Abstract: This paper describes how the IBM® SecureWay® FirstSecure solution meets the challenge of creating a secure and trusted environment for e-business. Backed by 30 years of enterprise security research and experience, and based on a comprehensive architecture for trusted e-business, SecureWay FirstSecure can help reduce risk by lowering the total cost of secure computing and reducing complexity with an integrated, yet modular, solution. Organized around an innovative security policy director, SecureWay FirstSecure will fulfill the trusted e-business requirements of today's dynamic, global enterprises.

**e-business intensifies security requirements**

In today's marketplace, across all industry segments, businesses are realizing that transformation to e-business is required in order 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 increasingly 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

The e-business transformation is not only changing the competitive landscape, it is changing the very nature of how IT groups should view security. There is a wealth of data supporting the point that security is the primary concern that IT managers have in terms of moving to e-business. But in order for e-business to take place successfully, the role that security plays must change, from being solely a preventative measure, to being an enabling force as well. Marlo Kosanovich, META Group's program director of Service Management Strategies and Global Network Strategies, asserts: "I T 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]

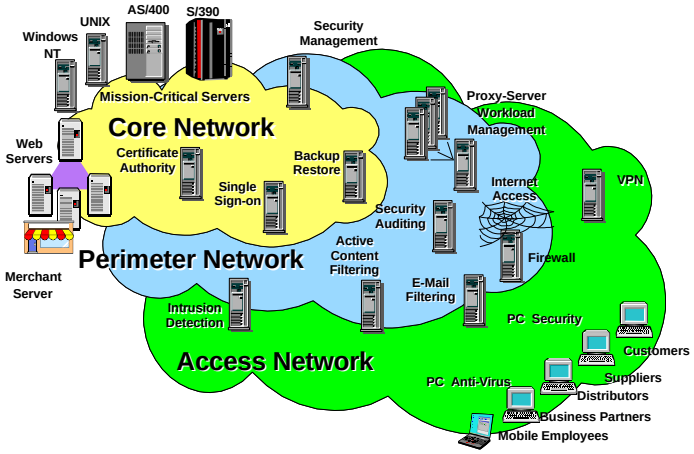


Figure 1. Multiplicity of Security Point Products

[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.

Although e-business fosters entire new business models , many enterprises are addressing security needs by continuing to apply a traditional approach to security - - adopting multiple proprietary technologies and installing point products from different vendors. This ap proach, typified by Figure 1, leads to four major problems.

***Lack of integrated security products drives complexity***

One of the reasons for security complexity 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] For example, this Forrester report 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 a security policy or an inability to implement policies, if they are defined. In a 1998 survey of 1,600 information professionals conducted by PricewaterhouseCoopers LLP, 73 percent of the respondents reported security breaches during the previous year and yet fewer than 1 in 5 respondents had a comprehensive security policy. Implementing even a simple policy can introduce an enormous amount of complexity, given how policy is typically 'delivered' in today's security offerings:

- Policy is dispersed over a broad range of products that do not interoperate. Because no single, central repository exists for policy, it is difficult to determine exactly what the current policy is.
- Policy is defined and accessed in varied ways. Because there are no standard methods for defining or accessing policy, implementing new kinds of policy is complex, and therefore ineffective and expensive.
- Policy data is duplicated. Because policy data is maintained in multiple places, it is often incorrect or "out of synch", leading to administrative difficulties, duplication of effort, and most importantly - increased business risk.

***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 the products into a cohesive security infrastructure. According to GartnerGroup, "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." [3]

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 offerings 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. Even purchased applications must first be integrated into the existing security infrastructure before being used. Custom applications require writing

---

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

[3] Bill Malik, Information Security Strategies Scenario: Are You Feeling Secure? GartnerGroup Symposium ITexpo98: The Future of IT, October 12 - 16, 1998, Lake Buena Vista, Fl., page 6 of conference presentation in section entitled, "How will Enterprises Arm Themselves To Address Increasing Information Security Risk.

application-specific security code, necessitating additional programming skill and time for each new application.

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

- Individual business units employ a variety of security point products for applications that do not easily integrate or interoperate
- Businesses deploy key applications without the necessary security mechanisms, thereby increasing risk
- Businesses delay deploying key applications because the necessary resources are not available

Unfortunately, each approach 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 as companies move forward with e-business transformations.

A holistic security solution alleviates the customer pains associated with implementing secure e-business. First and foremost, it presents a solution that isn't overwhelmingly complex to install, implement and manage. Second, it provides a vehicle for central definition, deployment and management of security policy. Additionally, the solution reduces the overall cost of implementation and promote the rapid deployment of e-business applications. A key requirement 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 IT infrastructure. An effective solution also minimizes the risk of business data being lost and ensures that applications remain available, performing as designed.

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

- Authorization: to allow only entitled users access to systems, data, applications or networks. You can verify everyone follows the policy rules.
- Asset Protection: to ensure data is kept confidential, privacy rules are enforced, so that the integrity of that data is maintained.
- 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 validate the committed level of security is being enforced. You can confirm the system enforces policy rules.
- Availability: to keep systems, data, networks and applications usable. You can reduce the downtime of system and network resources.
- Administration: to define, maintain, monitor and modify policy information. You can customize and update policy rules.

