White paper

IBM SecureWay FirstSecure enables secure e-business.

e-business

Abstract: This paper explains to an IT executive how IBM® SecureWay® FirstSecure intends to meet the challenge of securing e-business. Backed by 30 years of enterprise security research and experience, and based on a comprehensive architecture, SecureWay FirstSecure can help reduce risk by lowering the total cost of secure computing and reducing complexity with integrated, yet modular, solutions. Organized around a security policy director, SecureWay FirstSecure will fulfill the requirements of today's dynamic, global enterprises.

e-business intensifies security requirements

In today's marketplace, businesses must transform to e-businesses to remain competitive. Analysts predict that companies that don't make the necessary changes will be overrun by competition and ultimately fail. As enterprises around the world undergo transformations, they are leveraging Internet technologies to:

- Broaden their markets by extending their reach globally
- Enter new business areas through collaborations or expanded services made possible with Web-based interactions
- Increase employee productivity by providing easier access to corporate information and services
- Reduce costs through improved operations that integrate Web access and traditional information technology (IT) systems

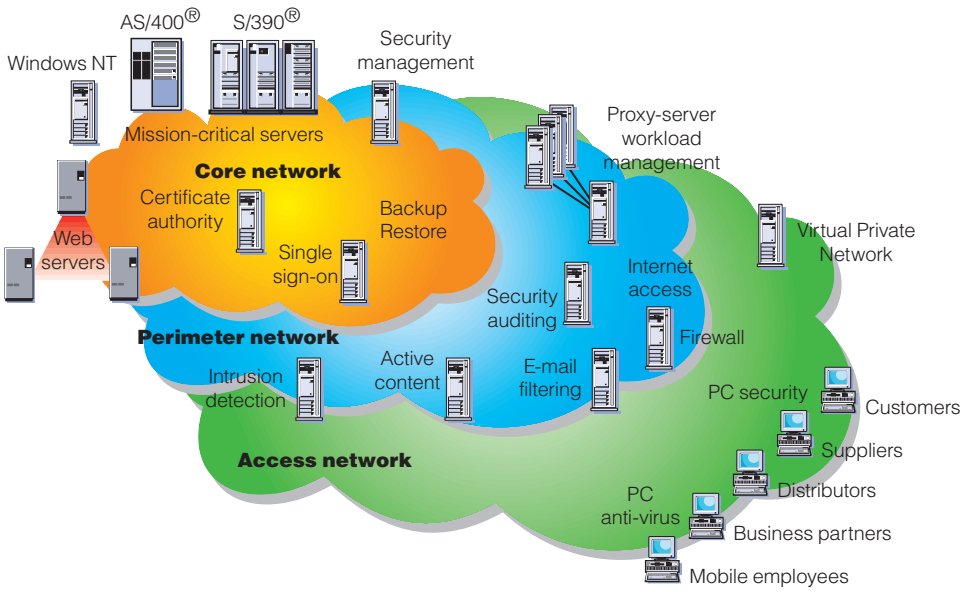


Figure 1

Increasingly, companies realize the significant business value of developing and deploying enterprise-wide security to the rapid growth of e-business. To deliver high availability and easy manageability, they must consider security requirements as an important part of their e-business transformation. Marlo Kosanovich, META Group's program director of Service Management Strategies and Global Network Strategies, asserts: "IT organizations can no longer view security as a burden. Rather, security must be viewed as an enabler, and security policies must become an integral part of IT as businesses continue to expose themselves and collaborate with key partners, customers and employees.[1]

To benefit from Web-based technologies running in a secure, connected environment, many companies adopt various proprietary technologies and install point products from multiple vendors. Figure 1 illustrates a typical installation which can result from deploying multiple security point products in one enterprise.

This type of computing environment can cause four major problems:

Lack of integrated security products drives complexity
One of the reasons that security can be so complex is the large number of products required to protect an enterprise. According to Forrester Research, Inc., "Most companies secure their networks with products from at least three different vendors – leading to management complexity and interoperability snags."[2] The Forrester report also quotes a utility company representative who says, "…We struggle with interoperability and require highly trained staff to integrate complex tools."

Security policy is difficult to implement
Many security breaches are a result of a lack of policy or an inability to implement policy. In a 1998 survey of 1,600 information professionals conducted by PricewaterhouseCoopers LLP, 73 percent of the respondents reported security breaches during the past year and yet, fewer than 1 in 5 respondents had a comprehensive security policy.

