



**RSA**

The Security Division of EMC

RSA, The Security Division of EMC

## Überblick über das Lösungsportfolio

In zunehmendem Maße werden Informationen, die das wertvollste Gut eines Unternehmens darstellen sollten, zur größten Belastung. RSA führt ein neues Sicherheitskonzept ein, das führende Unternehmen weltweit in die Lage versetzt, diese Herausforderung anzunehmen und mit dem Selbstvertrauen aufzutreten, das nötig ist, um im internationalen Markt erfolgreich bestehen zu können. Wir sind überzeugt, dass Sicherheitssysteme geschäftliche Einschränkungen aufheben und nicht selbst einschränkend sein sollten.

## RSA, The Security Division of EMC

RSA, The Security Division of EMC, ist der führende Anbieter von Sicherheitslösungen zur Beschleunigung von Geschäftsabläufen. Als bevorzugter Sicherheitspartner von mehr als 90 % der Fortune 500-Unternehmen unterstützt RSA den Erfolg der weltweit führenden Unternehmen bei der Lösung komplexer und heikler Herausforderungen in puncto Sicherheit.

RSA, The Security Division of EMC, wurde im September 2006 nach der Übernahme von RSA Security Inc. und Network Intelligence durch die EMC Corporation gegründet. Die Kräfte wurden gebündelt, um der Tatsache Rechnung zu tragen, dass die Kundenanforderungen sich verändert haben und traditionelle Sicherheitskonzepte nicht mehr ausreichen.

Die nachfolgende Lösungsübersicht gibt einen Einblick in das Service- und Produkt-Portfolio von RSA und EMC, das den zunehmend anspruchsvolleren Herausforderungen an die Informationssicherheit Rechnung trägt. Das Portfolio richtet sich an einem Security-Framework aus, das es ermöglicht, die Sicherheitsaspekte in Form eines übergreifenden und ganzheitlichen Prozesses umzusetzen und dauerhaft zu pflegen. Dieser Sicherheitsprozess ist als Information Risk Management bekannt und soll aufzeigen, welche Geschäftsrisiken durch Sicherheitsmängel auftreten und wie entsprechende Sicherheitsmaßnahmen Geschäftsrisiken mindern können.

### Die Methodik des Information Risk Management lässt sich in vier Bereiche unterteilen:

- **Discover & Classify:** Erfassen der Risiken und Ableiten einer entsprechenden Sicherheitsstrategie mit erforderlichen Maßnahmen
- **Secure Data:** Sicherung (Verschlüsselung) sensibler Informationen
- **Secure Access:** Zugriffsschutz und Zugriffs-Management
- **Audit & Report:** Auswerten sicherheitsrelevanter Informationen

Grundprinzip der Information Risk Management-Methodik ist also der Schutz der vertraulichen Information selbst und nicht allein das Vertrauen darauf, dass die kom-

plexe und virtuelle Infrastruktur den Zugang zu allen Informationen insgesamt ausreichend regelt.

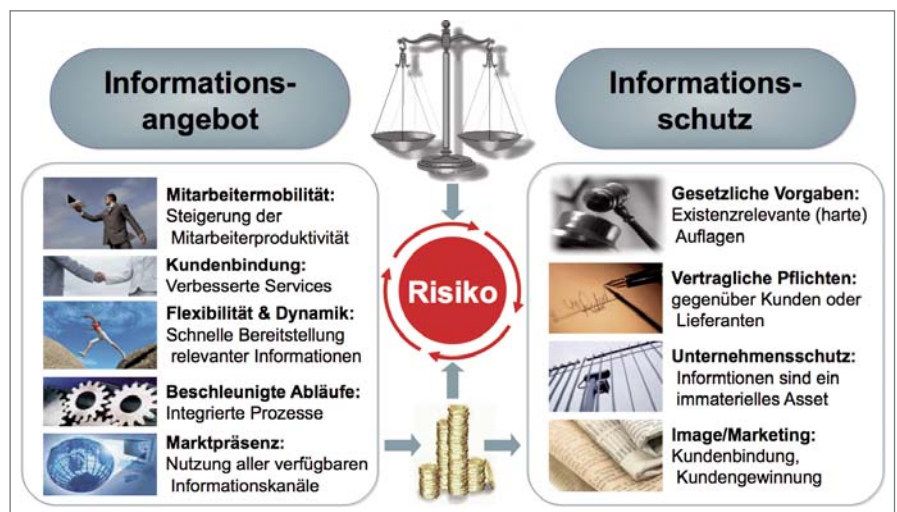
## „Discover and Classify“: Definition von Sicherheitsstrategie und Richtlinie

