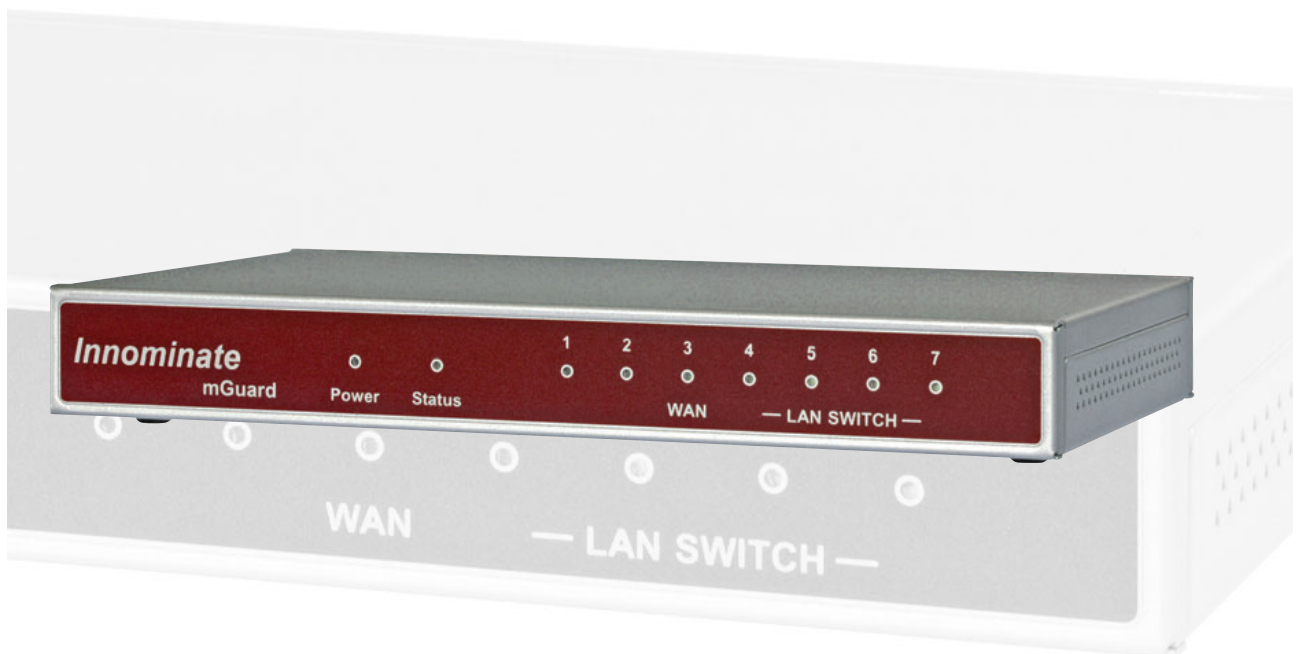


**Innominate**

# mGuard delta

Integrierte Firewall und VPN Appliance



**Erhältlich ist der mGuard delta  
in den Varianten**

- mGuard delta
- mGuard delta VPN

Der mGuard delta ist ein kompakter LAN Switch, der eine maximale Schutzwirkung mit integrierter Firewall-Funktionalität und optionalem VPN und Anti-Virus-Schutz bietet. Die mGuard Firewall kann auf bis zu vier LAN-Segmente verteilt werden. Der mGuard delta ist flexibel im Back-Office und als Schnittstelle zum Produktionsnetz einsetzbar. Sein robustes Metallchassis ist für den Desktop-Einsatz oder für den Einsatz im Verteilerraum geeignet.



## Grundlegende Funktionen

Die Security-Lösung mGuard delta von Innominate vereint alle Funktionen, um IP-Verbindungen zuverlässig abzusichern:

- Konfigurierbare Firewall schützt vor unberechtigten Zugriffen von „außen“. Die Stateful Inspection Firewall untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr auch von „innen“.
- VPN (optional) für die sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES-, 3DES- und AES-Verschlüsselung, IPsec-Protokoll).
- Integrierter Anti-Virus-Schutz (optional) mit Unterstützung für die Protokolle HTTP, FTP, SMTP und POP3. Die Virenprüfung erfolgt bereits außerhalb des Systems. Also: höhere Systemverfügbarkeit bei voller Leistung für die Produktion und das Back-Office.
- Der mGuard delta verfügt über einen 4-Port 10/100TX Ethernet Switch, der die Security-Funktionalität auf maximal vier Netzwerk-Segmente verteilt.

