INTERNATIONAL DATA CORPORATION

eSecurity

The Essential eBusiness Enabler

An IDC White Paper

Analysts: Roseann Day, John Daly, and Christian A. Christiansen

What is eSecurity?

The Internet has changed how and where business is conducted. IDC estimates that by the year 2003 eBusiness — business conducted on the Internet among businesses or between businesses and consumers — will top $1.3 trillion dollars. With this tremendous opportunity there also comes serious challenges. Enter eSecurity: The complex interaction of multiple computer environments, communication protocols, system infrastructures, policies and procedures that together comprise a trusted means of communicating over public and private networks.

eSecurity marks a departure from traditional security. In the past, security technologies -both physical and electronic — essentially operated to limit outsiders' access to corporate resources. eSecurity assumes

IDC Opinion

Why is eSecurity an essential enabler of eBusiness??

Enterprises are rushing to keep pace with the eBusiness imperative, integrating suppliers and customers over public network infrastructures. Protecting valuable corporate assets while opening up these eBusiness opportunities raises serious security concerns in companies expecting to manage a substantial portion of their business over intranets and extranets. Organizations are concerned about the direct economic risks of compromised security. They also fear severe "loss of business " through compromised web presence. The stakes are high.

Any eBusiness security solution needs the flexibility and capacity to expand as more users and more applications are Internet-enabled. IDC recommends beginning with an eBusiness architecture that addresses both security and scalability.

With a wide range of products to select from, IDC also recommends users deploy best-in-class products integrated with the most popular desktop clients and enterprise servers by companies with eSecurity experience, expertise and scale.

5 Speen Street
Framingham, MA 01701
(508)872-8200
(508)935-4015

IDC
www.idc.com

outsider access and works to encourage and enable that access. That is, pre-eBusiness security's main function involved limiting access to corporate data networks to only those individuals who had been previously identified and deemed trustworthy. Today's eSecurity model invites outside access. It works within an Internet architecture that assumes some degree of "street level access" for all.

This eSecurity model addresses the conflicting goals of providing open access and the continued need for strict asset protection. At the heart of eSecurity is a secure infrastructure that permits low-level anonymous web access with high-level transactional security. The greater the level of authentication and authorization control desired, the more sophisticated an eSecurity architecture must be. IDC recommends identifying these requirements early and building the eSecurity framework before moving applications to the Internet.

What eSecurity Requirements Do Businesses Face?

Businesses in general reported considerable and growing losses due to computer security breaches, according to a recent Computer Security Institute/FBI poll — considered by most to underestimate the actual amount of business fraud loss. For example, companies reported annual increases of over 35% per year in data or network sabotage incidents from 1997 to 1999. In this same survey, organizations reported annual increases of over 25% in financial fraud perpetrated on-line. Insider abuse of network access, as measured by these companies, increased over 20% resulting in losses of over U.S. $8 million. The problems are increasing within and without the corporate IT infrastructure.

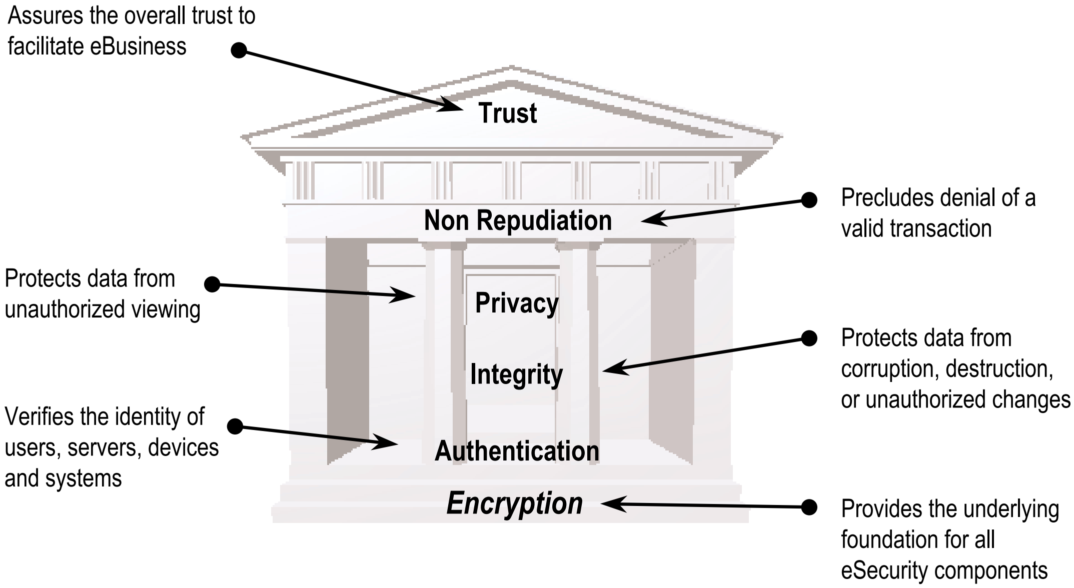
The corresponding requirements for eSecurity thus span the use of the Internet for internal and external networks, but vary depending on how businesses use the web. The essential requirements include trust, encryption for privacy and protection, data integrity, strong authentication, non-repudiation, and integration.

