



RSA[®]

The Security Division of EMC

RSA Solution Brief

Die RSA-Lösung für VMware View: Sicherheit in der virtuellen Desktop-Umgebung

Nach Angaben der Open Security Foundation sind 28 Prozent aller gemeldeten Datensicherheitsverletzungen auf den Diebstahl von Desktops oder Notebooks zurückzuführen¹. Um dieses Risiko zu senken, stellen viele Unternehmen nun auf gehostete virtuelle Desktop-Umgebungen um. Durch das Verschieben der Daten von Hunderten oder Tausenden einzelner Desktops in das Rechenzentrum können Unternehmen die Risiken senken, die mit der Erstellung, Erfassung und Speicherung von vertraulichen Daten und geistigem Eigentum verbunden sind.

Die virtuelle Desktop-Infrastruktur von VMware View im Überblick

Mit VMware View kann die IT-Abteilung virtuelle Desktops im Rechenzentrum betreiben und gleichzeitig den Endanwendern eine einheitliche Ansicht bereitstellen, die ihre jeweiligen Anwendungen und Daten in einer vertrauten, personalisierten Umgebung enthält – auf verschiedenen Geräten und an jedem Standort. VMware View nutzt Virtualisierung, um die enge Verknüpfung zwischen Desktop-Hardware, Betriebssystem und Anwendungen zu lösen und eröffnet Unternehmen folgende Vorteile:

- **Höhere Sicherheit.** VMware View minimiert die Sicherheitsrisiken, die mit dem Verlust oder Diebstahl von Geräten verbunden sind, da alle Daten innerhalb der Firewall des Unternehmens bleiben.
- **Niedrigere Kosten.** Unternehmen können die Verwaltungs- und Wartungskosten für einzelne Desktops und Anwendungen um bis zu 50 Prozent senken².
- **Bessere Verwaltung und Steuerung.** Die IT-Abteilung kann alle Desktops zentral im Rechenzentrum verwalten und Desktops für neue Benutzer, Abteilungen oder Zweigstellen sofort bereitstellen.
- **Business Continuity und Disaster Recovery.** Bei Ausfällen kann die Sicherung und Wiederherstellung von Desktops automatisiert und schnell auf einen anderen Server oder in ein anderes Rechenzentrum verlagert werden, um die Auswirkungen auf den Geschäftsbetrieb zu minimieren.

Sicherheitsprobleme bei virtuellen Desktop-Umgebungen

Die gehostete virtuelle Desktop-Umgebung von VMware View ist eine wertvolle strategische Investition, die Unternehmen zahlreiche Vorteile eröffnet, darunter eine erhöhte Sicherheit. Doch diese Investition erfordert eine gewisse Verwaltung und Absicherung. Wenn Anwender beispielsweise vertrauliche Daten auf einem virtuellen Desktop aufrufen und bearbeiten, sind diese Daten weiterhin gefährdet. Ohne geeignete Zugriffs- und Datensteuerung besteht die Möglichkeit, dass vertrauliche Unternehmensdaten für Anwender ohne entsprechende Berechtigungen zugänglich werden.

Die Risiken, denen Daten in einer virtuellen Desktop-Umgebung ausgesetzt sind, müssen genauso sorgfältig wie alle anderen Datenrisiken in der gesamten IT-Infrastruktur verwaltet werden. Unternehmen, die VMware View nutzen, stehen also weiterhin vor Herausforderungen hinsichtlich der Sicherheit und müssen geeignete Kontrollmechanismen einführen, um die folgenden Sicherheitsziele zu erreichen:

- **Anwenderauthentifizierung.** Wie können Anwender beim Zugriff auf virtuelle Desktops authentifiziert werden?
- **Datensteuerung.** Wie lässt sich sicherstellen, dass Anwender mit vertraulichen Daten während einer virtuellen Desktop-Sitzung richtig umgehen?
- **Überwachung und Berichterstattung.** Wie können Auffälligkeiten und Schwachstellen erkannt werden, z. B. in Übersichten über den ein- und ausgehenden Datenverkehr, der mit vertraulichen Ressourcen in der gehosteten virtuellen Desktop-Umgebung verbunden ist?
- **Sicherheitskonfiguration und Schwachstellenverwaltung.** Wie lässt sich eine sichere Konfiguration des virtuellen Endpunkts gewährleisten, um Schwachstellen bei Hunderten oder Tausenden von Desktops schnell zu erkennen und zu beseitigen?