## mGuard delta – segmentierbare Security

Der mGuard delta ist eine kompakte Security Appliance, die in Firmennetzen sowohl im Produktionsumfeld als auch im Back-Office zum Einsatz kommt. Gerade in logisch segmentierten Netzen ist oft eine verteilte Security-Funktion gefordert. Mit dem mGuard delta lassen sich intelligente und hochperformante Security-Funktionen mit den Vorteilen eines Standard Ethernet/Fast Ethernet Switches koppeln.

Der mGuard delta bietet dabei alle Vorzüge der „device attached security“ – ein Konzept, welches gegenüber den klassischen Office-Firewalls oder softwarebasierten Lösungen klare Vorteile für den Schutz von dedizierten Systemen oder unterschiedlichen Netzwerksegmenten bietet.

## Redundante Firewall (optional)

Zwei mGuard delta können im High Availability Mode (HA) redundant betrieben werden. Der aktive mGuard delta überträgt die Firewall Stati auf den im „stand-by“ befindlichen mGuard delta. Beim Ausfall eines mGuard delta kann so ein lückenloser Schutz und eine hohe Verfügbarkeit des Gesamtsystems sichergestellt werden (mGuard Redundant Firewall Option).

## Benutzer-Firewall

Die Benutzer-Firewall ermöglicht es, dass einzelne Benutzer mit dynamischer IP-Adresse, zum Beispiel Servicetechniker, erst nach Anmeldung an der mGuard Appliance Zugriff auf interne oder externe Ressourcen bekommen. Die Passwörter können lokal auf der Appliance oder zentral auf einem RADIUS Server des Unternehmens hinterlegt werden.

## Mehr Sicherheit geht nicht

Mit herkömmlichen Gateway Appliances sichern Sie in der Regel ganze Netzwerke oder Netzwerksegmente mit einem einheitlichen Sicherheitsstandard. Unterschiedliche Sicherheitslevel, individuell eingegrenzte Zugriffsberechtigungen oder genau geregelte Zugriffszeiten sind damit kaum zu realisieren. Außerdem gilt: Access-Listen oder Firewall-Regeln, die im Backbone gepflegt werden, sind schnell zu komplex und unübersichtlich und erhöhen zusätzlich die Gefahr von Sicherheitslücken.

Mit dem mGuard delta können Sie jedem Produktionssystem oder Netzwerksegment seine eigene Sicherheitskomponente zuweisen: mit individuellem Sicherheitslevel, mit speziell konfigurierter Zugriffsberechtigung und mit zahlreichen weiteren einzigartigen Vorteilen.

## Maximaler Datendurchsatz für VPN und Firewall

Die Basis der integrierten Sicherheitslösung ist das von Innominate konfigurierte Embedded Linux, das auf einem speziellen Netzwerkprozessor mit XScale-Kern von Intel (IXP 42x) läuft: mit 533 MHz Prozessorleistung, 128 MByte SDRAM Arbeitsspeicher und 16 MByte Flash-Speicher. Im Intel Prozessor gibt es fest verdrahtete Befehle für die Verschlüsselungsverfahren DES, 3DES und AES. Das garantiert den überragenden Durchsatz bei Firewall (bis zu 99 Mbit/s und VPN-Verbindungen (bis zu 70 Mbit/s).

## Innominate Device Manager

Mit dem Innominate Device Manager (IDM) können große Populationen von mehreren tausend mGuard Appliances effizient konfiguriert und verwaltet werden. Der Roll-Out von vielen gleichartig konfigurierten Geräten ist durch den Template-basierten Ansatz des IDM schnell und komfortabel durchführbar.