Trust: On the **Internet**, corporations are concerned about employees visiting untrusted sites that may contain malicious code, viruses, or objectionable content. On the **Intranet**, corporations must face the fact that not all employees can be trusted to access all assets. As Intranets are deployed for more sensitive applications — HR, legal, accounting, sales, and R&D — that were formerly on separate networks, there is a greater need for two-factor user authentication, granular access control, and security audit. **Extranet** sites link business partners together for specific types of business activity but maintain strict separation of other corporate information. This means that strong encryption, authentication, authorization, anti-virus, firewalls, intrusion detection, security audit, and security management should all be installed before Extranet roll-out.

Encryption for Privacy and Protection: IDC believes that the definition of privacy varies sharply between owners and users. Organizations hosting **Internet** sites are forced by law and by good practice to protect data and consumer privacy. Even on an **Intranet**, privacy issues are important for data with financial, personnel, or research value. **Extranet** sites often face the biggest challenges in handling data since individual and corporate data must be protected while multiple corporate entities are provided some degree of access. The entire set of trust requirements for eSecurity builds upon the foundation of encryption.

Integrity: Integrity involves protection of data from corruption, destruction, or unauthorized changes. Similarly, the configurations and basic integrity of servers, applications, and networks must also be protected.

Figure 1
Essential Elements of eSecurity


Assures the overall trust to facilitate eBusiness
Trust
Non Repudiation
Precludes denial of a valid transaction
Protects data from unauthorized viewing
Privacy
Integrity
Protects data from corruption, destruction, or unauthorized changes
Verifies the identity of users, servers, devices and systems
Authentication
Encryption
Provides the underlying foundation for all eSecurity components

Source: International Data Corporation, © 1999

Authentication: Authentication verifies the identity of users. On the **Internet**, “cookies” can provide automatic authentication with user name and password after the user registers at a site. This low-level interaction is protected by simplistic passwords and secure socket layer (SSL) encryption of personal data such as credit cards. On **Intranets**, authentication can range from simple passwords to two-factor authentication with tokens and/or smart cards to biometrics that utilize the user’s physical characteristics for identification. Current **Extranet**

deployments often use stronger authentication by relying on tokens and smart cards. IDC expects that digital certificates, in combination with passwords, tokens or smartcards, will soon become increasingly common for extranet usage. Their adoption for highly sensitive partner environments will pave the way to acceptance for Internet and Intranet usage.

Non-repudiation: For a business transaction to be valid, neither party can later deny the existence or execution of that transaction. Use of digital signatures is growing in practice and in legal acceptance as a means of protecting transactions from later dispute.

One customer pointed out the importance of non-repudiation. He said that customers were getting e-mail confirmation of their on-line flower orders from the portal web site. However, the portal web site received many customer complaints about non-delivery of flowers to spouses, parents, and other disappointed loved ones. When the portal site investigated, it found that transmission of the flower orders to the fulfillment vendor was never confirmed. The portal vendor implemented non-repudiation at the transaction level to solve this problem and ensure satisfied customers.

Systems Integration Services: All of the previously mentioned factors are complex to implement. Consequently, even the largest security customers employ systems integration services. For example, a tire manufacturer told IDC that, "We are tire, not Internet experts. Why should we re-invent the wheel, when we can hire expert systems integrators for all our Internet, Intranet, and Extranet projects."

How Does eBusiness Build Upon eSecurity?

While most enterprises are aware of the security risks involved in eBusiness initiatives, implementation remains a major challenge. Because of the costs involved and the seemingly overnight success of several eBusiness startups, the unique security challenges of eBusiness are often left unaddressed when enterprises launch new web-based applications. Additionally, the open nature of the Internet actually increases the risks to both the assets and the reputation of companies participating in this trillion-dollar market. For these reasons, IDC recommends organizations address eSecurity early as a critical part of a total eBusiness solution.

At a minimum, a good eSecurity foundation requires companies to offer stronger user authentication and increased access control. The traditional perimeter defenses of firewalls and smart routers that protect corporate assets from the outside are not the foundation of a good eSecurity model. Instead, an effective architecture is built upon a model of controlled access where the perimeter is strongly defined but access is equally well managed throughout the distributed enterprise.

Does eSecurity Destroy Perimeter Defenses?

The Medieval castle provides a rough analogy to standard perimeter defense models. These structures protected their inhabitants with a series of obstacles (a moat and a concentric ring of walls). To conquer the castle, enemies must break these perimeter defenses. This is similar to today's perimeter security rings, which often include firewalls, isolation of sensitive systems, security hardened operating system, and intrusion detection software.

