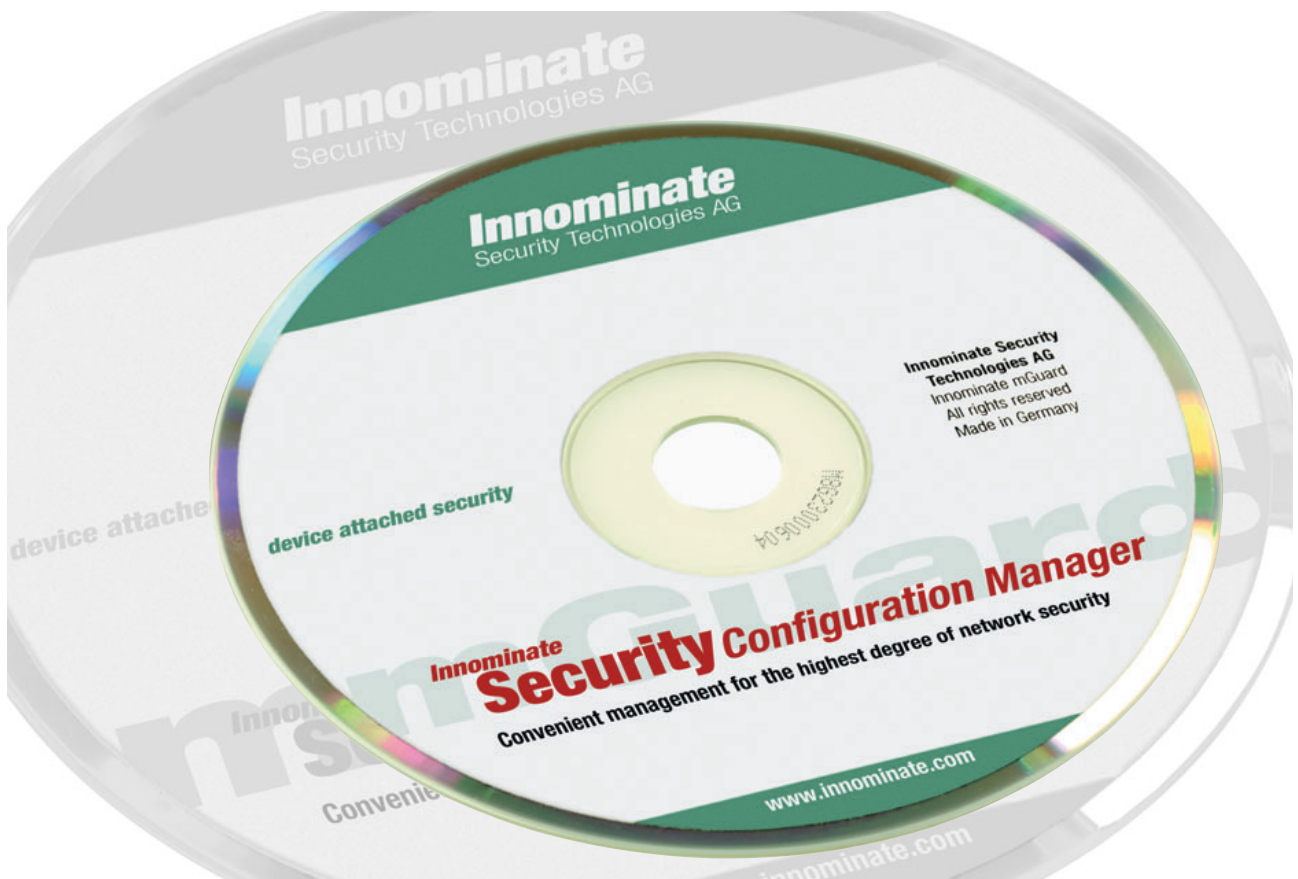


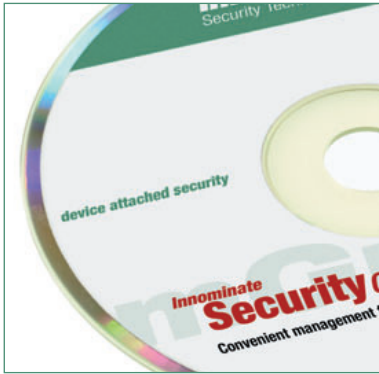
**Innominate**

# **Security Configuration Manager**

Die plattformübergreifende Konfiguration und Administration  
Ihrer Netzwerk-Sicherheit



Der Innominate Security Configuration Manager (ISCM) basiert auf der bewährten Technologie des Solsoft Policy Servers und unterstützt die Konfiguration und Administration der Innominate mGuard Produkte ebenso wie die aller anderen Sicherheitsappliances in Ihrem unternehmensweiten Netzwerk.



