RSA SecurID® Appliance

SALES GUIDE

RSA SecurWorld™ Partner Program

Legend

	Business Drivers
	Identifying Customers
	Discovery Questions
	Positioning Statements
	Presentation of Solution
	Objection Handling
	How to Quote

Other guides in this series include:
Building Success with the RSA SecurWorld™ Partner Program, the RSA Security® Value Proposition,
the RSA SecurID® Authentication Sales Guide, the RSA SecurID for Microsoft® Windows®, VPNs,
Wireless and Citrix® Sales Guides, the RSA SecurID Competitive Sales Strategies
and the RSA® Sign-On Manager Sales Guide.

RSA SECURID® APPLIANCE SALES GUIDE

Contents

This RSA SecurID Appliance Sales Guide, part of The Essential Guide series, delivers practical, real-world information about this solution. This guide helps you identify customer requirements, present the RSA SecurID Appliance solution effectively and run a successful sales campaign.

The resources in these pages provide sales personnel with current information on RSA SecurID. The topics progress through a typical sales cycle, including a product overview, market drivers, product positioning, discovery questions, objection handling, price quoting and common questions. This guide can help you develop new sales opportunities and generate greater revenues.

You may also wish to refer to the RSA SecurID Authentication Sales Guide for background on two-factor authentication and the RSA SecurID solution.

The RSA SecurID® Appliance makes strong authentication easier than ever, giving a quick path to improving network security. This reliable and proven approach, based on the RSA SecurID system, features the world's leading two-factor user authentication solution. This system is used by thousands of organizations worldwide to protect networked resources.

Used in combination with RSA SecurID authenticators, the RSA SecurID Appliance validates the identities of users by means of two unique factors—something they know (a PIN) and something they have (a token code that is automatically generated). Following authentication, users can gain access to network resources—whether they are connecting to the network locally or remotely.

An RSA SecurID Appliance solution consists of:

> RSA SecurID Appliance with an embedded, dedicated version of Microsoft® Windows® Server 2003 and the RSA® Authentication Manager Base Edition software

> RSA SecurID SID700 tokens

> RSA Authentication Manager Base Edition software license

> RSA SecurCare® maintenance for one year, including software and hardware replacement

Millions of people worldwide use RSA SecurID authenticators to securely access virtual private networks (VPNs), web servers, wireless LANs, network operating systems, routers, firewalls and more. RSA SecurID solutions work effectively in all these areas, but—for maximum success—sales presentations should be crafted to address the challenges faced by the target audience. This sales guide can help you identify customer requirements and explain to customers how the solution can help them achieve their business objectives.

Benefits to the Reseller

The design and packaging of the RSA SecurID Appliance make it particularly attractive to resellers, offering these benefits:

> **Shortens sales cycles and lowers the cost of sales.** The RSA SecurID Appliance is exceptionally easy to demonstrate to customers and to deploy for on-site evaluations. The product design eliminates the need to locate a dedicated server platform, install the software, configure the hardware, harden the operating system and perform other set-up tasks. This can often shorten sales cycles to days rather than weeks.

> **Creates opportunities for broader security solutions and sales.** Many Given that most small- to mid-sized businesses (SMBs) have restricted budgets for security investments, while larger enterprises are looking to reduces security management costs. The RSA SecurID Appliance gives these companies a mechanism for instituting the strong authentication portion of a security solution for a lower acquisition cost. This unlocks opportunities for additional company-wide sales and movement toward broader security implementations.

Advantages of an RSA SecurID Two-Factor Authentication Solution

> Ensures the positive identification of users before they gain access to valuable resources

> Makes the solution extremely difficult to hack because it requires two forms of identification—something the user has and something the user knows

> Ensures greater network security than the traditional and easily hacked static password

> Helps to create a trusted e-business environment with new possibilities for innovation and growth

Advantages of the RSA SecurID Appliance

> Provides an easy entry path for organizations seeking a strong authentication security solution

> Features a streamlined installation process that takes as little as fifteen minutes to complete

> Lowers the total cost of ownership (TCO) through an intelligent, low-maintenance design and simple operational requirements

> Delivers industry-leading security (the proven capabilities of RSA SecurID two-factor authentication) in a convenient package

> Simplifies compliance with government regulations mandating accountability and data privacy for businesses engaged in networked computer transactions

To protect sensitive data on networks and to comply with regulatory mandates, organizations need secure access methods that restrict unauthorized users without inconveniencing staff members and customers. SMBs face the challenge of devising effective security solutions without the benefit of a large IT department to design, implement and maintain the solution infrastructure, while larger enterprises are looking to reduce costs and simplify deployment of security solutions.