¹ Open Security Foundation, Data Loss DB

² IDC-Whitepaper (gesponsert von VMware)

Quantifying the Business Benefits of VMware View, September 2009



Die RSA-Lösung für VMware View

RSA und EMC haben eine Sicherheitslösung entwickelt, mit der Unternehmen die Vorteile von gehosteten virtuellen Desktops nutzen und gleichzeitig die üblichen Sicherheitsprobleme lösen können, die beim Anwenderzugriff auf Daten in einer Desktop-Umgebung entstehen.

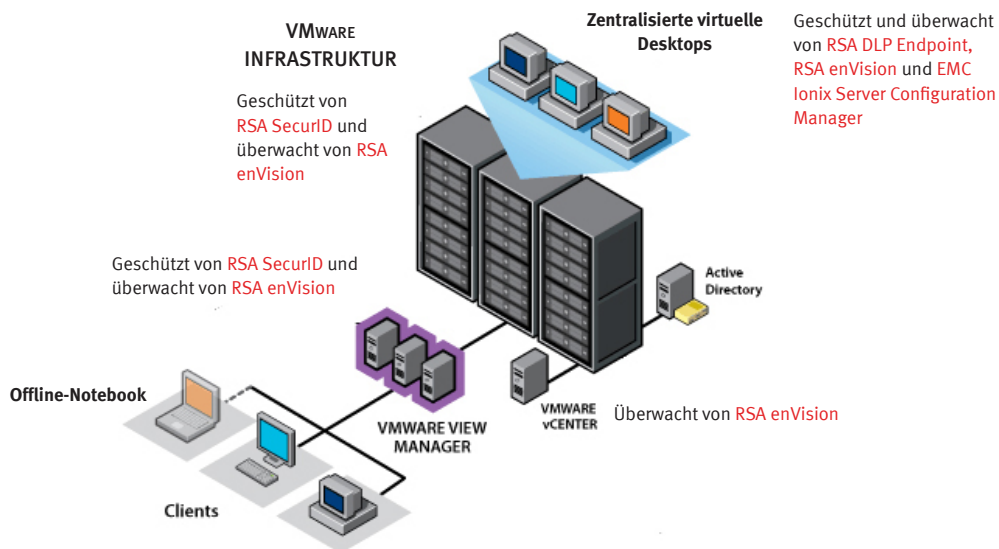
Anwenderauthentifizierung

Die Identität von Anwendern muss immer überprüft werden, bevor Zugriff auf Informationen und Anwendungen gewährt wird. Dies gilt insbesondere für eine gehostete virtuelle Desktop-Umgebung, in der Anwender jederzeit Zugriff von beliebigen Standorten aus benötigen und dabei häufig Geräte nutzen, die das Unternehmen nur bedingt unter Kontrolle hat. Die Überprüfung der Anwenderidentität vor der Zugriffsgewährung auf einen virtuellen Desktop stellt ein wichtiges Sicherheitsziel dar, vor allem bei Anwendern mit Administratorrechten.

Die Zwei-Faktor-Authentifizierung sorgt für eine zusätzliche Sicherheitsebene, damit nur die richtigen Anwender auf die richtige virtuelle Sitzung und auf vertraulichen Inhalt in der virtuellen Desktop-Umgebung zugreifen können. Unternehmen können das Risiko unbefugter Datenaufrufe während der virtuellen Sitzung senken, wenn Mitarbeiter und Dritte eine starke Authentifizierungstechnologie einsetzen müssen, durch die nur autorisierte Anwender über ihr Desktop-Image auf vertrauliche Informationen zugreifen dürfen.

Die Zwei-Faktor-Authentifizierung von RSA SecurID® generiert alle 60 Sekunden einen neuen, einmalig gültigen Passwortcode, sodass nur der echte Anwender den richtigen Token-Code zu einem bestimmten Zeitpunkt eingeben kann. Für den Zugriff auf ihren virtuellen Desktop kombinieren die Anwender einfach ihre geheime PIN mit dem Token-Code, der zu einem bestimmten Zeitpunkt auf der SecurID-Authentifizierungskomponente angezeigt wird. Diese Methode liefert ein eindeutiges, einmalig gültiges Passwort für die zuverlässige Überprüfung der Anwenderidentität.