Ultimately, the castle's defense function was made obsolete by market forces. The castle walls simply could not hold all the town's people during wartime. The town's people were also not willing to abandon their homes, shops, trade goods, and farms to the invader's pillaging and looting. Therefore, towns developed armies and diplomacy to eliminate the threat before it reached their town.

eSecurity, in its place in the modern world of eBusiness, has evolved to address equally significant changes in the way trade and communications occur. Castle walls and perimeter defenses are not sufficient protection as web sites open access to all customers. One large financial customer recently said, "Perimeter defense based on firewalls is still important, but more sophisticated security systems are needed because we don't even know where the perimeter is anymore."

While perimeter defenses become less central to the security framework, the protection of assets themselves rather than the perimeter will grow in importance. In the world of eBusiness, it is essential to know with whom you are conducting business. Strong authentication and authorization management will take the roles of diplomats by negotiating agreements between different parties. Strong authentication, authorization, and access control ensure that everyone acts in a manner conducive to eBusiness. Finally, the analogy extends to armies (or defensive forces) that will exist in the form of vulnerability assessment and intrusion detection tools.

Castles to Airports: Moving toward eSecurity

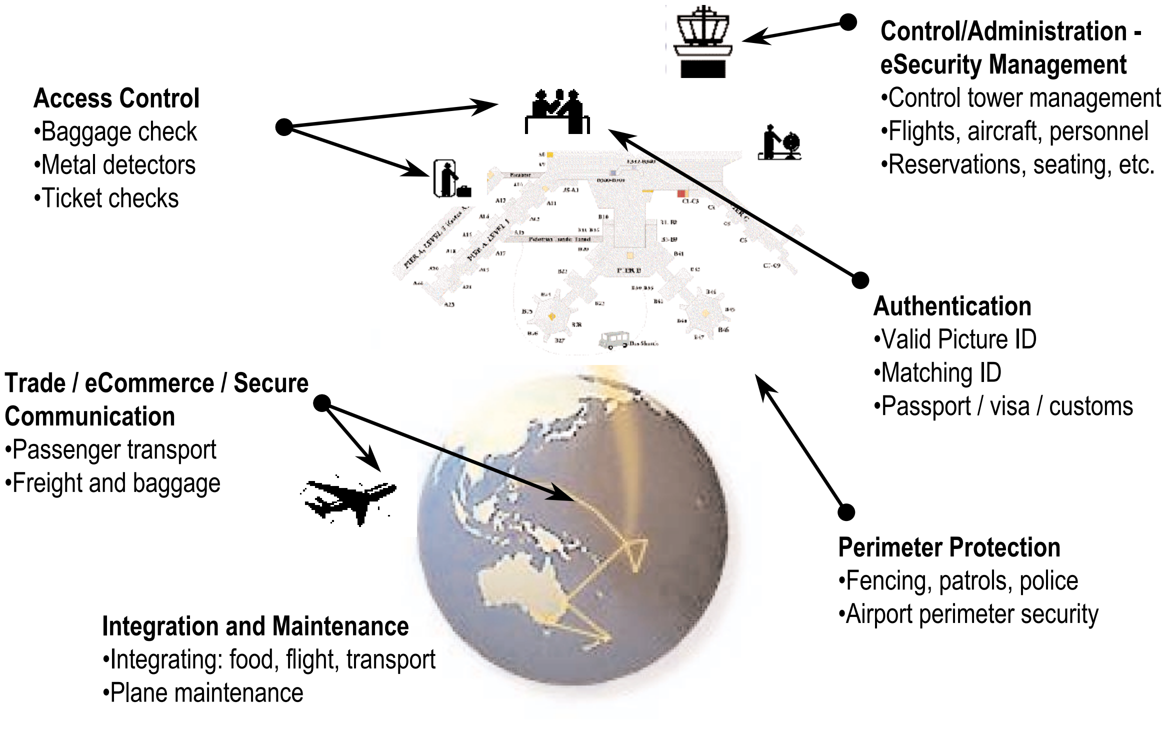
The traditional castle and moat analogy is better replaced by an air transportation analogy. The airport is well protected on its boundaries by fences, staffed gates, x-ray machines and hidden cameras. However, access to facilities — ticketing levels, departure gates, staff areas, hangars, cockpits, and the tower — is tightly controlled on a need-to-use basis and restricted to only those with proper credentials. While hundreds and thousands of travel agents and ticketing personnel worldwide can issue boarding passes, only the appropriate government aviation authority, such as the FAA in the United States, can issue credentials that permit access to the airport control tower. Vacationing families at the gate may give it little attention, but the safety and efficiency of the airport hinges on the tight control that allows only the right staff into the proper airport facilities. The eSecurity protecting eBusiness over the Internet parallels this complex array of varying security components

Even airport security must respond to ongoing changes. For example, recent increases in threats to airline safety resulted in the enforcement of two-factor authentication for passengers. In addition to presenting a valid boarding pass or ticket, travelers in most parts of the world must now also show a picture identifier before boarding a plane.