### RSA® Professional Services

Die Professional Services von RSA können Sie dabei unterstützen, Informationen (Daten) hinsichtlich ihrer Sicherheitsrelevanz für Unternehmen zu bewerten und zuzuordnen. Darauf aufbauend kann das Risiko des Unternehmens im Umgang mit vertraulichen Informationen bestimmt und eine angemessene Sicherheitsstrategie abgeleitet werden. RSA Professional Services helfen also dabei, Sicherheitsrichtlinien zu formulieren, die den Schutzbedarf unterschiedlichster Informationsarten berücksichtigen und zugleich die Wirtschaftlichkeit empfohlener Sicherheitsmaßnahmen sicherstellen.

### RSA® Risk Advisor

RSA Risk Advisor ist ein Tool-gestütztes Serviceangebot zum Erkennen vertraulicher Informationen in der Infrastruktur. Unter Verwendung von vorgefertigten und bei Bedarf kundenspezifisch erstellten „Content-Templates“ wird auf Inhaltebene nach vertraulichen Informationen gesucht und aufgezeigt, wo diese gespeichert und verarbeitet werden. Auf dieser Basis können angemessene Sicherheitsmaßnahmen abgeleitet und umgesetzt werden.



Informationsangebot vs. Informationsschutz

## „Secure Data“: Sicherheit auf Datenebene

### RSA® Data Loss Prevention-Suite

Die RSA DLP-Suite ist eine integrierte Lösung, welche es ermöglicht, vertrauliche Informationen in einer Infrastruktur aufzufinden, um entsprechende Risiken identifizieren und geeignete Maßnahmen einleiten zu können. Entsprechend erarbeitete Sicherheitsrichtlinien können somit auf Inhaltsebene überprüft und umgesetzt werden.

Die RSA DLP-Suite besteht aus folgenden drei Komponenten:

- **RSA® DLP Datacenter:** Findet sensitive Informationen in Datenbanken, in Content Management-Systemen und weiteren Speicherorten von Daten.
- **RSA® DLP Network:** Überwacht den Netzwerkverkehr und spürt vertrauliche Daten auf, die unzureichend geschützt sind und deren Versendung gegen bestehende Sicherheitsrichtlinien verstößt.
- **RSA® DLP Endpoint:** Erkennt kritische Daten auf Desktops und Laptops und überwacht den Umgang mit und die Verarbeitung von diesen Daten.

Die DLP-Komponenten können bei Bedarf in die Verarbeitungsprozesse eingreifen, um so vertrauliche Informationen zu schützen. Die für alle Systeme gültigen Sicherheitsrichtlinien werden über eine zentrale Management-Plattform verwaltet. Die Einhaltung dieser Richtlinien bzw. Richtlinienverstöße werden dann ausgewertet.

