

**Innominate**

# mGuard

## Innominate mGuard: die innovative Lösung für mehr IT-Sicherheit bei der Medizintechnik

Der Datenaustausch verschiedener medizinischer Systeme und PCs innerhalb der Klinik und darüber hinaus bis in die Praxis von Hausarzt oder Spezialist gehören inzwischen zum Alltag. Die Verfügbarkeit und Sicherheit der Patientendaten ist dabei ein Thema, das starke Beachtung findet.



### Immer mehr Technologie zum Nutzen des Patienten ...

Die Informationstechnologie (IT) ist auch in den medizintechnischen Bereichen immer stärker eingebunden. Digitale Röntgenfotografie oder vollelektronische Analysesysteme bis hin zu hochtechnologischen Computertomographen werden zunehmend Standards in der medizinischen Diagnostik. Dazu kommen die technologischen Fortschritte selbst im OP-Bereich. Rechnergesteuerte Laserskalpelle sind die Spitze dieser Entwicklung. Die Video-Aufzeichnung und -Archivierung oder die so genannte Telemedizin – im Prinzip eine Videokonferenzschaltung, z. B. zwischen entfernten Spezialisten – wird bei schwierigeren OPs zunehmend eingesetzt, aber auch bei alltäglichen Eingriffen werden inzwischen immer mehr rechnergesteuerte Systeme genutzt.

### ... und mit dem Vorteil eines effizienteren Betriebsablaufs

Immer mehr dieser medizintechnischen Systeme werden vernetzt, um Zeit und Kosten zu sparen. Durch die Vernetzung können alle Patientendaten – vom Aufnahmeformular über Laborergebnisse bis zum OP-Bericht – komplett, lückenlos und zentral gespeichert werden. Die Daten stehen dann allen autorisierten Nutzern sofort und umfassend zur Verfügung. Ein Knopfdruck am PC und der behandelnde Arzt ist „im Bilde“.

Der andere Vorteil: Die Verfügbarkeit der Systeme kann ständig „remote“ überwacht werden und im Ernstfall sind erforderliche Wartungsarbeiten oder Software-Aktualisierungen möglich, ohne dass ein Servicetechniker vor Ort zum System kommt. Auch das spart Zeit und Kosten und gewährleistet die Einsatzbereitschaft der Systeme.



### Vorausgesetzt, die Verfügbarkeit und die Sicherheit sind gewährleistet

Der Nachteil der Vernetzung ist, dass im medizintechnischen Umfeld viele Rechnersysteme nur ungenügend gegen Angriffe abgesichert sind. Manchmal, weil sie auf proprietären Plattformen laufen. Herkömmliche Sicherheitslösungen können dann nicht integriert werden, weil Software oder Hardware nicht kompatibel sind. Manchmal, weil sie mit älteren Prozessor-technologien (z. B. Intel 386 oder 486) und älteren Betriebssystemversionen arbeiten und deshalb oft nicht über die erforderliche Performance verfügen. Aber auch neuere Standard-Systeme unter Windows sind hochgefährdet. Die Sicherheitslücken von Windows sind ja hinreichend bekannt.

Meistens aber ist die Sicherheit lückenhaft, weil medizintechnische Systeme validiert sind, also der gesetzlich verankerten Pflicht unterliegen, nachvollziehbare Dokumentationen der Geräte- und Anlagenlebensläufe zu führen. Damit ist jede Änderung am System, ob an der Software oder der Hardware, mit Aufwand und zusätzlichen Kosten verbunden.

Ausgerechnet Systeme, die Standards wie Windows, Ethernet, TCP/IP und HTTP nutzen und deshalb vermeintlich Vorteile bieten, sind unter dem Aspekt der Validierung enorme „Kostenfresser“. Denn die zahlreichen Sicherheitspatches, die von Microsoft ständig ausgegeben werden, können das Budget kräftig belasten. Also verzichtet man häufig auf diese Systemupdates, weil sich viele Verantwortliche nicht darüber bewusst sind, dass ihre rechnergesteuerten medizintechnischen Systeme genau den gleichen Gefahren, z. B. durch Virus-Attacken ausgesetzt sind wie die PCs der Verwaltung. Nur dass Fehlfunktion oder Ausfall eines medizintechnischen Systems unter Umständen Menschenleben kosten kann.