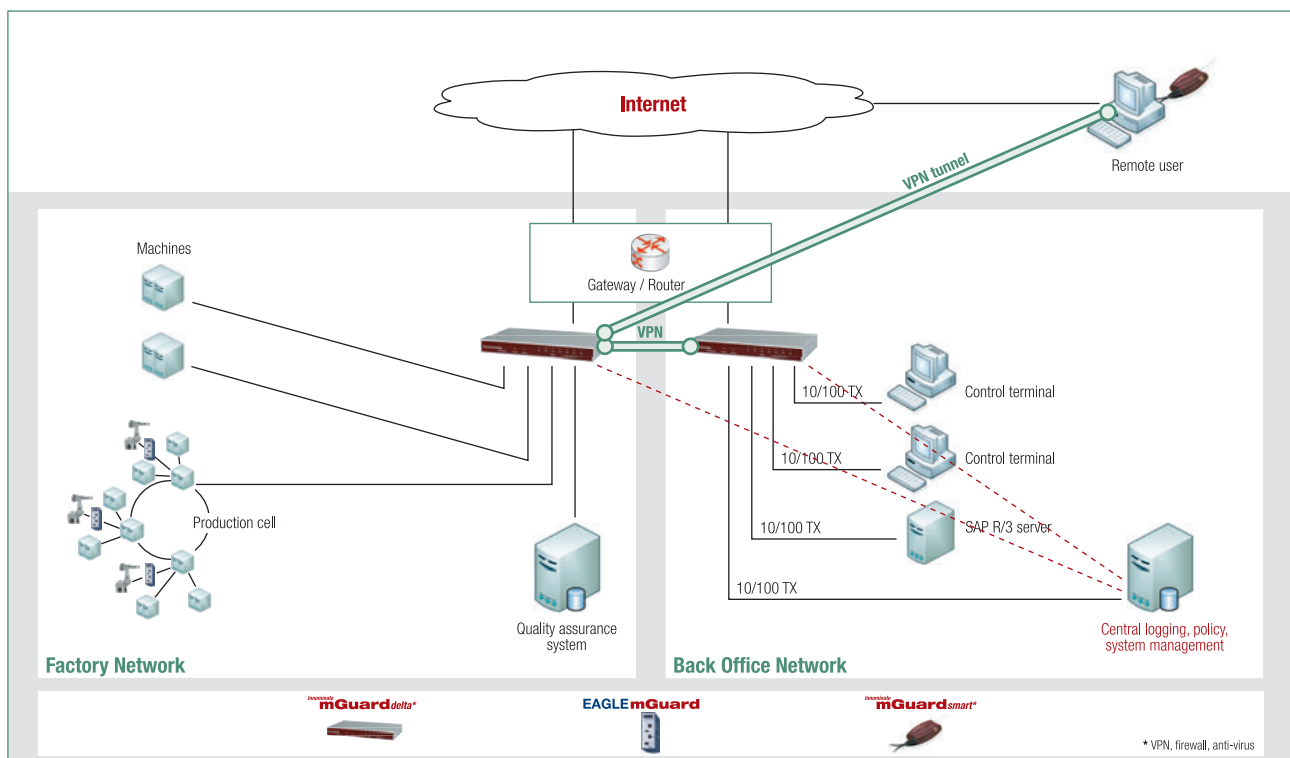
Für ein intuitives Monitoring und Logging kommunizieren die mGuards mit allen handelsüblichen SNMP-Systemen. Die volle grafische Einbindung wird zum Beispiel in der Industrial HiVision Management Plattform der Firma Hirschmann angeboten.

## Auf einen Blick

- Basiert auf Intel IXP 42X series, Security Prozessor.
- Stateful Inspection Firewall.
- Benutzer-Firewall für personenbezogene Zugriffsregel (RADIUS Server).
- VPN Tunnelling mit 3DES-/AES-Verschlüsselung.
- Virtuelle Adressierung (1:1 NAT) im VPN Tunnel zur Vermeidung von Adresskonflikten.
- Optionaler Anti-Virus-Schutz.
- Redundanter Betrieb (Aktiv/Passiv) mit dem VRRP (Virtual Router Redundancy Protocol).
- 10/100Mbps Ethernet WAN Port.
- 4-port 10/100TX Fast Ethernet Switch.
- Konfiguration mit dem Innominate Device Manager (IDM).
- Managebar über SNMP, HTTPS, SSH.
- RS-232 Port für Management.

## Unangreifbar durch den Innominate Stealth Mode

Die mGuard-Systeme von Innominate verfügen über eine besondere Funktion, den Stealth Mode. Sie arbeiten dabei absolut transparent und benötigen nicht einmal eine eigene IP-Adresse. Stattdessen nutzen sie dieselbe IP wie der zu schützende Rechner und sind dadurch für einen Angreifer nicht zu erkennen und deshalb auch nicht angreifbar. Durch den Innominate Stealth Mode muss nicht einmal das Netzwerk geändert werden.