The secure access market is growing, driven by these key factors:

> **Business demands:** Increasing numbers of staff members depend on remote access in their daily work. Many organizations also rely on their workforce being able to access information while traveling or from home. With more business processes moving to the Internet, customers, trading partners and employees need access to the network. To stay competitive, organizations must provide this access while maintaining data security.

> **Technological advances:** Advances have given us faster networks, intranets, extranets and mobile access to resources, raising risk factors to unauthorized information access. Information can be stolen by hackers, identity thieves and cyber-terrorists, as well as industry competitors. Careless or malicious employees can also violate data security provisions. To counter these risks, a positive means of authenticating users is essential.

> **Regulatory requirements:** Greater accountability mandated by government regulations and industry best practices places a burden on organizations to restrict access to private information. In many cases, organizations must also monitor and track who accesses information. Strong authentication establishes accountability and helps meet audit and compliance requirements.

> **Rising Password Management costs:** Passwords are becoming unmanageable for end users, password-related help desk calls are on the rise. This all adds to the increased costs of password management.

Organizations at every level require strong, reliable authentication and network access mechanisms that support workflow and routine business processes without compromising security. Online environments for partner and consumer access must be trusted and trustworthy. Regulatory compliance is also a vital concern. A substantial portion of the market consists of companies that require rigorous security, but lack the in-house resources to deploy and manage an effective solution on a daily basis. For these companies, a well-designed, cost-effective package that includes both the hardware and software to implement strong authentication effectively addresses their requirements.

IDC anticipates that, by 2007, security solutions based on dedicated security appliances will reach 80 percent of the industry market share. This trend illustrates the strong potential for sharply increasing sales of RSA SecurID Appliance products to an expanding market segment.

To eliminate the barriers associated with component-based solutions, a number of appliance solutions have been introduced to provide access to VPNs and to manage firewalls. Appliances typically consist of a hardware unit that has been preloaded with all required applications and a pre-configured operating system, ready for rack mounting and operation. The success of this type of appliance in the market highlighted the need for an easily deployed means of providing strong authentication to ensure that remote access connections meet security guidelines. With these market conditions in mind, RSA Security developed the RSA SecurID Appliance to deliver two-factor authentication technology to customers in an acceptable format—a security appliance.

The need in the market for a plug-and-play security solution encouraged RSA Security to take the software capabilities of the RSA SecurID solution and embed them in a hardware appliance for quick deployment and easy maintenance. Without sacrificing any of the features that have made RSA SecurID authentication a success in the market, the RSA SecurID Appliance offers a turnkey approach to security, providing the industry's leading two-factor authentication system in a rack-mountable form factor. The fully integrated package extends the capabilities of the RSA SecurID solution with additional features, such as comprehensive remote management tools in a familiar and easily navigable web browser interface.

The RSA SecurID Appliance combines RSA SecurID technology—the world's leading two-factor user authentication system—with a rack-mountable hardware unit that streamlines deployment. Providing protected access to a variety of environments—including Microsoft® Windows® and UNIX® operating environments, IP/SEC and SSL VPNs, wireless networks, web servers and business applications—this appliance simplifies maintenance requirements, scales to meet the needs of growing businesses, and substantially reduces the TCO.

Hardware Platform Specifications

The hardware platform for the RSA SecurID Appliance includes these features:

> Intel® Pentium® processor (2.0 GHz)

> 512MB DRAM

> 40GB hard drive

> Universal power supply (350W)

The front panel includes:

> Serial port console

> USB 2.0 interface

> Two 10/100 Ethernet ports

> Two Gigabit Ethernet ports

> LCD panel (40x2 characters)

> Control knob

> Status LED ports

The back panel includes:

> Two USB 2.0 interfaces

> One keyboard port

> One serial port

> One VGA port

> Three cooling fans

**RSA SECURID® APPLIANCE
SALES GUIDE**

Overview of Solution

**RSA SECURID® APPLIANCE
SALES GUIDE**

Identifying Customers

Software Configuration

The software configuration consists of:

> **Hardened Microsoft® Windows® Server 2003**—A hardened operating system deactivates those features that represent security risks, and configures the overall settings for optimal security.