### Warum übliche Sicherheitstechnologien wenig nutzen

Nun gibt es verschiedene Sicherheitstechnologien, die auch für medizintechnische Systeme genutzt werden könnten, aber alle – ob hardware- oder softwarebasiert – haben in diesem Anwendungsbereich den entscheidenden Nachteil, dass das Rechnersystem verändert werden muss. Unter dem Aspekt der Validierung also wieder ein hoher Aufwand und entsprechende Kosten, zusätzlich zu den Kosten, die die aufwendige Implementierung und Konfiguration durch einen Techniker vor Ort verursachen.

Hardwarebasierte Systeme (Router, Bridges) haben den Nachteil, dass sie immer an ihrer IP im Netz erkennbar und deshalb angreifbar sind. Vor allem, weil in aller Regel bei vielen Systemen sämtliche Standard Ports offen stehen, um den problemlosen Datentransfer zu ermöglichen.

Softwarebasierte Lösungen (Personal Firewall, Anti-Viren-Software) haben andere, zusätzliche Nachteile: Sie sind auf manchen proprietären Betriebssystemen nicht lauffähig. Auf Systemen mit älterer Prozessor-technologie können sie oft nicht eingesetzt werden, weil die erforderliche Performance fehlt. Die Abwehr einer Virus-Attacke würde die Prozessorleistung derart beanspruchen, dass das ganze System lahm gelegt wird. Und: Software erfordert stets regelmäßige Updates, sonst können Virus-Attacken aufgrund der immer wieder aufgedeckten Sicherheitslücken ganz einfach zum Betriebssystem durchdringen. Updates sind schon bei normalen Computern aufwendig und erfordern teure Ressourcen. Bei validierten Systemen verursachen sie noch zusätzliche Kosten.

## Sichern Sie Ihr medizinisches System einfach, zuverlässig und wirtschaftlich

Die mGuard Technologie ist eine überragende, innovative Sicherheitslösung, die als „device attached security“ bezeichnet wird. Alle bekannten Nachteile herkömmlicher Sicherheitstechnologien – insbesondere für validierte Systeme – werden mit den mGuard Komponenten auf einzigartig einfache, zuverlässige und wirtschaftliche Art gelöst. Mit der mGuard Technologie sind keinerlei Veränderungen am medizintechnischen System erforderlich. Nicht bei der Installation und auch nicht danach. Die mGuard Produkte sind einfach und schnell zu installieren, arbeiten unabhängig von Prozessortechnologie und Betriebssystem und erfordern keine regelmäßigen Software-Updates. Die mGuard Technologie sichert also Systeme zuverlässig und dauerhaft und verursacht in der Regel keine Kosten mehr für eine Validierung. Zusätzlich kann es Validierungskosten sparen, weil die Sicherheits-Updates für Windows-Betriebssysteme nicht mehr installiert werden müssen.

## Höchster Sicherheitslevel, unabhängig vom Netzwerk

Rechnergesteuerte, medizintechnische Systeme sind üblicherweise in das Klinik-Netzwerk eingebunden und deshalb in der Regel vor Angriffen von außen durch herkömmliche Gateway Appliances mit dem gleichen Sicherheitsstandard geschützt wie die Büro-PCs. Aber kritische Systeme wie medizintechnische Anlagen erfordern einen Sicherheitslevel, der weit höher liegt. Dazu kommt: Egal, mit welchen Komponenten ein Netzwerk vor Angriffen von außen geschützt wird, es bleiben immer noch genügend Gefahrenpotenziale innerhalb eines Unternehmens, wie z. B. Viren, die unwissentlich durch das Notebook eines Mitarbeiters eingeschleust werden können.



Mit der mGuard Technologie können Sie jetzt jedem rechnergesteuerten medizintechnischen System seine eigene Sicherheitskomponente zuweisen: mit individuellem Sicherheitslevel, mit speziell konfigurierter Zugriffsberechtigung und mit zahlreichen weiteren einzigartigen Vorteilen.

## Einfach integriert, ruck, zuck installiert

Der mGuard ist ein eigenständiges System, das entweder direkt an der rechnergesteuerten medizintechnischen Anlage vor das Netzkabel gesetzt oder bei Bedarf als PCI-Karte integriert wird. Es ist auch unerheblich, mit welchem Betriebssystem oder mit welcher Hardware-Plattform die Anlage arbeitet. Der mGuard ist zu allen Systemen kompatibel.