<http://www.rsa.com/node.aspx?id=3426>

Content at Rest	Content in Motion	Content in Use
<p><b>Visibility:</b> File Systems Desktops Laptops CMS Databases SAN/NAS Email Archives</p> <p><b>Control:</b> Move to Secure Quarantine Delete Notify</p>	<p><b>Visibility:</b> Email IM/Chat Web HTTP/S FTP</p> <p><b>Control:</b> Allow Audit Quarantine Block Encrypt Notify</p>	<p><b>Visibility:</b> All Document Types</p> <p><b>Control:</b> USB CD/DVD Print Print Screen Open Paste Save Save As Notify</p>
<b>Content</b>	<b>Content Alarm</b>	<b>Content Alarm</b>

RSA Data Loss Prevention Suite

### RSA SecurView für Microsoft SharePoint®

Das einfach anzuwendende Tool RSA SecurView für Microsoft SharePoint ermöglicht eine ganzheitliche Sicht auf die SharePoint-Infrastruktur – von den implementierten Servern bis hin zu den darauf abgelegten Dateien und Dokumenten. Darüber hinaus wird ersichtlich, welche SharePoint- und ActiveDirectory-Gruppen Zugriff auf die SharePoint-Ressourcen haben.

In Kombination mit der RSA DLP-Suite (Datacenter) und Microsoft Rights Management Services (RMS) können ganzheitliche und informationsbezogene Sicherheitskonzepte für die gesamte SharePoint-Umgebung implementiert und genutzt werden. Informationsbezogene Risiken aus der SharePoint-Umgebung werden somit transparent und lassen sich frühzeitig mindern oder ausschließen.

### RSA Encryption Suite

Die RSA Encryption Suite bietet unterschiedliche Lösungsbausteine, um vertrauliche Informationen über Verschlüsselungsmechanismen vor unerlaubtem Zugriff zu schützen.

### RSA BSAFE®

RSA BSAFE ist ein professionelles Toolkit für Applikationsentwickler, das Design, Erstellung und Integration von Verschlüsselungs- und Signatur-Funktionen vereinfacht und schnell ermöglicht.

<http://www.rsa.com/node.aspx?id=1204>

### RSA Key Manager

Hierbei handelt es sich um eine Lösung für die zentrale Verwaltung von symmetrischen und asymmetrischen Encryption Keys. Entwickler können über spezielle APIs aus ihren Anwendungen auf den Key Manager zugreifen. Master-Keys können in einem optionalen HSM zusätzlich gesichert werden. Darüber hinaus bietet der „RSA Key Manager for DataCenter“ bereits vordefinierte Schnittstellen, zum Beispiel für die Verwendung mit Tape- und SAN-Systemen sowie SQL-Datenbanken.

<http://www.rsa.com/node.aspx?id=3013>

### EMC® Documentum® Information Rights Management-Suite

Der EMC Information Right Management Server und die breite Palette an zugehörigen Client-Komponenten bieten eine integrierte Lösung mit dem Ziel einer starken und durchgängigen Sicherheit von Informationen in elektronischer Form. Die Informationen (Dokumente) werden direkt bei der Erstellung durch eine starke Verschlüsselung und dynamische Zugriffskontrolle über den gesamten Lebenszyklus hinweg geschützt. Die IRM-Server-Komponente dient dabei zur Speicherung der erforderlichen Zugriffsschlüssel und der zu den jeweiligen

Dokumenten zugehörigen Sicherheitsrichtlinien. Die Client-Komponenten stellen sicher, dass die gesicherten Dokumente über eine Vielzahl von Anwendungssystemen entsprechend der geltenden Richtlinien geöffnet und bearbeitet werden können. Folgende Client-Komponenten sind u.a. verfügbar:

- IRM Client for Adobe® Acrobat
- IRM Client for E-Mail
- IRM Client for Microsoft® Office
- IRM Client for RIM BlackBerry®

## „Secure Access“: Starke Authentifizierung und Berechtigungs-Management

### RSA Authentication Manager

Der RSA Authentication Manager ist die Management-Komponente der RSA SecurID®-Lösung. Über den RSA Authentication Manager werden Sicherheitsrichtlinien für eine sichere Zwei-Faktor-Authentifizierung durch Verwendung von RSA SecurID-Token verwaltet und Zugriffe auf angebundene Systeme verifiziert. Der RSA Authentication Manager unterstützt dabei eine breite Palette an Netzwerk-, Remote-Access-, VPN-, Internet-, Wireless- und Anwendungssysteme.