## Die wichtigsten Vorteile im Überblick

### Reduzierung der Kosten

Der ISCM unterstützt Ihre Teams dabei, fehlerfreie Sicherheitsregeln für alle Systeme im Netzwerk automatisiert zu entwerfen und zu entwickeln, anstatt einzelne Devices manuell zu konfigurieren. Änderungen komplexer Netzwerke können in Minuten durchgeführt werden, egal, ob ein Device oder hunderte modifiziert werden müssen. Der Roll-out Support garantiert die problemlose und schnelle Installation einer großen Anzahl von Devices. Das bringt zusätzliche Vorteile und einen optimalen Return on Investment.

### Schnellstmögliche Ereignismeldung

Der ISCM macht Ihr Unternehmen dynamischer und verbessert Ihre Möglichkeiten, auf Viren, Würmer und Netzwerkattacken zu reagieren. Noch wichtiger ist, dass das Policy-basierte Konzept des ISCM Ihr Netzwerk vor zukünftigen Angriffen abschottet, weil sichergestellt ist, dass die Sicherheitsregeln eine einheitliche und fehlerfreie End-to-End Konfiguration gewährleisten – etwas, das in komplexen Netzwerken manuell unmöglich ist.

## Technologie und Organisation: Moderne Herausforderungen dargestellt an komplexen Netzwerkstrukturen

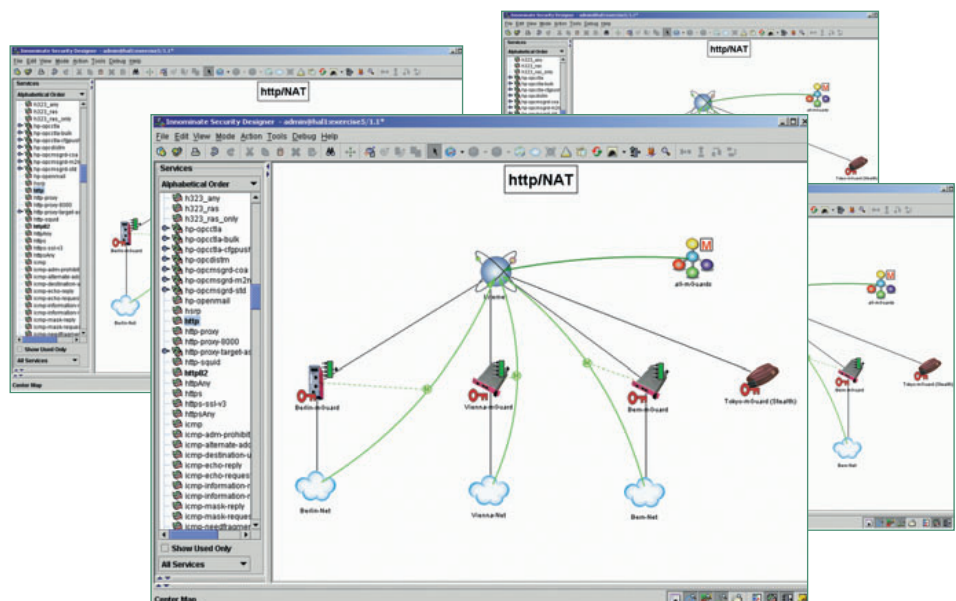
Die Konfiguration und Administration von Sicherheitsappliances stellt für jeden IT-Verantwortlichen eine technische und organisatorische Herausforderung dar. Für gewöhnlich ist das ein aufwendiger, manueller und fehleranfälliger Prozess. Mit dem Innominate Security Configuration Manager (ISCM) wird die Konfiguration und Administration der „device attached security“-Plattform von Innominate ganz einfach.

