



The Security Division of EMC

RSA Solution Brief

Die RSA® Data Loss Prevention-Suite

Identifizieren Sie Ihre Risiken und übernehmen Sie die Kontrolle.

Übersicht

Die RSA Data Loss Prevention-Suite (DLP) unterstützt Sie dabei, Risiken in Ihrem Unternehmen zu erkennen, die durch den Verlust sensibler Daten entstehen. Mittels einer richtlinienbasierten Fallbehandlung können manuell oder automatisch Aktionen zur Vermeidung des Datenverlusts ergriffen werden. Dabei spielt es keine Rolle, ob die Daten in einem Rechenzentrum liegen, sich im Netzwerkverkehr befinden oder von einem Benutzer an einem Endpunkt verwendet werden. RSA DLP nutzt die einheitliche Richtlinienverwaltung für alle drei Lösungsbestandteile: RSA DLP Datacenter, RSA DLP Network und RSA DLP Endpoint. Das vereinfacht die Implementierung im gesamten Unternehmen und führt zu einem konsistenten Prozess zum Schutz vor dem Verlust Ihrer sensiblen Unternehmensdaten.

Risk Management in Unternehmen verlagert sich

Die Informationslandschaft verändert sich. In den vergangenen Jahren haben sich Aufmerksamkeit und Investitionen vom Schutz des Netzwerks gegen Angriffe von außen immer mehr hin zum Schutz der Systeme innerhalb des Netzwerks und schließlich hin zum Schutz der eigentlichen Daten verlagert. Dieser Paradigmenwechsel beim Schutz sensibler Daten und der Risikominderung in Unternehmen ist durch mehrere Faktoren bedingt:

- Immer mehr Daten gehen innerhalb des Unternehmens verloren.
- Unternehmen speichern zunehmend mehr sensible Daten unterschiedlicher Art.
- Daten werden sowohl intern als auch extern immer öfter gemeinsam verwendet.
- Es gibt neue Märkte für gestohlene Daten.
- Die durch Richtlinien geprägte Umgebung wird größer und zunehmend komplexer.

Der Paradigmenwechsel wird dadurch verstärkt, dass herkömmliche Sicherheitstechnologien, die sich auf Hacker und den Peripherieschutz konzentrierten, zur Minderung interner Risiken längst nicht mehr ausreichen. Ein Umdenken ist erforderlich, um Bedrohungen von innen zu begegnen, die durch kriminelle Absicht oder auch unwissentlich durch fehlerhafte Unternehmens- und Sicherheitsprozesse entstehen können. Im Laufe der Zeit bringen die Risiken des Verlusts sensibler Daten immer höhere Kosten für das Unternehmen mit sich, z.B. durch Fehlerkorrektur, Compliance-Kosten, unzufriedene Kunden und Imageverluste.

Die RSA DLP-Suite auf einen Blick:

- Erkennen und minimieren Sie Ihr Risiko des Verlusts sensibler Daten unternehmensweit mittels Erkennung, Überwachung, Durchsetzung von Richtlinien, Auditing und Berichterstellung
- Identifizieren Sie sensible Daten unmittelbar im Augenblick ihrer Entstehung durch die verteilte Architektur
- Senken Sie Ihre Gesamtkosten dank einer äußerst präzisen Engine zur Datenanalyse und einer effizienten und zentralen Richtlinienverwaltung
- Mindern Sie Ihre Risiken durch deren Klassifizierung nach Art und Schwere im Bezug auf Ihre Geschäftsprozesse

„Die RSA DLP-Suite (früher Tablus) sollte bei allen Unternehmen in der engeren Wahl stehen, bei denen Daten in Bewegung sind, die umfangreiche Datenspeicher einsetzen und die sich nicht über ihren Bestand an sensiblen Daten im Klaren sind. Außerdem erfüllt sie sämtliche Anforderungen an Lösungen zur Erkennung von Daten, die in großen verteilten Umgebungen abgelegt sind.“