> **RSA Authentication Manager 6.1 Base Edition**—The base license includes support for one replica appliance, which requires purchase of a second appliance unit.

> **Browser-based web administration tool** that supports up to 400 users (includes a feature-rich web interface and streamlined seven-step wizard for installing and configuring RSA SecurID software)

"*This appliance simplifies maintenance requirements, scales to meet the needs of growing businesses, and substantially reduces the total cost of ownership.*"

Many large enterprises have implemented secure remote access to their networks to increase the productivity of their mobile workforce, but are increasingly looking to reduce costs related to security management. The technology to provide secure remote access, has been adopted at a slower pace by SMBs, but they are now responding to the limitations of passwords. Cost factors and the complexities of setup and maintenance are key issues in these market segments.

The typical SMB prospect for the RSA SecurID Appliance needs to provide anytime, anywhere, any-device, any-connection access to organizational resources. Continuous access to real-time information is an important driver of business productivity. Accomplishing this across the Internet, or the business network, requires robust, centralized application delivery and management capabilities.

Larger enterprises often have the need to address multiple remote locations and branches, often with limited IT expertise in these remote sites. A solution that can be deployed simply and rapidly is of great benefit in this scenario.

Requirements across a variety of industries include:

> Increased productivity by giving their mobile workforce a familiar desktop-to-go—accessible from anywhere

> Accelerate delivery of a full range of business applications that power everyday activities, including ERP, CRM and office productivity software

> Increased availability of business resources to remote workers while maintaining all necessary regulatory and accountability requirements

> Simplified administration and maintenance of remote access through a centralized management tool

> Do you have a security policy for remote users? Although VPNs provide privacy, they don't address all security issues.

> What would happen if a hacker penetrated your company's network through the VPN?

> Besides sales people, are there other groups within your company who would benefit from accessing information anywhere, anytime?

> When did you last go through an audit? How did you fare?

> Do you have an available IT staff with the expertise to deploy and manage a security solution?

> How much do you think it would cost your company if your network security was breached?

> Do you have the ability to determine if your network has been breached?

> Does a strong authentication solution that costs less than $5000 and is easy to administer appeal to you?

> Do you feel that your company has adequately complied with the multiple regulatory mandates for privacy and security?

> Do you have any method in place for monitoring and tracking remote access that provides full accountability?

Refer to the RSA SecurID Authentication Sales Guide for further authentication discovery questions.

The RSA SecurID Appliance solves a common challenge by implementing a comprehensive strong authentication security system in a hardware package designed for ease of use and manageability.

The advantages include:

> **IT-friendly.** Perfect for businesses such as small law firms, doctor's offices, insurance companies and the like without extensive IT resources, and for larger enterprises looking to simplify the deployment of an authentication solution.

> **Low ongoing administration costs.** The appliance makes it very simple to validate users and bind a token to a user.

> **Packaged for convenience and ease of use.** Includes the essential components for implementing strong authentication in an easily deployable form

Companies gain all the benefits of an RSA SecurID solution in a convenient bundle, including efficient, centralized management of heterogeneous computing environments, while providing secure, on-demand access to a wide array of resources from any location, device or connection.

Based on RSA Security's technology and expertise in encryption, the RSA SecurID solution provides world-class two-factor authentication, using a patented, time-synchronous mechanism to validate users. Customers gain the best of both worlds—strong user authentication and secure access to corporate resources. Businesses benefit from industry-leading security technology packaged in an easily deployed hardware component.

The RSA SecurID Appliance is a comprehensive security solution that consists of a hardware unit, RSA SecurID authentication software and a hardened operating system. The operating system—a dedicated version of Microsoft® Windows® Server 2003—has been customized to disable functions that jeopardize security or that don't apply to the core operations. The hardware unit, covered by a one-year replacement contract, fits in a standard, single-space rack.

