Abstract: This paper describes how the Tivoli® SecureWay® family of solutions meets the challenge of creating a secure and managed environment for e-business. Backed by 30 years of enterprise security research and experience, and based on a comprehensive architecture for trusted e-business, Tivoli SecureWay solutions can help reduce risk by lowering the total cost of computing and reducing complexity. Organized around an innovative security policy management director, Tivoli SecureWay solutions will fulfill the most demanding requirements for trusted e-business in 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 controlling and managing 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: "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]

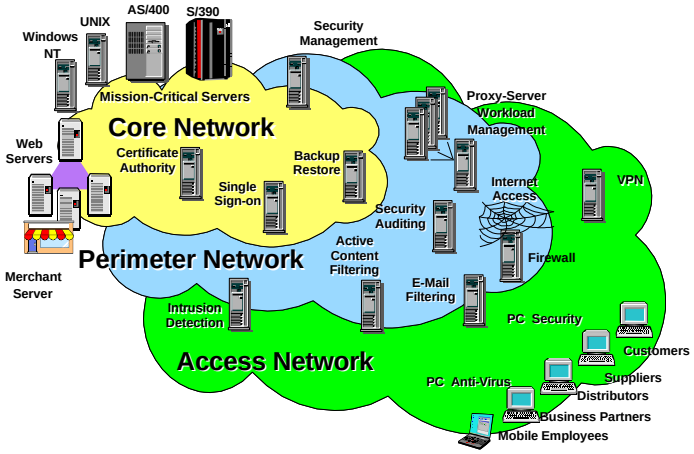

Figure 1. Multiplicity of Security Point Products

[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, the vast majority of enterprises are addressing security management and control needs by continuing to apply the "traditional" approach to security - - adopting, installing and independently managing many proprietary technologies and point products from different vendors. This approach, typified by Figure 1, leads to four major business issues:

Lack of integrated security drives complexity
Security complexity is driven by the large number of products - each with independent administration and application development interfaces - 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 states, "...we struggle with interoperability, and require highly trained staff to integrate complex tools."

Security costs are escalating
Security costs can quickly get out of hand when adopting e-business solutions – not only from the purchase of many specialized (i.e. expensive) security products, but also from the considerable level of specialized resources needed to manage and integrate the products into a cohesive security control infrastructure. Most importantly, in order to be effective, *this infrastructure must then be leveraged by the many key applications actually driving the e-business,* which contributes even more significantly towards escalating costs.

Simplifying the number of security components - for example, limiting the security infrastructure to anti-virus software and a firewall-based Virtual Private Network (VPN) - seems like an obvious way to limit these costs. Unfortunately, many more components are required to securely manage and control e-business applications. 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]

Security policy is difficult to implement
Many security breaches are a result of a security policy that cannot be applied and enforced consistently across the environment - if the security policy is actually defined at all. 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 difficulty in enforcement, given how a security policy is typically 'delivered' in today's security offerings. That is, <u>each security point product can only enforce a small portion of the security policy.</u> Since these security point products are not integrated with each other, the responsibility for the accurate implementation and enforcement of the policy is essentially strewn across a large number of administrators, many of whom may be physically and/or organizationally dispersed..

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

---

[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.

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 has costly consequences.

e-business calls for a holistic security approach

Although the word holistic may evoke images of acupuncture, meditation or yoga, it's actually a very apt term for describing how enterprises must 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 management and control 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 consistent, 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.

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 Killer App A, the IT administrative staff must essentially start over when setting the policies for Killer App B.

This redundancy – and complexity – is significantly reduced, if not eliminated, with a centralized approach to policy management and control. Once the correct definitions are in place for one element of the system, they apply to any new security mechanism that is 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.

Tivoli SecureWay: a centralized, policy-based security portfolio for trusted e-business.
Tivoli's answer to creating a secure environment for trusted e-business is Tivoli SecureWay, a standards-based portfolio of security management and control solutions 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. Tivoli SecureWay offers businesses the opportunity to:

- Transform core business processes into e-business applications that create maximum value
- 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 scalable, available, secure environment that can respond to changing business demands
- Leverage information and experience to create faster, smarter organizations with business intelligence capabilities

Tivoli SecureWay accomplishes this through a focused portfolio of solutions:

- **Tivoli SecureWay User Administration** provides an automated, secure way to manage user attributes and user services across heterogeneous, distributed networks. Designed to give IT staff centralized control, Tivoli SecureWay User Administration features policy-based management, management by subscription, secure delegation and a platform-independent interface.
- **Tivoli SecureWay Security Management** provides an open solution for role-based distributed and OS/390 security management, enabling administrators to consistently enforce security policy across multiple platforms with a single security model. Tivoli SecureWay Security Management addresses security policy at the operating system level.
- **Tivoli SecureWay Policy Director** unites core security technologies around common security policies, reducing implementation time and management complexity, thereby lowering the total cost of secure computing for e-business. It augments Tivoli SecureWay Security Management by providing a complementary capability by defining and enforcing security policy at the network and application layers. Tivoli SecureWay Policy Director also provides Single Sign-On support to Web-based resources.
- **Tivoli SecureWay Global Sign-On** provides a highly secure solution that gives users seamless access to resources, reduces corporate security risks and reduces help-desk costs associated with password management. It complements the Single Sign-On support offered by Tivoli SecureWay Policy Director by adding support for automated log-on to host-based resources, network operating systems, databases and local workstation applications. By using Tivoli SecureWay User Administration to manage the Tivoli SecureWay Global Sign-On information, companies have a powerful solution for administering and managing access to resources from a single administrative interface.
- **Tivoli SecureWay FirstSecure** provides a basic foundation for security in e-business environments, providing a comprehensive framework to help companies secure all aspects of networking via the

Web and other networks, while helping them build on their current investments with modular, interoperable offerings and minimize total cost of ownership for conducting secure e-business.

Smooth installation with Tivoli SecureWay Implementation Services
Tivoli SecureWay Implementation Services help businesses to get the Tivoli SecureWay solutions up and running quickly and efficiently. These separately billable services are provided by Tivoli and performed by an experienced team of consultants. The consultants work closely with the Tivoli product development organization, improving the level of effective resolution of implementation issues. The Tivoli SecureWay Implementation Services include an Implementation Workshop and product level QuickStart installation services. IBM can also provide system integration services that are customized to the environment of an individual customer.

In addition to these services that are specific to Tivoli SecureWay, 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.

Promoting e-business success
Tivoli SecureWay enables trusted e-business by providing solutions for integrated security management and control. Organizing security elements around policy management, Tivoli SecureWay 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, Tivoli SecureWay offers one-stop shopping. Tivoli SecureWay delivers integrated security management and control solutions that work with your existing security products to create a comprehensive security infrastructure. These offerings include IBM, Tivoli and DASCOM technologies, as well as those from other well-respected security providers.

Tivoli SecureWay:
- 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, Tivoli SecureWay 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 – Tivoli SecureWay can enable a common, cross-system security scheme with fully enforceable security practices. Tivoli SecureWay offers companies a holistic approach to creating a trusted environment and hence enables successful e-business transformation.

For more information
For more information about Tivoli SecureWay, visit our Web site at *http://www.tivoli.com.*