Implementing even a simple policy creates an enormous amount of work. For example, providing an external sales group with user access to an online forecasting application on the last Friday of each month requires the administrator to configure the following:

- An access control program to authorize application access
- A firewall to authorize network access
- One or more authentication schemes to identify users
- An anti-virus application to protect the application and network
- An intrusion detection product to protect against unauthorized access to valuable resources

For the administrator, the configuration task is nearly impossible because various products often have their own unique directories and languages to describe policy.

Security costs are escalating
Security costs can quickly get out of hand – not only from the purchase of numerous products but from the considerable resources necessary to install, configure and integrate them into a cohesive security infrastructure. According to GartnerGroup[3] , "Enterprise-wide security consists of policies, standards, architecture, processes, education, products and monitoring. Any security initiative that does not include these elements will fail. Enterprises lacking a comprehensive approach will incur large, unwarranted costs for product-only initiatives."

Ultimately, piecemeal solutions can become quite unwieldy to manage, often requiring companies to employ multiple security experts to maintain the different programs. Eventually the cost of implementation and integration can become more expensive than the products themselves.

Security issues inhibit e-business application deployment
Today's security systems are intrusive. Companies must either buy applications with embedded security or write security code into their applications; both choices can delay or inhibit e-business deployment. Purchased applications must first be integrated into the existing security infrastructure before being used. Custom applications require writing unique security code, necessitating additional programming skill and time for each new application.

All of these factors can delay deployment and contribute to the increasing total cost of implementing a comprehensive security solution. To overcome these hurdles, companies rolling out e-business applications have typically taken one of three security approaches:

- Individual business units employ a variety of security point products for applications that do not easily integrate or interoperate

- They deploy e-business applications without the appropriate security mechanisms because they don't realize the risk

- They delay deploying e-business applications because they don't have the necessary resources to address the related security issues

Unfortunately, each of these approaches can have costly consequences.

e-business calls for a holistic security solution

Although the word holistic may evoke images of acupuncture, meditation or yoga, it's actually a very apt term for describing how enterprises should approach security as they progress along the e-business path. Holism asserts that a whole entity is more than just the sum of its parts. And that's exactly what is required to establish an effective security solution. As a result, the interdependence of security technologies must be taken into consideration when companies move forward with e-business transformations.

A holistic security solution must alleviate the critical pains associated with implementing security. First and foremost, it must present a solution that isn't overwhelmingly complex to install, implement and manage. Second, it must provide a vehicle for central definition, deployment and management of security policy. The solution must also reduce the overall cost of implementation and promote the rapid deployment of e-business applications.

One of the most important requirements of a holistic security solution is that it be based on an integrated, standards-based architecture. An open and flexible solution can substantially reduce the risk of undetected flaws compromising an entire security infrastructure. An effective solution must also minimize the risk of business data being lost and ensure that applications remain available, performing as designed.

To adequately reduce these risks, an effective security solution requires the following capabilities:

- Authorization: to allow only legitimate users access to systems, data applications or networks. You can ensure everyone follows the stipulated policy rules.
- Accountability: to determine who performed any given action and which actions occurred during a specific time interval. You can identify who did what, when.
- Assurance: to demonstrate and periodically validate the claimed level of security protection is being enforced. You can confirm the system carries out policy rules.
- Availability: to keep systems, data, networks and applications usable. You can ensure systems and network resources are available when needed.
- Administration: to define, maintain, monitor and modify policy information. You can customize and update the policy rules.

These capabilities must be based on corporate-wide policies that can provide protection for the entire set of networks, systems and applications installed in an enterprise. In addition, good security deployment requires an effective link from the administrative definition of policy to the operational enforcement of that policy. Furthermore, if security products do not conform to open standards, real integration is extremely complicated to manage; the results may be security exposures as well as higher costs from vulnerable patchwork integration. The presence of one vulnerable link between point products can jeopardize the effectiveness of the remaining infrastructure. Therefore, using even the best individual security products can yield a second-rate solution, weakening the overall infrastructure.

The importance of policy management in a enterprise security solution cannot be overemphasized. Managing separate policies for several point products is not only very complicated but extremely costly. Without integration, a company needs a team of experts to maintain and enforce the policy associated with each security mechanism. And, in most cases, each mechanism has different administrative tools. So if everything is defined and working well for KillerApp A, the IT administrative staff must essentially start over when setting the policies for KillerApp B.

This redundancy – and confusion – is significantly reduced, if not eliminated, with a unified policy management scheme. Once the correct definitions are in place for one element of the system, they apply to any new mechanism added. Furthermore, a security structure with a common policy interface that communicates across the enterprise, makes it relatively easy to grow and change as new e-business opportunities arise.

