IBM Integrated Security Solutions: Comprehensive Security Solutions for Enabling e-business

Abstract: **This paper explains how the IBM integrated security solutions approach the challenge of securing an e-business holistically. This set of offerings addresses risk through a comprehensive architecture, lowering the total cost of secure computing, reducing complexity with integrated yet modular solutions, and applying over 30 years experience securing mainframes to the new world of e-business. This integrated set of solutions, organized around a Security Policy Director, fulfills the security requirements of today's dynamic global enterprises.**

e-business Intensifies Security Requirements

A year or so ago, businesses could choose whether to transform into an e-business. Today, they have no choice. Forecasters are predicting that companies that don't make the necessary changes will be overrun by competition and ultimately fail. As a result enterprises around the world are undergoing transformation. They are leveraging Internet technologies to:

- Broaden their markets by extending their reach globally
- Enter new fields through collaborations or expanded services made possible with Web-based interactions
- Increase employee productivity with easier access to corporate information and services
- Reduce costs through improved operations that integrate traditional information systems into e-business designs.

As corporations discover the benefits of exploiting Web technologies, they are also uncovering some of its corresponding perils. Inherent in the e-business transformation is the process of exposing valuable corporate systems and data to increased risks. Once a computer links to the Internet or even intranets and extranets, it becomes visible to a wide audience and vulnerable to the hazards associated with broad exposure. As this transformation occurs, a company's dependencies on security, availability and manageability significantly increase.

Security no longer only plays the role of protector but also e-business enabler. A manufacturing company acknowledged that *the utilization of web technologies and reliance on extranets for supply chain integration is the primary reason for the budget priority now being accorded to security*[1]. This example indicates how important security is to the growth and deployment of e-business.

An even more compelling example is a security mechanism such as digital signature which makes it possible to conduct monetary and business transactions over the Internet with confidence. *For instance, when a company responds to a bid for goods, the interaction between the buyer and vendor can take place on-line only if there is a way to avoid repudiation. The seller needs to ensure that the buyer won't renege on an agreed-upon price.

Without digital signature, a very serious problem could arise if a buyer of a small quantity of goods claims that his price was a discounted amount usually reserved for larger quantity purchases. It's not like the vendor never sold the items for that price; so without a digital signature, vendors have no legal recourse to make the buyer pay the agreed upon price. These examples indicate how security technologies can contribute to a company's ability to enhance and strengthen itself with new ways of doing business.

---

[1] Aberdeen*Group*, IBM NCSD - Value Proposition Research: Interview Notes, December,1998, p. 68.