<http://www.rsa.com/node.aspx?id=1166>

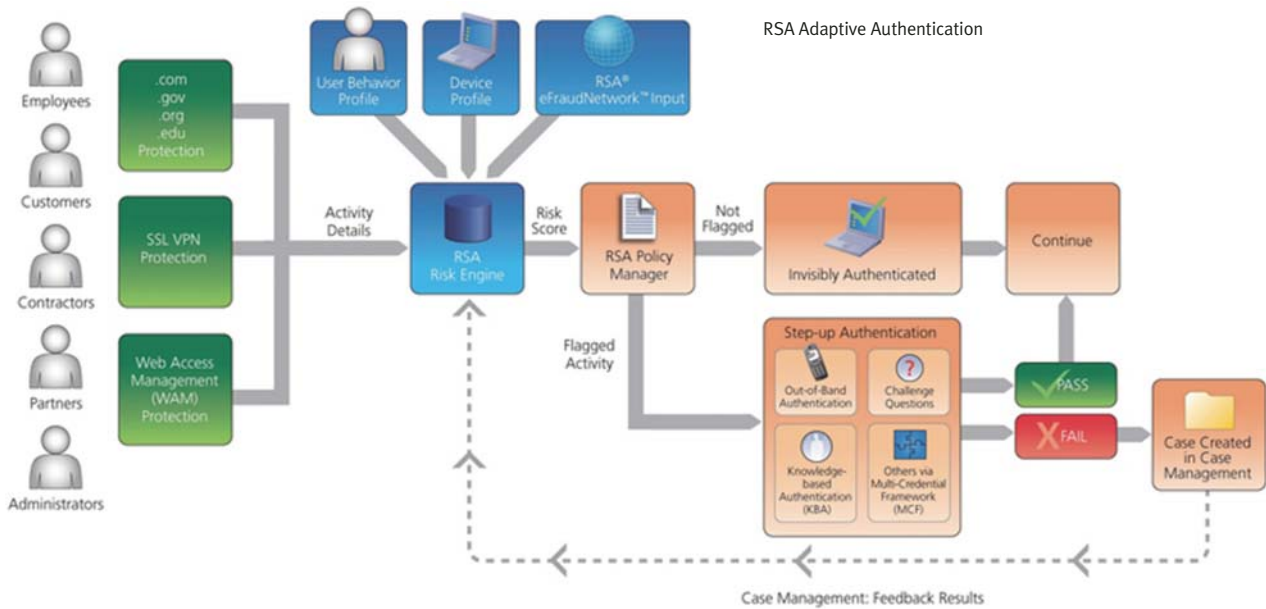
### RSA Credential Manager

Der RSA Credential Manager ermöglicht die Bereitstellung von automatischen, Web-basierten Workflows, damit Unternehmen, RSA SecurID-Hardware- und Software-Token schnell und mit geringem Aufwand bereitstellen können. Über das „Self-Service“-Modul des RSA Credential Manager können Benutzer z.B. eigenständig Token beantragen, aktivieren oder die Ausstattung eines Mitarbeiters mit einem Token genehmigen.

### RSA Adaptive Authentication

Abhängig von der Art der Information, auf die zugegriffen werden soll, bzw. der Transaktion, die getätigt wird, kann flexibel unter Berücksichtigung der entsprechenden Security-Policy entschieden werden, wie sich der Benutzer authentifizieren muss. Diese Lösung wurde speziell für Online-Transaktionen (z.B. Online-Banking) entwickelt, bei denen nicht immer und überall eine starke Authentifizierung gewünscht oder möglich ist. Mit der adaptiven Authentifizierung kann nach flexiblen Regeln, abhängig von individuell definierbaren Parametern und fallabhängig entschieden werden, welche Authentifizierungsmethode erforderlich ist.