The RSA SecurID Appliance favors ease of operation. A customer can turn it on and be fully operational in about 15 minutes in most situations. Setup is simplified by means of a seven-step wizard, and ongoing maintenance can be performed through a graphical browser-based interface. Through the web interface, customers can perform a number of tasks:

> Adding and deleting users

> Assigning tokens

> Installing and configuring agents

> Viewing the activity monitor

> Viewing system details

> Specifying the location of the backup files

The RSA SecurID Appliance squarely addresses the market need for an easy-to-deploy, easy-to-manage, all-in-one security solution. The RSA SecurID Appliance delivers genuine business value in a cost-effective package.

The following are typical objections you might encounter while attempting to sell the RSA SecurID Appliance. Responses to these objections are included to help you keep the prospect in your sales pipeline and close the deal.

We have a very small IT department and can't support an infrastructure-level security solution.

> Because of its innovative turnkey design and preinstalled software, the RSA SecurID Appliance eliminates problems associated with software setup and maintenance. All of the components that are needed to implement the security solution are contained in the hardware unit—you can quickly integrate it into your network and begin experiencing the benefits of two-factor authentication within minutes.

We don't need RSA SecurID two-factor authentication—we already have a firewall and/or VPN.

> A firewall shows that you have a sense of the importance of security for your organization. But if you are authenticating through the firewall with passwords, there is still vulnerability in your IT infrastructure.

> A VPN ensures that your data is private and encrypted, but this does not ensure that you know who is on the other end of the communication.

> Privacy does not necessarily mean security. Strong authentication is also as critical as a firewall or VPN because it prevents unauthorized entry in a way that static passwords do not.

> The RSA SecurID Appliance is designed to work "out of the box" with the leading VPN vendors such as Cisco, Juniper, Check Point and Nortel Networks.

Passwords are secure. Why would I need more protection?

> Vulnerabilities exist simply because your systems and information are connected to outside networks beyond your control. Passwords can be sniffed (eavesdropped), cracked by means of dictionary attack programs, shared by users, copied from post-it notes stuck on PC monitors, and so on.

Users will not readily accept tokens.

> RSA SecurID tokens are very easy to use. The approach is very similar to the two-factor authentication (bank card and PIN) used by ATM users on a daily basis.

> The several form factors available for RSA SecurID authenticators provide many options for users. Options such as key fob tokens offer a convenient, popular approach to overcome user resistance to adopting tokens.

Tokens are too expensive.

> When you consider the cost of helpdesk calls related to passwords and the burden and expense of password administration for multiple employees, tokens are surprisingly cost-effective.

The RSA SecurID Appliance can be obtained through the network of RSA SecurWorld distribution partners. For the most current pricing information, contact your distributor directly.

The RSA SecurID Appliance is designed primarily to be sold as a bundled solution that includes the appliance (with software preloaded), a software license, tokens and a hardware warranty. The component pricing model can be used to address larger installations above 250 users, different token requirements, staggered token deployment or the requirement for multiple replicas.

Quoting an RSA SecurID Appliance Bundle

Step 1: Determine which RSA SecurID Appliance offering is right for your customer, emphasizing bundled configurations where possible. The sales presentation might offer the product in terms similar to these: "The RSA SecurID Appliance is typically sold as a solution bundle, which includes the software, tokens, maintenance and the appliance hardware." Through further questions, you can then identify the specific customer needs.

a) How many users does the customer want to support?

Hint: The RSA SecurID Appliance is available in 10-, 25-, 50-, 100-, 150- and 250-user configurations.

Step 2: Determine whether a bundled offering meets customer requirements.

a) Does the customer want or need the number of tokens which come packaged as a standard part of the bundled offering?

Hint: Some customers may want to purchase a 100-user appliance, but initially plan to issue a smaller number of tokens.

b) Do the tokens that come as part of a bundled offering meet your customer's needs?

Hint: The RSA SecurID Appliance bundles include RSA SecurID SID 700 three-year tokens. If your customer wants a different form factor or time length, order the individual components as required.

Step 3: If one of the RSA SecurID Appliance bundled offerings meets customer requirements, place your order for that bundle. If the bundled offerings do not match your customer's needs, go to the following section, titled "Quoting RSA SecurID Appliance Components."