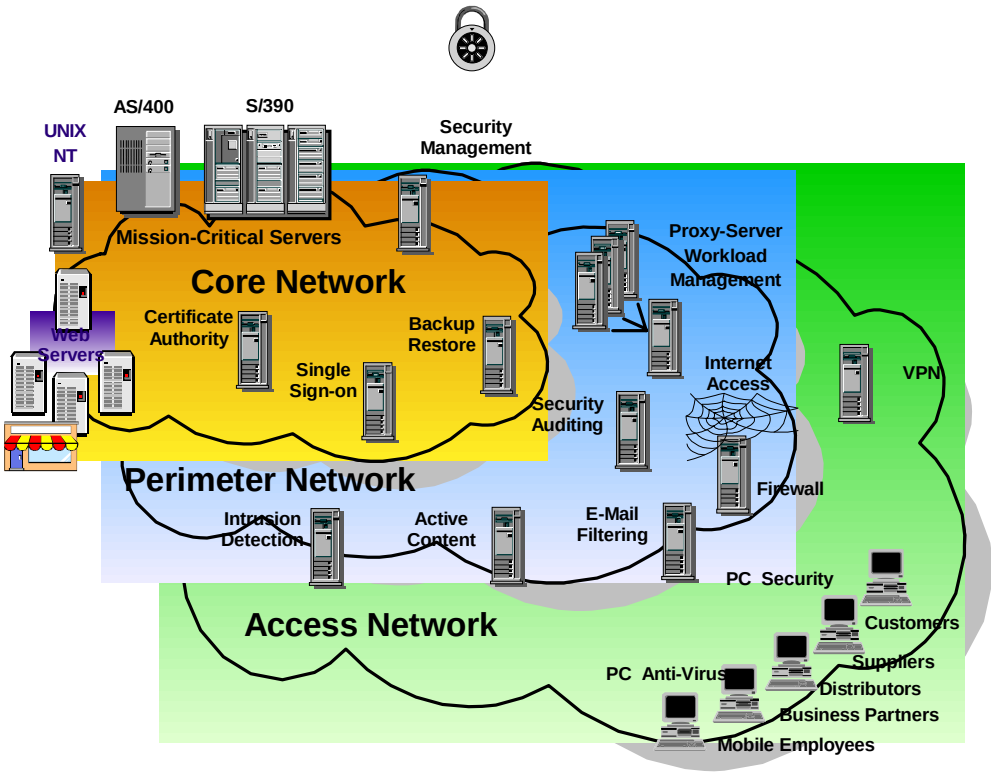


Figure 1.

But this growth and business transformation does not come without pain. To benefit from web-based technologies running in a secure connected, many companies are adopting numerous proprietary technologies and installing many point products from multiple vendors. The result is an installation like that shown in Figure 1. The sheer number of security products is causing numerous problems.

- **Lack of integrated security products drives complexity.** The single cause of complex security is the large number of products required to protect an enterprise. According to Forrester Research, Inc.,[2] "*most companies secure their networks with products from at least three different vendors - leading to management complexity and interoperability snags*". The Forrester report also quotes a Utility company as saying, " .... *We struggle with interoperability and require highly trained staff to integrate complex tools.*"

  Doing business on a web-based network means the customer must protect itself from many threats not present on a traditional network. Enabling a secure e-business requires new products such as digital signatures. Integration of all the security products required for both protection and enablement is extremely difficult. Lack of integration leaves the enterprise exposed to significant risk, and unequipped to deliver new business solutions in today's networked world.

- **Security Policy is impossible to implement**. A good security system starts with a well-structured security policy. Many breaches are encountered when companies fail to

[2] Ted Julian, Brandon Halligan, Mathew Wakeman, Ashley Davis, Forrester Research, Inc, Security Suites: Dead on Arrival, Volume 12 No. 12 November 1998, p. 2.

recognize this. In a survey in 1998 of 1,600 information professionals by PricewaterhouseCoopers LLP, *73% reported security breaches during the past year, but fewer than 1 in 5 had a comprehensive security policy*. Implementing a security policy becomes an extremely complex task without product integration.

Without integration even implementing a simple policy creates a ton of work. For example, defining a user group as external sales with access to the forecasting application over the Web on the last Friday of each month means an administrator needs to configure:

1. An access control program to authorize application access
2. A firewall to authorize network access
3. An authentication scheme - such as PKI - to identify the user
4. An anti-virus application to protect the application and network
5. An intrusion detection product to protect against hackers, etc.

And doing the configuration is nearly impossible since all of the products use unique directories and policy engines.

Without policy definition and enforcement, there is no security. As stated in the Aberdeen report[3] a consumer goods company concluded, "*Technology is driving security - the interdependencies of technologies must be taken into consideration from an end-to-end point of view. There is no such thing as security in a vacuum any more.*"

- **Security costs are escalating.** Security costs quickly grow out of hand not only from purchasing the many required products but also from the considerable resources necessary to install, configure, and integrate these products into a cohesive security infrastructure. According to GartnerGroup[4], '*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*."

  Implementing a policy-based security infrastructure, a complex and evolutionary process, requires numerous iterations. Consequently, companies are needing more technical security skills and/or are relying on external services providers. These factors all contribute to increase the total cost of a security solution.

- **Security issues inhibit deployment of e-business applications**. In addition to the three problems described previously, other leading inhibitors to e-business adoption also exist. Today's security systems are intrusive. Customers must either write security code into their applications or buy applications with embedded security. Both actions result in slowing

---

[3] AberdeenGroup, IBM NCSD - Value Proposition Research, December, 1998 p. 80.

