
Command line interface (SSH)	•	•
SNMP v1, v2, v3	•	•
Innominate Device Manager	optional	optional
<b>Anti-virus protection*</b>		
Integrated scan engine	optional	optional
Scans HTTP, FTP, POP3, SMTP, HTTP proxy	optional	optional
Block by file size	optional	optional
Automated pattern file updates	optional	optional

\* For anti-virus software option the use of an 533 MHz appliance is recommended.

Technical overview	Firewall	mGuard Software Options
Serial interface	RS232, optional	Firewall data throughput
Power supply	3,3 V or 5 V PCI bus	User licenses
Operating temperature	0 to 70 °C	Stateful Inspection Firewall
Relative humidity	20 to 90 %, non-condensing	NAT, 1:1 NAT
MTBF	102.3 years	Port forwarding
Dimensions	low profile PCI	MAC-Filtering
Operational mode	with driver or without driver via PoPCI (Power over PCI) mode	Firewall rules in VPN connections
<b>Approval/ conformity</b>		IP spoofing protection
CE, FCC, UL508		Syn flood protection
		Configurable DoS protection
		Redundant Firewall (VRRP)
		Innominate mGuard VPN-10
		IPSec VPN Gateway, max. 10 VPN tunnels
		Innominate mGuard VPN-250
		IPSec VPN Gateway, max. 250 VPN tunnels
		Innominate mGuard Anti-Virus-50
		50 appliances, perpetual license for CLAM AV™ virus patterns
		Innominate mGuard Anti-Virus-200
		200 appliances, perpetual license for CLAM AV™ virus patterns
		Innominate mGuard Anti-Virus-1000
		1000 appliances, perpetual license for CLAM AV™ virus patterns
		Innominate mGuard Redundant Firewall Option
		Requires two mGuard Security Appliances

Innominate mGuard is a registered trademark of Innominate Security Technologies AG. Several national and international patents have been registered or are pending for the mGuard technology. All other trademarks, brands and names are property of the corresponding firms. Product specifications are subject to change. Errors and omissions excepted. Status 09.2008