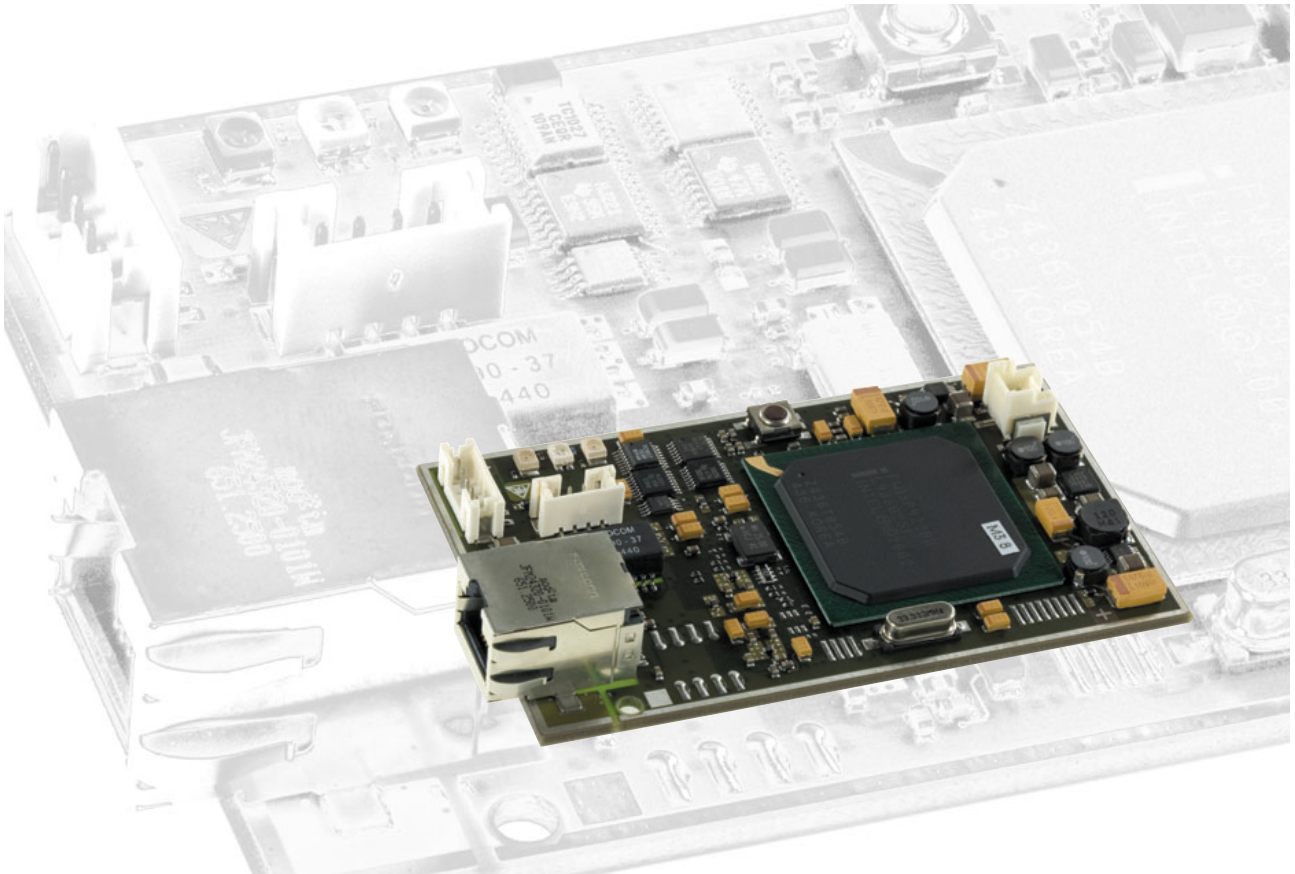


Innominate

mGuard core

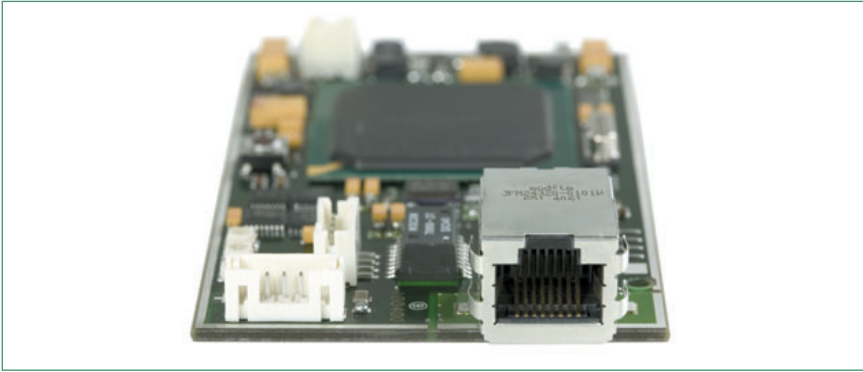
The integrated, all-in-one security solution as a built-in module



The mGuard core is available in the performance classes

- mGuard core/266
- mGuard core/533

The mGuard core is a security module in extremely small form, uniting all the required security functions for IP connections in a single component. Its small size allows it to be integrated directly into machines, appliances, vending machines, automatons and many other computer-assisted systems, regardless of the processor technology or operating systems currently being 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.

Higher security risks due to networked systems

The networking of automatons and facilities for machine and industrial process measurement and control technology, as well as many other computer-based systems, is getting widely accepted. Every additional network system also entails a problem for the security overview of the operator's entire network.