[4] Bill Malik, Information Security Strategies Scenario: Are you Feeling Secure? GartnerGroup Symposium ITxpo98: The Future of IT, October 12-16, 1998, Lake Buena Vista, Fl., p6 of conference presentation in section entitled, "How will Enterprises Arm Themselves To Address Increasing Information Security Risk?"

e-business deployment. Purchased applications must then be integrated into the existing security infrastructure before being used. The custom application requires writing unique security code which requires additional programming skill and time. Both options increase the cost of e-business application deployment. This can result in the deployment of new business applications without the needed security, exposing critical business assets.

To overcome these hurdles, companies rolling out e-business applications typically have taken one of three security approaches.

- Individual business units have employed a variety of security point products for their applications that do not easily integrate or interoperate.
- They deploy e-business applications without the appropriate security mechanisms because the don't realize the risk or don't have the resources so they take the risk.
- They delay deploying e-business applications because they don't have the necessary resources to address the security issues.

Each of these paths has potentially costly consequences. By implementing a unique security function into each new e-business application, an organization can wind up with a potpourri of disparate pieces that don't work together. Taking this route can lead to continually solving similar security issues for each new application. Pieced-together solutions become quite unwieldy to manage, often requiring a company to employ multiple security experts to maintain the different programs. Eventually implementation and integration can become more expensive than the products themselves.

So if these inhibitors can be overcome for a price that makes sense, clearly security technologies can and will contribute to a company's ability to progress and grow. With that mission in mind, IBM architected the SecureWay Integrated Security Solution as complete security for e-business. The unique advantage of these offerings will be the integration of core security technologies around a policy director that defines and implements policy across various security components. Its design goals are to:

- reduce the complexity of security implementation
- minimize the total cost of secure computing
- promote the rapid deployment of secure e-business applications

All in all, IBM's integrated approach to security will combine the necessary features, functions and tools for a successful and profitable e-business transformation.

Summing it Up

The e-business challenge is to preserve the integrity, confidentiality and invulnerability of information and applications while taking advantage of the power of the Internet. IBM integrated security solutions address that challenge by organizing core security technologies around a policy director, thereby reducing complexity and application deployment time, which has a direct effect on the bottom line.

Characteristics of a Holistic Security Solution for e-business

Although the word holistic may bring up 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. The theory of holism professes that a whole entity is more than just the sum of its parts. And that's exactly the case with an effective security solution.

Reducing Risk

The most important requirement of a security solution is that it substantially reduces the risk that valuable data will be lost or systems compromised. An effective solution must also minimize the chance that business data is disclosed to unauthorized parties and ensure that applications remain available, performing as designed.

To adequately reduce risk, at a minimum, an effective solution requires the following capabilities:

- **Authorization** - protection that admits only legitimate user access to systems, data, applications or networks
- **Accountability** - the facility to determine who performed any given action and which actions occurred during a specific time interval
- **Assurance** - the ability to demonstrate and periodically validate the claimed level of security protection is being enforced
- **Availability** - the capability to keep systems, data, networks and applications usable
- **Administration** - the means to define, maintain, monitor, and modify policy information.

Furthermore, these capabilities need to be based on corporate-wide policies so that they can provide a protective mesh across the entire set of networks, systems and applications installed in an enterprise. The presence of one vulnerable link between point products in that mesh can render the remaining infrastructure practically useless. Therefore even using the best individual security products can yield a second-rate solution that can easily weaken the overall infrastructure.

A holistic security solution must also alleviate the common pains that companies associate with implementing security. First and foremost, it must present a solution that isn't overwhelmingly complex to install and manage. Since defining and enforcing polices across a wide variety of point products is one of, if not the key, contributor to complexity, the most effective solutions will use policy as a focal point of integration. Another of the pains associated with security is that it is costly to implement. And a direct consequence of the first two pains is the third -- the hindrance of speedy deployment of e-business applications.

The importance of policy management in a holistic and integrated security solution cannot be overemphasized. Managing policies for all the required products in a secure environment is not only overwhelmingly complex to administer but also extremely costly to maintain. 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 even if everything is defined and working well for, KillerAppA, 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 that is added. Furthermore, a security structure with a common policy interface that communicates changes across the computing infrastructure makes it relatively easy to grow and change as new e-business opportunities appear.