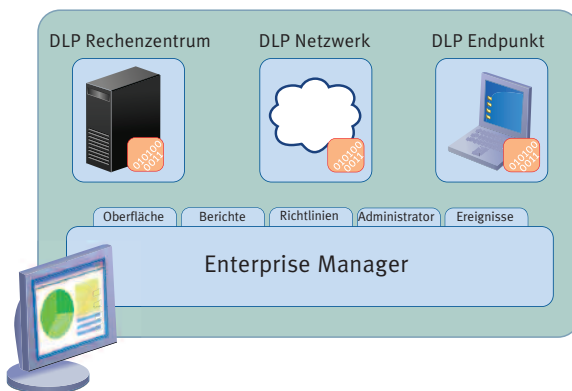
Gartner Magic Quadrant
Content Monitoring and Filtering
and Data Loss Prevention
2Q 07, 13. April 2007

RSA DLP: Ein proaktiver Ansatz zur Entwicklung von Datenschutzrichtlinien

Die RSA DLP Suite bietet einen proaktiven Ansatz zum Management von Geschäftsrisiken durch Datenverluste im Unternehmen. Sie besteht aus drei integrierten Lösungen: RSA DLP Datacenter, RSA DLP Network und RSA DLP Endpoint. Die Produkte sind je nach den Datenschutzanforderungen des Kunden separat oder im Paket erhältlich und werden zentral mittels der Enterprise Manager Konsole verwaltet. Unternehmen werden dabei unterstützt, die bestehenden Risiken aufzuschlüsseln und zu priorisieren und dann eine systematische Korrektur

im Einklang mit bestimmten Datenschutzrichtlinien durchzuführen.

Üblicherweise beginnen Kunden damit, informationsbezogene Sicherheitsrichtlinien zu erstellen und zu entwickeln. Dabei werden sensible Daten mithilfe von RSA DLP direkt an der Quelle durch präzise Such- und Klassifizierungstechniken erkannt. Sind die sensiblen Daten gefunden, lässt sich mithilfe von RSA DLP ein geeigneter Kontrollmechanismus einrichten, der auch die neuen Herausforderungen im Datenschutz (siehe Tabelle) berücksichtigt. Ein ausgereifter Workflow sowie Benachrichtigungs-, Audit- und Berichtsmechanismen arbeiten Hand in Hand, um fehlerhafte Geschäftsprozesse aufzudecken und zu definieren, die oft die Ursache eines Datenmissbrauchs sind.



RSA DLP-Lösungen

Die RSA DLP-Produktpalette ermöglicht Einblick in den Risikostatus und die Trends für sensible Daten in Ihrem Unternehmen auf der Basis von Richtlinien. Es spielt dabei keine Rolle, ob sich die Daten in einem Rechenzentrum, einem Netzwerk oder an Endpunkten befinden.

Herausforderungen im modernen Datenschutz

Das mit dem Verlust sensibler Daten einhergehende Risiko zeigt sich in Bereichen mit und ohne Richtlinien und Vorschriften. Um diese Risikoarten zu minimieren, müssen Unternehmen Lösungen der nächsten Generation einsetzen, z.B. die RSA DLP-Suite. Solche Lösungen konzentrieren sich auf die Sicherung der Daten selbst, egal wo sich diese gerade befinden.

GESCHÄFTS-RISIKO	GRÜNDE FÜR DEN SCHUTZ	RISIKOBEHAFTETE DATEN (BEISPIELE)	FOLGEN DES DATENMISSBRAUCHS
Regulatorisch	Einhaltung der Compliance	Finanzdaten: bestimmte Daten für internationale und US-Richtlinien wie Sarbanes-Oxley (SOX) und Gramm-Leach-Bliley Act (GLBA)	Geldstrafen, geringeres Kundenvertrauen, Kosten für Aufdeckung des Betrugs
		Personenbezogene Daten (PII): Mitarbeiter- und Kundendaten für Richtlinien wie Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) und California SB 1386	
Nicht regulatorisch	Schutz von Geschäftsstrategie und betrieblichen Informationen	Preisgestaltung, Fusionen und Übernahmen (M&A), Vertriebs- und Marketingdaten	Verlust des Wettbewerbsvorteils, unzufriedene Kunden, Umsatzverluste, Schaden des Markenwerts und geringe Arbeitsmoral
	Schutz von geistigem Eigentum	Quellcode, Patente, Entwürfe oder Entwicklungsdokumentationen	

Die Benachrichtigungs- und Durchsetzungsfunktionen von RSA DLP sind so flexibel, dass sie sich problemlos an die besonderen Anforderungen der jeweiligen Geschäftsbereiche, der Compliance-, Rechts- oder der Personalabteilung anpassen lassen.