What Are the Important Technologies in the eSecurity Product Space?

eSecurity goes beyond traditional security while building upon many of the traditional components. eSecurity integrates tight authentication and increased encryption for greater protection of assets. Figure 2 uses the air transportation model to show how the key security capabilities play together in a complex environment. For both, the essential components are control and administration, authentication, perimeter protection, secure communication, and integration.

Figure 2
eSecurity Components Model


Control/Administration - eSecurity Management
•Control tower management
•Flights, aircraft, personnel
•Reservations, seating, etc.
Access Control
•Baggage check
•Metal detectors
•Ticket checks
Authentication
•Valid Picture ID
•Matching ID
•Passport / visa / customs
Trade / eCommerce / Secure Communication
•Passenger transport
•Freight and baggage
Perimeter Protection
•Fencing, patrols, police
•Airport perimeter security
Integration and Maintenance
•Integrating: food, flight, transport
•Plane maintenance

Source: International Data Corporation, © 1999

eSecurity Components Model

Substituting: a.) networks and enterprise architectures for airports; b.) users of different authority and access levels for passengers, crew and flight support personnel, and c) TCP/IP-transported data and transactions for air freight, passengers and planes; one can see the analogy between eSecurity's complexity and the air transportation system's.

The basic foundation remains a security policy, the overall "route map" of what are the electronic events that are desired and who can do what. The desired events might be securities trading transactions or purchases of fashion items from an online retailer. The questions are: Who can purchase or trade? Are their credit cards valid? Are they a registered user with a specific government or banking institution. A good policy identifies clearly, how such control will be managed no matter how distributed resources become.

The next step is centralization of security controls. This means mapping policy into practice for setting up systems, user accounts, and networks. It also requires tools for auditing activities and triggering actions when unexpected events occur.

Using the enterprise security policy as a foundation, firewalls and routers can be added to the network to protect and audit activity. Intrusion detection software can be layered on the network and hosts to keep aware of ongoing activity on all perimeters. If secure point-to-point connections are desired, the firewalls can be modified for virtual private networking (VPN) to allow encrypted transactions through those firewalls. SSL, secure socket layers, can be set up for secure transmissions between clients and servers, such as the exchange of credit card numbers. Sites wanting secure messaging may opt for secure email, such as S/MIME.

Strong eSecurity also requires tight identification, authentication, and authorization of users and control of what they access. According to IDC's 1998 Internet Security Survey of 300 medium to large corporations, 70% of the respondents reported that unauthorized access to personnel and legal files from both internal and external sources was a major concern. At its very core, eSecurity ensures the privacy of this critical corporate data, along with individual's transactional activity, remains confidential.

An essential enabler of these steps is encryption since the credentials that must pass between widely distributed customers and web servers must not be easily disclosed to outsiders. Specialized authentication tools, including tokens, tickets, smart cards, or biometrics, can be added to this encryption framework for a higher level of control over users and resources.

Moving Toward an eSecurity Framework

Policy, perimeter protection, access control, and centralized security management can be handled with individual technologies. However, eSecurity requires more than the pieces, it also requires an integrated solution with:

1. Simple support for a wide range of desktop and user environments is essential since customers in eBusiness environments must find use of the online system easy.
2. Implementation of underlying software on the most popular enterprise server operating environments so that the requirement for specialized equipment — with its associated administrative overhead — is minimized.
3. Strong authentication of all players in an eBusiness environment including servers, desktop clients, and any authorizing or credential-producing bodies.
4. Tight authorization of specific users for access to specific resources and restriction of general user ability to access other parts of a system or enterprise.
5. Support of popular directories tools — such as LDAP — so that authorization and authentication databases that span the Internet or the enterprise can be managed centrally and easily.
6. Knowledgeable planning, installation, and support staffing on the vendor side to back up the enterprise as security features are enabled.

How to Choose an eSecurity Provider

Enterprises have a variety of options for securing their eBusiness initiatives. The key to finding a security solution that works as an integrated, manageable solution rather than a collection of products is identifying a reliable security technology provider. Essential characteristics of such a provider include:

1. **Quality**: High quality products with a proven track record and satisfied installed base.
2. **Experience**: The length of time the technology has been in practical use and the number of testimonial customers available.
3. **Alliances and Partnerships**: No single vendor can satisfy every customer's diverse needs for integrated, best-of-breed products. Alliances and partnerships increase product breadth and insure integration of other vendors' products and technologies .
4. **Continuous Global Support**: The vendor's ability to provide 24 x 7 support worldwide and the ability to understand the requirements of the enterprise's business and industry

5. **Commitment**: Because eSecurity is so complex and dynamic, vendors must constantly improve products and services. Customers should ask vendors, “Is security technology an area of expertise for the vendor or is security primarily a means of leveraging sales of other products?” The answer indicates the vendors’ commitment to eSecurity.

In a market in which new ventures crop up daily, IDC believes it is important for enterprises to resist the lure of unproven technologies. The best choice is usually the one backed by a long history of product delivery and support.