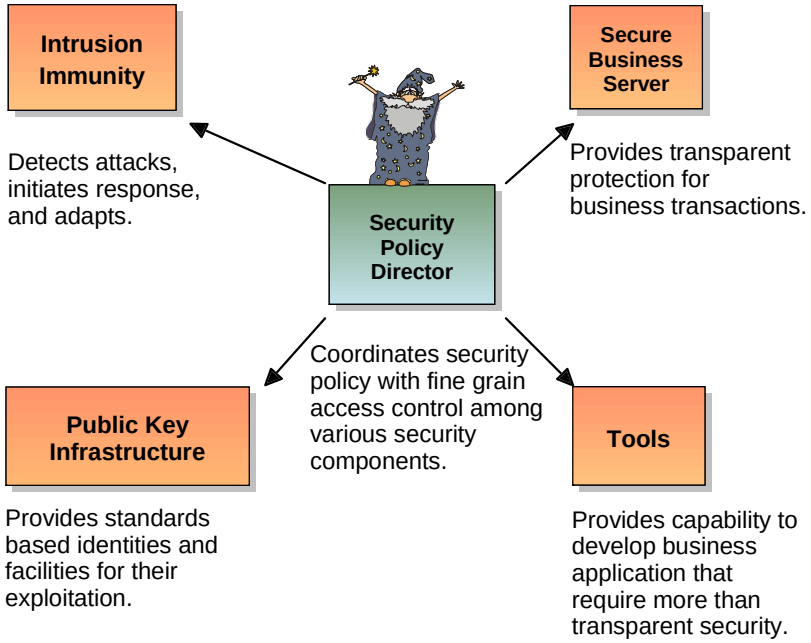
Summing it Up

A holistic security solution must reduce risk, but it must do so without introducing overwhelming complexity and cost. Creating the right security for the e-business environment is more than piecing together point products, it's facilitating the continual monitoring and adjusting of solution elements according to corporate-wide policies. Policy needs to be the focal point of an integrated security solution.

A Protected environment for e-business with IBM integrated security solutions

IBM's answer to creating a protected environment for e-business is the IBM integrated security solutions. These offerings address the security risks that organizations face in the course of their e-business evolution. Its end-to-end design, which dovetails well with OS/390 and AS/400 security, satisfies businesses in the various stages of transformation:

- Securely deploying e-business applications
- Strengthening the security of existing operations
- Integrating a security solution with the legacy IT environment
- Helping companies leverage the potential of e-business.



The IBM integrated security solutions provide a modular approach to a complex problem. One such module is IBM SecureWay™ FirstSecure, with its policy management capabilities. In fact, the key security functions and focus areas within FirstSecure,

- **Intrusion Immunity**
- **Public Key Infrastructure**
- **Secure Business Server**
- **Toolkit,**

are organized around a **Security Policy Director**. For the capabilities comprising FirstSecure, the Security Policy Director will provide a centralized point for defining, administering, and serving security policy, as well as act as an access control manager for web applications/resources.

The Policy Director will direct the security activities among the other FirstSecure components, and optionally interact with a higher-level enterprise management control point. Through notifications from and directions to the other parts of FirstSecure, the Security Policy Director will allow quick and comprehensive policy-based responses to such events as intrusions, firewall alerts, and anti-virus detection of varying severity.

The focus of the FirstSecure's intrusion immunity capabilities is on detecting security problems and on comprehensively reacting to those problems. It also integrates with the Security Policy Director by accepting or requesting a component policy and sending security alerts/events. The potential benefits of combining intrusion immunity with a policy director are quite alluring. For example, if an alert comes in, the Policy Director will not just record the alert for someone to look at later but it will set the right gears in motion to handle the situation. Depending on the alert, the response could be to shut down access to a particular resource, to reroute access to a dummy data set to obtain more information on the intruder or to perform a virus sweep on the affected area.

For Public Key Infrastructure, the focus is on certificate authentication, secured communications, and validation of signed policy. It would be the Policy Director that sends out the changes to affected areas of the system. For the Secure Business Server, the Policy Director integrates access control with the gateway functions of a firewall and firewall content filters. And finally, the Toolkit which enables customers to build and deploy secure applications within their enterprise includes APIs for policy management.