IBM SecureWay FirstSecure: An integrated, policy-based security solution

IBM's answer to creating a protected environment for e-business is IBM SecureWay FirstSecure, a standards-based security solution that meets the challenges faced by organizations in the course of their e-business evolution. Its complete design satisfies the security needs of businesses in the various stages of e-business transformation. SecureWay FirstSecure offers businesses the opportunity to:

- Transform core business processes into e-business applications that create maximum value for their businesses
- Build new secure applications that are open, flexible and easy to change
- Run a scalable, available, secure environment that can respond to changing business situations
- Leverage information and experience to create faster, smarter organizations with business intelligence capabilities

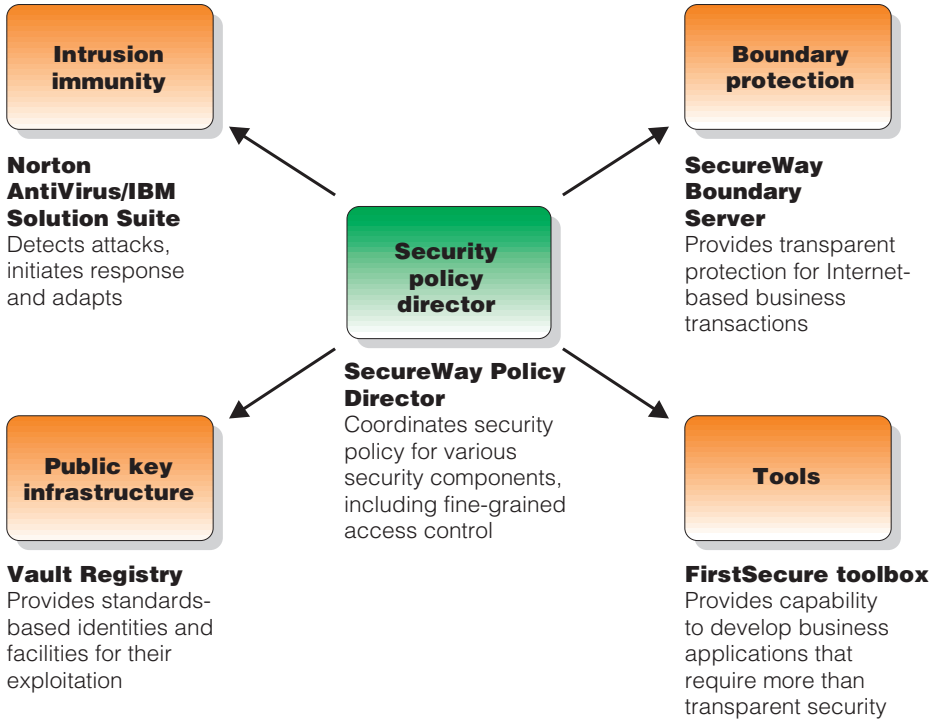


Figure 2

SecureWay FirstSecure components

SecureWay FirstSecure is an integrated security solution with modular, interoperable components that can help companies to quickly and securely deploy e-business applications (Figure 2). The unique advantage of SecureWay FirstSecure is the integration of core security technologies with SecureWay Policy Director (Policy Director), which defines and implements policy across each of the security components. As SecureWay FirstSecure evolves, IBM intends to seek additional security providers to include their products and technologies with SecureWay FirstSecure components and to integrate with Policy Director.[4]

Security policy director
SecureWay Policy Director provides a centralized point for defining, administering and enforcing security policy related to authentication and access control for standard IT and Web-based applications and resources. Access to Web pages in any environment (including OS/2®, OS/390®, OS/400® and Sun Solaris) can be controlled by Policy Director from any HTTP Web browser. Policy Director will direct security activities among all of the SecureWay FirstSecure components and optionally interact with a higher-level, enterprise-management control point, such as Tivoli. Through notifications from, and directions to, other parts of SecureWay FirstSecure, the Policy Director will allow quick and comprehensive policy-based responses to events, such as intrusions, firewall alerts and viral detection of varying severity. Policy Director also provides one-time authentication for access to information on multiple Web servers.

Boundary protection
SecureWay Boundary Server provides transparent protection for Internet-based business transactions through the use of firewall and content filtering technologies. It contains firewall technologies from IBM as well as content filtering technologies from IBM and other technology providers, including Symantec Finjan and Content Technologies. The boundary security solution provided is analogous to airline security access gates, metal detectors and x-ray scanners. The SecureWay Boundary Server controls who can enter or leave the network as well as what content is allowed to enter or leave it. Any operating environment can be included in the protection provided by the SecureWay Boundary Server. Real extranet security is provided when the SecureWay Boundary Server is used in conjunction with the Policy Director. The Policy Director defines the authentication and access control rights while the SecureWay Boundary Server enforces them.