In the area of cryptography, new algorithms are frequently proposed yet very few are considered strong enough to be put to practical use and only a handful successfully withstand the scrutiny of public examination and test. Other security technologies are brought to market which, while excellent unto themselves, never receive wide enough acceptance to become integrated with the most popular applications or ported to the very latest hardware or operating systems. Certainly, innovation is essential to the market, but in the security space stability and reliability are essential selection criteria.

Partnership with a supplier of key security technologies that has strong products, a long history in the market, and truly understands the challenges of eSecurity can help users move from an architecture to a product implementation.

Evaluating RSA Security Inc. as an eSecurity Provider

RSA Security is one example of a security vendor with a strong historical position and plans for continued innovation. Recently re-named, RSA Security combines two well-known eSecurity companies (RSA Data Security and Security Dynamics) into a single corporate entity.

When evaluated in terms of the criteria listed in section VI, RSA Security demonstrates the global support, product range, scaleability, and knowledge of customer requirements to bring trust to today’s online economy.

Quality

With the proliferation of eBusiness initiatives, the need for sophisticated security technologies and solutions grows increasingly critical. IDC believes that customers should look for vendors that have quality products in a few select areas.

In concert with this idea, RSA Security focuses on three core eSecurity disciplines. In each market, it is the leader or among the top five vendors.

Public Key Infrastructure — According to IDC, RSA Security is demonstrating emerging leadership in the PKI market with new approaches to integrated eSecurity. RSA Keon(is RSA Security’s family of interoperable, standards-based PKI products that deliver a range of flexible solutions for managing digital certificates. Digital certificates and digital signatures are emerging as a strong option for authenticating communications and transactions. The RSA Keon family — from a robust certificate authority to a turnkey enterprise solution — provides a common foundation for secure distributed applications including eCommerce, Intranets, Extranets, ERP and others.

In addition, RSA established a global reseller relationship with VeriSign to offer customers a choice between a product- and a service-oriented solution. This partnership offers organizations a service for outsourcing core certificate authority using VeriSign OnSite™. Because VeriSign was an RSA spin-off, the close association between the two companies ensures that PKI customers can implement a flexible configuration of products and services. This arrangement enables customers to build core certificate solutions that reconcile seemingly contradictory issues such as: cost, scalability, and rapid deployment.

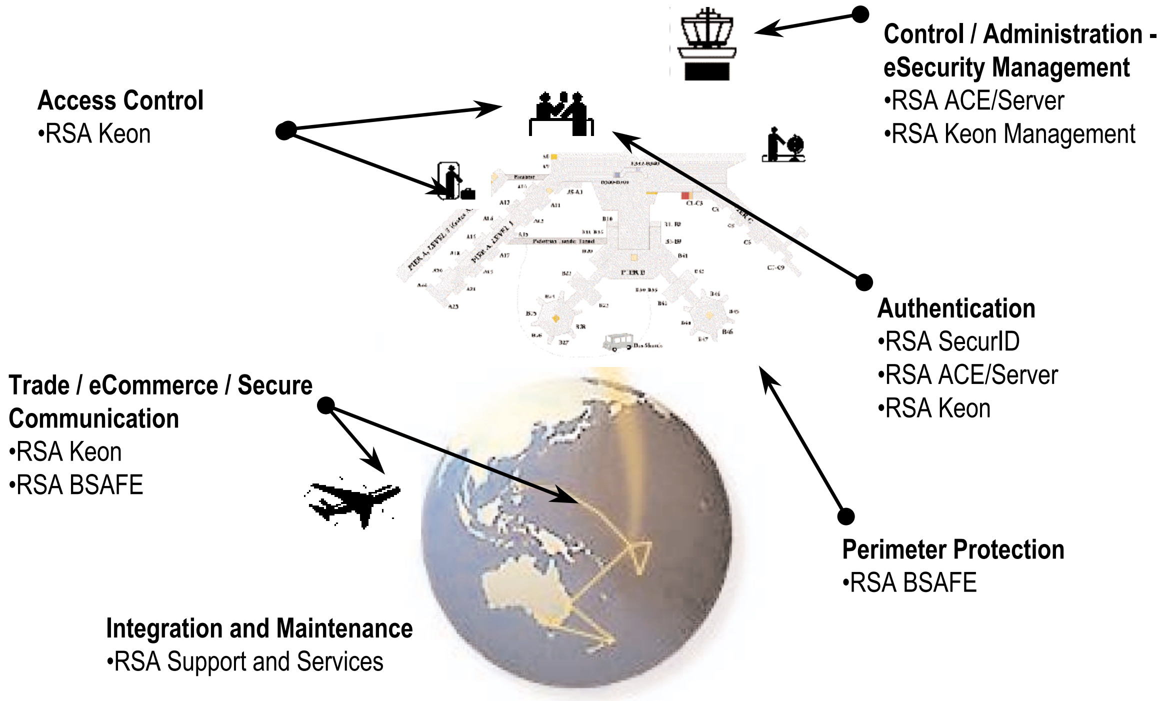
Authentication — IDC believes that RSA Security is the leader in two-factor authentication with over 5 million tokens installed. Its RSA SecurID® solutions provide centrally managed, strong, two-factor user authentication services. Supporting a broad range of authentication devices, including hardware tokens, key fobs, smart cards and software tokens, RSA SecurID solutions protect information assets against unauthorized access. RSA SecurID installations are managed through RSA ACE/Server authentication management software, providing the ability to scale deployments to more than 100,000 users.