Der Innominate Security Configuration Manager (ISCM) basiert auf dem bewährten Managementkonzept der Solsoft Produktlinie. Im Gegensatz zu vielen herstellerspezifischen Tools verwaltet der ISCM nicht einzelne Devices, sondern die Sicherheitspolicies, die Ihr Netzwerk schützen. Der ISCM erlaubt die Anordnung und Definition der Firewall, der NAT-Einstellungen und aller VPN-Regeln per Mausklick. Durch diese Zentralisierung und Automatisierung der Sicherheitsprozesse wird das Management der Netzwerksicherheit schnell, einfach und Kosten sparend. Man muss kein Experte sein, um in kürzester Zeit selbst komplexe Sicherheitsregeln verstehen, erstellen und anwenden zu können.

Gehen Sie proaktiv an Ihre Sicherheitsstrategie heran, und ziehen Sie zusätzlichen Nutzen aus Ihrer Investition in die Plattform-unabhängigen mGuard Devices. Denn eines der wesentlichen Merkmale des ISCM ist die Multi-Vendor-Managementfähigkeit, speziell zugeschnitten auf die Anforderungen der „device attached security“-Strategie von Innominate.

## Policy-basiertes Management

Im Unterschied zu Point-to-Point Management Tools, mit denen jedes Sicherheits-Device individuell konfiguriert werden muss, um den erforderlichen Sicherheitslevel zu erreichen, orientiert sich die Policy-basierte Managementlösung des ISCM an den Erfordernissen der Geschäftsabläufe. Der ISCM ermöglicht die unternehmensweite Festlegung von Regeln für Verbindungen zwischen Netzwerkinstanzen wie Anwendern und Anwendungen. So können Sie beispielsweise festlegen, dass eine Niederlassung bei Verbindung über einen VPN Tunnel nur auf bestimmte Anwendungen zugreifen kann. Die Policies sind in tabellarischer oder grafischer Form allgemeinverständlich definiert, so dass sich auch die Entscheider im Unternehmen aktiv an deren Erstellung beteiligen können.



## Kein manuelles Codieren

Der ISCM beseitigt viel von der Komplexität und Undurchschaubarkeit beim Management von Sicherheits-Devices, so dass Sie beim Entwurf und der Umsetzung Ihrer Sicherheitsstrategie Resultate erzielen, für die bisher ein Team von Netzwerkspezialisten und Sicherheitsexperten erforderlich war. Er lässt sich durch das drag-and-drop Interface einfach bedienen. Die erforderlichen Filter, NAT- und VPN-Konfigurationsparameter werden automatisch generiert und für alle Sicherheitssysteme im Netzwerk angewendet. Die Regeln werden optimiert, geordnet, auf Fehler überprüft und auf alle Devices geladen.

## Workflow-Unterstützung (nur bei enterprise Edition)

Die unternehmensweite Implementierung von Sicherheits-Policies erfordert eine enge Zusammenarbeit zwischen den Business- und den Netzwerk-Experten und deren Kollegen für die Sicherheitsorganisation. Die prozessorientierten und rollenbasierten Admi-

nistrations-Funktionen (nur bei enterprise Edition) ermöglichen den Anwender-Teams die Zusammenarbeit bei der Entwicklung, Einsetzung und Aktualisierung der Policies für das Netzwerk-Sicherheitsmanagement.