Implementing an e-business strategy can benefit from the accumulated wisdom and experience manifest in this latest set of security solutions from IBM. The architecture of these new solutions will allow them to integrate with the OS/390 or OS/400 security schemes that protect enterprise data and transactions. The IBM integrated security solutions will also accommodate the various e-business environments:

- Intranet, contained entirely within an organization,
- Extranet for business to business transactions and
- Internet for communicating and doing business with consumers.

The comprehensive nature of these solutions enables customer to avoid having to deal with multiple proprietary protocols and policy systems. A solution comprised solely of point products requires the continual reevaluation of security schemes and, consequently, additional investment. The IBM integrated security solutions for e-business unify the security elements into a single, corporate-wide scheme by providing:

- an integration point for authentication and access control across multiple platforms,
- centralized user-access policy management and enforcement,
- availability to reduce the burdens of security on the computing infrastructure,
- administration systems to centrally manage and coordinate the security elements, and
- a toolkit to integrate and deploy new applications securely within an enterprise.

The IBM integrated security solutions include IBM SecureWay™ FirstSecure, Tivoli User Administration, Tivoli Security Management and Tivoli ADSM. This combination of function covers the set of five high-level security requirements that serve as the conceptual base of IBM's Security Architecture for e-business, namely:

- Authorization
- Accountability
- Assurance
- Availability
- Administration.

SecureWay FirstSecure covers authorization, accountability and assurance from a corporate-wide perspective. FirstSecure includes virus protection, access control, content traffic control, encryption, intrusion detection, digital certification, firewall technology and a toolkit. FirstSecure also offers service solutions to speed and simplify its installation as well as validate that the operational environment is secure, with no back doors inadvertently left open.

Tivoli ADSM addresses backup and recovery. It enhances FirstSecure by addressing the factors that cause denial of service, helping ensure continuous operations for network services and offering the ability to recover lost or penetrated systems.

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

Summing it Up

IBM's integrated security solutions are organized around a Policy Director. The initial integrated security solutions, which include IBM SecureWay™ FirstSecure, Tivoli User Administration, Tivoli Security Management and Tivoli ADSM, set the stage for a comprehensive security system that reduces complexity and facilitates the quick deployment of e-business applications, which help manage the bottom line.

Promoting Success with IBM Integrated Security Solutions

By organizing around policy management, IBM integrated security solutions not only can reduce complexity in all phases of security implementation, they help lower overall security costs for a company. Rather than having to individually research, plan for and install individual products to handle the many aspects of security, the integrated security solutions for e-business offer one-stop shopping. IBM's menu of building blocks integrate with each other and with existing elements to create an encompassing security infrastructure.

Through their key architectural elements (Authorization, Accountability, Assurance, Availability, and Administration), the integrated security solutions address risk reduction comprehensively. The IBM technologies establish end-to-end security coverage from centrally located mainframe servers to browsers on PCs. These offerings will enable a common cross-system security scheme for functions such as authentication and user access policy management. This policy-based approach is fundamental to a centrally managed environment with fully enforceable security practices.

IBM has built these solutions on standards-based technologies. These open standards benefit businesses because standards acceptance requires rigorous and diverse technical reviews and therefore reduces the likelihood that undetected flaws can compromise an entire security infrastructure. Furthermore, these standards allow companies the option to integrate offerings from other security vendors. Open standards ensure against being locked into a particular solution or vendor.

The IBM integrated security solutions integrate a considerable set of open technologies that companies can enhance with additional IBM services to help them balance risk reduction with security costs. More importantly though, these offerings allow an organization to take advantage of a policy-based distributed security scheme to quickly and securely deploy Web applications. This single integrated security system with its modular, interoperable components offers a secure and evolving development environment for future application creation and deployment.

By effectively decreasing risk, reducing complexity and helping lower the cost of secure computing, IBM integrated security solutions remove many of the barriers that keep companies from fully exploiting the potential of the Internet. In fact, this holistic solution provides the critical elements that enable an enterprise's successful e-business transformation.

* Unless noted, customer examples are based on a composite of common customer situations and are not intended to represent a specific customer. Situations will vary based on the unique nature of each business. IBM is ready to help your business implement security. Contact an IBM representative for more information.