Encryption — RSA Security also leads the market for encryption algorithms and tool kits. With 50% and 70% of the Worldwide and U.S. ISV market. in 1998, RSA Security is almost four times larger than its next largest competitor.

RSA BSAFE® is the family of platform-independent cryptographic development tools. These tools enable corporate and commercial software developers to incorporate encryption technology into custom eBusiness applications. IDC expects to see wider use of encryption for enterprise security, entertainment, wireless communications, delivery of digital information over cable, and other uses.

Built to provide implementations of standards like SSL, S/MIME, IPSec, CDPD, and the PKCS family of open standards, RSA BSAFE products can greatly save development time and reduce risk in development schedules. Over 500 Software Vendors have licensed RSA BSAFE encryption technologies and have deployed these technologies in a variety of applications, including web browsers, email systems, commerce servers, and virtual private networks. Figure 3 shows the RSA Security product family as it relates to the essential security products in IDC's recommended framework.

Figure 3
RSA Products Within the eSecurity Components Model



Control / Administration - eSecurity Management
- RSA ACE/Server
- RSA Keon Management

Access Control
- RSA Keon

Authentication
- RSA SecurID
- RSA ACE/Server
- RSA Keon

Trade / eCommerce / Secure Communication
- RSA Keon
- RSA BSAFE

Perimeter Protection
- RSA BSAFE

Integration and Maintenance
- RSA Support and Services

Source: International Data Corporation, © 1999

Experience

With more than 5000 customers worldwide, RSA Security is well known for its RSA SecurID enterprise authentication products and its RSA BSAFE encryption technologies.

RSA Security is a public company with $171.3 million in revenue and $19.0 million in net income for the year ended December 31, 1998. International revenue represented 36.4% of total revenue in 1998. IDC estimates that fully 95% of this revenue is product-based, with the remainder received for its professional services

The company's RSA SecurID enterprise authentication products are protecting information in the majority of the Fortune 100 today, addressing the important need for easy, hacker-proof user authentication both inside and outside the corporate network. These same products are similarly used by leading eBusiness businesses, including securities trading and banking applications, to protect against external attack and fraudulent activity.

RSA Security holds a leadership position as the supplier of critical encryption and security technologies to most of the major IT vendors worldwide. While the average end user is unaware of the technologies underlying the operating systems, browsers, and tools he uses everyday, most of these products were developed using one or more of RSA Security's technologies. The RSA BSAFE line of encryption-based security technologies is embedded in over 450 million copies of today's most successful software applications, including web browsers, Internet commerce servers, email systems, and virtual private network products. The majority of all secure eBusiness and communications are conducted on the Internet using RSA Security technologies. Both RSA SecurID and RSA BSAFE are considered *de facto* standards worldwide.

RSA Security now also offers its customers the RSA Keon family of PKI products, a solution for enabling, managing, and simplifying public key authentication and encryption security. This technology is deployed in today's leading email, web browser, web server and VPN applications. Elements of RSA Keon are available on an OEM basis to allow application designers to build many core RSA Keon benefits into new applications. Other options are available to adapt existing, installed applications to gain RSA Keon security and management benefits.

Alliances and Partnerships

Recognizing that no single vendors can satisfy every customer's needs, RSA Security built its business through its commitment to interoperability. Today, the Company partners with over 500 industry leaders such as:

- 3COM
- AOL/Netscape
- Apple Computer
- Lucent
- AT&T
- Check Point
- Cisco Systems
- Compaq
- IBM
- Intel
- Microsoft
- Nortel Networks
- Novell
- Oracle

These partners integrate RSA Security technology into over 1,000 products.

Moreover, RSA Security's depth of alliances and partnerships is demonstrable. More than 200 of these vendors exhibit or present each January at the seminal security conference, the RSA Conference. Starting as a small gathering of like-minded cryptographers, this Conference attracted over 6,000 security professionals in 1999. For 2000, IDC expects over 8,000 Conference attendees all focused on using eSecurity to facilitate the growth of eBusiness.

Alliances and partnerships also extend to sales channels. To ensure that customers have the flexibility to purchase its products from multiple sources at various levels of integration, RSA Security has established a multi-channel distribution and sales network to serve the enterprise and data security markets.

The Company sells and licenses its products directly to end users through its direct sales force and indirectly through an extensive network of OEMs, VARs and distributors. The RSA SecurWorld channel program brings RSA Security's products to value-added resellers and distributors worldwide.

Continuous Global Support

Quality products and partners only partially satisfy customer requirements. Enterprise customers require continuous support (24 hours/day and 7 days/week) on a global basis because eBusiness is a global opportunity that never sleeps.