## Grundlegende Funktionen

Die „device attached security“-Lösung mGuard von Innominate vereint alle Funktionen, um IP-Verbindungen, z. B. für die Remote-Wartung des Systems oder für den Zugriff vom Chefarzt-PC aus zuverlässig abzusichern:

- VPN für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES-, 3DES- und AES-Verschlüsselung, IPsec-Protokoll).
- Konfigurierbare Firewall schützt vor unberechtigten Zugriffen. Der Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert als unerwünscht definierten Datenverkehr.
- Integrierter optionaler Kaspersky-Virenschutz mit Unterstützung für die Protokolle HTTP, SMTP und POP3 (ausschließlich empfohlen für die Versionen enterprise und enterprise XL). Die Virenprüfung erfolgt außerhalb des Rechners. Also: kein Eingriff in den Rechner und trotzdem Sicherheit und mehr verfügbare Leistung auf dem Rechner.

### Unangreifbar durch den Innominate Stealth Mode

mGuard, das „device attached security“-System von Innominate, verfügt über den einzigartigen Innominate Stealth Mode. Das Device arbeitet absolut transparent und benötigt keine eigene IP-Adresse. Es benutzt dieselbe IP wie der zu schützende Rechner, ist also für einen Angreifer nicht erkennbar und deshalb nicht angreifbar. Durch die werksseitige Standardeinstellung des Stealth Mode muss am mGuard nichts konfiguriert oder geändert werden. Es ist jedoch möglich, jeden einzelnen mGuard auch im Stealth Mode an spezielle Sicherheitsanforderungen und die Security Policies im Unternehmen individuell anzupassen.

Die Konfiguration, das Roll-out, die Verwaltung, aber auch die Wartung der mGuard Devices wird am besten und einfachsten durch den Innominate Security Configuration Manager unterstützt.

### 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 bis zu 533 MHz Prozessorleistung, bis zu 64 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 (bis zu 70 Mbit/s). VPN-Verbindungen sind auch im Stealth Mode schnell und zuverlässig aufzubauen.



### Auf einen Blick

- „device attached security“-System: unabhängig von Rechnerplattform und Betriebssystem.
- Einfachste Integration: keine Rechneranpassungen, keine Treiberinstallation, nie mehr Updates.
- Rückwirkungsfreie Netzwerkintegration durch transparenten Innominate Stealth Mode.
- Hoher Datendurchsatz durch hardwarebasierte Verschlüsselung für High Speed VPN/Firewall.
- Leistungsfähige Anti-Virus-Lösung basierend auf Kaspersky-Technologie (optional).
- Volle Interoperabilität mit anderen Standard-Security-Lösungen (IPsec) innerhalb des LAN/WAN.
- Integrierbar in zentrale Management-Umgebungen (SNMP).
- Komfortable, unternehmensweite Konfiguration aller Security Devices per drag and drop mit dem Innominate Security Configuration Manager (optional).

### Einfach integrieren, bequem administrieren

Maßgeblich unterstützt wird die plattformübergreifende Sicherheit der mGuard Devices durch den Innominate Security Configuration Manager (ISCM), der auf der bewährten Technologie des Solsoft Policy Servers aufsetzt. ISCM ist eine gruppenbasierte Plattform. Anhand eines grafischen Netzwerkmodells werden die Sicherheitseinstellungen für mehrere mGuard Systeme gleichzeitig schnell und komfortabel konfiguriert. Es werden die gesetzten Regeln automatisch überprüft und die Vollständigkeit und Korrektheit bestätigt. Es werden die generierten Firewall-Regeln, VPN-Konfigurationen und NAT-Einstellungen direkt auf alle Devices einer Gruppe geladen und sofort aktiviert. Darüber hinaus werden VPN-Verbindungen zwischen mGuard Devices untereinander und mit Gateways anderer Hersteller eingerichtet und verwaltet. Alles komfortabel über die grafische Oberfläche und einfach per Mausclick.

Was durch die Konfiguration einzelner Systeme bisher komplex, zeitraubend und fehleranfällig war, wird mit der Gruppenverwaltung des Innominate Security Configuration Managers plötzlich ganz einfach, in kurzer Zeit und fehlerlos konfiguriert. Der Aufwand und die Kosten werden deutlich reduziert.