TRENDS

May 11, 2006

Secure The Data, Not Just The Underlying Infrastructure

by Paul Stamp

FORRESTER® Helping Business Thrive On Technology Change

TRENDS

May 11, 2006

Secure The Data, Not Just The Underlying Infrastructure

by Paul Stamp
with Ellen Daley, Erica Driver, Jonathan Penn, and Christine E. Atwood

EXECUTIVE SUMMARY

New business pressures mean that organizations need to share data across ever-widening organizational and geographical areas. However, at the same time, they are increasingly accountable for ensuring that data is properly protected, even when it resides on infrastructure over which they have little or no control. This has led organizations to look at ways to secure the data itself, rather than just the infrastructure that holds and transports it. What do they find? The technology to help them is still embryonic with only a few vendors offering solutions. Mainstream migration to a datacentric security model will take five years to evolve, but today, companies need to define a strategy for datacentric security starting with information classification and data encryption.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester interviewed 17 vendor and user companies, including: Adobe, AT&T, CGI Group, Cryptography Research, Cryptomathic, Entrust, IBM, nCipher, RSA Security, SafeNet, Trusted Computing Group, Wave Systems.

Related Research Documents

"Trends 2006: Identity Management"
February 14, 2006, Trends

"Securing The Network From The Inside Out"
November 2, 2005, Best Practices

"Mitigate Content-Related Risks With Enterprise Rights Management"
September 9, 2005, Trends

TARGET AUDIENCE

Chief information security officers (CISOs).

NEW BUSINESS DEMANDS RENDER OLD SECURITY MODELS OBSOLETE

CISOs are constantly challenged to align security with business strategy as well as manage information risk across new and existing initiatives.[1] Three major business changes affect how organizations approach security:

- **Increased data accountability.** Customers, business partners, and legislators demand greater accountability than in prior years when dealing with sensitive data. Some demands are very specific, like the Payment Card Industry (PCI) Data Security Standard, which has granular requirements for card payment data security.[2] Other regulations, like Sarbanes-Oxley, are less prescriptive but nonetheless demand a standard of care that drives many organizations to change the way they deal with sensitive information.

- **More intellectual property fluidity.** To remain competitive and accelerate time-to-market, leading organizations now share product information with a multitude of parties across the Digital Business Networks — like innovators, financiers, suppliers, and distributors.[3] In doing so, they rely on these parties to deal with their sensitive intellectual property. But, at present, this can only be enforced contractually, and corporations have no real control over the data and information once it is disseminated.

- **Highly distributed work environments.** Between 2003 and 2005, the number of teleworkers in the US increased by more than 9% and, in 2005, North American and European enterprises expected 23% of corporate users to take advantage of mobile applications while on the road.[4] This has led to an explosion in the number and diversity of people and devices that require access to corporate data. Moreover, greater globalization and international and organizational boundaries make it more difficult to enforce a consistent security policy.

Past Security Approaches Have Concentrated On Infrastructure Rather Than Data

Most security models today are hangovers from a time when: 1) fewer people used IT, 2) a more intimate relationship with users existed, and 3) you had the means and the authority to manage the devices they used to access your data. Consequently, this coziness and inherent trust meant that security systems were overlaid onto existing infrastructures as an afterthought. In addition, companies have had to retrofit security silently onto well-established business processes or older technology. For example, many organizations that deployed IP telephony a few years ago are only now introducing strong authentication and infrastructure protection measures. Today's security systems generally:

- **Leave data alone, and have the underlying infrastructure to secure it.** Any access controls for data that are in place today have been enforced by the infrastructure that stores or transfers the data. Once the data gets copied or moved to another place, it inherits the security of the infrastructure to which it is transferred. For example, sensitive data on an encrypted file server that users can only access over secure network connections can easily be transferred to an unsecured file server where data is not encrypted, thus taking away any protection that the data had.

- **Use blocking and tackling to enforce policy.** Most security systems rely on setting a policy, monitoring activity, and then taking action against violations to that policy. A better way? Build in measures to make sure that egregious activity doesn't happen in the first place. For example, an intrusion prevention system (IPS) looks for traffic that bears the hallmark of an attack and blocks it or alerts an IPS administrator. On the other hand, a network access control system prevents connections altogether that do not come from authenticated users, thus stopping the problem at the source.

- **Rely heavily on contracts and processes.** Once the data has left the confines of managed corporate systems, the only way to enforce policy has been contractually. The only checkpoint was verification of measures that are in place through audit — rather than tools to protect the data itself. Customers tell us that this drains resources for organizations that have many partners. They waste huge amounts of time auditing or being audited by them — with still only triage, rather than preventive results.