DIE RSA-LÖSUNG FÜR VMWARE VIEW



RSA SecurID-Authentifizierung lässt sich derzeit auf zwei Arten mit VMware View integrieren:

- Sicherstellen, dass nur vertrauenswürdige Identitäten auf virtuelle Desktop-Sitzungen zugreifen
- Durchsetzung der Anwenderauthentifizierung für Administratorzugriff auf die Backend-VMware ESX-Plattform. Mit der RSA SecurID-Authentifizierung kann eine starke Zwei-Faktor-Authentifizierung für die ESX-Servicekonsole konfiguriert werden.

Die RSA SecurID-Authentifizierungskomponenten sind in verschiedenen Formfaktoren erhältlich, darunter Hardware, Software und On-Demand (SMS), um die Bedürfnisse verschiedener Anwendergruppen abzudecken.

Datensteuerung

RSA® Data Loss Prevention (DLP) Endpoint überwacht und steuert die Verwendung vertraulicher Daten an Endpunkten wie z. B. Notebooks, Desktops oder mobilen Geräten.

RSA DLP Endpoint bietet zwei Module – Discover und Enforce. Das Discover-Modul erkennt vertrauliche Informationen, indem der Inhalt der Dateien auf der virtuellen Festplatte analysiert wird. Das Enforce-Modul überwacht die Anwenderaktionen für klassifizierte vertrauliche Daten, darunter Drucken, Speichern, Kopieren oder Senden per Web-E-Mail. Unternehmen können Richtlinien für den Umgang mit vertraulichen Daten und für deren Nutzung während einer virtuellen Sitzung aufstellen. RSA DLP Endpoint setzt diese Richtlinien durch und greift ein, wenn Anwenderaktionen dagegen verstoßen, z. B. durch Alarmer, Blockierungen oder andere Dateisteuerungsmechanismen. RSA DLP Endpoint verfügt über einen einzigen Agent und eine einheitliche Richtlinienverwaltungsarchitektur und lässt sich daher leicht implementieren und verwalten, unabhängig vom geografischen Standort der Workstation. Administratoren

können von einem zentralen Standort aus Richtlinien und Kontrollmechanismen für alle Workstations in der virtuellen Umgebung konfigurieren und durchsetzen. VMware View vereinfacht die Implementierung von RSA DLP Endpoint-Agents erheblich, da der Agent in das Master-Image integriert und anschließend schnell auf alle virtuellen Desktops verteilt werden kann.

Mit RSA DLP Endpoint werden vollständig konfigurierbare Agents permanent auf dem Endpunkt implementiert, um künftige Überprüfungen durchzuführen. Durch die verteilte Agent-Technologie kann das Enforce-Modul die Endpunkte aktiv überwachen und Richtlinien durchsetzen, selbst wenn das Gerät nicht mit dem Netzwerk verbunden ist.

Außerdem ermöglicht das Enforce-Modul eine detaillierte Steuerung am Point of Use (virtuelle Sitzung und physische Hardware), um bei Richtlinienverstößen dafür zu sorgen, dass nur die jeweilige Aktivität und nicht der gesamte Zugriff blockiert wird. Neben der Blockierung können weitere Richtlinienaktionen definiert werden, entweder um den Anwender über den Verstoß gegen eine Unternehmensrichtlinie zu informieren oder um vom Anwender eine Begründung für die Aktion anzufordern. Diese Begründungen werden zur späteren Überprüfung protokolliert.

Werden vertrauliche Daten erkannt oder Anwenderaktionen blockiert, leitet RSA DLP Endpoint einen Workflow zur Vorfallverfolgung ein, um die gefährdeten Daten zu protokollieren und zu überwachen. Die Lösung erfasst alle Vorfälle in einem Audit-Trail und bietet integrierte Workflows für Benachrichtigungen und Alarmer, die auf der Microsoft® Active Directory-Hierarchie beruhen, um die Dateneigentümer einzeln oder gruppenweise über potenzielle Verstöße zu informieren. Außerdem wird eine Option für die eigenständige Klärung von Vorfällen direkt durch den Anwender bereitgestellt.