Kunden, die RSA DLP nutzen, weisen ein wesentlich geringeres Risikoprofil in Bezug auf Datenverlust auf als ihre Mitbewerber, was wiederum zu einer höheren Sicherheit und besseren Zukunftsaussichten für das Unternehmen führt. Die Fähigkeit, gesetzliche Bestimmungen einzuhalten und Einblick in Daten mit geistigem Eigentum sowie strategische und betriebliche Daten zu limitieren, spiegelt sich direkt in höherem Kundenvertrauen, einem stabileren Kundenstamm, möglichst keinen Geldstrafen und einem verbesserten Gesamtschutz für das Unternehmen wider.

Herausragende Vorteile der DLP-Suite

Zentrale Richtlinienverwaltung

Die zentrale Richtlinienverwaltung für sensible Daten im Rechenzentrum, im Netzwerk oder an Endpunkten ermöglicht eine durchgehende Erkennung, Korrektur und Kontrolle auf Basis des Unternehmensrisikos und den jeweiligen Sicherheitsanforderungen.

Leistung und Skalierbarkeit der Spitzenklasse

Eine verteilte Architektur der Spitzenklasse sorgt für ein äußerst schnelles Scannen an Endpunkten und in Rechenzentren, um sensible Daten bereits während der Erstellung erkennen und analysieren zu können.

Höchste Präzision

Die hohe Präzision bei der Erkennung sensibler Daten wird durch ausgereifte Algorithmen für die Datenerkennung und Richtlinienvorlagen möglich, sodass sensible Daten auf der Grundlage einer Inhaltsanalyse und über den Kontext bestimmter Schlagwörter innerhalb der Datei erkannt werden.

Flexibler Ereignis-Workflow, Audit und Berichtserstellung

Ein ausgereifter und flexibler Workflow, Benachrichtigungs-, Audit- und Berichtsmechanismen arbeiten Hand in Hand, um fehlerhafte Geschäftsprozesse aufzudecken und zu definieren, die oft Ursache eines Datenmissbrauchs sind.

RSA® DLP Datacenter

Sensible Daten an der Quelle erkennen und korrigieren

Der Hauptzweck eines Rechenzentrums ist es, die Anwendungen vorzuhalten und zu unterstützen, die von den verschiedenen Anwendergruppen innerhalb eines Unternehmens genutzt werden. Konsequenterweise werden in Rechenzentren große Datenmengen gespeichert. Manche dieser Daten sind vertraulich und verteilen sich üblicherweise auf mehrere Dateisysteme, Datenbanken, E-Mail-Systeme, Content Management-Systeme oder große SAN-/NAS-Umgebungen. Darin liegt oft die Hauptursache eines Datenverlusts, da diese Systeme von unzähligen Anwendern genutzt werden, die auf die Daten zugreifen. Viele dieser Anwender benötigen für ihre Arbeit nicht alle der üblicherweise zugewiesenen Zugriffsrechte. Diese unnötigen Zugriffsmöglichkeiten stellen ein internes Sicherheitsrisiko für das Unternehmen dar. RSA DLP Datacenter spürt sensible Daten mithilfe einer detaillierten Analyse auf und bietet einen Überblick über das Risiko dieser Daten im Rechenzentrum.

Benutzer könnten z.B. versehentlich oder auch absichtlich sensible Daten von einem Dateisystem oder aus einer Datenbank herunterladen und diese Informationen damit nicht autorisierten Anwendern außerhalb des Unternehmens zugänglich machen. Dieser Verlust sensibler Daten stellt ein erhebliches Risiko für das Unternehmen dar. Mit RSA DLP Datacenter lässt sich dieses Risiko bereits an der Quelle eindämmen, indem alle sensiblen Daten im Rechenzentrum schnell und präzise erkannt werden.



RSA DLP Datacenter erkennt sensible Daten an allen Speicherorten im Rechenzentrum.