THE FUTURE OF SECURITY IS DATACENTRIC

Businesses need to prove that they manage sensitive data appropriately; however, simultaneously it is getting more difficult to exert control over the numerous places in which that data resides. Security measures can be characterized in one of the following two ways:

- **Infrastructure-centric measures**. Infrastructure-centric measures concentrate on protecting information by securing the infrastructure components that store, transmit, or process the data. One example is a personal firewall, which protects the client system that might store sensitive customer information from remote attackers. Another is a VPN, which protects the network connection that is used to transmit sensitive data. Most security in the past has concentrated on infrastructure-centric measures, which will continue to be important in the future, but only as part of a wider effort that directly addresses the security of the data an organization handles.

- **Datacentric measures.** Datacentric measures, on the other hand, protect the information directly, independently of the infrastructure components that store, transmit, or process it. One example is an encryption solution, which provides the means to encrypt a piece of data; and wherever that data travels, it remains encrypted. Only when an authorized user obtains the keys to decrypt the data does it become usable. Datacentric security measures have been less common in the past, but will be a central part of most organizations' security strategies in the future.

Datacentric Security Will Become The Primary Mode Of Infrastructure Protection . . .

To respond to new business pressures, organizations need to think about security differently. They will need to place a greater emphasis on securing the data itself, and use the infrastructure as a secondary layer of protection rather than as a primary layer, as it is today. Given these new challenges, security systems will:

- **Make security attributes travel with the data itself.** Data will be encrypted and protected by default, and it will be up to whoever needs it to get hold of the right keys and perform the right actions to unlock and use the data. That way, data owners don't need to be as worried about the security of where the information will reside. Contrast this approach with what's happening today, where users authenticate themselves, say, to the database or fileserver that holds the data, and the server performs the decryption before handing the unencrypted data to the user: The data is then only as secure as the user's device (see Figure 1).

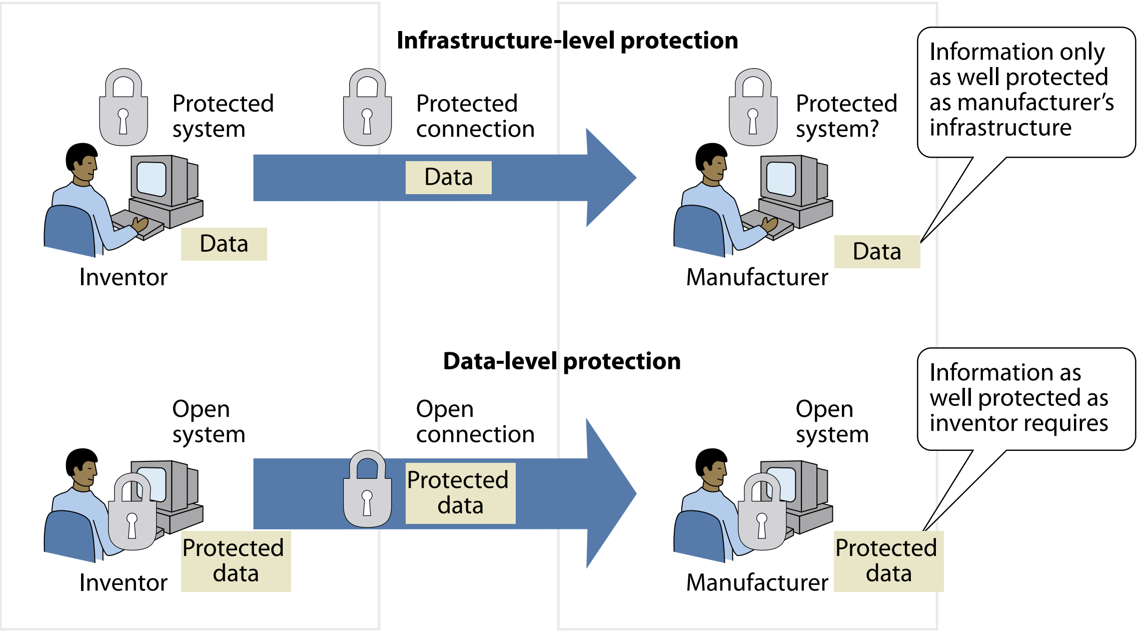
- **Enforce security policy at every stage in the information life cycle.** Data is stored, moved, presented, and transformed throughout its life cycle: New security mechanisms within systems need to interoperate better to ensure that they can consistently enforce policy around who can see, move, and modify data in that life cycle. Current measures rely on systems architects to manually piece disparate tools together to protect data at different points in the information life cycle. For example, organizations use separate mechanisms to encrypt data in the database, on file servers, and on the network, none of which typically interoperate.

- **Build security into the infrastructure from the ground up.** Infrastructure will still need to provide some security; however, infrastructure security will be more proactive. Infrastructure security systems need to be designed to strongly authenticate users and devices, and grant access only to the resources they need — they'll also be able to augment data-level security by providing information about the user's job function, and how well protected their working environment is. At the network level, this will mark a shift away from concentrating security efforts on firewalls, antivirus, and IPS — which will become more of a last line of defense — and more toward network access control and quarantine initiatives.[5]

. . . And Organizations Need To Focus On Secure Design And Information Protection

Organizations need to switch from a more defensive security model to one that places more emphasis on securing the information the infrastructure holds rather than the infrastructure itself (see Figure 2). What should organizations do?

Figure 1 Data-Level Protection In An Inventor-Manufacturer Relationship



39438 Source: Forrester Research, Inc.

Figure 2 Infrastructure Security Gets Complemented By Data Security

Old security model	New security model
Defensive, threat-protection-oriented	Securely designed from the ground up
Manual, audit-based policy enforcement	Automated policy enforcement
Focused on securing infrastructure	Focused on securing the data

39438 Source: Forrester Research, Inc.

- **Deploy more identity-driven security at the infrastructure level.** Identity is becoming a cornerstone of security. As organizations shift emphasis to secure design, they must concentrate more on technologies that enforce policy based on user identity and context rather than user behavior, once they've accessed the infrastructure.[6] Many organizations are already starting to evolve their use of identity management systems. Why? Primarily for policy enforcement through the implementation of role-based access controls as well as some efficiency gains.[7] At the network level, network access control solutions will proliferate and integrate with identity management systems.

- **Concentrate threat protection measures on critical systems.** Secure design technologies give greater visibility and control of who accesses the corporate environment. This will make threat protection technologies, antivirus, and IPS a second line of defense: meaning that organizations can deploy them closer to the assets that need to be protected rather than as a gateway to the corporation's computing environment.

  Some organizations, like participants in the industry group the Jericho Forum, de-emphasize the network perimeter as a security boundary and, instead, deploy firewalls and IPSes closer to the critical assets that are being protected.[8] For example, Ken Douglas, technology director at UK-based energy firm BP, recently announced to the UK Technology Innovation & Growth Forum that BP treats all users as Internet users, whether they connected from a BP-managed network or not.[9] Forrester expects more organizations to follow suit in the coming years, creating more open connections between corporate user networks and the Internet.

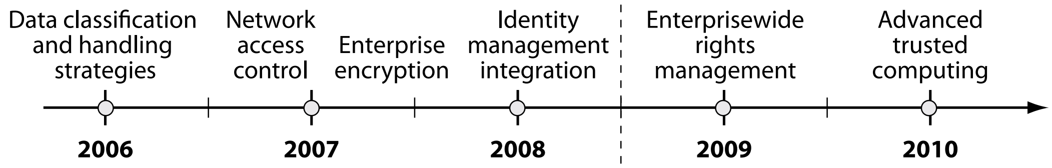
- **Adopt an enterprisewide approach to encryption.** Today's existing encryption solutions are usually single function — they encrypt data at only one stage in its life cycle: for example, when it's being transmitted in an email, or being stored on a particular file server. Most organizations have deployed a patchwork of encryption technologies to secure their data, usually in response to regulatory or contractual requirements. For example, the PCI standards have very strict requirements around encrypting data in transit and at rest. However, HIPAA lets organizations decide for themselves on the need to encrypt protected health information (PHI) in transit or at rest. This variability in requirements causes companies to adopt a more strategic approach to encryption. Organizations must look for solutions that can address their multiple data protection needs across infrastructure components, like email, databases, and file repositories.

A Datacentric Security Model Will Evolve Over The Next Five Years

Once organizations have identified the resources that they need to protect, and they've defined the right role profiles to get access to that data, new tools will complement existing security measures to allow organizations to enable data-level protection. This will take place in stages (see Figure 3):

- **2006–2008: Encryption, identity management, and network access control dominate.** Existing stovepipe encryption solutions will evolve into cross-platform offerings that share a common key management infrastructure, so the data can be protected consistently throughout its life cycle. Identity management solutions will start to interoperate with key management and document management systems to grant users access to the data itself, rather than just the system in which it resides, like applications, databases, and file servers. Network access control will underpin the system, ensuring that only trusted users and devices can connect and get access to the data.

Figure 3 Datacentric Security Timeline For Mainstream Organizations


Data classification and handling strategies
Network access control
Enterprise encryption
Identity management integration
Enterprisewide rights management
Advanced trusted computing
2006
2007
2008
2009
2010

39438

Source: Forrester Research, Inc.

- **2009–2010: Rights management and trusted computing enable true datacentric security.** Enterprise rights management (ERM) in the business world provides process-level security beyond plain old encryption solutions — it controls what users are able to do with the information once they access it.[10] Most companies that have deployed ERM have only done so for limited audiences that need very sensitive information, like confidential financial information. Although Forrester expects ERM adoption to be relatively slow in the next three years, datacentric security will be a catalyst for more widespread adoption in 2009 and 2010.[11]

Trusted computing — the term given to a framework that builds security into computing systems, from the hardware level up through a trusted platform module (TPM)— will help drive toward a datacentric model in this time frame because it provides hardware-level protection of the encryption keys and keeps them from falling into the wrong hands, and it gives data owners a level of assurance about the security of devices where sensitive information data needs to be transferred, even if it is outside of their control.[12] While some organizations have already started to use the key storage features of TPMs built into new PCs, Forrester expects widespread adoption of the advanced features of trusted computing to come with Microsoft's next major client operating system revision after Vista in the 2009–2010 timeframe.

A DATACENTRIC SECURITY MODEL IS A HARD TASK — BUT HELP IS APPEARING

The organizational shift from just securing servers and networks to securing data is no small task: It will require new technology and new business processes as data owners take more responsibility for securing their own data. However, the seeds are already planted in some mature organizations — and the vendor community is starting to offer solutions that can aid the process of change.

Interoperability, Maturity, And Governance Are Barriers To Greater Adoption

Early movers find that the business demands justify a datacentric security focus but face certain hurdles:

- **Datacentric technology is immature.** Few of the pieces for creating a comprehensive datacentric model are in existence today. Most organizations that have moved toward a datacentric model have had to use proprietary technology to do so. For example, Europe's

Standard Chartered Bank plans to expand into the developing world where the infrastructure simply won't support network-level encryption. Moreover, the company can't rely on the physical security of the environment where the data is going to end. As a result, it has developed its own proprietary solution to provide data-level encryption of information that it needs to distribute to associates in those parts of the world.

- **Existing solutions are not interoperable.** There are so many configurable options and architectural considerations in encryption solutions that product interoperability is usually a result of heavy integration work rather than true standards compliance. In other areas, like ERM, no universally adopted standards exist. This means that early adopters will experience vendor lock-in, at least in the medium term, while standard approaches to data-level security evolve.

- **Organizational slowness hinders wholesale changes.** Changing an organization to think about datacentric rather than infrastructure-centric security goes way beyond the security team. IT requires a new way of thinking across the IT organization and across the business. This means that early adopters will likely be large organizations with CISOs who: 1) are able to articulate the business value of datacentric security and 2) mandate appropriate changes across the organization and with business partners.

Vendor Community Rises To The Data Security Challenge

Data security tools are nothing new: Many of the players are veterans of the encryption and public key infrastructure (PKI) industry. Many have extended their legacy offerings to address the wider problem of data security.[13] For example:

- **Encryption vendors focus on solutions that span platforms.** Encryption vendors like nCipher, Ingrian Networks, and Venafi already have solutions that standardize encryption across applications, file servers, and databases. RSA recently released tools to automate the key management process plus solutions to easily set and enforce data-level security policy in homegrown applications. SafeNet has a wide range of encryption products that span platforms. And many organizations have had considerable success in integrating these products as part of an enterprise encryption strategy.

- **Entrust addresses information classification and handling.** Entrust takes a two-pronged approach to data-level security. It has added to its core competency in the encryption and identity management space and introduced content analysis technologies that can automatically classify and, if necessary, encrypt a document or message based on the natural language characteristics of its contents. In fact, Entrust has worked with systems integrator CGI Group to integrate automated classification and encryption features into the Canadian federal government document management system.

Other vendors have responded to customer needs by building features that enable data-level security into wider infrastructure and application technologies:

- **Trusted computing consortia address hardware-level security.** Millions of PCs containing TPMs that were developed by member companies of the Trusted Computing Group shipped last year, and companies are already taking advantage of some of its key storage and secure networking functionality. In Europe, the Open Trusted Computing (OpenTC) consortium and European Multilateral Secure Computing Base (EMSCB) are planning to extend this functionality across open source systems. This promises companies the ability to set and automatically enforce policies around verifying the security of a partner's computing environment before sharing data with it.

- **Adobe and IBM look to secure the collaborative design process.** Adobe and IBM Germany recently announced a partnership to provide the automotive, aerospace, and military technologies with a solution to control the distribution and use of intellectual property as it is shared between manufacturers and suppliers. In the automotive, aerospace, and military technologies industries, a single manufacturer might work with many suppliers, who in turn might each work with multiple other manufacturers. Thus, both sets of participants need a consistent ERM system: for manufacturers to protect their intellectual property, and for suppliers to protect their integrity.

RECOMMENDATIONS

PREPARE PROCESS AND INFRASTRUCTURE TO ACCOMMODATE THE NEW MODEL

Enabling a datacentric security model is not going to happen overnight. However, there are some things you need to start looking at to give yourself enough flexibility to manage risk around information handling. To get off the ground:

- **Start with information classification.** Revisit your data classification policy, if you haven't in the last year or so, and assess how well it: 1) is being used and enforced and 2) maps to your business processes. For data confidentiality, most organizations have three or perhaps four classifications. Create templates and workflows so that, at the time of data creation, data owners can determine how to classify the data, label and handle it, and make sure that only the right people have access to it. Rigid information classification schemes, like those typically found in government organizations, often prove overkill for organizations that need to share data freely. But many of the associated processes behind identifying the sensitivity of information and mapping that to a well-defined set of measures defines how well it needs to be protected and can be extremely useful to an organization.

- **Then, move onto roles.** Many organizations are looking toward role-based access controls to help them centralize access policy management and streamline the privilege management process.[14] Take a look at your existing role profiles: For a datacentric security model, you'll need at least some high-level roles that specify a user's general job function or business unit. This will greatly simplify data owners' task of granting access to their information based on its classification.

- **And get a handle on your encryption strategy — start with homegrown applications.** If your organization is anything like most organizations, encryption is currently a hodgepodge of tools and approaches. Identify all your encryption tools and consolidate where possible. Take steps to adopt an enterprise encryption tool, starting with homegrown applications, and create development standards so that everyone is using the same encryption and key management mechanisms in-house. Then, when selecting commercial applications, make compatibility with your encryption infrastructure a priority.

WHAT IT MEANS

eCOMMERCE FLOURISHES AND AUDITS FLOUNDER AS DATA-SHARING ISSUES DIMINISH

Greater control over information will allow data owners to share it with the parties they trust, safe in the knowledge that they won't accidentally or maliciously share it with anyone else. This means:

- **Overcoming the privacy pandemic will spur online commerce.** Forrester surveys show that consumers' trust in the privacy of their online data is dwindling, and this could threaten growth prospects for online commerce.[15] Applying a datacentric model to personal data will allow consumers greater control over access to their personal data. This will finally allay growing concerns over privacy and identity theft, because users will have direct control over the keys that govern access to their personal data: thus, rebuilding lost confidence in sharing it with "trusted" partners.
- **Security audit budgets will get slashed and burned.** Since more and more data controls will be actively enforced through technology rather than through ponderous assessments of organizations' infrastructure and processes, organizations will be able to do business with partners without innumerable painful security audits. This will drastically cut spending on expensive external audits, and free up budgets for security organizations to spend on securing new business initiatives.

ENDNOTES

[1] Increased business pressures of integrity, risk management, and compliance are driving information security into an expanded role and function in protecting the organization as a part of enterprise risk management. See the June 10, 2005, Best Practices "From IT Security To Information Risk Management."

[2] The Payment Card Industry (PCI) Data Security Standards provide a common set of standards for protecting credit and debit cardholder information. Source: Visa (http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf).

[3] Firms increasingly operate and compete as parts of networks of functions and companies — Forrester calls these Digital Business Networks (DBNs). Organizations participating in DBNs provide one or more of three specialist services: brokerage for orchestration, transformation for value creation, and customer interactions for responding to the ultimate customers' needs. See the January 26, 2006, Forrester Big Idea "Digital Business Networks."

[4] Telecommuting, defined as the number of employed Americans who performed any kind of work from home with a frequency as little as one day per year to full-time, grew from 41.3 million to 45.1 million in 2005 — a 9.2% growth rate. Source: "2005 American Interactive Consumer Survey" conducted by The Dieringer Research Group (http://www.workingfromanywhere.org/news/pr100405.htm). On average, enterprises that Forrester surveyed stated that they expect 22% of their workforce to use mobile applications. Source: Forrester's Business Technographics® May 2005 North American And European Network And Telecommunications Benchmark Study. See the August 16, 2005, Trends "Mobile Application Adoption Leaps Forward."

[5] With recent announcements by both Cisco and Microsoft, network quarantine has become IT security's hottest topic. Done right, network quarantine solutions will let firms enforce policy on every client that tries to join their networks. Firms can deploy a server- or port-based architecture for implementing network quarantine. See the August 3, 2004, Tech Choices "Making Sense Of Network Quarantine."

[6] As any security pro will tell you, the network perimeter is getting harder and harder to define, let alone defend. Moreover, those who have authorized access to internal resources are often far more dangerous than those who need to breach a perimeter firewall to get inside the network. Companies should adopt a twofold strategy of secure design and threat protection. How? By constructing a security life cycle that evaluates, assigns, segments, and monitors the network, according to security policies. See the November 2, 2005, Best Practices "Securing The Network From The Inside Out."

[7] This year, the primary driver for enterprise investment in identity management will shift from compliance to security and, specifically, to information protection. Compliance will continue to strongly influence market direction, but firms will focus on new areas, such as physical-logical security convergence projects and restricting privileged user rights. See the February 14, 2006, Trends "Trends 2006: Identity Management."

[8] The Jericho Forum, a powerful and vocal security user group that includes organizations like BP, Procter & Gamble, and the UK's Royal Mail, aims to change the way we think about IT and network security. The Jericho Forum claims that current security models that concentrate on the network perimeter just don't cut it in today's business environment. Jericho members introduced the concept of "de-perimeterization" and encourage organizations to look at securing the data rather than the infrastructure that supports it. See the July 8, 2005, Quick Take "Jericho Forum Looks To Bring Network Walls Tumbling Down."

[9] "By putting deperimeterization into practice, BP's technology director is hoping to make his company's computers more secure." Source: ZDNet UK (http://news.zdnet.co.uk/internet/security/0,39020375,39253439,00.htm).

[10] ERM is beginning to pick up steam among Forrester clients who are driven by needs for regulatory compliance, legal risk mitigation, and intellectual property protection. See the September 9, 2005, Trends "Mitigate Content-Related Risks With Enterprise Rights Management."

[11] ERM is still an early-stage market (estimated at $30 million in 2004) but it will grow slowly (20% a year, to reach $50 million in 2008) and steadily during the next three years, as it is on the cusp of becoming one element of the information workplace. See the September 9, 2005, Trends "Mitigate Content-Related Risks With Enterprise Rights Management."

[12] Trusted computing is a framework that builds security into computing systems, from the hardware level up through a trusted platform module (TPM). Source: http://www.trustedcomputinggroup.org/home.

[13] Technology pundits have long predicted huge growth in PKI, which has not yet materialized. However, recent rumors of PKI's demise have been greatly exaggerated. Vendors and experts have methodically chipped away at the barriers that have slowed PKI adoption and digital certificate use has grown steadily and evolved. See the January 14, 2005, Trends "PKI: Alice And Bob Have Still Got A Job."

[14] IT departments are increasingly interested in role-based access control (RBAC) models, especially the groups tasked with security or compliance. However, adoption lags because the RBAC model remains poorly understood. Forrester recommends business views and compliance considerations drive role development from the top down. Focus on a few higher-level roles, organized hierarchically to keep the model stable. See the June 23, 2004, Best Practices "Building A Role-Based Access Control Model."

[15] As computer attacks on consumers and companies mount, consumers are losing trust in the Internet as a channel for doing business. Companies must respond by addressing security in a way that aligns with consumer concerns, providing four types of protection: identity assurance, usage assurance, service assurance, and privacy assurance. They must also highlight security as an integrated feature of their services to address the emotional issues around lost confidence and trust. Thus, smart companies will aggressively pursue and promote new technologies that offer such consumer protections, similar to the way today's automobile manufacturers market safety. See the February 24, 2005, Best Practices "Rebuilding Consumers' Trust In The Internet."

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

- Australia
- Brazil
- Canada
- Denmark
- France
- Germany
- Hong Kong
- India
- Israel
- Japan
- Korea
- The Netherlands
- Switzerland
- United Kingdom
- United States

For a complete list of worldwide locations, visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®