Step 4: Specify maintenance option for the selected RSA SecurID Appliance Bundle.

> **Hint:** Maintenance is available in either **RSA SecurCare Plus** (8 x 5) or **RSA SecurCare Extended** (24 x 7).

Step 5: Recommend a replica server to the customer to ensure continuous authentication coverage.

> **Hint:** A replica server ensures that the authentication application will continue if the primary server fails.

a) Order another RSA SecurID Appliance (hardware only).

Quoting RSA SecurID Appliance Components

Step 1: Although bundled sales are favored, in some cases a customer may need to purchase components individually. When ordering RSA SecurID Appliance components separately, ask the following questions:

a) How many users does the customer want?

b) How many tokens does the customer want?

> **Hint:** Sometimes the number of tokens will not match the RSA SecurID Appliance size.

c) Determine the type of tokens the customer wants.

> **Hint:** RSA SecurID tokens can be purchased in both hardware and software formats.

d) Determine the life of the tokens.

> **Hint:** RSA SecurID tokens are available in two-, three-, four- and five-year versions.

Step 2: Order the RSA SecurID Appliance components.

a) Order the RSA SecurID Appliance (hardware with the software preinstalled)

b) Order the RSA Authentication Manager software license for the number of desired users (priced per user).

c) Order the tokens in the form and life span desired.

d) Order maintenance for the number of users for the software license (priced per user).

Step 3: Recommend a replica server to the customer to ensure continuous authentication coverage.

> **Hint:** A replica server ensures that the authentication application will continue if the primary server fails.

a) Order another RSA SecurID Appliance (hardware only) if the customer wants replica functionality.

To assist resellers in becoming familiar with the RSA SecurID Appliance and demonstrating this product to customers, RSA Security has established a Not For Resale (NFR) program. NFR Kits are limited to one per reseller and are intended for internal use only by resellers or for the sole purpose of presenting sales demonstrations to customers. This program is temporary and may be discontinued at any time.

The NFR Kit for the RSA SecurID Appliance is a chargeable item and can be ordered by both Solutions and Access Partners on completion of RSA SecurID solutions sales authorization. The Appliance NFR Kit cannot be discounted.

The RSA SecurID Appliance NFR Kit **(P.N. SIDAPP-NFR-KIT)** contains the following items:

> RSA SecurID Appliance hardware with RSA Authentication Manager 6.1 software installed

> Five RSA SecurID SID 700 tokens

> Ten user software licenses

> RSA SecurCare Maintenance 8 x 5 contract, which includes advanced hardware replacement

> **Cost: $2,000.00 US**

Q. What is RSA SecurID two-factor authentication?

RSA SecurID two-factor authentication is like an ATM card for securing network or system access. It provides an easy, one-step process to positively identify a user and prevent unauthorized access.

Used in combination with the RSA Authentication Manager software and RSA Authentication Agent software, RSA SecurID authenticators generate a new, unpredictable access code every sixty seconds.

RSA SecurID technology offers strong security for a wide range of platforms—so users have a single method of sign-on to gain access to a remote dial-up session, protected web pages, mainframes and more.

Q. What are the benefits of RSA SecurID two-factor authentication?

RSA SecurID solutions help prevent unauthorized users from accessing enterprise network and information resources—the protection corporations need to secure valuable information assets. Two-factor authentication provides more powerful protection than traditional passwords.

For a sophisticated hacker or a determined insider, it doesn't take much to compromise a user's password and gain access to resources that are off-limits.

Single-factor identification—a reusable password—is not enough.

Q. What components are included with an RSA SecurID Appliance?

The RSA SecurID Appliance system includes four components:

> RSA SecurID Appliance hardware

> RSA Authentication Manager software

> RSA SecurID authenticators

> RSA Authentication Agent software

Each component contributes to the overall interoperability, scalability, manageability and flexibility that set this product apart from its competitors.

Q. Can customers add users to their appliances?

Yes, customers can add users to their RSA SecurID Appliance licenses as needed. The RSA Authentication Manager license for the RSA SecurID Appliance is the same as for the stand-alone RSA Authentication Manager Base Edition. A user can purchase any of the user upgrade options that are currently available from RSA Security.