These capabilities must be based on corporate-wide policies that can provide a balance of protection and detection capabilities 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 entire infrastructure. Therefore, using even the best individual security products can yield a second-rate implementation, weakening the overall infrastructure.

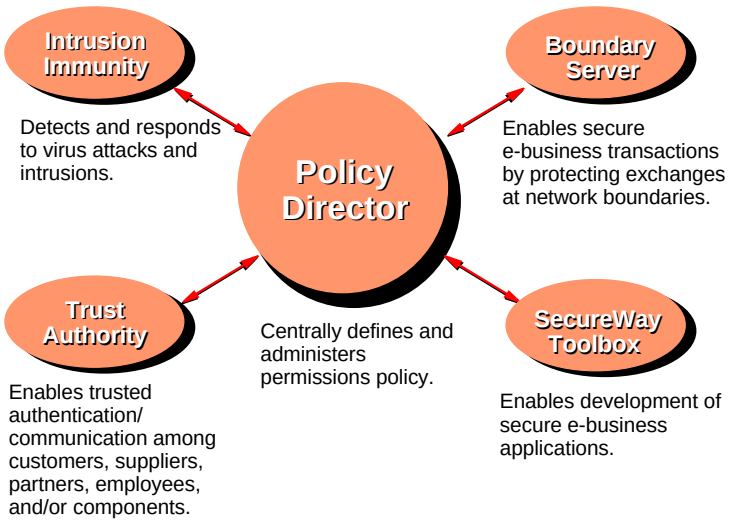


Figure 2. SecureWay FirstSecure Components

The importance of policy management in an 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 complexity – is significantly reduced, if not eliminated, with a centralized approach to policy management Once the correct definitions are in place for one element of the system, they apply to any new security 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: A centralized, policy-based security solution for trusted e-business.**
IBM's answer to creating a secure environment for trusted e-business is IBM SecureWay FirstSecure, a standards-based security solution that meets the challenges that organizations face in the course of their e-business transformation. Its complete design satisfies the security needs of businesses in the various stages of e-business. SecureWay FirstSecure offers businesses the opportunity to:

- Transform core business processes into e-business applications that create maximum value for their businesses
- Build new applications that are open, integrated, secure and easy to maintain
- Define and enforce business rules that distinguish one e-business participant from another
- Run a scaleable, available, secure environment that can respond to changing business demands
- Leverage information and experience to create faster, smarter organizations with business intelligence capabilities

**SecureWay FirstSecure components**
IBM SecureWay FirstSecure enables companies to build and operate secure environments for conducting trusted e-business. As shown in Figure 2, FirstSecure offers an integrated, policy-driven solution for your IT security needs, including digital identities, network boundary protection, detection for viruses and intrusions, and tools for developing secure applications.

*SecureWay Policy Director*
SecureWay Policy Director provides a centralized point for defining, administering and enforcing security policy related to authentication and access control for IT and Web-based applications and resources. Access to Web pages in any environment ( such as OS/2 ® , OS/390 ® , OS/400 ® and Sun Solaris) can be controlled by Policy Director from any HTTP based Web browser. Policy Director will direct security activities among the SecureWay FirstSecure components, and its open authorizat ion interface will enable any security component to have Policy Director make authorization decisions. Policy Director also provides one-time authentication for access to information on multiple Web servers.

*SecureWay Boundary Server*
The SecureWay Boundary Server controls all traffic flowing between networks, providing essential firewall filtering at the application, session, and transport levels. The Boundary Server enables virtual private networks to be established, and protects confidential data as it is transported over relatively untrusted networks. The Firewall capabilities within the Boundary Server are enhanced with content filtering (analysis of content as it passes between networks) and through integration with the Policy Director enforces authentication and access control policy (also known a 'permissions policy'.) Content analysis is becoming an item of increasing focus, because it can help manage employee productivity and limit legal liability and loss of confidential information. In order to deliver a comprehensive Boundary Server, IBM has partnered with the premier industry content filtering providers, Content Technologies and Finjan.

The tight coupling between the Boundary Server and Policy Director enable requests flowing from one network to another to be fully checked out, with the checks involving the requester's permissions (identity and access control settings). This is an essential facet to enabling secure, end-to-end communication from a browser to a middle tier, and possibly to a target system in a private network.

*Intrusion immunity*
The Intrusion Immunity component detects security problems. With the initial delivery of FirstSecure, the Intrusion Immunity component was focused on comprehensive detection of and reaction to the full range of viruses on a wide range of workstations, servers and gateways. Now network intrusion detection technology from IBM Research has been added. This leading edge technology enables the quick discovery of intrusions before further penetration into private networks can be attempted. The network intrusion detection product (Tivoli Cross-Site for Security) offers centralized administration of intrusion defenses and greatly enhances the reliability and availability of the operational e-business environment.