<http://www.rsa.com/node.aspx?id=3017>



## RSA-Multi-Faktor-Authentifizierung

### RSA SecurID®

Hierbei handelt es sich um eine „Standardlösung“ für starke Zwei-Faktor-Authentifizierung. Der SecurID-Token generiert einen einmal gültigen Tokencode, der zusammen mit einer geheimen PIN anstelle eines herkömmlichen Passworts eingegeben wird. Die Authentifizierung mit RSA SecurID stellt sicher, dass nur autorisierte Anwender Zugang zu Remote-Access-Servern, E-Mails, WLAN-Netzwerken, Netzwerk-Betriebssystemen, Intra- oder Extranet, Webservern oder anderen Informationen bzw. Anwendungen auf einem UNIX-Server oder im Microsoft® Windows®-Netzwerk erhalten. RSA SecurID-Token sind in unterschiedlichsten Hard- und Softwareausführungen erhältlich. Weitere Infos unter:

<http://www.rsa.com/node.asp?id=1156>



RSA-Authentifizierungskomponenten

### RSA Digital Certificate Solutions

Mit den RSA Digital Certificate Solutions ist RSA in der Lage, seinen Kunden eine komplette Zertifikats-Infrastruktur für Verschlüsselung, digitale Signaturen, Secure E-Mail (inklusive Certificate Authority und Registration Authority), Validierungsinstanz und Key Recovery zur Verfügung zu stellen. Die RSA Professional Services unterstützen Sie hier bei der kompletten Konzeptionierung und Implementierung.

<http://www.rsa.com/node.asp?id=2604>

### RSA Validation Manager

Der RSA Validation Manager bietet eine vollwertige Client-/Server-basierte OCSP-Responder-Funktionalität. So ist die Gültigkeitsprüfung von Zertifikaten dynamisch und über eine Vielzahl von CRLs (Certificate Revocation List) hinweg möglich. Auch bestehende PKI-Infrastrukturen können sinnvoll mit dem RSA Validation Manager ergänzt werden.

### RSA Root Signing Service

Mit dem RSA Root Signing Service können eigenständig aufgesetzte Certificate Authorities (CAs) zertifiziert werden. Über diese Zertifizierung spricht RSA der geprüften CA das Vertrauen aus, die an Browser und andere externe Anwendungen weitergegeben wird. Dadurch können vertrauenswürdige Verbindungen zwischen Server- und Client-Systemen aufgebaut werden, ohne dass eine Benutzerinteraktion erforderlich ist, um die einzelne Verbindung als vertrauenswürdig einzustufen.

### Kontextbezogene Autorisierung

#### RSA Access Manager

Der RSA Access Manager bietet sowohl eine Web-Access-Management- als auch eine Web-SSO-Umgebung, in der Benutzerberechtigungen, Zugriffsregeln und Single-Sign-On für Web-Applikationen zentral verwaltet werden können. Über Partner-Lösungen ist die nahtlose Integration mit Provisioning Tools möglich.

<http://www.rsa.com/node.asp?id=1186>

#### RSA Federated Identity Manager

Über den Federated Identity Manager (FIM) kann die Anmeldung eines Benutzers an einem Portal sowie der Wechsel auf z.B. ein Partnerportal ohne erneute Registrierung bzw. Anmeldung durchgeführt werden. Dabei wird ein Set von zuvor festgelegten Benutzerinformationen an eine vertrauenswürdige Partnersite als SAML-Assertions an einen weiteren FIM oder ein anderes SAML-fähiges Produkt übergeben. Der Benutzer kann durchgängig und transparent alle Informationen in einem Partner-Webverbund nutzen, ohne sich bei jedem einzelnen Partner des Verbunds separat anmelden zu müssen. Trotzdem bleiben die Partner bzw. deren Sites autonom.

<http://www.rsa.com/node.asp?id=1191>

### RSA Proactive Threat Protection & Identity and Activity Verification

#### RSA eFraudNetwork

Das übergreifende Netzwerk führt Informationen zu aktuellen Betrugsaktivitäten zusammen und verteilt diese. Mitglieder des eFraudNetwork sind u.a. 50 der weltweit größten Finanzdienstleister, Kreditkartenunternehmen, regionale Banken und die wichtigsten Internet Service Provider. Das eFraudNetwork liefert wertvolle Informationen für die weiterführenden RSA-Services FraudAction, Transaction Monitoring und Adaptive Authentication.