Sorgfältige Aufgabentrennung und Rechteverwaltung spielen eine wichtige Rolle, um böswillige oder unbeabsichtigte Administratorzugriffe ohne entsprechende Berechtigungen zu verhindern.



Überwachung und Berichterstellung

Aufgrund der raschen Ausbreitung virtualisierter Infrastrukturen müssen Unternehmen dringend neue Aktivitäten überwachen, darunter der Anwenderzugriff auf virtuelle Desktops über eine Vielzahl von Geräten, administrative Vorgänge wie z. B. zentrales Erstellen, Ändern und Löschen von Desktop-Images und der Zugriff auf vertrauliche Daten über virtuelle Desktops. Darüber hinaus müssen Unternehmen, die ihre IT-Infrastruktur zunehmend virtualisieren, die Konformität, Betriebsanforderungen und allgemeine Sicherheit ihrer Systeme bewerten.

Bei der RSA enVision®-Plattform handelt es sich um eine Lösung zur Verwaltung von Sicherheitsinformationen und –ereignissen (SIEM), die eine skalierbare und verteilte Architektur bietet und das Erfassen, Speichern, Verwalten und Korrelieren der Ereignisprotokolle ermöglicht, die vom VMware View Manager, der Backend-VMware-Infrastruktur und den RSA SecurID- und RSA DLP Endpoint-Lösungen generiert werden. RSA enVision meldet wichtige betriebliche und administrative Ereignisse, die mit VMware View und den Übersichten über den ein- und ausgehenden Datenverkehr für vertrauliche Ressourcen verbunden sind. Durch diese effektive Lösung können Sicherheitsvorfälle in der von VMware gehosteten virtuellen Desktop-Umgebung mit Prioritäten versehen werden.

Mit der RSA enVision-Plattform können Unternehmen die Ereignisprotokolle auf einheitliche und zentralisierte Weise analysieren und dabei alle physischen und virtuellen Systeme der IT-Infrastruktur einbeziehen. Die RSA enVision-Technologie eröffnet Unternehmen mit einer virtuellen Umgebung diverse Vorteile:

- Richtlinien für Informationssicherheit überwachen, die für Folgendes gelten: Nutzung virtueller Maschinen, Cluster- und Ressourcenverwaltung, virtuelle Netzwerkinfrastruktur, Speicherung, Anwender, Gruppen und Berechtigungen zur Einhaltung der unternehmensweite Compliance, Anwenderaktivitäten auf virtuellen Desktops (z. B. Anwenderauthentifizierung für Zugriff auf virtuelle Sitzungen) und Administratoraktivitäten in der virtuellen Desktop-Umgebung (z. B. Erstellen von Berechtigungen für virtuelle Desktops, Ändern von Profileinstellungen)
- Daten auf sichere, ungefilterte und nicht reduzierte Weise erfassen, schützen und speichern
- Baselines für Aktivitäten in der gesamten virtuellen Umgebung festlegen, um „normale“ Aktivitäten zu definieren und ungewöhnliche Aktivitäten zu erkennen

Mit RSA enVision-Technologie können Unternehmen die Ereignisprotokolle auf einheitliche und zentralisierte Weise analysieren und dabei alle physischen und virtuellen Systeme der IT-Infrastruktur einbeziehen.

- Alarme ausgeben, wenn Abweichungen von Baselines auftreten oder schädliche Aktivitätsmuster über mehrere verteilte Geräte erkannt werden
- Forensische Analysen durchführen, um Richtlinien und Systemeinstellungen zu optimieren, und alle Änderungen sowie ihre Auswirkungen in der Umgebung auf Debug-Ebene anzeigen
- Einen vollständigen Workflow für die Vorfallsverwaltung erstellen, damit Vorfälle aufgezeichnet, eskaliert und zeitnah behoben werden
- Datenverkehr und Ereignisse in der virtuellen Umgebung aus verschiedenen Perspektiven anzeigen, z. B. nach Standort, Anwender, System, Geschäftsbereich, Abteilung usw.
- Den Audit- und Berichtsprozess durch über 1.400 vordefinierte Berichte optimieren, die sich leicht an interne und externe Compliance-Anforderungen anpassen lassen

Die RSA enVision-Plattform kann auch über die Grenzen der virtuellen Desktop-Umgebung hinaus genutzt werden, um das System lokal oder aus der Ferne zu überwachen und die Konformität, Sicherheit und Betriebsanforderungen der verbundenen Systeme zu beurteilen.

