

EAGLE mGuard

The integrated security solution for industrial Ethernet networks



The EAGLE mGuard is available in the versions

- EAGLE mGuard (Firewall)
- EAGLE mGuard VPN (Firewall + VPN)

The EAGLE mGuard is a joint development with the "Industrial Security Alliance" partner Hirschmann Automation and Control GmbH. The EAGLE mGuard fits for rail mounting and is equipped with a redundant power supply and two 10/100 BaseTX Ethernet ports, as well as a signaling switch. It can be integrated into a full range of production networks, without modification to the system settings or driver installation, regardless of the processor technology and operating system currently in use.

The optional configuration adapter that allows for a quick swap of defect devices in the field and the option to dial-up/dial-in via the V.24 interface further underline mGuard's unique feature set for industrial use.





Primary functions

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

- 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”.
- VPN (optional) for secure data transmission via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Integrated anti-virus protection (optional) supporting the HTTP, FTP, SMTP and POP3 protocols. Anti-virus protection takes place outside of the system. Therefore, no incursion into the system takes place – offering more protection while assuring high performance for the production.
- High system availability through the optional firewall redundancy. Firewall policies and rules are maintained redundantly. In the case of an mGuard outfall, they are automatically available for use within the shortest time periods.

Simply incomparable: integrated security for your production network

Innominate’s EAGLE mGuard is at home in every Ethernet-based production network. Its fields of application are virtually unlimited. Regardless of which production systems you currently use, regardless of which operating system you work with, with this unique “device attached security” solution, you can guarantee the highest security standards for uniform data communication companywide.

Various application scenarios for the EAGLE mGuard exist, depending on the design of the network. For example, office environments can be separated from production environments. Individual production cells can also be segmented via firewall functions. What’s more, secure access can be set up for remote administration via Internet, or a service port within the network, allowing external technicians to carry out maintenance on individual systems.

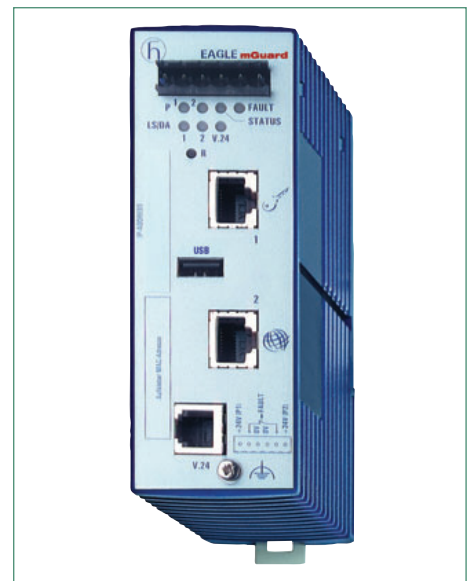
Unlimited protection

Conventional gateway appliances are generally used to protect entire networks or network segments using a universal security standard. In this case, important options can only be realized with great difficulty, including alternate security levels, individually customized access rights or regulated access times. What’s more, access lists and firewall rules, which have to be administered across the network backbone, quickly become too complex – increasing the danger of security holes in the system.

With the EAGLE mGuard, you can assign each production system its own security components – with individual levels of security and specifically configured access rights, as well as numerous other unique advantages.

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. For intuitive monitoring and logging, the mGuards communicate with all standard SNMP



systems. The full graphic integration can be realised on the Industrial HiVision management platform from the firm Hirschmann, for example.

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.

At a glance:

