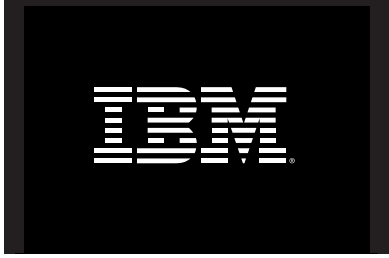
A technical discussion of security management
April 2002



Tivoli software

Establishing information security as a business enabler

How IBM helps deliver a secure infrastructure for e-business

Contents

Introduction

Companies continue to view information security as a hindrance in the deployment of e-business initiatives. This perception has deep roots in the underlying philosophy that the role of security is almost exclusively to protect against technology threats, not to help solve business issues that could stimulate a firm's growth. Simply put, many companies have been focused on keeping out the bad guys rather than letting in their most profitable customers to conduct business.

But this view is quickly changing as corporate leaders—such as Kemper Insurance, T. Rowe Price and Shell Canada—use security management to launch secure e-business applications more quickly and cost-effectively. This white paper discusses the move to transform security into a business enabler, the IT security challenges organizations face today and how Tivoli® software from IBM can help companies address these challenges.

A new model for security

With the spotlight focused on how to keep out intruders, hackers and the like, technology vendors have created sophisticated point products—for example, firewalls, intrusion detection software, content filters—to protect corporate network infrastructures. Because these complex products address potential technology threats rather than support advanced business initiatives for customer acquisition and corporate expansion, understaffed IT security organizations must scramble to justify the costs of acquiring, deploying and managing them. This justification often takes an insurance policy approach: "If we spend $X on this security technology, then we'll mitigate the firm's risk of downtime by $Y."

Unfortunately, unlike a real insurance policy, it is difficult to reliably quantify the potential loss from security threats. IT security is seen as a cost center to the business instead of a business enabler; as a result, many companies delay the purchase and implementation of such products as they prioritize other IT initiatives that promise quantifiable return on investment (ROI) in revenue and customer satisfaction.

Yet as businesses increasingly adopt e-business and internal resources are exposed to customers, partners and employees, information security has become crucial. Noting the explosion in deployed applications, portals and servers, leading analysts—including IDC, META Group and Gartner—have declared that information security must enable the business.* Therefore the fundamental question becomes this: Given these dynamics, how can IT security be transformed from a cost center into a true business enabler?

The high cost of today's security approach

A significant challenge in creating an IT security infrastructure that acts as a business enabler rather than simply as a security guard is in how information security policies generally are enforced today. Often three different organizations are interpreting, implementing and managing the policy:

- ***IT security***, *which focuses on securing the network infrastructure using a variety of point product technologies for protecting against a wide range of threats.*
- ***IT operations***, *which works with the business units to define the list of valid users (customers, partners and employees) of its IT resources (such as operating system servers, portals and applications). Then, to get each user online and productive as quickly as possible, IT operations must coordinate the following tasks across the business while maintaining compliance with the firm's security policy:*
  - *Creating the user definition, including the appropriate group and role memberships*
  - *Defining which IT resources each user is allowed to access*
  - *Defining what level of access each user will have within each IT resource*
  - *Querying for and obtaining the necessary approvals across the business units for provisioning the needed IT resources*
  - *Provisioning the actual IT resources for each user, with a user account featuring the appropriate access rights created for and administered within each resource*

*For example, Gartner has commented that "businesses often view security as an afterthought in the race to offer the latest services and solutions. … For e-business to be successful, security solutions must be seen as business enablers rather than a limitation or an inhibitor and must be addressed early." (Claire Woffenden, "Invest in security or pay the price, warns Gartner," *vnunet.com*, May 24, 2000.)

