

**Innominate**

# mGuard bladePack

The unique security solution for rack installation



**The mGuard blades are available in the performance classes**

- mGuard blade/266
- mGuard blade/533

The mGuard bladePack is the integrated, all-in-one security solution for installation in 19-inch rack systems. Featuring a redundant power supply and quick and easy integration, it requires neither modifications to the current system settings nor driver installation – regardless of the processor technology and operating system currently being used.



## Primary functions

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

- VPN (optional) 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 Stateful Inspection Firewall filters data packets based on the originating and target address, blocking undesired data traffic – also from „inside“.
- Integrated anti-virus protection (optional) supporting the HTTP, FTP, SMTP and POP3 protocols. Anti-virus protection takes place outside of the server. Therefore, no incursion into the system takes place – protecting the server while assuring high performance.
- High system availability through the optional firewall redundancy. Firewall policies and rules are maintained redundantly. In the case of an mGuard outfall, they stay automatically available for use.

## Simply incomparable: The integrated, all-in-one security solution

The mGuard bladePack by Innominat is at home in any IT environment, for its compatibility is unparalleled. Regardless of which server system you use, regardless of which operating system you work with, with this unique “device attached security” solution, you can guarantee the highest security standards. Uniformly and around the clock. In every industrial environment – from automotive to pharmaceutical – in medical technology areas, at remote maintenance applications and also in your industry.

The mGuard bladePack is the convenient solution for individually protecting business critical systems. These include:

- SAP or Oracle servers
- Citrix application servers
- OS/2 and Windows server farms
- Web hosting servers
- UNIX/Linux and MacOS X servers

## Unlimited protection

Conventional gateway appliances are generally used to protect entire networks or network segments with a universal security standard. However, a critical company server system often requires a security level that is much higher. And different systems call for various levels of security.

The mGuard blades enable you to assign each of your critical server systems its own security components – with individual levels of security and specifically configured access rights, not to mention numerous other unique advantages.

## Maximum data throughput for the VPN and firewall

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).

## Virtual addressing in VPN tunnel

Virtual private networks often connect networks in which non-public IP addresses are used. These arbitrary address spaces are often used on a multiple basis. In order to avoid address conflicts, the mGuard offers an address translation feature (1:1 NAT) within the VPN. The components which can be reached via VPN are each displayed under a different IP address to local devices.

## Maximal availability, minimal time and effort

The mGuard bladePack consists of the mGuard bladeBase (which can be integrated effortlessly into every 19-inch standard 3 U rack system) and up to 12 mGuard blades. In order to guarantee the highest possible level of availability, the mGuard bladeBase is standard-equipped with a redundant power supply, which is controlled by a monitoring unit. In the case of a problem, alerts are immediately transmitted via SNMP traps to the administrator. Additionally, every integrated mGuard blade is identified and monitored.

Up to 12 mGuard blades can be used with each mGuard bladeBase, allowing up to 12 individual server systems to be individually protected. By combining two mGuard blades into a hot standby system, you guarantee maximum protection and availability for up to six server systems. In this case, the mGuard blades monitor one another reciprocally. In the case of error, the twin mGuard blade takes over the complete range of functions (optional mGuard Redundant Firewall Option).

### Innominate Device Manager

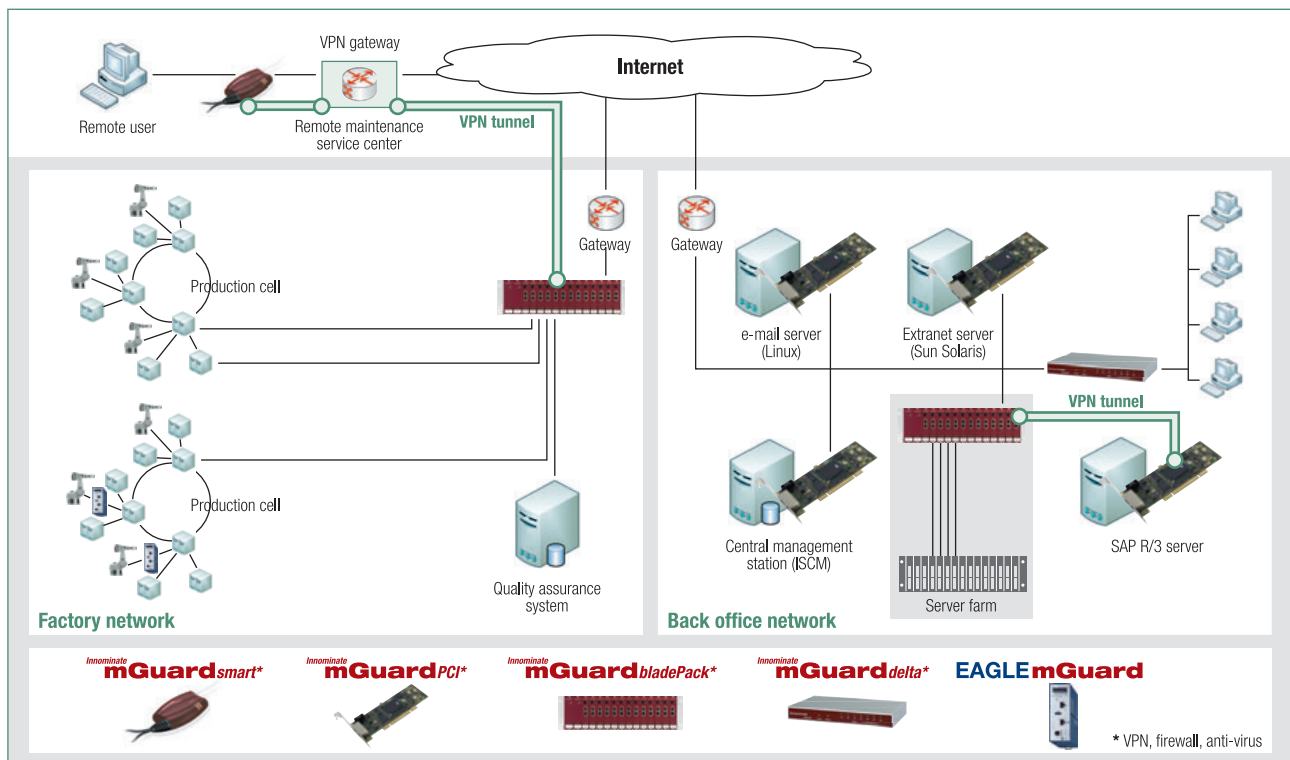
With the Innominate Device Manager (IDM) large populations encompassing several thousand mGuard appliances can be efficiently configured and managed. Due to the Innominate mGuard's template-based approach, the roll-out of numerous identically-configured appliances can be carried out quickly and conveniently.