Sicherheitskonfiguration und Schwachstellenverwaltung

Die häufigste Ursache vieler Sicherheits- und Compliance-Vorfälle im IT-Bereich sind durchgeführte Änderungen ohne sorgfältige Vorplanung. Das Zentralisieren von Endpunkten als virtuelle Maschinen im Rechenzentrum vereinfacht zwar die Prozesse für Systemhärtung, Virenschutzaktualisierung und Patching, doch Unternehmen müssen fortan sicherstellen, dass diese Prozesse ordnungsgemäß funktionieren und die Konfigurationen keine Sicherheitsrisiken verursachen. In vielen Unternehmen wird die Änderungsverwaltung für Endpunkte zu einem echten Problem, und sie benötigen ein Tool, das die Erkennung von nicht richtlinienkonformen Konfigurationsänderungen automatisiert, um Sicherheitsrisiken zu reduzieren.

EMC Ionix Server Configuration Manager (SCM) prüft und analysiert detaillierte Konfigurationsprobleme auf Servern und Workstations in physischen und virtuellen Umgebungen und ermöglicht die Behebung dieser Probleme. EMC Ionix SCM überwacht virtuelle Desktops und generiert automatisch Alarme, wenn Systeme angepasst werden müssen, um Probleme zu beheben oder für Compliance zu sorgen. Außerdem automatisiert die Lösung gängige Aufgaben, um die betriebliche Effizienz zu steigern, Kosten zu sparen und sichere, konforme, aktuelle Konfigurationen zu gewährleisten.

Des Weiteren liefert EMC Ionix Server Configuration Manager einen genauen Einblick in die IT-Infrastruktur. Umfassende Übersichten liefern die notwendigen Informationen, um Änderungs-, Konfigurations- und Patch-Verwaltungsprozesse effektiver zu gestalten, z. B. indem die Patch-Bereitstellung überprüft wird und Sicherheitsbedrohungen durch falsche Konfigurationen erkannt und behoben werden. Darüber hinaus können Unternehmen auch Details zu Änderungen in der virtuellen Umgebung anzeigen und die Auswirkungen dieser Änderungen auf Service Level und Compliance verfolgen.

Das EMC Ionix Center for Policy and Compliance bietet detaillierte Inhalte für Sicherheits- und Compliance-Analysen, die auf bewährten Branchenverfahren und gesetzlichen Auflagen beruhen. Die Inhalte des Centers gewährleisten zusammen mit Ionix SCM, dass sowohl physische als auch virtuelle Systeme den Sicherheitsstandards des Unternehmens entsprechen.

Die häufigste Ursache vieler Sicherheits- und Compliance-Vorfälle im IT-Bereich sind Änderungen ohne sorgfältige Vorplanung.

Die RSA-Lösung für Sicherheit in VMware View-Umgebungen

Die RSA-Lösung für VMware View ermöglicht Unternehmen Folgendes:

- Vertrauliche Daten auf Endpunkten wie z. B. Desktops und Notebooks erkennen und analysieren
- Höchste Präzision und Geschwindigkeit bei der Erkennung vertraulicher Daten erzielen
- Die Verwendung vertraulicher Daten am Endpunkt verwalten, indem Aktionen wie z. B. Drucken, Speichern, Kopieren oder Senden per Web-E-Mail überwacht und gesteuert werden
- Sicheren Anwenderzugriff auf vertrauliche Daten bereitstellen, jederzeit und überall
- Die Erfassung, Korrektur und Verwaltung von Konfigurationsänderungen vereinfachen und automatisieren, um die Einhaltung der Compliance zu gewährleisten
- Eine einheitliche, konsistente Sicherheitsrichtlinie einführen, die sich auf andere virtuelle und physische Infrastrukturressourcen erweitern lässt
- Den Sicherheitszustand der virtualisierten Infrastruktur erkennen und Konzepte entwickeln, um Richtlinien oder Compliance-Vorgaben einzuhalten



Risikomanagement in einer virtualisierten Umgebung

VMware View löst viele Probleme, mit denen Unternehmen beim Risikomanagement konfrontiert werden, führt aber zu einem neuen technologiebedingten Risikopotenzial. RSA hat zusammen mit EMC Consulting herausragende Lösungen entwickelt, um Risiken in der gesamten virtualisierten Infrastruktur eines Unternehmens zu erkennen, von Desktops über Netzwerke und Server bis hin zum Speicher.