- ***Business unit application development****, which enforces the appropriate level of access for each user within every application and portal. This is commonly done by writing a customized security enforcement model within each application and portal, and then, in many cases, replicating the relevant list of users and access rights that IT operations has already defined elsewhere.*

In other words, because most point network security tools do not support these critical tasks, both IT operations and business unit application developers are left to manually implement security policies. Within IT operations, administrators have had to manually obtain approvals and then create and administer user identities and rights across each manually provisioned resource. This approach has been a widespread practice for decades, despite the fact that it causes three fundamental business problems for IT operations:

1. *Long cycles for getting users online and productive.* As administrators are forced to manually obtain approvals, provision resources and create multiple accounts for each user, it can take a long time to get a new user operating online.

2. *High costs for administering users.* Having multiple accounts for each user can lead to a high number of help desk inquiries for forgotten passwords and other common administrative tasks.

3. *High total cost of ownership (TCO) for user management.* Although the process for getting new users operating online is manually intensive and therefore costly, an even greater cost can be managing users and user access on an ongoing basis. A security policy doesn't typically change substantially over time, but users' relationships to the policy often do. For example, the relationship with a partner might change based on a new partnership agreement, a new entry-level customer might evolve into a high-margin customer over time, employees might receive promotions into higher-tier roles or reorganizations might lead to reassignment for groups of employees. All these changes must be reflected across a firm's entire e-business infrastructure. However, because each application, portal and server is typically populated with customized user definitions

and security access rules, each relationship change must be encoded manually within each customized security model. This generates a frequent management cost that can grow proportionally with the number of deployed resources.

Similarly, application developers within each business unit end up coding customized user definitions and security rules within each application and portal. This creates three additional business problems for organizations:

1. *Long deployment cycles for business initiatives.* As developers are forced to encode customized user definitions and security rules in each application and portal, they can take a long time to develop, test and deploy initiatives. This is especially problematic when deploying e-business initiatives, where time-to-market is critical for success.

2. *High costs for developing applications.* Encoding customized user definitions and security rules generally increases the amount of code that must be written for each application. With today's challenging economy, meeting each application's development budget has become an important factor—and customized security coding can significantly increase the risk of exceeding a budget.

3. *High TCO for application development.* Because each application or portal typically is deployed with customized user definitions and security rules, each relationship change must be encoded manually with each application's customized security model. This added management cost can grow proportionally with the number of deployed applications and portals.

These inefficiencies also open the door to potential security exposures. With three distinct groups within an organization implementing security policies and relying on manual processes, differences and omissions in actual policy implementation across each application, portal and server inevitably occur. For example, it might take several days for a terminated employee's access rights to be removed from all systems, resources and applications.

Security management as a business enabler

Many companies are realizing that the concentration on network-level threats has masked the real issue: Information security is more than a network

protection issue; it is a fundamental component of business policy that can proactively help a firm achieve its business goals. Advanced IT security business tools—such as identity and access management solutions—can help organizations deploy their applications and portals, quickly get users operating online and maintain policy compliance across the entire e-business infrastructure.

For example, Kemper Insurance (www.kemperinsurance.com), a leading provider of property and casualty insurance and risk management services based in Long Grove, Illinois, faced challenges in providing new users with access to applications and wanted to lower the cost of managing more than 70 production servers. By deploying an identity management solution, Kemper now can manage the day-to-day delivery of services to customers.

T. Rowe Price, a leading financial services firm based in Baltimore, Maryland, had a business imperative to deploy its www.troweprice.com portal to customers. To meet its deployment and cost goals, the company needed to eliminate the writing and maintenance of customized security rules into each application or portal. T. Rowe Price deployed an access management solution that implements and enforces security rules on behalf of all application types—Web, distributed and legacy. By removing the need to code customized security rules into each application, applications and portals can be deployed quickly and at a low cost. And because the underlying security rules are managed by the access management solution, the policy is consistently implemented without incurring the cost-of-ownership issues that previously plagued the organization. Additionally, customer satisfaction is increased through the Web single sign-on capability that this solution delivers.

Shell Canada Ltd. (www.shell.ca), based in Calgary, Alberta, has taken a similar approach. To meet the deployment and cost goals of its strategic e-business initiatives, such as its innovative *easy*PAY program, Shell has deployed an access management solution. This lets its application developers focus on writing business logic, while its security policy is consistently implemented by the IT security organization through the access management solution. Additionally, this solution allows management of the policy to be delegated from IT to business units and others to help meet the cost and flexibility needs of the business.