*Trust Authority*
The Trust Authority component provides the basis for a company's public-key infrastructure (PKI). Trust Authority integrates the components needed to issue highly trusted identities. These identities form the basis for a trusted environment that supports key e-business activities, such as secure access to Web applications, objects and e-mail. Trust Authority offers digital equivalents of many necessities that are typical when conducting business in the physical business world.

The highly trusted identities that Trust Authority issues and manages provide a basis for drawing distinctions among employees, suppliers, partners and customers, enabling businesses to deliver customized information and services. For many e-businesses, the capability to make these distinctions provides a definite competitive advantage and is key to their long term success and viability. Similarly, PKI enables companies to draw needed distinctions and define the type of information made available in their business-to-business and business-to-consumer relationships.

Trust Authority issues certificates that can be used for many purposes, including SSL based communication, such as VPN and e-mail. In keeping with the overall SecureWay FirstSecure approach, Trust Authority uses industry standards for certificates (X.509v3 and PKIX), directory access (LDAP), and crypto operations (CDSA), to enable interoperability and provide investment protection.

*Tools*
The SecureWay Toolbox is a collection of software development toolkits, APIs and protocols that let you build and customize your security implementations. These related security and cryptographic toolkits and

APIs allow enterprises to have their applications and middleware take advantage of functions offered by FirstSecure components such as Policy Director (Authorization API) and Trust Authority (PKIX Toolkit), using tools, protocols and APIs which are based on open standards. Sample applications are provided as a guide for integrating applications with the FirstSecure components.

**FirstSecure and Integration**

Solutions built on FirstSecure realize immediate installation, customization and operational benefits, because of the integration that is built into FirstSecure's components. Consider these two aspects of FirstSecure integration;

Integration among FirstSecure components: Out of the box, FirstSecure comes tested and integrated. By running a Policy Director supplied proxy on the Boundary Server, the level of protection that takes place at network boundaries comes up to e-business standards. And of course, Lightweight Directory Access Protocol (LDAP) directories are used by Policy Director, PKI, and the SecureWay Boundary Server, to store and share information about users. Another significant example of this integration is the ability for a user to register once for digital identities (certificates) from the PKI component, and to have those identities used by the Policy Director for establishing permissions for e-business participants to access various resources.

Integrating applications with FirstSecure: With FirstSecure there is an obvious focus on enabling applications to integrate with the FirstSecure framework. Policy Director's Authorization API, which is the basis for proposed The Open Group's aznAPI authorization standard, is an essential element. This integration — highly secure client, to middle tier Web server, and on to the private network, to access data or transactions, according to centrally defined permissions — is a prime illust ration of enabling the end-to-end security that is critical in a successful e-business environment. Additionally, the ToolBox enables Directory (LDAP), digital identity (PKIX) and Web browser/server interactions (SSL).

**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 FirstSecure Implementation Workshop and product level QuickStart installation services. IBM can also provide FirstSecure system integration services that are customized to the environment of an individual customer.

In addition to these services that are specific to FirstSecure, IBM Global Services offers a wealth of security and privacy services (consulting, implementation, outsourcing, and so on) for companies at any point in the cycle of secure application deployment.

**FirstSecure andTivoli Enterprise**

FirstSecure and Tivoli Enterprise provide complementary security capabilities:

Tivoli Enterprise is IBM's strategic systems management framework . The Tivoli Security Management offering includes policy management and addresses security policy at the operating system level. Policy Director augments Tivoli's offering with a complementary capability by defining and enforcing security policy at the network and application layers. The Policy Director also provides a coordinated log-on to only Web-based resources. For customers wanting a single sign-on solution for their enterprise to log-on to host based resources, network operating systems, and databases, Tivoli Global Sign-On is recommended.

Tivoli Enterprise provides the management and administration of the systems under its control. Those systems include the following FirstSecure components: Norton AntiVirus and Tivoli Cross-Site for Security.

**Promoting e-business success**

SecureWay FirstSecure enables trusted e-business by providing an integrated and centralized, policy-based security solution. Organizing security elements around policy management, SecureWay FirstSecure will not only be able to reduce complexity of security implementation but will help to lower a company's overall security costs. Rather than researching, planning and installing individual products to handle various security requirements, SecureWay FirstSecure offers one-stop shopping. FirstSecure delivers an integrated security solution that works with your existing security products to create a comprehensive security infrastructure. This offering includes both IBM technologies and those from other well-respected security providers.

IBM's SecureWay FirstSecure:

- Enables trusted e-business among customers, suppliers, partners, and employees by delivering permissions based security
- Speeds deployment of secure e-business applications and services
- Increases the return on security investments

By effectively decreasing risk, reducing complexity and helping to lower the cost of secure computing, IBM's SecureWay FirstSecure removes many of the barriers that prevent companies from fully exploiting e-business. Through the key architectural elements – authorization, asset protection, accountability, assurance, availability and administration – FirstSecure can enable a common, cross-system security scheme with fully enforceable security practices. SecureWay FirstSecure offers companies a holistic approach to creating a trusted environment and enabling successful e-business transformation.

**For more information**

For more information about IBM SecureWay FirstSecure, visit our Web site at:
*www.ibm.com/software/security/firstsecure*