#### RSA eFraudAction

Mit dem RSA eFraudAction-Service haben Unternehmen die Möglichkeit, sich proaktiv und mit kürzesten Reaktionszeiten vor Online-Betrugsversuchen zu schützen. Im Fall von Phishing-

oder Trojaner-Angriffen können die Mitglieder des Netzwerks über den RSA eFraud-Service bereits frühzeitig gewarnt und geschützt werden. Anschließend werden unmittelbar Gegenmaßnahmen eingeleitet. Die über das eFraud-Netzwerk zusammengeführten Informationen werden dabei durchgängig überwacht und aktualisiert. Das RSA Anti-Fraud Command Center (AFCC) zeichnet seit 2003 für das Erkennen und Abwehren von über 100.000 Phishing-Angriffen verantwortlich und reduzierte dabei beispielsweise die durchschnittliche Lebenszeit von Phishing-Angriffen von 115 auf nur 5 Stunden. Die Erkenntnisse des RSA eFraudAction-Service fließen wiederum in das eFraud-Netzwerk ein.

### RSA Transaction Monitoring

RSA Transaction Monitoring bietet Finanzinstituten eine umfassende Lösung zur Betrugserkennung beim Online-Banking. Das typische Verhalten eines Benutzers wird dabei ebenso berücksichtigt wie dessen Arbeitsumgebung (aktueller Standort, Identifikation des PC, usw.). Transaction Monitoring ermöglicht Unternehmen Folgendes:

- die transparente Überwachung von Online-Transaktionen,
- das Erkennen und Anzeigen von riskanten Aktivitäten und
- das Überprüfen und Unterbinden risikoreicher Aktivitäten.

So werden Betrugsversuche rechtzeitig erkannt und unterbunden oder deren Auswirkungen zumindest minimiert.

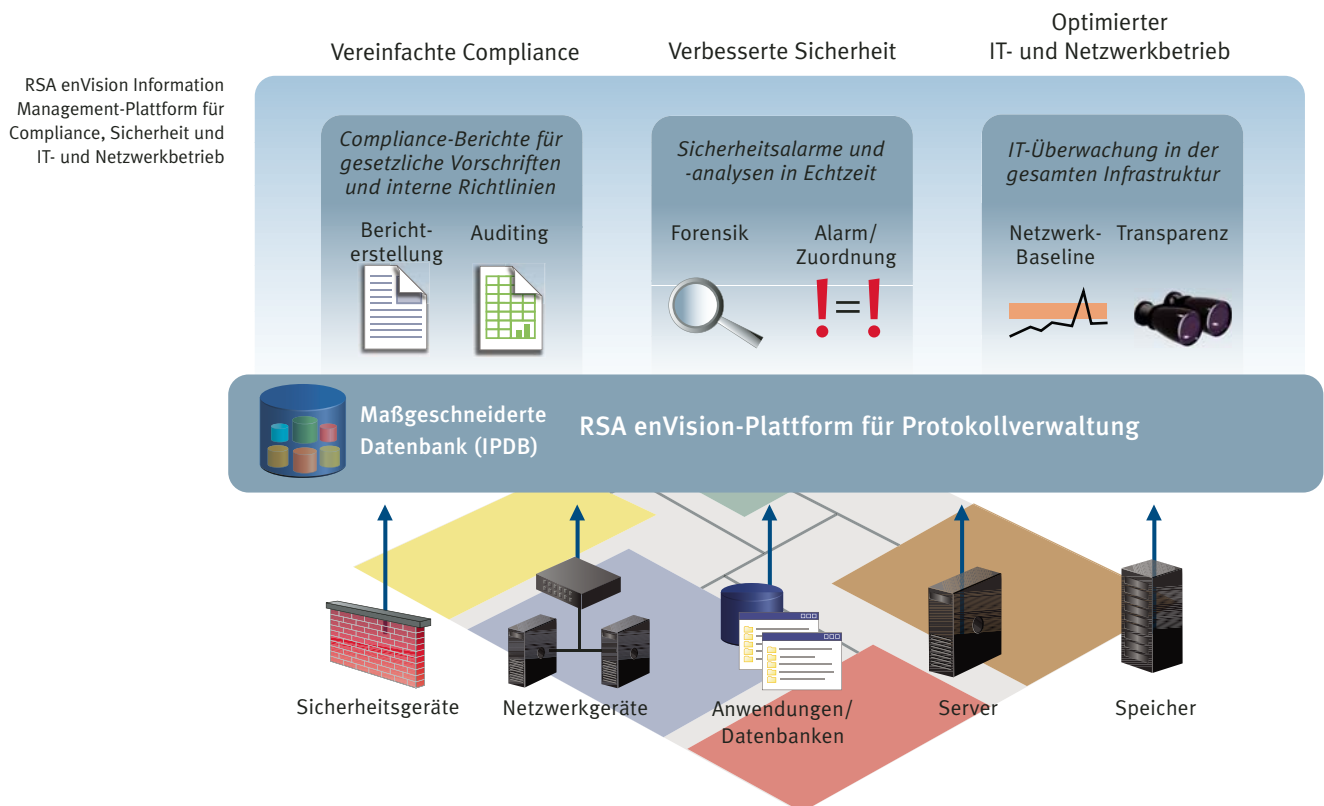
### RSA eCommerce Authentication/3D Secure