## Rollenbasiertes Änderungs-Management (nur bei enterprise Edition)

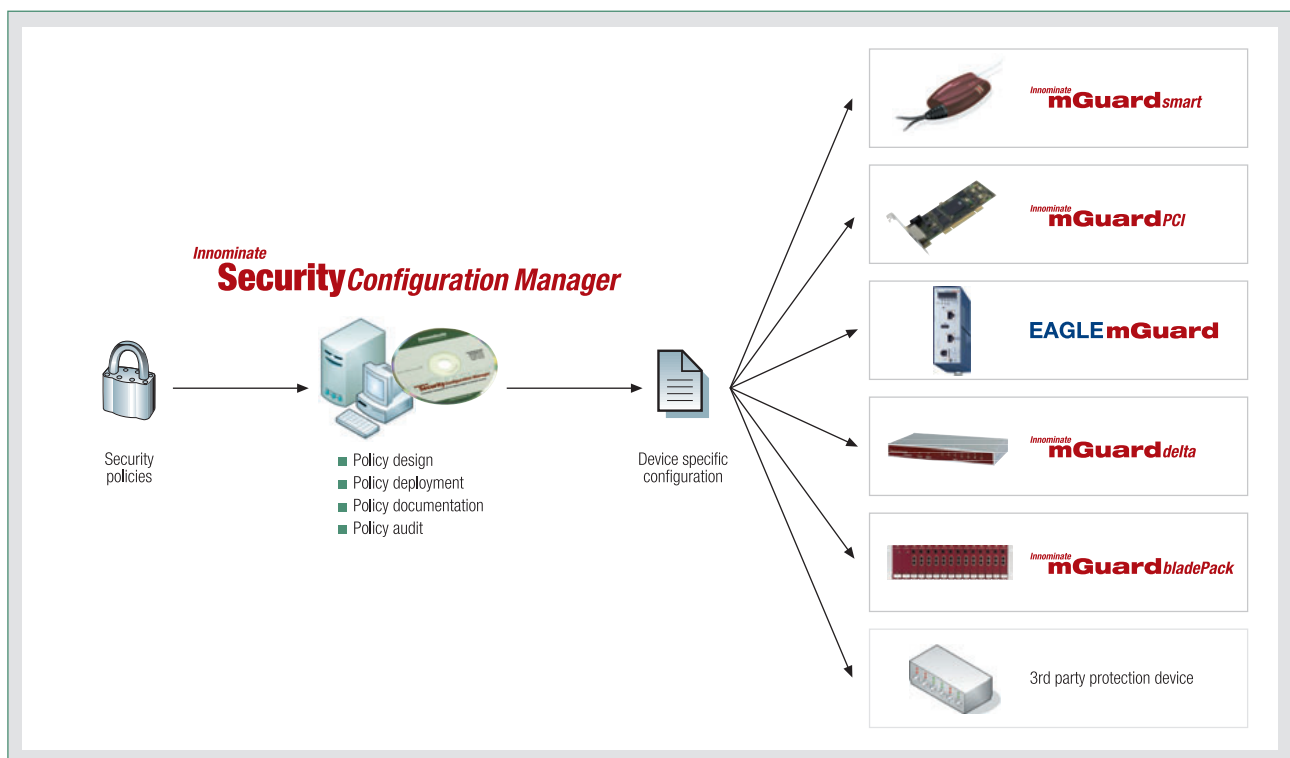
Der ISCM bietet die Möglichkeit, eine unbegrenzte Zahl an Policies und Anwender-Rollen zu speichern. Policy Histories zeichnen jede einzelne Veränderung durch die Anwender auf, und Merkmale für verschiedene Policy-Versionen können für ein Roll-Back genutzt werden. Für jede Rolle ist es möglich, detaillierte Rechte zu definieren, um speziellen Anforderungen gerecht zu werden.

## Optimale Sicherheitskonfiguration

Mit dem ISCM werden Policies umfassend zu einheitlich angewandten Regeln, die für alle Devices gelten, unabhängig von Hersteller oder Funktion. Die Regeln

## Erhöhte Transparenz

Das Security Reporter Modul (nur bei enterprise Edition) macht die Erstellung von Reports mit einer hohen Transparenz für alle Prozessbeteiligten ganz einfach. Die Berichte bilden das Bindeglied zwischen den Betriebsabläufen und den implementierten Netzwerk-Sicherheits-Policies und Unternehmen können von den integrierten Analyse-Funktionen profitieren, um die Audit-Kosten zu senken, wenn Prüfungen zur Einhaltung der Vorschriften regelmäßig erforderlich sind.



sind für jedes System exakt gleich und durchgehend gültig. Darüber hinaus erkennt der ISCM die komplexen Beziehungen zwischen allen Netzwerkeinheiten und der Sicherheitsstruktur. Diese umfassende Kenntnis des Netzwerkes ermöglicht es der ISCM ein „deny by default“-Policy anzuwenden, die das das Netzwerk gegen Attacken auf ungenutzte Ports immun macht.