Datenquelle	Aktion
File Share	Quarantäne
NAS/SAN	Löschen
Datenbankdateien	Benachrichtigen
SharePoint-Standorte	Verschieben an einen sicheren Speicherort
Content Management-Systeme	



RSA DLP Datacenter senkt das Risiko durch Aktionen wie das Verschieben der sensiblen Daten in einen Quarantäne-Ordner, das Löschen nicht benötigter bzw. falsch abgelegter Daten oder das Verschieben auf ein sicheres System.

Anwendungsbereiche

- Erkennen und Priorisieren sensibler Daten und Korrektur im Einklang mit Richtlinien
- Berichterstellung und Audits von sensiblen Daten im Rechenzentrum
- Erkennen und Minimieren der Risiken ungeeigneter oder ungewünschter Zugriffssteuerung für Daten



RSA DLP Network erkennt und überwacht sensible Daten im Netzwerk und ergreift Maßnahmen wie z.B. das Blockieren des Zugriffs.

Unterstützte Übertragungsarten	Maßnahme
E-Mail (SMTP, IMAP usw.)	Erlauben Blockieren
IM/chat	Verschlüsseln
HTTP/S	Benachrichtigen
FTP	
Generisches TCP	

RSA® DLP Network

Überwachung des Netzwerkverkehrs auf sensible Daten und Durchsetzung geeigneter Maßnahmen

Sowohl die interne als auch die externe Zusammenarbeit ist von großer Bedeutung für den Erfolg eines jeden Unternehmens. Angesichts der engen Verflechtung in der modernen Wirtschaft ist ein Informationsfluss in Form von E-Mails, Sofortnachrichten (IM) und anderen Arten der Netzwerkkommunikation unabdingbar. Dieser Datenfluss ist das Lebenselixier der Wirtschaft und für Erfolg und Produktivität eines Unternehmens von enormer Bedeutung. Der rege Informationsaustausch hat jedoch eine Kehrseite: Häufig geraten sensible Daten an Personen, die nicht autorisiert sind, diese Daten zu erhalten. Eine vertrauliche Datei kann z.B. sehr leicht versehentlich, aber auch vorsätzlich als E-Mail-Anhang versendet werden, oder ein Betriebsgeheimnis wird per Sofortnachricht übermittelt.

Des Weiteren können die sensiblen Daten während der Übertragung abgefangen werden, versehentlich an eine falsche Adresse geraten oder sich einfach außerhalb des Rahmens der Compliance-Vorgaben befinden. Jede dieser nicht autorisierten Übertragungsarten kann für ein Unternehmen ein Risiko bedeuten.

RSA DLP Network hilft dabei, diese Risiken zu mindern – durch die schnelle und präzise Erkennung und Analyse von Daten, die das Netzwerk verlassen und über die Durchsetzung von Datenschutzrichtlinien, die im Einklang mit der jeweiligen Geschäftstätigkeit und den damit einhergehenden Sicherheitsbedürfnissen stehen.

RSA DLP Network verhindert den Datenverlust auf zwei Arten. Zum einen durch den passiven Überwachungsmodus, der es Ihnen ermöglicht bestimmte Risiken im Unternehmen besser zu verstehen und fehlerhafte Geschäftsprozesse aufzudecken. In diesem Modus übermittelt RSA DLP Network Benachrichtigungen und Alarme an die zuständigen Personen, um Audits zu unterstützen und Anwender über risikoreiche Transaktionen oder Geschäftspraktiken aufzuklären. Darüber hinaus ist der Betrieb im aktiven Modus möglich, in dem zusätzliche Maßnahmen wie E-Mail-Blockierung oder -Verschlüsselung durchgeführt werden. Unabhängig davon, welche Methode am besten zum Risikoprofil des Unternehmens passt, verringert RSA DLP Network die Wahrscheinlichkeit, dass die Übermittlung sensibler Daten das Unternehmen und das Unternehmensergebnis beeinflussen.