### At a glance:

- "device attached security" system: independent of the hardware platform and operating system used.
- Redundant Firewall for high system availability (optional).
- Redundant power supply, monitoring unit and hot standby mode for maximum security and availability.
- Independent reconfiguration of the standby system when blades are exchanged.
- Maximum data throughput using hardware-based encryption for high speed VPN/firewall (optional).
- Virtual addressing (1:1 NAT) in the VPN tunnel avoids address conflicts.
- User firewall regulates access to internal or external resources via user login to the mGuard and central RADIUS server.
- High-capacity anti-virus solution (optional).
- Configuration with the Innominate Device Manager (IDM).
- Hot swapping allows replacement during operation.

### Unavailable with the Innominate Stealth Mode

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



Hardware performance features	mGuard blade/266 mGuard blade/533
CPU	Intel IXP 42x with 266/533 MHz
RAM / Flash	64 MB SDRAM/16 MB Flash
1 LAN / 1 WAN port	Ethernet IEEE 802.3 10 / 100 BaseTX, RJ45, full-duplex, Auto-MDIX
MAU management	•
<b>Internet</b>	
Internet support	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi-Stealth
<b>Network Services</b>	
DHCP support	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
<b>Virtual Private Network (optional)</b>	
VPN data throughput (3DES)	266: 35 Mbit/s; 533: 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 pre-shared keys (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 Security Configuration Manager	optional
Innominate Device Manager	optional
<b>Anti-virus protection*</b>	
Integrated scan engine	optional
Scans HTTP, FTP, POP3, SMTP, HTTP proxy	optional
Block by file size	optional
Automated pattern file updates	optional

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

Technical overview mGuard blade		Firewall	
Serial interface	RS232	Firewall data throughput	99 Mbit/s
Power supply	Via bladeBase	User licenses	unlimited
Operating temperature	0 to 40 °C	Stateful Inspection Firewall	•
Relative humidity	20 to 90 %, non-condensing	NAT, 1:1 NAT	•
MTBF	MTBF: 102,3 years; MIL-HDBK 217F: Gb 25 °C	Port forwarding	•
Dimensions (W x H x D)	160 x 100 x 26 mm	MAC-Filtering	•
Weight	approx. 200 g	Firewall rules in VPN connections	•
		IP spoofing protection	•
		Syn flood protection	•
		Configurable DoS protection	•
		Redundant Firewall (VRRP)	optional

### The all-in-one system mGuard bladePack

The integrated mGuard bladePack security solution consists of the mGuard bladeBase with redundant power supply and a monitoring unit. Up to 12 mGuard blades can be integrated into the mGuard bladeBase – for the protection of up to 12 individual server systems. Maximum security and availability are assured by combining two mGuard blades into a hot standby system. In the case of error, all functions (including complete configuration) are automatically carried out by the standby module.

### Technical overview mGuard bladePack

- 19-inch rack installation, 3 RU (rack units)
- Operation temperature: 0 to 40 °C
- Ambient temperature (transport and storage): -40 °C to 70 °C
- Relative humidity: 20 to 90 %, non-condensing
- Power supply: 90–264 V AC, 50/60Hz
- Power consumption (fully equipped): approx. 100 W
- Conformance: CE
- Dimensions (W x H x D): 483 x 133 x 235 mm
- Weight (fully equipped): approx. 13 kg

mGuard Software Options
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