To meet this need, RSA Security operates offices in the US, Canada, United Kingdom, Germany, France, Scandinavia, Singapore, Korea, Hong Kong and Malaysia, with additional international expansion underway. In May 1998, the Company established a Japanese subsidiary to capitalize on the significant opportunity in the Japanese security market. In January 1999, the Company opened an international development center in Brisbane, Australia, where RSA Security develops and distributes strong encryption products to global markets.

Commitment

Commitment means that a vendor focuses on one area. It builds expertise in products, services, partnerships, and sales channels. To grow its business, it actively anticipates its customers evolving needs. Commitment also means focus. A large conglomerate whose security products only constitute a small percentage of corporate revenues may not hold a strategic view of its security products and the customers using these products. In the interests of vendor profitability, the customers' best interest may be sacrificed so that investments can be made in other technologies. When eSecurity products are an integral part of a customer's eBusiness architecture, this vendor selection criterion becomes particularly important.

Through its research arm, RSA Laboratories, and its code breaking competitions, the Company invests heavily in research and actively participates in relevant standards bodies. Both investments are critical to ongoing success in this marketplace.

In addition, RSA Security leads the industry in communicating information about security technologies to users and developers. Its annual RSA Conference and its online web site resources are examples of media the company has set up to increase understanding and use of IT security technologies.

RSA Security's offerings represent a set of open, standards-based products and technologies that integrate easily into organizations' IT environments, with minimal modification to existing applications and network systems. Standards provide interoperability, investment protection for existing applications, and the basis for greater security by eliminating holes that are sometimes created when two products fail to work together properly. RSA Security's solutions and technologies are designed to help organizations deploy new applications securely, while maintaining corporate investments in existing infrastructure. In addition, RSA Security maintains active, strategic partnerships with other leading IT vendors to promote interoperability and enhanced functionality.

Security as a Primary Focus

One of a handful of companies totally focused on security technology, RSA Security is well recognized for establishing public key cryptography and strong user authentication as essential IT tools. Its developers, sales force, and partners are focused on providing security solutions rather than leveraging the sale of other products.

Conclusion

The boom in eBusiness promises new markets and new opportunities for all forward-looking companies. Continued business survival demands the quick uptake of eBusiness opportunities. However, eBusiness participation also demands that enterprises understand, design and implement robust, flexible eSecurity infrastructures. The risks of inadequately secured eBusiness parallel the opportunities.

To ensure adequate eSecurity, organizations will need sophisticated professional analysis and planning, proven technology, and integrated security products. IDC recommends that organizations think security FIRST, assessing where and how security requirements differ. Then, given the range of security infrastructure frameworks and technologies available, IDC recommends selecting a strong and experienced security technology partner. Finally, IDC recommends that organizations select a partner, like RSA Security, with a long-term vision and a commitment to ongoing security innovation. With such a partner, enterprises can position themselves for growth in the rapidly evolving eBusiness space.

Corporate Headquarters
5 Speen Street
Framingham, MA 01701
508-872-8200

IDC Irvine
18831 Von Karmen Ave, Ste 200
Irvine, CA 92612
949-250-1960

IDC Miami
Latin America Headquarters
5301 Blue Lagoon Drive, Suite 490
Miami, FL 33126
305-267-2616

IDC New Jersey
120 Wood Ave South, Suite 509
Iselin, NJ 08830
732-632-9222

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212-726-0900

IDC Texas
100 Congress Ave, Suite 2000
Austin, TX 78701
512-469-6333

IDC Washington
8304 Professional Hills Drive
Fairfax, VA 22031
703-280-5161

IDC West
2131 Landings Drive
Mountain View, CA 94043
650-691-0500

IDC Argentina
Trends Consulting
Lavalle 715 - Piso 7 B
CP 1047 Buenos Aires, Argentina
54-11-4322-3159

IDC Asia/Pacific
2901-2, Universal Trade Center
3 Arbuthnot Road
Central, Hong Kong
852-2530-3831

IDC Australia
Level 4, 76 Berry Street
North Sydney
NSW 2060, Australia
61-2-9922-5300

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
A-1040 Vienna, Austria
43-1-50-50-900

IDC Beijing
Suite A18, Yintai Office Bldg.
A-137, Xizhimen Wai Dajie
Beijing 100044, PRC
86-10-6833-1179

IDC Benelux
29 Avenue Louis Gribaumont
B-1150,Brussels, Belgium
32-2-779-46-04

A. Fokkerweg 1
1059 CM Amsterdam
The Netherlands
31-20-669-2721

IDC Brasil
Alameda Ribeirão Preto, 130 cj 41
01331-000 São Paulo
SP Brazil
55-11-253-7869

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario
Canada M5C2C5
416-369-0033

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 12
Providencia, Santiago 9, Chile
56-2-231-0111

IDC Colombia
Carrera 90 No. 156-19, Piso 5
Santafe de Bogota, Colombia
571-682-4993

IDC East Central Europe
Male Namesti 13
Praha 1 110 00, Czech Republic
420-2-2161-2260