RSA eCommerce Authentication/3D Secure ist bereits seit 2001 als Software as a Service-Lösung (SaaS) verfügbar und ermöglicht die sichere Authentifizierung von mehr als 400 Millionen Kreditkarten und den zugehörigen Transaktionen mithilfe des 3D Secure-Verfahrens. RSA eCommerce Authentication/3D Secure ist eine modulare Payment-Sicherheitsplattform, die unterschiedlichste Authentifizierungs- und Kartensicherheitsverfahren umfasst. Das System ist verifiziert durch Visa®, MasterCard SecureCode™ und JCB J/Secure™.

### Security Information & Event Management

#### RSA enVision®

Die zentrale Zusammenführung und Auswertung von sicherheitsrelevanten Informationen ist ein zentraler Baustein, um die Sicherheit von vertraulichen Informationen ganzheitlich und systemübergreifend zu implementieren und insbesondere dauerhaft durch entsprechendes Monitoring und Reporting aufrechtzuhalten. Security Information & Event Management (SIEM) ist eine wichtige Technologie, um diese Anforderung abzudecken. Mit RSA enVision werden hierbei die drei Grundfunktionen Log-Management, Compliance Reporting und Security Operations abgedeckt.



Security-Reporting und forensische Analysen nach kritischen Vorfällen können mit der RSA enVision-Plattform in kurzer Zeit und über alle ausgewerteten Plattformen hinweg durchgeführt werden. Eine Log-Analyse „von Hand“ ist nicht mehr notwendig, und „Silo-Lösungen“ für Berichte können über eine zentrale Datenbasis zusammengeführt werden. Vordefinierte Compliance Report-Vorlagen (z.B. für Basel II, PCI, SAS70, SOX usw.) können schnell und einfach zur Generierung verwendet werden.