Q. How does the RSA SecurID Appliance compare to the software version of the RSA SecurID solution?

The RSA SecurID Appliance includes the RSA Authentication Manager 6.1 software preinstalled on a rack-mountable unit running a hardened version of Microsoft® Windows® Server 2003. The web administration interface—unique to the appliance—supports management of up to four hundred individual users. As an easily deployed, easily integrated security solution, the appliance lets companies implement two-factor authentication within their networks in minutes instead of hours.

Q. Are there additional hardware service requirements for the RSA SecurID Appliance?

Through an intuitive, comprehensive, browser-based graphical interface, many of the common management and troubleshooting tasks for the RSA SecurID Appliance can be handled remotely. This feature simplifies service requirements—setup issues and basic troubleshooting can often be accomplished without requiring a technician on-site. The streamlined design of the web interface makes many administrative tasks simple enough for a moderately proficient staff member to handle, but it also provides full-featured access to all of the configuration settings and controls for the appliance and RSA SecurID software.

The preconfiguring of the RSA SecurID appliance also minimizes the deployment and integration of the security solution into an existing business network. Customers can typically be up and running in a matter of minutes using the plug-and-play design features of the product.

Q. What is required to deploy and set up the RSA SecurID Appliance?

The streamlined setup process for the RSA SecurID Appliance typically requires about fifteen minutes from the time the unit is powered on. The administrator follows a guided setup process, consisting of seven questions presented through a web-based graphical interface, to accomplish these tasks:

1. Initialize the time and date

2. Set the administrator password

3. Configure the appliance host name and IP address

4. Install the license

5. Import token records

6. Assign the administrator token

7. Test and enable authentication

Q. What if I need replica functionality to ensure high availability for my security system?

Replica functionality can be achieved by adding a second RSA SecurID Appliance to your system. If the primary unit fails, the secondary appliance immediately takes over the authentication operations, much in the same way that a mirror disk backs up the operation of a corporate server. The replica setup for the RSA SecurID Appliance has been streamlined by means of a wizard that guides the administrator through the process. The replica environment can be centrally administrated and managed from a single point (including the delivery of logging and audit information) while protecting RSA Authentication Manager agents across the entire organization. The replica appliance communicates in real time with the primary server, verifying that the primary server is up and running and ensuring its data is current. In the event that the primary server goes down, the replica server processes all authentication requests and users receive uninterrupted service.

Q. What are the key benefits of the RSA SecurID Appliance?

> Provides industry-leading security in a convenient package

> Consistently lowers TCO through an intelligent design that is easy to deploy and easy to maintain

> Offers flexible interoperability with leading third-party products, including products from Cisco, Juniper, Citrix, Microsoft and others

> Helps ensure regulatory compliance and accountability with strong, two-factor authentication and audit tracking tools

For further FAQs on RSA SecurID Authenticators, RSA Authentication Manager Software and RSA Authentication Agent Software refer to The RSA SecurID Authentication Sales Guide.

The Company

www.rsasecurity.com

RSA Security (NASDAQ: RSAS) is the expert in protecting online identities and digital assets. The company invented the core security technologies for the Internet and continues to build on its 20 years of innovation. Built to work seamlessly and transparently in the complex environments of thousands of customers, the company's comprehensive portfolio of identity and access management solutions—including a complete suite of authentication and web access solutions—is designed to allow customers to confidently exploit new technologies for competitive advantage.

RSA Security's strong reputation is built on a history of ingenuity and leadership, proven technologies and long-standing relationships with more than 1,000 technology partners.

Web Seminars

www.rsasecurity.com/events/webseminars

These free RSA Security web seminars allow you to learn right from your desktop, at a time convenient for you. Register for upcoming web seminars on a range of e-security topics and also view archives of past events.

RSA Security News Center

www.rsasecurity.com/news.asp

Keep up to date with RSA Security's latest breaking news, media releases, past news and background information.

Security Glossary

www.rsasecurity.com/glossary/

The RSA Security Information Security Glossary is offered as an aid to understanding current concepts and initiatives in the realm of Information Security. The terms were chosen based on their importance in understanding the solutions, services and products that RSA security provides for its customers.