Anwendungsbereiche

- Passive Überwachung sensibler Daten, die das Netzwerk verlassen
- Aktive Blockierung und Korrektur beweglicher Daten auf der Basis von Richtlinien
- Übermittlung von Alarmnachrichten über den Workflow sowie Audits oder Berichterstellung bei Verstößen gegen die Datensicherheit

RSA® DLP Endpoint

Sensible Daten an Endpunkten erkennen und steuern

Endpunkte wie Notebooks oder Desktop-Computer haben die Geschäftswelt revolutioniert. Ein Großteil des Tagesgeschäfts findet an diesen Endpunkten statt. Sie sind für eine erfolgreiche Geschäftstätigkeit unabdingbar und ermöglichen Mitarbeitern eine äußerst mobile und produktive Arbeitsweise. Da viele Mitarbeiter einen Großteil ihrer Arbeitszeit an diesen Endpunkten verbringen, ist es nur logisch, dass Unmengen sensibler Daten auf Desktops und Notebooks abgespeichert werden. Statistiken zeigen, dass über 50 % der Daten in modernen IT-Umgebungen verloren gehen, wenn Daten von diesen Endpunkten auf mobile Geräte übertragen werden.

Sensible Daten gelangen schließlich über einen Datei-Download von einem Dateisystem oder einer Datenbank zum Endpunkt – als Überbleibsel einer archivierten E-Mail-Übertragung oder gar als manueller Dateneintrag, der auf einer Workstation generiert und auf

„Die RSA DLP-Suite (Tablus Content Sentinel) beurteilt die Effizienz Ihres Datenschutzes durch die Erkennung risikofälliger Inhalte auf Notebooks, Desktops und Servern. Sie können Maßnahmen zum Schutz dieser Daten einleiten, bevor sie verschoben werden oder in falsche Hände geraten. Das allein zeigt Auditoren, dass Sie proaktive Sicherheitsmaßnahmen ergreifen. Darüber hinaus senkt der Schutz vertraulicher Daten das Risiko, dass Mitbewerber an diese Daten geraten. Diese Lösung spielt in der Gesamtstrategie eine wichtige Rolle, um gesetzliche Vorgaben und Unternehmensvorschriften einzuhalten.“

Infoworld

Quickly discover sensitive content

26. Juni 2007

Mike Heck

eine Festplatte heruntergeladen wurde. Die einzige Möglichkeit, sensible Daten am Endpunkt zu schützen, ist die schnelle und präzise Erkennung und Analyse der Speicherorte, die Überwachung der Datenbewegung und die Durchführung entsprechender Maßnahmen, z.B. die Blockierung, um die Verwendung durch nicht autorisierte Personen zu verhindern.

RSA DLP Endpoint verfügt über zwei besondere Funktionen, die im Verbund das Risiko des Verlusts sensibler Daten auf Notebooks und Desktops verringern. Zunächst lassen sich auf Basis zentraler Richtlinien mit RSA DLP Endpoint sensible Daten auf Notebooks und Desktops auffinden und analysieren. Darüber hinaus verbessert RSA DLP Endpoint die Sicherheit durch das Blockieren der Übertragung sensibler Daten auf mobile Geräte wie USB-Laufwerke oder CDs/DVDs und durch zusätzliche Kontrollfunktionen für den Druck.

Anwendungsbereiche

- Erkennung, Überwachung und Analyse sensibler Daten an Endpunkten
- Verhinderung und Kontrolle nicht autorisierter Datenübertragung von Firmen-Workstations und richtlinienbasierte Einschränkung der Benutzerrechte
- Richtlinienkonforme Berichterstellung mit Details zu sensiblen Daten bei Notebook-Diebstahl



RSA DLP Endpoint erkennt und überwacht sensible Daten und leitet Maßnahmen an Endpunkten wie Notebooks und Desktops ein.

Endpoint unterstützt regelkonforme Maßnahmen auf Basis des Netzwerkverbindungsstatus.

Unterstützte Endpunkte

Notebooks und Desktops mit Windows 2000 SP4 oder höher (Hinweis: Vista wird noch nicht unterstützt)