<http://www.rsa.com/node.aspx?id=3170>

## IT-Management

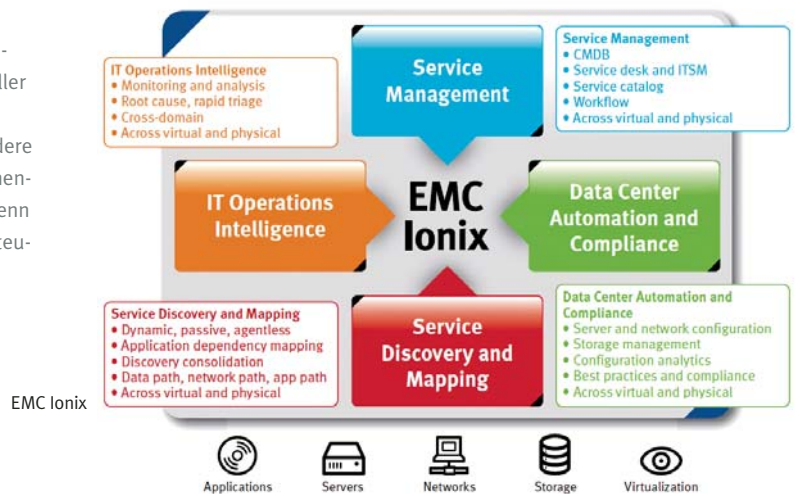
### EMC Ionix

Unter der Bezeichnung EMC Ionix fasst EMC das IT-Management-Portfolio zusammen. Das in den letzten Jahren durch Akquisitionen und organisches Wachstum aufgebaute Portfolio mit Lösungen wie Smarts, NLayers, Voyence, Infra und ControlCenter wird um Lösungen für automatisierte Server-Compliance und -Konfiguration des übernommenen Unternehmens Configuresoft ergänzt und unter dem Label EMC Ionix zusammengeführt.

Mit EMC Ionix sind Unternehmen in der Lage, ein ganzheitliches und effizientes IT-Management klassischer und virtueller Infrastrukturen zu implementieren. Diese umfassen Server, Netzwerke, Speichersysteme und Applikationen. Insbesondere der Einsatz von Virtualisierungstechnologien auf allen Rechenzentrumsebenen stellt ein höheres Sicherheitsrisiko dar, wenn die IT-Infrastruktur nicht durchgängig und ganzheitlich gesteuert und überwacht wird.

Die EMC Ionix-Familie umfasst nachfolgende Systemkomponenten:

- **EMC Ionix for Service Discovery and Mapping:** Bietet einen Überblick über Anwendungen und Server sowie ihre physischen und virtuellen Abhängigkeiten.
- **EMC Ionix for IT Operations Intelligence:** Ermöglicht die automatisierte Analyse von Fehlern sowie deren Ursachen und Auswirkungen in physischen und virtuellen Umgebungen.
- **EMC Ionix for Data Center Automation and Compliance:** Configuration Compliance nach gesetzlichen Vorgaben, Best Practices und internen Governance-Richtlinien für Server, Netzwerke, Speichersysteme und Anwendungen.
- **EMC Ionix for Service Management:** Erlaubt Anwendern den Aufbau eines skalierbaren und kosteneffektiven IT-Infrastructure-Library-Service-Managements (ITIL).





## RSA – Ihr vertrauenswürdiger Partner

RSA, The Security Division of EMC, ist der führende Anbieter von Sicherheitslösungen, um Geschäftsprozesse zu beschleunigen und zu optimieren. RSA unterstützt weltweit operierende Unternehmen bei der Bewältigung ihrer anspruchsvollen und sensiblen Sicherheitsanforderungen. Der Sicherheitsansatz von RSA ist hier fokussiert auf die Informationen, um ihren Schutz und die Vertraulichkeit über die gesamte Lebensdauer zu gewährleisten – unabhängig davon, wohin sie bewegt werden, wem sie zugänglich gemacht werden oder wie sie verwendet werden.

RSA bietet führende Lösungen in den Bereichen Identitätssicherung und Zugriffskontrolle, Kryptographie und Schlüssel-Management, Compliance- und Security-Information-Management sowie Fraud Protection. Diese Lösungen schaffen Vertrauen bei Millionen Nutzern von digitalen Identitäten, bei ihren Transaktionen, die sie täglich ausführen, und bei den Daten, die erzeugt werden. Mehr Informationen erfahren Sie unter [www.RSA.com](http://www.RSA.com) und [www.EMC.com](http://www.EMC.com).

©2009 RSA Security Inc. Alle Rechte vorbehalten.

RSASOL DE 1009



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)