Intrusion immunity
FirstSecure intrusion immunity provides proactive detection and protection against a broad range of security exposures. This component ensures that the network is actively secured from intrusions by communicating policy-based security alerts and events management across the solution, while inoculating secured systems against viral attacks with Symantec™ Norton AntiVirus™ software. The potential benefits of combining this component with the Policy Director are striking – the Policy Director will be queried to determine the appropriate action based upon the policy. Depending upon the type of alert, the Policy Director will provide the proper component with the information necessary to take an action, such as shutting down access to a particular resource, rerouting access to a dummy environment to obtain more information about the intruder or performing a virus sweep on the affected area. Norton AntiVirus/IBM Solution Suite covers a broad range of workstations, servers and gateways.

Public key infrastructure (PKI)
The SecureWay FirstSecure PKI component, Vault Registry, provides a trusted environment that supports key e-business activities, such as secure access to Web applications, objects and e-mail. Security capabilities within applications are easy to use and transparent to users. The PKI component offers digital equivalents of many necessities and nuances that are typical when conducting business in the physical business world. The highly trusted identities that PKI issues and manages enable distinctions to be drawn among customers, allowing businesses to deliver customized information and services to those customers. For many e-businesses, the capability to make these distinctions is the key to transforming customer satisfaction into customer loyalty. Similarly, PKI enables companies to draw needed distinctions in their business-to-business relationships, allowing them to define the type of information made available to particular partners or suppliers.

Vault Registry issues certificates that can be used for strong authentication between Web browsers and Web servers. In keeping with the overall SecureWay FirstSecure approach, the PKI component follows the appropriate certificate (X.509v3 and eventually PKIX) and directory (LDAP) standards to ensure interoperability and investment protection.

Tools
SecureWay FirstSecure also provides the means for application development through the FirstSecure toolbox, a software development kit (SDK) that enables companies to customize and expand on their security implementations. The initial release of the toolbox contains the IBM KeyWorks Toolkit and IBM Key Recovery Service Provider. These tools require detailed advanced designer or programmer knowledge of various cryptographic and other security functions. FirstSecure toolbox supports application development on AIX®, Microsoft® Windows NT®, Windows® 95 and Windows 98 systems. Subsequent releases of the toolbox will address higher-level security application protocol interfaces (APIs) for SecureWay FirstSecure components and security middleware.

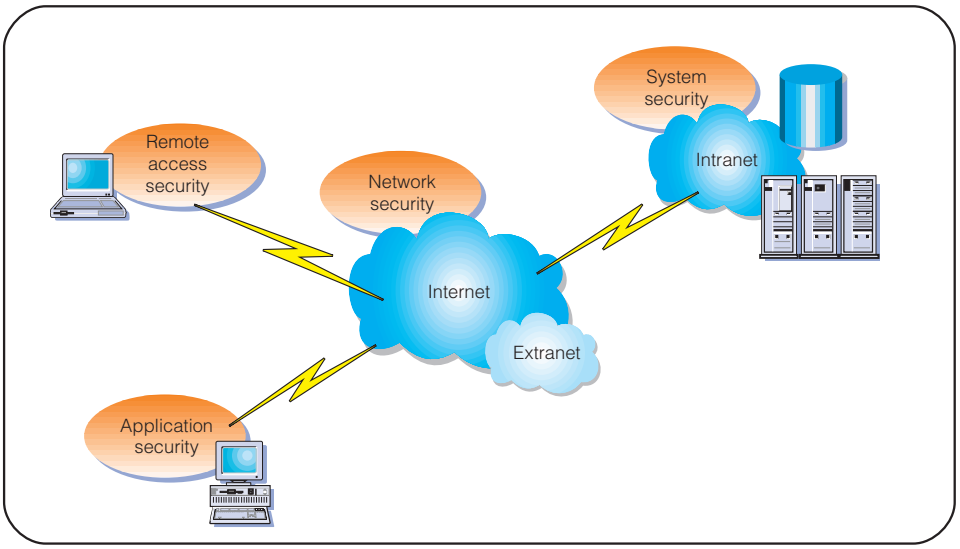
Smooth installation with SecureWay FirstSecure Implementation Services

IBM SecureWay FirstSecure Implementation Services help businesses to get the SecureWay FirstSecure framework up and running quickly and efficiently. These separately billable services are provided by IBM and performed by an experienced team of consultants. The consultants work closely with the IBM product development organization, improving the level of effective resolution of implementation issues. The SecureWay FirstSecure Implementation Services include:

- A workshop that covers design, architecture and education for Policy Director, Vault Registry and SecureWay Boundary Server
- Development of a high-level implementation plan using the information gathered during the workshop
- QuickStart installation that provides customer-selected SecureWay FirstSecure components installation and testing in a non-production environment

IBM SecureWay integrated security solutions

In addition to SecureWay FirstSecure, which covers authorization, accountability and assurance, IBM SecureWay integrated security solutions also provide availability and administration solution offerings. Together, IBM SecureWay integrated security solutions, consisting of SecureWay FirstSecure, Tivoli® User Administration, Tivoli Security Management and Tivoli ADSM™, address the set of five, high-level security requirements which serve as the conceptual base of IBM's security architecture for e-business: authorization, accountability, assurance, availability and administration (Figure 3).



Administration

- Tivoli User Administration
- Tivoli Security Management
- Services and consulting

Availability

- Tivoli ADSM for data backup and recovery
- eNetwork™ Dispatcher
- Services and consulting

Authorization **Accountability** **Assurance**

SecureWay FirstSecure, including:

- Policy management
- Virus protection
- Access control
- Enhanced firewall (VPN, content filtering, proxies)
- Intrusion detection
- Encryption
- PKI
- Tools
- Non-intrusive security for existing applications
- Services and consulting

Figure 3

The IBM integrated security solutions accommodate various e-business environments for internal and external communication, such as intranet, extranet and the Internet. Backed by years of experience, IBM provides companies with quality security solutions that reduce the complexity and security risks of implementing e-business applications.

SecureWay FirstSecure includes policy enablement, virus protection, access control, content traffic control, intrusion detection, digital certification, firewall technologies (filtering, proxies, network address translation), registry (for issuing and managing certificates for strong authentication, secure communication, and signing and verifying signatures) and a toolkit. It also offers service solutions to speed and simplify installation, and to validate that the operational environment is secure.

Tivoli ADSM addresses backup and recovery, enhancing SecureWay FirstSecure by addressing availability, helping ensure continuous operations for network services and offering the ability to recover lost or penetrated systems. The FirstSecure toolbox includes the capability to build key recovery into applications.

Tivoli User Administration and Tivoli Security Management help ensure that security mechanisms are managed efficiently and effectively. These solutions offer a simplified, single point of control by providing the mechanisms to manage a complex security environment, including functions that deal with security policy, identities, privileges and auditing for both users and programs.

Promoting e-business success with integrated security solutions

SecureWay FirstSecure is an essential element of the IBM SecureWay integrated security solutions, providing the initial steps toward an integrated, policy-based approach to e-business security. With SecureWay FirstSecure, IBM provides components that have been tested together; attractive pricing options for the integrated package of products; and IBM support for the complete solution, which includes technologies from other providers.

Organizing security elements around policy management, SecureWay FirstSecure will not only be able to reduce complexity in all phases of security implementation, but will be able to help lower a company's overall security costs. Rather than researching, planning and installing individual products to handle various security requirements, SecureWay FirstSecure and the integrated security solutions for e-business offer one-stop shopping. IBM provides a broad range of security solution offerings that work together, and with existing elements, to create an comprehensive security infrastructure. These offerings contain both IBM technologies and those from other well-respected security providers.

By effectively decreasing risk, reducing complexity and helping to lower the cost of secure computing, IBM integrated security solutions remove many of the barriers that prevent companies from fully exploiting the potential of the Internet. Through their key architectural elements – authorization, accountability, assurance, availability and administration – the integrated security solutions can enable a common, cross-system security scheme with fully enforceable security practices. SecureWay FirstSecure and the integrated security solutions offer companies a holistic approach to enabling successful e-business transformations.

For more information

For more information about IBM SecureWay FirstSecure, visit our Web site at:

www.ibm.com/software/security/firstsecure

IBM Corporation
Department VK4A
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in United States of America
3-99

[1] META Group. 1999. META Group unveils enterprise security issues; research reveals that third-party access will drive increase in external security breaches. META Group press release, 15 March 1999.

[2] Julian, Ted, Brandon Halligan, Matthew Wakeman, and Ashley Davis. 1998. Security Suites: Dead on Arrival. Forrester Research, Inc. 12 (November): 2

[3] Malik, Bill. 1998. Information Security Strategies Scenario: Are you Feeling Secure? Paper presentation at GartnerGroup Symposium ITxpo98: The Future of IT, 12-16 October, at Lake Buena Vista FL.

[4] All statements regarding IBM future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only.

Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.

G325-3817-01