IDC Egypt
39 Iraq Street
Mohandesseen, Cairo, Egypt
20-2-336-7355

IDC France
Immeuble La Fayette
2, Place des Vosges, Cedex 65
92051 Paris la Defense 5, France
33-14-904-8000

IDC Germany
Westerbachstr. 23A
61476 Kronberg/Ts., Germany
49-6173-7098-0

IDC Hungary
Bajcsy-Zsilinszky út. 57
Building 3, Rooms 103-104
H-1065 Budapest, Hungary
36-1-153-0555/ext. 165, 166

IDC (India) Limited
Cyber House
35 (4 Bays)
Echelon Institutional Area, Sector 32
Guragon - 122002
Haryana, India
91-124-381673

IDC Israel
4 Gershon St.
Tel Aviv 67017, Israel
972-3-561-1660

IDC Italy
Viale Monza, 14
20127 Milano
390-2-284-571

IDC Japan
10F The Itoyama Tower
3-7-18, Mita Minato-ku
Tokyo 108-0073, Japan
81-3-5440-3400

IDC Korea Ltd
13th Floor, Textile Center
944-31, Daechi-3Dong
Kangnam-Ku
Seoul, 135-713 Korea
82-2-528-5100

IDC Malaysia
Suite 23.1 23rd Floor Menara Genesis
33 Jalan Sultan Ismail
50250 Kuala Lumpur, Malaysia
60-3-244-3715

IDC Mexico
Select - IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo, Condesa
C.P. 06100 Mexico, D.F.
52-5-256-1426

IDC Middle East Research Center
(with City Consultary)
M 04, Al Moosa Group Bldg
P.O. Box 27727
Umm Hurair Rd
Dubai, United Arab Emirates
971-4-362-200

IDC New Zealand
Level 4, 43 High Street
Auckland, New Zealand
64-9-309-8252

IDC Nigeria
House 2, 'C' Close
403 Road, 4th Avenue
New Extension, Festac Town
Lagos, Nigeria
234-1-883585

IDC Nordic
Jagtvej 169B
DK-2100 Copenhagen, Denmark
45-39-162222

Jarrumienkatu 2
SF-00520 Helsinki, Finland
358-98770-466

Kistagången 21, Box 1096
SE-164 25 Kista, Sweden
46-8-751-0415

IDC Philippines
W/S Research Group
7F, SCDCCO 1Bldg
Rada Street Corner
Legaspi Village
Makati City, Philippines
632-894-4808

IDC Poland/ProMarket
Wrobla 43
02-736 Warszawa, Poland
48-22-644-4105

IDC Portugal
c/o Ponto de Convergencia S.A.
Rua Leopoldo de Almeida 4A
1750 Lisbon, Portugal
351-1-758-3126

IDC Russia
c/o PX Post, RDS 186
Ulitsa Zorge 10
Moscow 125525
Russian Federation
7-501-929-9959

IDC Singapore
71 Bencoolen Street, #02-01
Singapore 189643
65-226-0330

IDC South Africa
c/o BMI-TechKnowledge
3rd Floor, 356 Rivonia Blvd.
PO Box 4603, Rivonia, 2128
South Africa
27-11-803-6412

IDC Taiwan
8F-3, #547
Kuang Fu South Rd
Taipei, Taiwan, R.O.C.
886-2-2729-6040

IDC Thailand
27 Soi Charoen Nakorn 14
Charoen Nakorn Road, Klongtonsai
Klongsan Bangkok 10600, Thailand
66-2-439-4591-2

IDC Turkey
Tevfik Erdonmez Sok. 2/1 Gul Apt.
Kat 9D; 46 Esentepe
Istanbul, Turkey
90-212-275-0995

IDC U.K.
6 Dukes Gate, Acton Lane
Chiswick, London W4 5DX
United Kingdom
44-181-987-7100

2 Bath Road
Chiswick, London W4 1LN
United Kingdom
44-181-987-7100

IDC Venezuela
Trends Consultores
Av. Francisco de Miranda
Centro Perú, Torre A, Piso 9
Of. 91, Chacao 1060
Caracas, Venezuela
58-2-261-0352

International Data Corporation delivers accurate, relevant, and high-impact data and insight on information technology to help organizations make sound business and technology decisions. IDC forecasts worldwide IT markets and adoption and technology trends, and analyzes IT products and vendors, using a combination of rigorous primary research and in-depth competitive analysis. IDC is committed to providing global research with local content through more than 500 analysts in more than 40 countries worldwide. IDC's customers comprise the world's leading IT suppliers, IT organizations, and the financial community. Additional information on IDC can be found on its Web site at http://www.idc.com.

IDC is a division of International Data Group, the world's leading IT media, research, and exposition company.

IDC
INTERNATIONAL DATA CORPORATION
5 Speen Street • Framingham, MA 01701
(508) 872-8200 • Fax (508) 935-4015 • www.idc.com

Sponsored by RSA Security
99-242SYSTEM2377