



# CORISECIO secRT Enterprise Security Plattform

*Simplify Security - the Platform!*

**CORISECIO**  
Corporate Information Security



FACTSHEET

Enterprise Security ist komplex. Zur Absicherung der gesamten Unternehmens-IT bedarf es einer Vielzahl von Lösungen unterschiedlicher Hersteller. Implementierung, Administration und Wartung beherrschbar zu machen, ist eine Herausforderung. Die Entwicklung hin zu verteilten Systemen (bspw. in SOA- und Portalumgebungen) verstärkt diese Forderung.

Nutzer von Security Software benötigen automatisierte Lösungen, um Enterprise Security heute beherrschbar und für die Anforderungen von z.B. SOA- und Portalumgebungen einsatzfähig zu machen.

## SICHERE LAUFZEITUMGEBUNG

Die CORISECIO secRT-Plattform in der Enterprise-Version erweitert die Open Source-Laufzeitumgebung secRT, eine Security Plattform des Bundesamtes für Sicherheit in der Informationstechnik (BSI), um weitere Sicherheitskomponenten. Es werden nur von CORISECIO signierte und zertifizierte Adapter verwendet; die Verwendung von unsicheren Fremdadaptern wird unterbunden. Somit ist sichergestellt, dass nur Adapter genutzt werden, die den höchsten Qualitätsanforderungen genügen. Bei ablaufender Gültigkeit der Signaturen wird der Administrator frühzeitig gewarnt und hat somit die Möglichkeit, auf die aktuelle Version der einzelnen Komponenten zu aktualisieren.

## ZENTRALE ADMINISTRATION

Ein weiterer Vorteil beim Einsatz der Enterprise Variante ist eine zentrale Verwaltung aller Instanzen über die sogenannte managementRunTime (mRT). Hierbei werden über eine übersichtliche Administrationsoberfläche die benötigten Policy Einstellungen vorgenommen und können anschließend per Mausklick an alle angeschlossenen secRT Instanzen verteilt werden. Somit entfällt die lokale Konfiguration der einzelnen Instanzen und der Administrator hat die Möglichkeit die gesamte Sicherheitsinfrastruktur mit wenigen Aktionen zu kontrollieren.

## MODELLIERUNG & ORCHESTRIERUNG

CORISECIO bietet in der Enterprise-Variante der secRT durch Modellierungsfunktionen die Möglichkeit, komplette Security Prozesse ohne Programmieraufwand zu erstellen. Auf Basis von Security Erweiterungen des BPEL Standards können Sicherheitsmethoden zu Security Services zusammengefügt und an spezielle Unternehmensanforderungen angepasst werden. Einmal konfigurierte Security Prozesse werden automatisch an die Laufzeitumgebungen verteilt und dort umgesetzt.

## FACTS

- Sichere Laufzeitumgebung für Sicherheitslösungen
- Vollständige Kontrolle und Orchestrierung
- Security Modellierung – ohne Programmieraufwand
- Automatisierte Überprüfung der eingesetzten Komponenten
- Plattformunabhängige Laufzeitumgebung für Security Software
- API Funktionalität für Partner Produkte

## BENEFITS

- Geringer Implementierungsaufwand
- Modellierung per Mausklick
- Höchste Flexibilität und Zukunftssicherheit
- Bester Investitionsschutz
- Hohe Interoperabilität
- Ready-to-go Gateway-Lösungen





### FLEXIBILITÄT DURCH ADAPTERKONZEPT

Die Enterprise secRT ist über das Adapterkonzept vollständig erweiterbar. CORISECIO Standardprodukte bestehen aus der secRT und produktspezifischen Adaptern. Die Enterprise secRT Security-Plattform ermöglicht zudem die Integration herkömmlicher Anwendungen in eine zentral administrierte Security Plattform.

### SECURITY-ENABLER FÜR BEWÄHRTE LÖSUNGEN

Aufbauend auf der secRT Security-Plattform bietet CORISECIO Gateway-Lösungen an, die die unterschiedlichen Anforderungen verschiedener Unternehmensbereiche erfüllen.

Mit der Data Security Produktfamilie liefert CORISECIO intelligente Lösungen zur transparenten Verschlüsselung von Dateien und Datenbanken mit integriertem Berechtigungsmanagement. Unabhängig von den eingesetzten Lösungen lässt sich mit geringem Implementierungsaufwand ein hohes Sicherheitslevel für Ihre Daten herstellen.

Die Produktfamilie Mobile Enterprise sorgt für die zertifikatsbasierte Absicherung der Kommunikation mit mobilen Endgeräten (z.B. Blackberry). Installation, Zertifikatsverwaltung und Datenverschlüsselung erfolgen komfortabel und unter Umgehung risikobehafteter Infrastruktur.

SOA Security Gateway-Lösungen stellen Absicherungsmethoden für SOA Architekturen bereit. Schutzziele wie Authentisierung, Autorisierung, Vertraulichkeit, Integrität und Nichtabstreitbarkeit werden auch in SOA Umgebungen einfach realisiert.

Darüber hinaus bietet CORISECIO Gateway-Lösungen zum Schutz von Portalen an. Datenverkehr wird in Echtzeit geprüft und zuschaltbare Filter (bspw. AntiVirus und Web Application Firewall) wehren Gefahren ab, bevor sie Portal oder Applikationen erreichen. CORISECIO Portal Security Komponenten sind SAP zertifiziert und bieten so mit den umfangreichsten Schutz für Portale – powered by SAP NetWeaver.

### ARCHITEKTUR UND LAUFZEITKOMPONENTEN

CORISECIO arbeitet mit einer Architektur, bestehend aus managementRunTime (mRT) als zentrale Administrationskomponente, sowie lokalen Laufzeitkomponenten (secRT), die als Policy Enforcement Point agieren. Die mRT ist die zentrale Administrationsengine und übernimmt in erster Linie Aufgaben der Policy Administration. Die secRT Instanzen setzen die Security Rules auf den Systemen um und bieten über den Security Service Bus die modellierten Security Services an.

### KEY FEATURES

- Zentrale Administration
- Entity- & Key Management
- Bereitstellung eines Security Service Bus
- Sichere Laufzeitumgebung durch automatisierte Prüfung der Komponenten
- Einfache Modellierung von Security Prozessen
- Automatisierte Orchestrierung der Policy
- Integration bestehender Sicherheitslösungen
- Gateway-Lösungen für Security-Anforderungen in Unternehmen