Highlights

Tivoli software from IBM helps companies worldwide quickly deploy new applications, including e-business initiatives, for business growth; reduce the costs of security management and administration; and effectively manage security risks and user privacy.

How IBM can help

These leading firms have transformed their IT security investments into business-enabling functions through the use of Tivoli security management software from IBM. Tivoli software helps companies worldwide quickly deploy new applications, including e-business initiatives, for business growth; reduce the costs of security management and administration; and effectively manage security risks and user privacy. Its leadership in addressing real business issues is reflected by its winning of numerous industry awards. These include *Information Security*'s inaugural 2001 Excellence Award in the Enterprise Security, Authorization and Central Administration category; Frost & Sullivan's Market Engineering Leadership Award for the European Web Access Control Software Market; and first place for security management software in the 2001 *VARBusiness* Annual Report Card Awards.

Tivoli security management software includes the following products for addressing identity management, access management, threat management and privacy management.

IBM Tivoli Identity Manager is a powerful identity management solution for getting new users online and productive quickly, while helping minimize the costs of managing users across complex environments.

Identity management

IBM® Tivoli Identity Manager, the company's flagship product for identity management, is a powerful solution for getting new users online and productive quickly while helping minimize the costs of managing users across complex environments. In use by hundreds of companies today, including Kemper Insurance, Tivoli Identity Manager centrally coordinates the creation of user accounts (including self-registration), the workflow for automating the approval process and the actual provisioning of resources.

From the user's point of view Tivoli Identity Manager provides outstanding ease-of-use, with support for self-service, Web-based password resets and account updates. From the administrator's point of view Tivoli Identity Manager is extremely powerful, with support for N-level Web-based delegated administration and advanced auditing and reporting. It also supports a broad set of resources, including applications and portals (through IBM Tivoli Access Manager for e-business, which enforces the policy on behalf of these resources) and heterogeneous servers (through integration with Microsoft® Windows®, UNIX® and mainframe operating systems, which then natively enforce the policy set by Tivoli Identity Manager).

Highlights

Tivoli Identity Manager features strong integration across IBM e-business infrastructure offerings. It can manage identities across Lotus Notes® and RACF®, and through support of Tivoli Access Manager for e-business, across IBM WebSphere®, WebSphere MQ®, DB2® and others. A new addition to the suite of Tivoli security management software, Tivoli Identity Manager supports the capabilities of Tivoli Access Manager for e-business, extending consistent security policy implementation through a single point of administration to application and portal solutions.

IBM Tivoli Access Manager for e-business avoids the need for application developers to code customized security into each application, helping reduce the deployment time and cost for new e-business applications.

Access management

IBM Tivoli Access Manager for e-business is the access management solution that T. Rowe Price, Shell Canada Ltd. and hundreds of other companies use to avoid the need for application developers to code customized security into each application. This helps reduce the deployment time and cost of new e-business applications.

This access management solution for e-business, enterprise and legacy applications supplies two critical technical requirements for e-business: the ability to support virtually any type of user authentication, and the ability to then control access to virtually any type of resource from the authenticated users. Tivoli Access Manager for e-business supports user ID/password, token card, digital certificate (through most leading public key infrastructure vendors) and other authentication mechanisms for user access and protects access to the most common applications and portals through its support for Web servers and Java™, J2EE™ and JAAS technology. It also supports many other application types through its implementation of a standards-based authorization application program interface.