Maßnahme: Erlauben oder blockieren

Drucken
Speichern/
Speichern als
Brennen auf CD/DVD
USB-Export

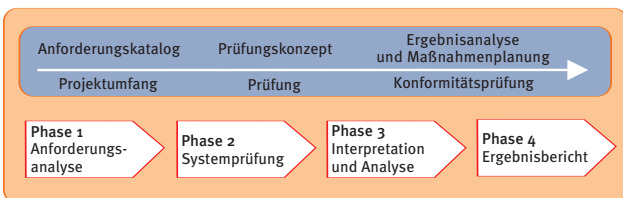
RSA DLP RiskAdvisor-Service

Geschäftsprozesse verbessern und Datenverlust vermeiden

Der RSA DLP RiskAdvisor-Service legt fest, welche Daten als vertraulich anzusehen sind, und bestimmt deren Speicherorte und die Art der Datenablage. Auf dieser Basis können die Geschäftsprozesse für die Verwaltung vertraulicher Informationen optimiert werden, und das Unternehmen kann eine Strategie gegen Datenverlust aufstellen, um potenzielle Risiken zu erkennen und auszuschalten. Dadurch schafft der RSA DLP RiskAdvisor erstklassige Voraussetzungen für eine umfassende Strategie zum Schutz vor Datenverlust. Seit Januar 2005 waren mehr als 150 Millionen Datensätze, die vertrauliche personenbezogene Informationen enthielten, von Datenschutzverletzungen betroffen. Diese Zahlen nannte das PrivacyRightsClearing House, eine gemeinnützige Organisation für Verbraucherinformation und -beratung. Der Verlust vertraulicher, zum Teil regulierter Daten, die oft über das gesamte Unternehmen verteilt sind, kann sich auf den Gewinn auswirken, das Vertrauen der Kunden beeinträchtigen und den Ruf des Unternehmens schädigen. Daher müssen Datenverluste nicht nur aus gesetzlichen, sondern auch aus geschäftlichen Gründen unbedingt vermieden werden.

Überblick

Der RSA DLP RiskAdvisor-Service nutzt die bewährte Technologie der RSA DLP-Suite und umfasst vier Phasen, die je nach Projektumfang unterschiedlich lang ausfallen können.



Machen Sie jetzt den ersten Schritt – mit einer Bestandsaufnahme Ihrer Risiken.

Der Service RSA DLP RiskAdvisor ist eine qualifizierte Dienstleistung, die die RSA DLP-Suite nutzt, um Unternehmen die Umstellung von einem reaktiven auf einen proaktiven Datenschutz zu erleichtern. Durch die Definition sensibler Daten und die Bestimmung der Speicherorte bildet dieser Service die Basis zur Erkennung fehlerhafter Geschäftsprozesse und unterstützt Unternehmen beim Aufbau einer Strategie zur Vermeidung von Datenverlusten. Der Service beinhaltet einen detaillierten Risikobericht mit Empfehlungen zur Verbesserung von Prozessen und einer optimierten Verwaltung richtlinienkonformer und nicht richtlinienkonformer Dateneinsicht.

Der Service RSA DLP RiskAdvisor beinhaltet:

- Bestandsaufnahme sensibler Daten
- Durchsuchen von Desktops und Notebooks
- Scannen von File Shares
- Zusammenfassender Bericht über das aktuelle Risikoprofil sowie Empfehlungen

RSA Data Classification

Zusätzlich zum RiskAdvisor Service bietet RSA Ihnen Unterstützung bei der Klassifizierung Ihrer unternehmenskritischen Daten.

RSA hilft Ihnen, die in Ihrem Unternehmen vorhandenen Daten unter Berücksichtigung Ihrer Geschäftsziele zu klassifizieren und bezüglich Ihres Schutzbedarfs und des vorhandenen Risikopotentials zu bewerten.

Somit wird sichergestellt, dass Investitionen für Sicherheitsmaßnahmen angemessen getätigt und optimale Ergebnisse erzielt werden.

Der Umfang des RiskAdvisor Services ist jederzeit erweiterbar und kann individuell an Ihre Unternehmensanforderungen angepasst werden.

Weitere Informationen erhalten Sie über Ihren RSA Ansprechpartner oder unter www.rsa.com



Über RSA

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. Weitere Informationen finden Sie unter www.rsa.com und www.emc2.de.

©2007 RSA Security Inc. Alle Rechte vorbehalten.

RSA, RSA Security und das RSA Logo sind eingetragene Warenzeichen oder Warenzeichen von RSA Security, Inc. in den Vereinigten Staaten oder anderen Ländern. EMC ist ein eingetragenes Warenzeichen der EMC Corporation. Alle weiteren hier aufgeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.

DLPST SB 1207



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC