The Technology Guide Series

Visit techguide.com

This Technology Guide is one in an ongoing series of over 100 solutions-focused Guides. These Guides assist IT professionals in making informed business decisions about specific aspects of technology development and strategic deployment.

The Technology Guide Series® offers a broad array of titles, each presenting objective information and practical guidance in a non-biased, "easy-to-understand" style and tone. Our editorial writing team has many years of experience in IT and communications technologies, and is highly conversant in today's emerging technologies.

The Technology Guide Series and techguide.com are supported by a consortium of leading technology providers. The Sponsor has lent its support to produce and publish this Guide.

This Guide, as well as the entire Technology Guide Series, is made available to view and print at no charge by visiting techguide.com.

Securing E-Business

Over 100 Technology Guides in the following categories:

- Software Applications
- Network Management
- Enterprise Solutions
- Network Technology
- Telecommunications
- Convergence/CTI
- Internet
- Security

produced and published by

techguide.com

This Guide has been sponsored by

Tivoli

Table of Contents

Abstract	2
Introduction	3
Requirements for an E-Business Security Solution	7
A Coordinated Approach to E-Business Security	12
Monitoring Technology	20
Conclusion	22
Case Study	24
Glossary	30

Editorial Writing Team

ATG's Technology Guides and White Papers are produced according to a structured methodology and proven process. Our editorial writing team has years of experience in IT and communications technologies, and is highly conversant in today's emerging technologies.

209 West Central Street, Suite 301, Natick, MA 01760
Tel: (508) 651-1155, Fax: (508) 651-1171
E-mail: info@techguide.com, Web site: http://www.techguide.com

Abstract

E-business is a powerful tool for business transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for suppliers and employees. However, implementing the e-business applications that provide these benefits may be impossible without a coherent, consistent approach to e-business security.

Traditional network security has focused solely on keeping intruders out using tools such as firewalls. This is no longer adequate. E-business means letting business partners and customers into the network, essentially through the firewall, but in a selective and controlled way, so that they access only the applications they need.

To date, organizations have controlled and managed access to resources by building authorization and authentication into each e-business application. This piecemeal approach is time-consuming, error-prone, and expensive to build and maintain.

Emerging technology provides a new role-based access control infrastructure for all of the enterprise's e-business applications. With this infrastructure, developers no longer need to code security features into each application. This can greatly speed up and simplify the deployment of new applications, cut maintenance costs, and give organizations a consistent security policy. This new access control infrastructure also lets organizations implement consistent privacy policies and ensures that authorized people are denied access to sensitive business information sources.

In addition, a centralized security solution lends greater flexibility to supporting new technologies such as mobile Internet devices, which are expected to proliferate over the next few years.

Besides controlling access, organizations also need to monitor security events across the enterprise so that suspicious activities can be quickly pinpointed. This is becoming critical as enterprise networks grow rapidly in complexity and strategic importance. New monitoring technology lets organizations consolidate data from all their disparate security sensors—firewalls, anti-virus software, host systems, and routers—and provides a coordinated single image of potential intrusions for effective incident response.

Introduction

Organizations cannot ignore the potential of e-business. Companies now have the opportunity to integrate supply-chains with their strategic partners, which lets them cut costs and accelerate business processes. These companies can reach new customers with e-commerce applications, and then keep those customers happy with online customer service. Companies can improve employee satisfaction and lower administrative overheads with intranet applications. Indeed, organizations that ignore these potential e-business benefits run the risk of becoming uncompetitive.

These new e-business applications often replace human relationships with electronic interfaces. As Web applications become the interfaces to customers and partners, businesses need to provide the same level of trust and confidence through these Web interfaces that they have historically provided. The security technology that underpins these e-business applications is vital in building this trust, enabling partners and customers to have confidence in the electronic relationship. Security is, in effect, the glue strengthening the relationships and helping to tie a business more closely to its customers and partners.

These requirements mean that the security technology needed for e-business is very different from the tools traditionally used to protect an enterprise network.

Traditional enterprise security has focused almost entirely on keeping intruders out by using tools such as firewalls and content filters. This approach, however, doesn't fit the security demands of the emerging world of e-business. Now organizations want to make enterprise systems and information more available to internal employees as well as people outside the organization like business partners and customers. At the same time, they need to maintain tight controls over exactly which information and applications are made accessible to which users.

This desire to provide wider access has emerged at a time when security has become a topic of huge concern. With security breaches attracting national attention, there are strong reasons for corporations to pause before putting critical systems online. Security has corporate image implications, in addition to real business and legal implications. Businesses need to be certain of the integrity of their solutions before opening up their networks.

These new priorities—a need to allow wider access to systems, accompanied with heightened concerns over network security—mean that existing security products, though useful, are inadequate. Traditional barriers such as firewalls and content filters can help prevent viruses from corrupting the network and intruders from stealing sensitive data, but a more sophisticated approach is needed to provide strategic partners and customers with the ability to fully leverage e-business applications. In addition, corporations need to protect applications from unauthorized use by users within their own organizations.

So far, businesses have generally tried to resolve access and security problems by building authorization and authentication functions separately into each of their e-business applications. This piecemeal, one-application-at-a-time approach requires considerable software expertise, is time-consuming, and is expensive. It slows application deployment in a business environment where time to market is often critical. Finally, this approach becomes increasingly unsustainable as an organization's e-business portfolio grows, and as online interactions between companies become more complex.

Nevertheless, businesses have had little choice but to take this piecemeal approach, because of the absence of products capable of providing a security infrastructure for all their e-business applications. Though security infrastructure products have been widely used in the mainframe environment for years, the emergence of e-business has been so rapid that technology of comparable scope has not, until recently, been available for distributed Web-based systems. The situation is changing, however, and this Guide describes the infrastructure technology that is emerging onto the market.

An e-business issue that has become a major concern is the need for privacy protection. Many e-business applications store information about customers or employees. Often, the value of the application is directly dependent on this information. Indeed, an e-commerce site may be personalized to fit each customer's needs, using stored information about the customer.

Businesses that store this information need to protect it from unauthorized use. There are legal, ethical, and business reasons for this pending in the major markets, requires businesses to implement specific levels of privacy protection, and track changes to personal information. Often, businesses choose to publicly declare their privacy policy in order to assure customers that their information is safe. It is essential then that the declared policy be consistently implemented in each application.

Privacy requirements can be considered an extension of other e-business security needs. The goal is to provide access to specific information, but also to ensure that only the right level of access is provided to exactly the right people.

It is clear that implementing privacy protection separately within each application creates problems with regard to development, maintenance, and consistency. These are similar to those problems caused by a piecemeal approach to e-business security in general. To avoid these problems, it makes sense that enterprises use a coherent and all-encompassing infrastructure for e-business security as well as privacy policy, giving businesses the option of using a single technology for both areas. Implementing an infrastructure technology for authentication, authorization, and privacy protects the organization's e-business applications from inappropriate use.

In addition, as networks grow larger and more complex, there are further needs to monitor the network as a whole to minimize the risk of intrusion. Today, businesses use firewalls, intrusion detection systems, anti-virus software and other tools to prevent unauthorized network access. However, each of these products only handles specific aspects of the problem, and there is little coordination between them. This can result in a dangerous information overload as each product generates large numbers of alarms in an attempt to provide a warning of potential problems. This makes it difficult for administrators to quickly pinpoint the real source of a problem.

There is a technology infrastructure available today that can correlate incoming information from many different products, as well as from servers, routers and other network elements. This minimizes the business risk associated with network intrusions by letting administrators rapidly identify and respond to network problems. The technology can also automate corrective action to common problems.

Requirements for an E-Business Security Solution

The demands on a comprehensive e-business security solution are considerable. Businesses need a rock-solid, easily managed, extensible hardware and software security infrastructure that must satisfy a demanding set of user and developer requirements.

Since this security system will play a part in every user's interactions with an e-business application, it must meet user expectations in every area, including performance and transaction integrity. The system must also meet the needs of e-business system developers and provide capabilities such as speed of deployment and scalability, as well as providing the flexibility to accommodate evolving technologies such as wireless devices.

These requirements can be grouped into three general categories: The e-business needs of users and developers; support for pervasive computing; and support for specific security functions.

E-Business User Requirements

As an integral part of the e-business environment, the security solution must be constantly available. In addition, because the solution handles each user's access to the e-business environment, performance must be carefully considered. Other key user requirements are assuring the integrity of the transactions and assuring the privacy of the information. Both of these requirements are essential to building trust in the electronic relationship.

Availability

Often, the availability requirements for e-business applications are greater than those for the human relationships that they replace. It's com-

monly acknowledged that e-commerce and other customer-facing Web sites are available day and night. Clearly, the same requirements apply to the e-business security infrastructure.

Performance

Users have a low tolerance for unresponsive e-business systems. If users don't find the system responsive enough for their needs, they will rapidly lose faith in it and look to use other methods or other business partners.

Integrity

In order to place their trust in the system, users need to have confidence that transactions will be secure. It is the job of the security infrastructure to underpin user confidence by ensuring appropriate levels of authorization and authentication.

Privacy

Users must be confident that their privacy will be protected against unauthorized access both from outside an organization and from unauthorized people within an organization.

E-Business Developer Requirements

Developers of corporate e-business systems place exacting requirements on the technology they use to build the e-business environment, and with good reason. These developers are under intense pressure to get systems up and running quickly, as well as to accommodate changing requirements. This means that the e-business security infrastructure must satisfy specific needs for speed of deployment, flexibility, scalability, and manageability.

Speed of Deployment

Typically, developers of e-business systems are under tremendous pressure to get applications online quickly. For example, a supply-chain application may be immediately needed to cut inventory costs and keep the company competitive as its industry moves to supply-chain integration.

Flexibility

The development pressure often does not go away once the initial version is up and running. The rapidly evolving nature of e-business means that requirements are also changing rapidly. As a result, new pressures mount to add more capabilities. Solutions must be flexible enough to support this pace of change.

Scalability

As some organizations have found, it is extremely difficult to predict the demand for e-business applications. Applications may have to handle sharp spikes in demand, or overall use that rapidly accelerates to unexpected levels—perhaps even millions of users. To avoid a potentially disastrous inability to meet user expectations, it's important to look for solutions that will scale smoothly.

Manageability

An e-business solution should increase business efficiency—not create additional administrative burdens. A security solution should be easily managed, and remain so as it grows to support the organization's expanding e-business environment.

Support for Pervasive Computing

An e-business application and its security infrastructure must be able to handle user access "any time, from anywhere." Over the next few years companies will expect to be able to access systems with non-traditional clients, like wireless thin-client handheld devices, which are beginning to proliferate worldwide. Market-research firm IDC estimates that the number of mobile Internet users worldwide is growing at a compound rate of more than 100% a year, and will reach more than 500 million by 2004.

Businesses must plan their e-business security approaches to provide the maximum flexibility in accommodating current and future generations of these wireless devices. One approach is to channel all access, whether from mobile or desktop devices, through the same security infrastructure. This means that users can get exactly the same access rights no matter whether they are accessing systems from a desktop or mobile device.

This approach also reduces the development effort because it avoids the need to build a separate security infrastructure to handle a wireless population that may grow to tens of thousands of handheld machines. These devices are handled by the scalable, reliable infrastructure that is already in place, and if security policies change the changes are automatically applied to all devices.

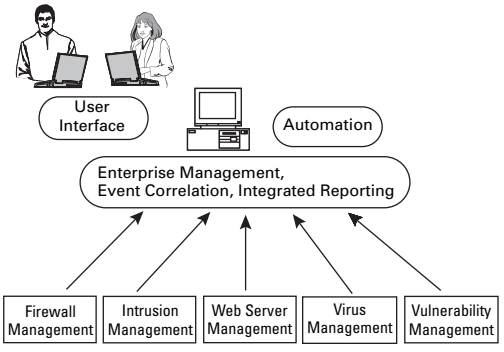
To ensure that e-business systems are flexible enough to support this approach, businesses need to look for products that are being extended to embrace wireless access. Enterprise e-business security technology should be able to work with standards-based Wireless Access Protocol gateways, so that incoming access requests from wireless networks are directed to the existing enterprise security infrastructure, where users can be authenticated and authorized.

Businesses also should ensure that the security infrastructure is extremely scalable. Typically, the requirement to support wireless access involves adding large numbers of new devices to the environment, and the infrastructure must be able to handle it.

Specific Security Tasks

It may be useful to contrast the role of an e-business security solution with that of traditional network security tools. Traditional tools, such as firewalls, are designed to exclude potential intruders. In contrast, an e-business security solution supports the business need to let in selected outsiders. Partners and customers need access, but that access must be limited to specific systems.

Figure 1: Enterprise Monitoring



Another difference is that the e-business security solution must ensure that both outsider access and insider access must also be controlled. Surveys have shown that unauthorized access from within the organization is a widespread and fast-growing threat.

To support these needs and protect the e-business environment and its users, the security solution should handle several specific security tasks:

- *Authentication and authorization* — To control access to applications and resources, the solution must first to be able to identify users with confidence. This process is called authentication. There are many methods for doing this, ranging from simple usernames and passwords to token-based technologies and digital certificates. Once users are authenticated, the security solution should define and control exactly which resources they are allowed to use. This process is called authorization.
- *Monitoring* — Today's networks are large, heterogeneous and complex. Even with a security infrastructure in place to protect e-business applications, there's still a need to monitor this

environment for attacks and misuse. This requires a centralized tool that can monitor the many elements in a complex network and correlate information from them, in order to quickly identify problems so that action can be taken.

A Coordinated Approach to E-Business Security

Once the organization has defined a clear list of security requirements, it can begin to identify technology that meets its needs. By combining authentication and authorization with monitoring technology a comprehensive e-business security solution can be built.

First, authentication and authorization technology is used to control access to e-business applications. This technology is valuable for any organization building e-business applications. Businesses should evaluate the technology's capabilities in multiple areas:

- core authentication and authorization functions, including single sign on
- the ability to set policies for security
- support for existing enterprise software
- manageability
- scalability and reliability
- privacy
- software quality

Second, monitoring technology minimizes the business risk associated with potential network intrusions. This technology is particularly useful for organizations with large, complex networks. Key features to consider are the technology's ability to correlate information from a wide range of data sources; its ability to automate responses to routine problems; and its manageability.

Authentication and Authorization Technology

To date, Web application developers have generally coded security logic into each of their applications. Each application had to maintain its own access control list of users, resources and the rights granted to each user. As the e-business environment grows, this approach rapidly becomes problematic for several reasons:

- It is expensive because of the need to replicate development and maintenance work across multiple systems.
- It requires time-consuming development when there is often corporate pressure to get online as quickly as possible.
- Maintenance is time-consuming and error-prone. Once the applications are online, it is vital to ensure that access control lists are kept up to date and in step across multiple applications, and to make sure that as security policies change, those changes are simultaneously reflected across the whole e-business environment. Each of these steps is an opportunity for error, inconsistency or delay, and can result in security loopholes.

An alternative approach is now possible. Technology is available that provides a security infrastructure for all of an enterprise's Web-based applications, eliminating the need to code and maintain security logic for each application. This approach has been accepted as a standard method for developing mainframe applications for years, but the technique is only now being extended to Web applications.

To be capable of managing access to the entire environment, this software should handle a broad range of functions.

Authentication and Authorization

The fundamental requirement is for technology that handles the authentication and authorization of all users (whether inside or outside the enterprise) accessing all e-business applications. All user attempts to access an e-business system are handled by the security infrastructure technology, which authenticates the user and grants the appropriate access to the requested system or systems.

Many authentication methods exist, ranging from simple usernames and passwords to stronger methods such as tokens or digital certificates. Different types of authentication methods may suit different organizations. Applications and access methods tend to become less convenient for users and become more expensive as they increase in security.

Passwords and usernames encrypted on transmission may be adequate for some resources, and may be the most practical approach for access via mobile devices that have limited computing power. For access to sensitive business information, token-based products or digital certificates may be more appropriate. An additional factor is that organizations may have already installed one of these authentication technologies and want to extend use of the technology for new e-business applications as well.

A solution should be able to support all of these techniques, which implies that it must be able to interface to the leading specialized authentication technologies, such as Tokens from RSA, or PKI systems from Entrust or IBM. A major advantage of a security infrastructure is that organizations should not have to change their application logic in order to change or add new authentication technologies. Further, they should be able to implement changes at the security infrastructure level and have applications evolve transparently.

In many cases, centralizing security into an infrastructure product has the additional security benefit that of removing the need to hold authorization information in multiple places, such as application servers and desktops.

Adopting a security infrastructure also means it should not be necessary to change the security logic in applications in order to take advantage of new devices—a major consideration when organizations are looking at supporting access from thousands of handheld wireless devices during the next few years. The infrastructure should be able to handle access via wireless networks and handheld devices, so users can access applications whether at home, in the office, or on the road. This means that it must interface to the gateways that handle traffic from wireless networks.

Single Sign-On

A related and extremely useful benefit in some technology is the ability to provide single sign-on to all corporate applications. When security logic is coded into each application, the number of passwords and logins that users have to remember and enter grows along with the number of e-business applications. This also imposes a considerable management burden. Administrators have to add users to each system they will use, and delete them from each system if they no longer have access. Because the security infrastructure maintains authorization information for each user and resource, it is able to authenticate the user once, and then seamlessly provide access to each system the user is authorized to use.

Policy Setting

An infrastructure product provides a central point for implementing security policy across the organization. Ideally, a product will allow the establishment of security policies that reflect the structure of the organization, yet are flexible enough to fit the needs of specific groups or

applications. The default policy for employees could be to provide access to human resources and other general corporate information. Specific needs of different groups can be met simply by creating new group profiles where needed. For instance, marketing people might get access to the default systems plus specific sales information. This approach avoids the need to define and maintain separate sets of access rights for each user.

Support for Existing Enterprise Software

The solution should integrate with existing enterprise applications, so that an organization does not have to build and maintain two independent security infrastructures. This means that the solution should support standard interface technologies used by other applications. In addition, provide integration with specific products that are widely in use. The infrastructure should also be able to take on security tasks for other applications. Finally, it should be able to make use of existing authorization policies by accessing security technology that is already in place.

One key interface is the Authorization API (aznAPI), an industry standard supporting a full set of authorization services. AznAPI can be accessed from applications based on standard technologies such as C, CORBA, and Java. AznAPI support also enables other applications to use the e-business security infrastructure for authentication and authorization, making it easier to extend existing applications to the Web.

In addition, custom interfaces to specific industry-standard products speed the process of integrating with existing applications. An example of such a product is IBM's MQSeries, a message-passing technology that is widely used for application-to-application communications.

Another key standard is Lightweight Directory Access Protocol (LDAP), a standard directory interface. LDAP-compliant directories are used by many organizations and applications to store user and other information. An LDAP interface enables a security infrastructure to accommodate and integrate with LDAP-compliant products.

Manageability

The security solution occupies a central role in the e-business environment, and will be heavily used by administrators to maintain the access rights for all e-business applications. Manageability is key in keeping administrator workload to a minimum. The solution should let administrators define access rights for all users and applications from a central console. A role-based approach reduces the everyday workload by minimizing the need to set up access rights for individual users.

An additional useful feature, particularly in large organizations, is the ability to delegate subsets of management authority to different groups. This means that a business unit can be given responsibility to make changes for its own users, or that management tasks can be delegated to specific administrators.

Scalability and Reliability

E-business involves being available 24 hours a day, seven days a week.

The solution must be offered on well-supported, highly scalable server platforms and capable of operating in redundant configurations for increased reliability. It should also be able to operate in replicated, load-balanced configurations across multiple servers so that organizations can be confident that the software will scale to meet demands.

The security infrastructure can play a further role in improving resource use across the e-business environment. Because it processes all access requests, the infrastructure is in a position to direct requests to the least heavily used resources. In an environment where replicated e-business application servers are used to meet demand, the security structure can play a load-balancing role by monitoring server use and directing incoming requests accordingly.

Privacy

Many applications hold personal information about customers or employees. Protecting the privacy of those individuals is becoming an issue of great concern, particularly with emerging legislation in many countries aimed at preventing and punishing unauthorized use. Many organizations have developed privacy policies for ethical and legal reasons that define how they handle personal information. It's essential that the organizations are able to implement privacy policies, and the e-business security solution provides a powerful tool for that purpose.

Implementing privacy policies often requires fine-grained control over information access. For instance, an Internet financial application may allow only a named account advisor to change the financial information held in a specific customer record, although any bank teller can change limited information such as address and telephone number.

Traditional methods of implementing this fine-grained control involve generating huge access control lists that map each user's access permissions for each account. However, a policy-based security infrastructure can be extended to support privacy policies using a much simpler, less laborious approach. This approach defines rules for accessing account information based on the relationship between the data and the person trying to access it.

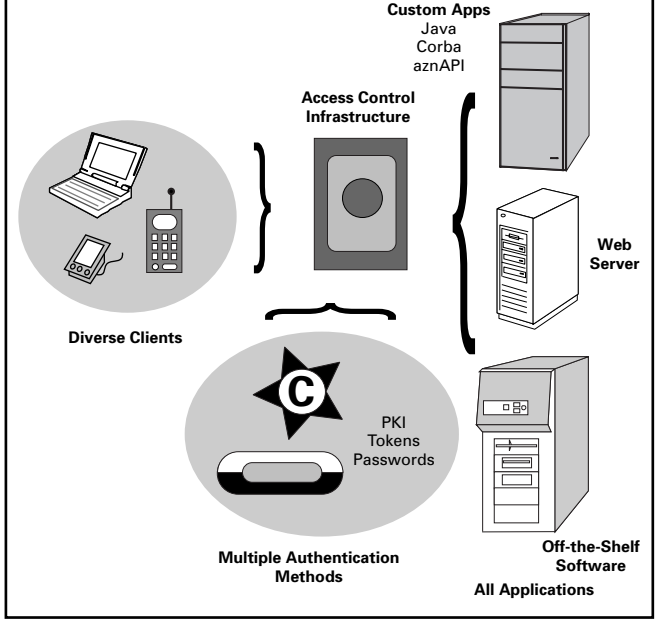
The ability to extend the security infrastructure to handle privacy provides the same kind of advantages as using the infrastructure for e-business security in general. The software can be used to define privacy policies across the organization in the same way as authorization policies. This reduces the programming effort involved in implementing privacy controls within each application. This also means that changes to privacy policy can be implemented centrally and take effect immediately in all applications. Instant changeability is key as the rules governing storage of personal information may change rapidly in response to impending legislation in the United States and other countries.

Greater Assurance through Software Quality

Most security breaches result from exploiting programming errors. A commercial, supported security solution has far greater programming resources behind it than one developed in-house.

In addition, using a commercial solution frees in-house developers to focus on implementing business application logic.

Figure 2



Monitoring Technology

By implementing authentication and authorization technology, a business can ensure that specific e-business resources such as applications and databases are protected from unauthorized access. Even so, there is a need for monitoring technology that can keep track of potential security problems for the network as a whole.

Malicious attacks on business Web sites have become a well-publicized phenomenon. Successful attempts to penetrate the security of business systems, or bring Web sites to a halt by generating huge amounts of traffic, regularly make headlines. It may not be possible to completely eliminate the business risk caused by such attacks. However, it is possible to take advantage of new technology that can help minimize the risk by identifying the threat and enabling the organization to react quickly.

To protect themselves against attacks, organizations have traditionally implemented a variety of technologies at the network boundary. These include:

- firewalls aimed at excluding attackers by admitting only certain types of network traffic
- intrusion detection systems that monitor the network or specific resources for anomalies such as the presence of unauthorized traffic
- filters to remove viruses before they spread to thousands of desktops

In addition, specific network elements such as Web servers, routers and application servers may attempt to detect problems. As a network grows, so does the number of these devices.

Each of these products generates information designed to alert administrators to potential dangers. This, however, rapidly leads to an overload of management information. Network problems may result in streams of alerts being generated by multiple products that detect the problems. Though each specialized product may be effective at sensing the problem, there is no coordination between them. In addition, not all alerts can be relied on to accurately indicate a real problem. Products such as intrusion detection systems generate numerous “false alarms” in an attempt to warn of network anomalies.

The result is that floods of alarms often swamp administrators. Dealing with this consumes large amounts of administrators’ time and hinders them from determining the real causes of the problems. This poses a considerable risk, because of the delay in being able to react to the original network intrusion.

However, technology is now available to ameliorate this problem. New monitoring tools correlate all of the information from these data sources and help determine and prioritize which are the most important events. To be most effective, the solution needs to interface with a wide range of security products and other sources of network alarm data and interpret the alarm messages coming from them. Because the number of potential data sources is vast and growing, this is not an easy task.

The technology correlates alarms from each of these devices to present administrators with a clear view of the real problem. The goal is to identify which alarms refer to the same problem and to eliminate the overhead caused by dealing with false alarms.

Automating responses to routine problems: Some events, such as the detection of a virus in incoming email, can be clearly identified by the monitoring technology, and therefore can be handled with a routine response. For this type of event, the technology can be set up to take automatic action, saving administrators considerable work in dealing with unambiguous everyday problems.

Manageability: Because this technology is integrated with an enterprise console, it can use the administrative features of an enterprise management system. These include the ability to delegate different management problems to different administrators. Administrators and security managers also can use capabilities of the enterprise management software to analyze network security by viewing historical reports of network data.

Conclusion

Enterprises that take advantage of e-business can reap the rewards of increased revenue, streamlined processes, and closer ties to suppliers and customers. However, the increased reliance on Web-based applications and the desire to open up networks to partners and customers inevitably generates greater concerns about the complex area of Internet security. These concerns are likely to grow as the Internet becomes an even greater part of everyday life.

Implementing an effective Internet security strategy is not easy. Still, new technologies enables businesses to make the security of Web-based applications much more manageable. These technologies provide ways to centrally implement policies to enforce security for all e-business and legacy applications. In addition, they accomplish this while retaining the flexibility to allow specific users and groups access to only the applications they need. By using these technologies, organizations will be able to implement approaches to e-business security that is as strategic as their overall approaches to e-business. Simply buying key technologies will not automatically solve problems. Expertise and careful implementation strategies are as critical as ever. When dealing with multi-faceted problems, organizations will find considerable benefits in seeking the help of experienced consultants and implementation partners. With the right help and technology in hand, Internet security may not seem as daunting a task.

T. Rowe Price Web-Based Applications Secured By Tivoli

T. Rowe Price and its affiliates manage about $147.8 billion in assets for more than seven million individual and institutional accounts and serve as investment manager to the T. Rowe Price family of no-load mutual funds. Founded in 1937, T. Rowe Price is the third largest no-load fund manager in the country, offering investors more than 75 different funds, discount brokerage services, and a wide range of electronic services and investor assistance tools.

The Business Challenge

Change moves at Internet speed in the financial services industry, and the ability to roll out applications quickly is essential to maintain an organization's competitive advantage. In order to provide improved access to its services, T. Rowe Price develops many new corporate applications each year.

To give customers easier access to information about their financial accounts, and provide new self-service options, T.Rowe Price wanted to give customers access to their accounts over the Web. The company had the ability to develop Web-based applications that could do this. However, in order to make that kind of information available over the Internet, T. Rowe Price needed a uniform security implementation for its network resources to ensure that information could only be accessed by appropriate people.

The IT Challenge

In order to develop new applications quickly enough to maintain its competitive advantage, T. Rowe Price needed to reuse services as much as possible. T. Rowe Price had defined a next-generation target architecture for its network based on Java and CORBA. This model emphasizes a distributed, component-based object-oriented architecture leveraging CORBA-based shared services. Unfortunately, current CORBA implementations do not provide security, and T. Rowe Price did not have a standard security implementation for its Web and other applications. Authorization was being coded into each corporate application, with much duplication of effort. This was slowing development and creating a complex security infrastructure.

T. Rowe Price needed to address the following issues:

- Multiple security implementations - Authorization was being coded independently for each application, leading to multiple implementations of the same functionality.
- High TCO security infrastructure - Each application's security framework had to be developed, tested, and administered separately.
- Multiple logins - Each application provided its own authentication, making life difficult for users.

The Solution Requirements

T. Rowe Price needed to implement an authorization framework that could be accessed by all applications. This framework would allow central management of access control policy and ensure that all applications were using trusted security mechanisms. To make Web-based access to information and self-service applications usable to its customers, T. Rowe Price needed to provide a single sign-on to all resources being accessed over the Web, including Web gateways to data in legacy systems and CORBA applications.

Project Description

T. Rowe Price has decided to deploy Tivoli SecureWay Policy Director to provide the authorization framework for its applications. Tivoli SecureWay Policy Director's strong access controls and its ability to secure Web, CORBA, and legacy applications will give T. Rowe Price the ability to standardize its applications on Tivoli SecureWay Policy Director security. Tivoli SecureWay Policy Director's flexible authentication model allows users to authenticate securely over the Web using a user name and password or a digital certificate from any SSL-enabled browser, and Tivoli SecureWay Policy Director provides a single sign-on to all resources that a user is authorized to access. Users will then be able to view their own account directly from the T. Rowe Price Web site. Deploying Tivoli SecureWay Policy Director allows T. Rowe Price to provide authentication and authorization as a shared service, rather than requiring authentication and authorization to be independently developed for each application. This results in shorter development and deployment cycles.

Benefits with Tivoli SecureWay Policy Director

- Tivoli SecureWay Policy Director allows T. Rowe Price to provide secure Internet access to new services to more customers. With Tivoli SecureWay Policy Director, T. Rowe Price can provide access to new services through an Internet connection using an SSL-enabled browser. This eliminates the need for proprietary client software, and provides a self-service option for many procedures that were previously handled by phone, fax, and mail. Because applications use Tivoli SecureWay Policy Director security, developers do not need to code authorization into each application. This means that user registries and authorization information do not need to be maintained for each application.
- Tivoli SecureWay Policy Director will give T. Rowe Price's users a single sign-on to the corporate Web and CORBA environment. Tivoli SecureWay Policy Director reduced the number of logins required to access some systems. With Tivoli SecureWay Policy Director, T. Rowe Price has a unified view of security for its network resources, and the ability to centrally manage security for all those resources. This reduces administrative overhead and the possibility of security breaches due to inconsistent policy or human error.

Table 1	
FEATURES USED	
➤	Authorized framework
➤	Fine-grained control of access to network resources
➤	Centralized management
➤	Single Sign-on for Web
➤	Secure remote access
➤	Replication and load balancing
➤	Web security
IT ENVIRONMENT	
➤	Solaris
➤	Netscape Web Server
➤	SSL-enabled Web Browsers
➤	Java Web Server
➤	Java Servlets (JSDK)
➤	Inprise VisiBroker applications
➤	Web Intelligence from Business
➤	Objects
➤	Dynabase from Inso
➤	In-house developed applications

We needed a highly scalable authorization framework and found it with Tivoli SecureWay Policy Director. Tivoli SecureWay Policy Director will provide the authorization backbone for all of our applications, allowing us to provide our employees, partners and customers with secure access to more information."

Timothy M. Tully, Jr.,
Senior Vice President, Investment Technologies,
T. Rowe Price

For a more current version of this story, please visit:

http://www.tivoli.com/inside/clients/rowe_price.html
http://www.tivoli.com/products/solutions/security/secureway_references.html

Access Control Infrastructure — Software that controls access to a broad range of computer resources, including Web-based applications and older host systems, typically within an enterprise network. The software handles *authentication* and *authorization.* The software may also be capable of enforcing access control policies that cover groups of users or entire departments.

Anti-Virus Software — Software that detects viruses in resources such as e-mail messages and hard drives and eliminates any that are found. This software must be updated regularly in order to defend against new viruses.

Authentication — The process of identifying an individual, based on user name and password or more sophisticated techniques. This process only verifies that the individual has proven he is who he says he is. Authentication is usually followed by the process of *authorization.*

Authorization — The process of denying or granting access to resources on a network.

Authorization API (Application Programming Interface) — An industry standard interface for providing authorization information. For instance, business applications may use the Authorization API to communicate with an access control infrastructure in order to determine users' access privileges. Abbreviated to aznAPI.

C — A highly flexible and compact programming language popular among programmers who develop applications for personal computers.

Certificate Authority (CA) — A third party that issues digital certificates used to create public keys and digital signatures. CAs have relationships with a wide range of organizations such as credit card companies and other financial institutions and corporations, which provide information to verify an individual's identity. CAs guarantee that two parties that are exchanging information—are who they say they are.

Common Object Request Broker Architecture (CORBA) — An architecture that allows discreet pieces of programming code, referred to as objects, to communicate regardless of what programming language they were written in or what operating system the are running on. CORBA is vendor independent and was developed as part of the industry consortium Object Management Group (OMG).

Digital Certificate — Encryption software attached to electronic messages used to verify that a user sending a message is authentic. Digital certificates also provide the receiver with the ability to send a similarly encoded reply. A Certificate Authority (see CA), a trusted third party organization, issues a digital certificate that contains the applicant's public key (see PKI) and other data used for identification. The recipient of an encrypted message uses the CAs public key to decode the digital certificate attached to the message and send an encrypted response.

Firewalls — Software (sometimes with hardware) or gateway that filters out unwanted network traffic, and aims to prevent hackers from breaking into a network. Firewalls control network access and monitor traffic flow.

Host System — A primary server in a network. Also, any computer connected to the internet that has a domain name associated with it.

Intranet — An IP-based enterprise network, usually highly secure and protected by firewalls *(see firewalls*) and other authorization *(see authorization)* and authentication *(see authentication)* systems.

Java — An object-oriented programming language, similar to but much simpler than, C++. Java, developed by Sun Microsystems, is used extensively to write applications and applets and build services that run on the web, handheld devices and other small devices.

Lightweight Directory Access Protocol (LDAP) — A set of protocols used to access information directories that reside on enterprise and service provider networks. LDAP is widely used because it is based on established standards and because it support IP. LDAP will allow almost any application running on nearly every computer platform to access directory information including public keys *(see PKI)* and email addresses.

Public Key Infrastructure (PKI) — A system of digital certificates *(see digital certificate)* and Certificate Authorities *(see CA).*

Supply Chain Integration — Business integration between between a company and its business partners, implemented with software applications. For instance, suppliers and their customers may share information about inventory or scheduling over a private IP-based network or extranet.

Thin Client — A more intelligent implementation of the old dumb terminal that relies on a server for most of its data processing and storage needs. For example, a diskless PC that resides on a network is an example of a thin client.

Wireless Access Protocol (WAP) — A set of open protocols for developing applications and services that use wireless networks. The WAP protocols are mainly based on already existing Internet protocols, but are optimized for mobile users with wireless devices. WAP is designed to enable the distribution of real time information and services to mobile users.