### Multi-Vendor Interoperabilität

Zusätzlich zur Verwaltung der mGuard Plattform unterstützt der ISCM das zentrale Sicherheitsmanagement aller Systeme im unternehmensweiten Netzwerk. Solsoft als Partner von Innominate arbeitet mit allen führenden Partnern für Netzwerksicherheit zusammen, um die Interoperabilität konstant zu gewährleisten.

### Detailliertes Audit Reporting

Über eine webbasierte Benutzeroberfläche (nur bei enterprise Edition) können Security Manager und Revisoren detaillierte Reports über die gesamte Laufzeit der Policies hinweg erstellen, einschließlich von Projekthinhalten, Regelsuchen und dem Abgleichen von Konfigurationsveränderungen. Und mit ausgeklügelten Nachbildungen der Netzwerkstruktur können An-

wender sofort und individuell einzelne Devices, IP-Adressen, VPN Tunnel oder das gesamte Netzwerk prüfen – einfach per Mausklick.

### Roll-out Unterstützung

Bei größeren Roll-outs oder zur Verwaltung von komplexen mGuard Implementierungen (bei mehr als 100 mGuard Systemen) unterstützt Sie der ISCM mit Tools, die für Sie die Konfigurations-Dateien für alle Devices erstellen. Bei Inbetriebnahme eines mGuard Devices holt sich jeder mGuard seine individuelle Konfiguration automatisch vom Server. Es muss nicht mehr jedes Device individuell konfiguriert werden, was die Kosten für das Roll-out deutlich reduziert.

### Learning Mode

In Umgebungen, die über lange Zeit gewachsen sind, können Administratoren ganz einfach den Überblick verlieren, welcher Traffic innerhalb des Netzwerkes ermöglicht werden muss, um alle Anwendungen verfügbar zu halten. Der ISCM bietet einen einzigartigen Lernmodus, der es ermöglicht, den Traffic automatisch zu scannen und zu analysieren und entsprechend der Traffic-Analyse Regeln zu generieren bzw. zu importieren.

### Auf einen Blick:

- Multi-Vendor Unterstützung
- Visuelle Drag and Drop Benutzeroberfläche
- Tabellarischer Policy Editor / Bildschirmerrstellung
- Generierung von Firewall- und NAT-Regeln
- IPsec VPN Konfiguration
- Automatische Policy-Prüfung / -Bereinigung
- Automatische Generierung Device-spezifischer Codes und Bereitstellung
- Zentralisierte Policy-Ablage
- Umfangreiche Audit-Möglichkeiten
- Roll-out Unterstützung
- Learning Mode
- Versionsverwaltung und Änderungskontrolle (nur bei enterprise Edition)
- Webbasierte Reporting Engine (optional, nur bei enterprise Edition)
- Verwaltung der Anwender-Rollen, der Anwender-Rechte und des Workflows (nur bei enterprise Edition)

### Über Solsoft

1997 gegründet, ist Solsoft einer der führenden Anbieter von Management Lösungen für Netzwerk-Sicherheits-Policies. Solsoft verwaltet einige der weltweit größten Netzwerke in unternehmenskritischen Umgebungen. Zu den Kunden von Solsoft gehören Unternehmen aus der Fortune 500 Gruppe, Regierungsstellen und Telekommunikations-Organisationen.

	ISCM professional Edition	ISCM enterprise Edition
Entwicklung von End-to-End Policies	•	•
Visuelle Policy Entwicklung	•	•
Multi-Vendor Unterstützung	•	•
Firewall Unterstützung	•	•
IPsec VPN Unterstützung	•	•
Gruppierung von VPN Tunneln	optional	optional
IPS/IDS Unterstützung	optional	optional
Import	optional	optional
Clustering	optional	optional
Virtuelle Systeme	•	•
Zusammenarbeit / Multi-User	-	•
Unterschiedliche Policy Versionen	-	•
Multi-Projects	-	•
Remote Client	-	•
Zentrale Objekt-Datenbank	-	•
Policy Plausibilitätsprüfung	•	•
Policy Reporting	-	optional
Server Hochverfügbarkeit	-	optional
Web Service API	-	optional

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