Die EMC-Sicherheitsbewertung für virtuelle Umgebungen verdeutlicht Unternehmen den Sicherheitszustand ihrer virtuellen Infrastruktur und entwickelt ausgereifte Konzepte, mit deren Hilfe Compliance-Vorgaben und Richtlinien eingehalten werden können, ohne den Mehrwert der Virtualisierungstechnologie zu beeinträchtigen. Die Sicherheitsbewertung kombiniert das Know-how von RSA mit bewährten Branchenverfahren und -standards und konzentriert sich auf die Nutzung von Virtualisierungstechnologie in der IT-Umgebung, um Sicherheitsrisiken und Korrekturmaßnahmen zu bestimmen, ohne den Geschäftswert der Virtualisierung zu schmälern.

Außerdem veranschaulicht der Service dem Unternehmen die geeignete Sicherheitsstufe für bestimmte betriebliche Anforderungen und empfiehlt die optimale Kombination von Richtlinien, Verwaltung und technologischen Verbesserungen, um eine umfassende Sicherheitsstrategie für die Virtualisierung festzulegen.

RSA SecurBook™ für VMware View

RSA bietet zahlreiche Funktionen, die Unternehmen benötigen, um Risiken zu senken und die einzigartige Virtualisierungsdynamik für höhere Sicherheit zu nutzen. RSA unterstützt die Ausbreitung der Virtualisierungstechnologie und verbessert laufend seine Produkte und Services, um die Integrität virtueller Umgebungen zu gewährleisten.

RSA hilft Unternehmen, die VMware View implementiert haben, beim Erkennen und Verwalten ihrer Informationsrisiken. Durch RSA-Sicherheitsmaßnahmen in virtuellen Sitzungen, an Endpunkten (z. B. Desktops, Notebooks) und in anderen Datenbeständen sind Unternehmen besser für neue Sicherheitsbedrohungen und Compliance-Auflagen gerüstet.

Das „RSA SecurBook für VMware View“ ist eine leicht verständliche Lösungsanleitung, die die Ursachen von Sicherheitsproblemen in der gehosteten virtuellen Desktop-Umgebung verdeutlicht und Tipps für die Einrichtung flexibler Steuerungsmechanismen gibt. So wird eine dynamische und dauerhafte Sicherheit für gehostete virtuelle Desktops gewährleistet, die auch bei wachsenden Implementierungen erhalten bleibt. Außerdem sorgt die RSA SecurBook-Anleitung für kürzere Implementierungszeiten im Unternehmen und für niedrigere Total Cost of Ownership.

Das SecurBook enthält Anleitungen für die folgenden Bereiche:

- Lösungsarchitektur für die Sicherheit von VMware View
- Anleitungen für die Implementierung und Konfiguration der Lösung
- Hinweise zum effektiven Einsatz der Lösung
- Anleitung zur Fehlerbehebung

Sie erhalten das RSA SecurBook für VMware View kostenlos unter www.rsa.com oder schreiben Sie eine E-Mail an: euro.info@rsa.com

Zusammenfassung

Sicherheit soll die Geschäftsinitiativen von Unternehmen nicht behindern, sondern fördern. Wenn Unternehmen eine geeignete Zugriffs- und Datensteuerung einrichten, zahlt sich ihre Investition in VMware View voll und ganz aus, denn sie können alle Möglichkeiten einer virtuellen Umgebung nutzen und die Compliance-Anforderungen effektiv verwalten.

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.

Mehr Informationen erfahren Sie unter www.RSA.com und www.EMC.com.

©2009 RSA Security Inc. Alle Rechte vorbehalten.
RSA, RSA Security, SecurID, enVision und das RSA Logo sind Warenzeichen oder eingetragene Warenzeichen von RSA Security Inc. in den Vereinigten Staaten und anderen Ländern. EMC und Ionix sind eingetragene Warenzeichen der EMC Corporation. VMware ist ein eingetragenes Warenzeichen von VMware, Inc. Alle weiteren angeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.

HVD SB 1009



The Security Division of EMC

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