Many manufacturers of those computer-based network systems integrate inappropriate security solutions or no security solutions for their products. In order for additional security technology to be integrated, such platforms either do not have enough performance, lack drivers or require extensive software support.

Other manufacturers produce systems that are subject to strict security conditions or validation and certification processes by law. For such systems, conventional security solutions have often not come into question because every configuration change to the system, along with every software update, has been tied to further expenditures for resources, both in terms of manpower and costs. For this reason, many manufacturers have abstained from using Windows operating systems, as these often require a series of security updates. Even worse, older Windows versions are no longer supported by Microsoft.

The most serious danger lurks from the “inside”. For example, a system can often unwittingly become infected with “malicious codes” from the laptops of service technicians when they are directly connected to it. The resulting damages can be immense – often starting with the widespread shutdown of the company network.

Unique added value through the mGuard security solution

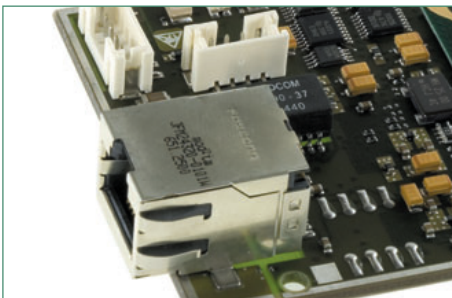
Whether you produce networked manufacturing robots for the auto industry, production systems for chemical and pharmaceutical engineering, medical technology systems, remote maintenance equipment, vending machines, telematic or monitoring systems – now you can eliminate all security risks to your products both reliably and economically. Regardless of which computer platforms you use; regardless of which operating systems you work with.

With the mGuard core, Innominate offers an outstanding, all-in-one security solution as a compact, built-in module, which can be integrated effortlessly into the Ethernet connection of almost any system. Innominate's “device attached security” platform guarantees the user a decisive added value, for manufacturers of all kinds of computer-assisted systems, which transmit data into company networks via cost-saving IP connections. The component unites firewall and VPN functionality and can be expanded with a powerful anti-virus solution (optional).

Quickly installed, reliably protected: the platform-independent security concept

With Innominate's singular mGuard technology, you will gain a decisive competitive advantage, guaranteeing the highest level of security for your systems' network environments. Without extravagant expense or complexity – and especially in those areas for which it has been difficult until now to find a reliable and, at the same time, economical security solution.

The mGuard solution unites all the advantages of hardware and software-based security concepts in a single module. All the security functions are integrated into the self-contained and fully independently-operating mGuard core. The protected computer system must not be reconfigured, nor do drivers or additional software have to be installed. In addition, thanks to the Innominate Stealth Mode, the mGuard core can be integrated completely transparently into the system and the network.



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.

At a glance:

- Better CPU performance and higher data throughput for VPN and firewall.
- No configuration modifications, no installation of drivers or additional software.
- Independent operation, regardless of the processor technology or operating system version used.
- Transparent Innominate Stealth Mode.
- Platform-overreaching security management with the Innominate Security Configuration Manager (optional).
- Integrated, high-capacity anti-virus solution (optional).
- Configuration with the Innominate Device Manager (IDM).
- Virtual addressing (1:1 NAT) in the VPN tunnel avoids address conflicts.

Unassailable with the Innominate Stealth Mode

Innominate's mGuard systems take advantage of a special function – the Stealth Mode. This allows the systems to perform absolutely transparent – as they do not 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.

Maximum data throughput for the VPN and firewall

The basis of the integrated security solution is the embedded Linux, running a special network processor with XScale core by Intel (IXP 42x) with up to 533 MHz processor capacity, 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).

Hardware performance features	mGuard core/266	mGuard core/533
CPU	Intel IXP 42x with 266 MHz	Intel IXP 42x with 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, RJ45, full-duplex, auto-MDIX	Ethernet IEEE 802.3 10 / 100Base TX, RJ45, full-duplex, auto-MDIX
MAU management	•	•
Serial interface	RS232, internal	RS232, internal
Internet		
Internet support	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi Stealth	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi Stealth
Network services		
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
Virtual Private Network (optional)		
VPN data throughput (3DES) 266/533	35/70 Mbit/s	35/70 Mbit/s
Max. number of VPN tunnels	10 or 250	10 or 250
Encryption procedures	DES, 3DES, AES-128, -192, -256	DES, 3DES, AES-128, -192, -256
Hardware-based encryption	•	•
IPsec mode	ESP tunnel / ESP transport	ESP tunnel / ESP transport
Authentication	X.509v3 certificates with RSA or PSK	X.509v3 certificates with RSA or PSK
Data integrity	MD5, SHA-1	MD5, SHA-1
Internet Key Exchange (IKE)	Quick mode, main mode, PFS	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	•	•
System management		
Web-based management (HTTPS)	•	•
Command line interface (SSH)	•	•
SNMP v1, v2, v3	•	•
Innominate Security Configuration Manager	optional	optional
Innominate Device Manager	optional	optional
Anti virus protection (optional)		
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
Power supply	5V/500mA	Firewall data throughput
Operating temperature	0 to 40 °C	User licenses
Relative humidity	20 to 90%, non-condensing	Stateful Inspection Firewall
Dimensions (W x H x D)	20 x 56 x 95 mm	NAT, 1:1 NAT
Weight	45 g	Port forwarding
		MAC-Filtering
		Firewall rules in VPN connections
		IP spoofing protection
		Syn flood protection
		Configurable DoS protection
		Redundant Firewall (VRRP)
		optional
		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 01.2007