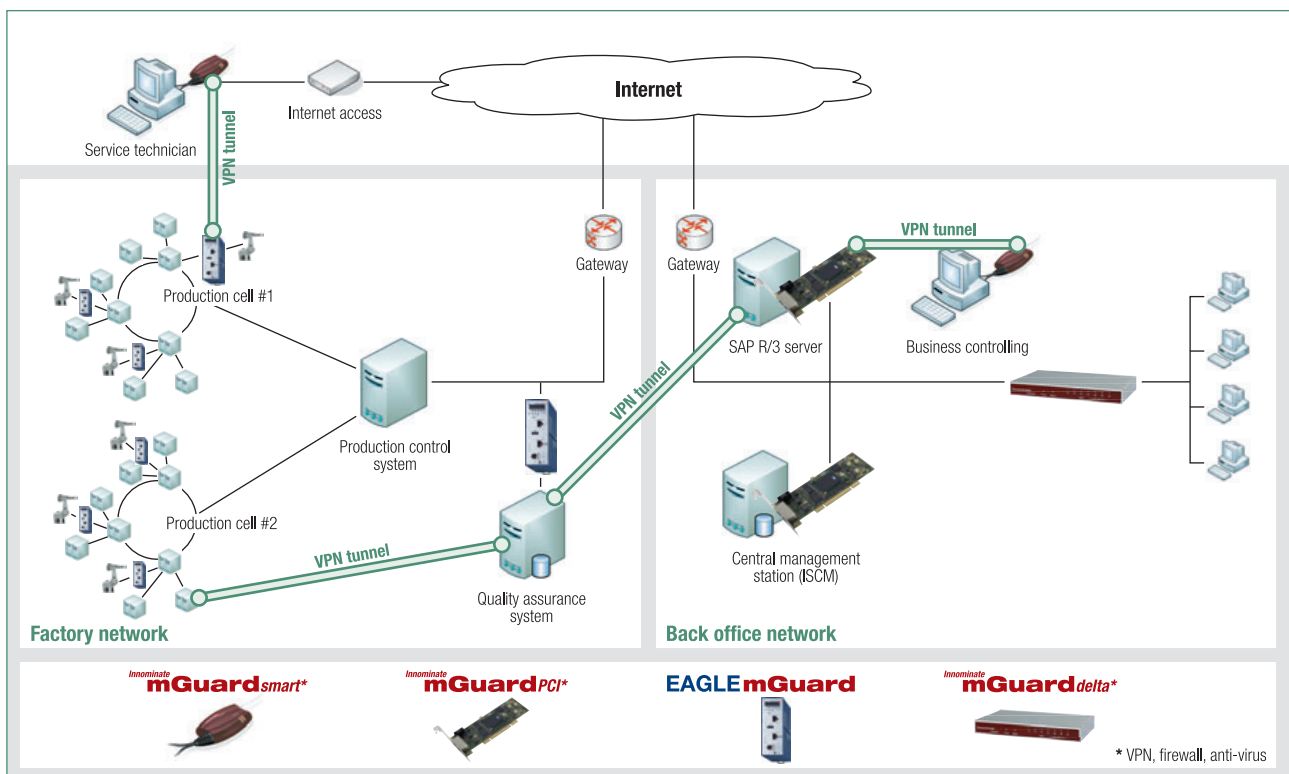
- Industry-suitable design: mounted on rails, IP20, ventilator-free, protected from shocks and vibrations.
- High system availability (MTBF 27,4 years).
- Maximum security and availability: 24 volt redundant input, signaling switch, status LEDs, logging on the syslog server.
- Maximum data throughput via hardware-based encryption for high speed VPN and firewall.
- Virtual addressing (1:1 NAT) in the VPN tunnel avoids address conflicts.
- High-capacity anti-virus solution (optional).
- User firewall regulates access to internal or external resources via user login to the mGuard and central RADIUS server.
- Configuration with the Innominate Device Manager (IDM).
- Also available with Fiber Optic WAN Interface.

Unassailable 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 – for they do not even 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. Moreover, the Innominate Stealth Mode does not require any modifications to the network.

Simple configuration

During service, the overall device configuration can be transmitted via the Configuration Adapter.



Hardware performance features	EAGLE mGuard
CPU	Intel IXP 42x with 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, optional 100 BaseFX (F0)
MAU management	•
Serial interface	V.24, RJ11 port
Power supply	24 V DC (-25 % to +25 %), max. 400 mA
Operating temperature	0 to 55 °C
Transport/storage temperature	-40 to +80 °C
Relative humidity	10 to 95 %, non-condensing
MTBF	MTBF: 27,4 years; MIL-HDBK 217F: Gb 25 °C
Mounting	rail mount
Protection class	IP 20
Dimensions (W x H x D)	47 x 131 x 111 mm
Weight	340 g

Mechanical stability	
IEC 60068-2-27 shock	15 g, 11 msec duration, 18 shocks
IEC 60068-2-6 vibration	1 mm, 2 Hz – 13.2 Hz, 90 min.; 0.7 g, 13.2 Hz – 100 Hz, 90 min.; 3.5 mm, 3 Hz – 9 Hz, 10 cycles, 1 octave/min.; 1 g, 9 Hz – 150 Hz, 10 cycles, 1 octave/min.

EMC interference immunity	
EN 61000-4-2 Electrostatic Discharge (ESD)	6 kV contact discharge, 8 kV air discharge
EN 61000-4-3 electromagnetic field	10 V/m (80 – 2000 MHz)
EN 61000-4-4 fast transients (burst)	2 kV power line, 1 kV data line
EN 61000-4-5 surge voltage (surge)	power line: 2 kV (line/earth), 1 kV (line/line), 1 kV data line
EN 61000-4-6 conducted emission	3 V (10 kHz – 150 kHz), 10 V (150 kHz – 80 MHz)

EMC emitted immunity	
FCC CFR47 Part 15	FCC CFR47 Part 15 Class A
EN 55022	EN 55022 Class A

Internet	
Internet support	PPPoE, PPTP, Static IP, DHCP client, Stealth/Multi Stealth

Network services	
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

System management	
Web-based management (HTTPS)	•
Command line interface (SSH)	•
Auto Configuration Adapter (ACA)	serial USB
SNMP v1, v2, v3	•
Innominate Security Configuration Manager	optional
Innominate Device Manager	optional

Firewall	
Firewall data throughput	99 Mbit/s
User licenses	unlimited
Stateful Inspection Firewall	•
NAT, 1:1 NAT	•
Port forwarding	•
MAC-Filtering	•
Firewall rules in VPN connections	•
IP spoofing protection	•
Syn flood protection	•
Configurable DoS protection	•
Redundant Firewall (VRRP)	optional
Anti-virus protection	
Integrated scan engine	optional
Scans HTTP, FTP, POP3, SMTP, HTTP proxy	optional
Block by file size	optional
Automated pattern file updates	optional

Virtual Private Network (optional)	EAGLE mGuard VPN
VPN data throughput (3DES)	70 Mbit/s
Max. number of VPN tunnels	10
Encryption procedures	DES, 3DES, AES-128, -192, -256
Hardware-based encryption	•
IPsec mode	ESP tunnel/ESP transport
Authentication	X.509v3 Zertifikate 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	•

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