Hardware-Leistungsmerkmale	mGuard delta	mGuard delta VPN
CPU	Intel IXP 42x mit 533 MHz	Intel IXP 42x mit 533 MHz
RAM/Flash	128 MB SDRAM / 16 MB Flash	128 MB SDRAM / 16 MB Flash
4 LAN/1 WAN port	Ethernet IEEE 802.3 10/100 BaseTX, RJ45, Full Duplex, Auto-MDIX	Ethernet IEEE 802.3 10/100 BaseTX, RJ45, Full Duplex, Auto-MDIX
MAU-Management	•	•
<b>Internet</b>		
Internetunterstützung	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 oder Relay Agent	Server oder Relay Agent
DNS-Cache	•	•
Dyn. DNS	•	•
NTP Client	•	•
LLDP (Link Layer Discovery Protocol)	•	•
VLAN (802.1Q)	•	•
Internet Updates	•	•
Remote Syslog Logging	•	•
Anwenderbasierte Konfigurationsprofile	•	•
Sprachen	Deutsch, Englisch und Japanisch	Deutsch, Englisch und Japanisch
<b>Virtual Private Network</b>		
VPN-Datendurchsatz (3DES)	-	70 Mbit/s
Max. Anzahl an VPN-Tunneln	-	10
Verschlüsselungsverfahren	-	DES, 3DES, AES-128, -192, -256
Hardwarebasierte Verschlüsselung	-	•
IPsec-Modus	-	ESP-Tunnel / ESP-Transport
Authentifizierung	-	X.509v3 Zertifikate mit RSA oder PreShared Keys (PSK)
Datenintegrität	-	MD5, SHA-1
Internet Key Exchange (IKE)	-	Quick mode, Main mode, PFS
IPsec L2TP Server	-	•
VPN in Stealth Modus	-	•
1:1 NAT im VPN	-	•
IPsec NAT-Traversal	-	•
Dead Peer Detection (RFC 3706)	-	•
Dyn. DNS VPN-Support	-	•
<b>Systemmanagement</b>		
Webbasiertes Management (HTTPS)	•	•
Command Line Interface (SSH)	•	•
SNMP v1, v2, v3	•	•
Innominate Security Configuration Manager	optional	optional
Innominate Device Manager	optional	optional
<b>Anti-Virus-Schutz</b>		
Integrierte Scan Engine	optional	optional
Prüft HTTP, FTP, POP3, SMTP, HTTP-Proxy	optional	optional
Block by File Size	optional	optional
Automatisierte Pattern File Updates	optional	optional
<b>Technische Details</b>		
Serielle Schnittstelle	RS232, internal	<b>Firewall</b>
Netzwerk Schnittstellen	4-Ports Ethernet 10/100 TX, 1 Port WAN 10/100 TX	Firewall-Datendurchsatz 99 Mbit/s
Stromversorgung	5V, 3A	Anwenderlizenzen unbegrenzt
LED-Anzeigen	Power x1, Status x1, link/active LAN Ports	Stateful Inspection Firewall •
Betriebstemperatur	0 bis 40 °C	NAT, 1:1 NAT •
Lagertemperatur	-20 bis +70 °C	Port-Weiterleitung •
Relative Luftfeuchtigkeit	5 bis 95%, nicht kondensierend	MAC-Filtering •
Maße (B x H x T)	239 x 156 x 30 mm	Firewall-Regeln in VPN-Verbindungen •
Gewicht	1.200 g	IP Spoofing Protection •
Zertifizierung	CE, FCC	Syn Flood Protection •
		Konfigurierbare DoS Protection •
		Redundante Firewall (VRRP) optional
		<b>mGuard Software-Optionen</b>
		Innominate mGuard VPN-10
		IPSec VPN Gateway, max. 10 VPN Tunnel
		Innominate mGuard VPN-250
		IPSec VPN Gateway, max. 250 VPN Tunnel
		Innominate mGuard Anti-Virus-50
		50 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
		Innominate mGuard Anti-Virus-200
		200 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
		Innominate mGuard Anti-Virus-1000
		1000 Appliances, unbegrenzte Lizenz für CLAM AV™ Virus Pattern
		Innominate mGuard Redundant Firewall Option
		Erfordert zwei mGuard Security Appliances

Innominate mGuard ist ein eingetragenes Markenzeichen der Innominate Security Technologies AG. Für die mGuard Technologie sind mehrere nationale und internationale Patente angemeldet oder erteilt worden. Alle weiteren Warenzeichen, Marken und Namen sind Eigentum der entsprechenden Firmen. Änderungen von Produktspezifikationen, Fehler und Irrtümer vorbehalten. Stand 01.2007