RSA SecurWorld Partner Program

www.rsasecurity.com/securworld

Membership in the RSA SecurWorld Partner Program confers a wide range of benefits and opens substantial opportunities for partners. *continued overleaf…*

Two categories of partnership exist: RSA SecurWorld Access Partners and RSA SecurWorld Solutions Partners. Each category has its own corresponding benefits and criteria, and requires that prospective partners meet the appropriate participation criteria and continue to comply with specific requirements throughout the duration of their membership.

RSA SecurWorld Partner Portal

https://www.rsasecurworld.com

RSA SecurWorld partners enjoy a number of valuable benefits, including exclusive access to the Partner Portal. The Partner Portal offers extensive online information for all RSA SecurWorld programs and the latest sales and marketing tools, including sales presentations, training materials, logos and photographic downloads, access to collateral and other materials designed to help you generate sales and build awareness of your business.

Presentation Materials

The RSA SecurWorld Partner Portal offers highly effective, professionally designed presentation materials that drive home the key messages and enhance your sales efforts.

Sales Presentations in Microsoft® PowerPoint® format highlight product benefits and provide a guided tour through the most important sales points.

Customer case studies help your customers visualize how products may meet their specific requirements.

Datasheets provide the details that an IT group or CTO may need to authorize purchase of RSA Security products.

Leave-behinds offer a well-rounded, technically complete picture of our e-security products to help you close sales.

RSA SecurWorld Partner Locator

http://partnerfinder.rsasecurity.com/PartnerLocator/plhome.aspx

RSA SecurWorld Partners are experienced in delivering authentication and secure access solutions in nearly 50 countries. The RSA SecurWorld Partner Locator provides a tool for customers to find a partner that will meet their needs. To ensure your details are displayed correctly on the Partner Locator, please keep your Company Profile up-to-date via the My Account section of the Partner Portal.

RSA Secured® Solutions Directory and Implementation Guides

www.rsasecured.com

The RSA Secured Solutions Directory has long been a valuable resource for corporate IT and IS directors looking for security products, and the general Internet user who is concerned about e-security. The directory lists vendor products that have RSA BSAFE® encryption technologies included into their products and vendor products that are compatible with RSA SecurID, RSA® Access Manager and RSA Digital Certificate technologies, as well as links to Implementation Guides for each individual product.

RSA Online

www.rsasecurity.com/go/rsaol_reg.asp

RSA Online is a comprehensive and evolving e-Business solution to provide our customers and business partners with industry-leading access to order information and RSA Security's product catalog over the web. This service is provided at no additional charge to select RSA Security enterprise customers and partners. Separate registration is required.

RSA Online offers:

> A personalized secure interface

> Real-time access to order-tracking and history information

> Quick and easy license lookups

> Proactive maintenance renewal notifications

> Same information used by RSA Security Customer Operations

RSA SecurCare® Online

https://knowledge.rsasecurity.com

RSA SecurCare® Online is a free service for RSA Security customers with an active support contract, as well as resellers and partners. This web-based customer support application can help you find answers to your most pressing technical questions. You must be registered with RSA SecurCare Online to use this service.

Americas Headquarters

International Headquarters

Corporate Headquarters

RSA Security Inc.
174 Middlesex Turnpike
Bedford, MA 01730

Tel: +1 781-515-5000
      +1 800-732-8743
      (800-SECURID)
Fax: +1 781-515-5010

RSA Security UK Ltd.
RSA House
Western Road
Bracknell
Berkshire RG12 1RT
United Kingdom

Tel: +44 1344 781 000
Fax: +44 1344 781 010

RSA Security Australia Pty Ltd
Level 3, 110 Walker St.
North Sydney, NSW, 2060
Australia

Tel: +61 2 9463 8400
Fax: +61 2 9955 0826

Local Offices

To locate an RSA Security office near you, visit this link:

http://www.rsasecurity.com/node.asp?id=1052

RSA Security Distributors

A current list of RSA Security Authorized Distributors can be found on the RSA Security partner
locator. To search for a distributor in your area visit:

http://partnerfinder.rsasecurity.com/PartnerLocator/plhome.aspx

RSA SecurWorld™ Partner Program

RSA SECURITY®

Confidence Inspired™

RSA Security Inc.

www.rsasecurity.com/securworld