Tivoli Access Manager for e-business—along with its family members Tivoli Access Manager for Business Integration and Tivoli Access Manager for Operating Systems—delivers broad support for enterprise applications and platforms, in addition to providing single sign-on to e-business applications and portals. Security rules can be enforced consistently across portals, based on platforms such as IBM WebSphere and Plumtree software; customer applications, from vendors such as Siebel; supply-chain applications, from companies such as SAP; messaging applications such as IBM WebSphere MQ; Java-based application servers such as IBM WebSphere and BEA WebLogic; object-oriented application servers; enterprise UNIX platforms; and many

Highlights

others out-of-the-box. Tivoli Access Manager for e-business also features strong support of IBM e-business infrastructure offerings. It helps secure applications leveraging the IBM WebSphere Application Server, IBM WebSphere Edge Server, IBM WebSphere Portal Server, IBM WebSphere Everyplace™ Suite and IBM WebSphere MQ. It also helps secure applications written to virtually any operating system, including z/OS™, and can store the secure user data in the DB2-based IBM LDAP Directory Server.

From the user's point of view Tivoli Access Manager for e-business provides outstanding ease of use, with support for single sign-on to Web applications and portals, as well as support for pervasive devices based on the Wireless Application Protocol and i-mode. From the administrator's point of view Tivoli Access Manager for e-business is easy to use and deploy, with Web-based delegated administration capabilities built into the core product (for situations in which Tivoli Identity Manager is not used).

IBM Tivoli Risk Manager can simplify and correlate the vast number of events and alerts being generated by numerous point products into a single console to help companies determine the severity of attacks.

Threat management

IBM Tivoli Risk Manager is a powerful solution for addressing threat management across the network infrastructure. To help administrators determine the severity of attacks, Tivoli Risk Manager automatically simplifies and correlates into a single console the vast number of events and alerts generated by numerous point products deployed across the network infrastructure. This can help reduce clutter, such as false-positive alerts, while quickly identifying real security threats to help speed response time. Decision-support tools provide insight into patterns of intrusions, as well as compliance with security policies. Tivoli software for threat management also includes IBM Tivoli Intrusion Manager, a specially engineered version of Tivoli Risk Manager for entry-level environments.

Tivoli Risk Manager can monitor the entire IBM e-business infrastructure portfolio through support of Tivoli Identity Manager, Tivoli Access Manager for e-business and native event collection capabilities.

IBM Tivoli Privacy Manager is a unique solution for dynamically defining, enforcing and managing enterprise privacy policies across the entire business.

Privacy management

Finally, IBM Tivoli Privacy Manager is a unique solution for dynamically defining, enforcing and managing enterprise privacy policies across the entire business. It allows the same consistent policy management capabilities of Tivoli security management software to be extended to business-to-business environments where privacy rules are critical.

Summary

In the past, IT security has focused solely on risk management—securing the network and sealing any openings to keep hackers, viruses and corporate thieves out. With the emergence of e-business and Web-based initiatives, many companies have expanded their view of security management, recognizing that effective security management can act as a business enabler and help them quickly launch applications and reduce IT costs.

Tivoli security management software has the proven ability to help solve the distinct challenges faced by each group within an organization. It can help IT security teams effectively manage risk by integrating alerts from various point products and reducing the number of false-positive alerts to which administrators must respond. It can help IT operations quickly provide new users with access to information and services and reduce the cost of administering all users on an ongoing basis. And it can support application developers in the business units, helping them shorten development time for new applications and reduce development costs.

IBM software integrated solutions

The Tivoli security management solution supports a wealth of other offerings from IBM software. IBM software solutions can give you the power to achieve your priority business and IT goals.

- *DB2 software helps you leverage information with solutions for data enablement, data management and data distribution.*
- *Lotus® software helps your staff be productive with solutions for authoring, managing, communicating and sharing knowledge.*
- *Tivoli software helps you manage the technology that runs your e-business infrastructure.*
- *WebSphere software helps you extend your existing business-critical processes to the Web.*

To learn more

For information on the Tivoli security management solution and integrated solutions from IBM, contact your IBM sales representative or visit **tivoli.com**/security

Tivoli software from IBM

An integral part of the comprehensive IBM e-business infrastructure solution, Tivoli technology management software helps traditional enterprises, emerging e-businesses and Internet businesses worldwide maximize their existing and future technology investments. Backed by world-class IBM services, support and research, Tivoli software provides a seamlessly integrated and flexible e-business infrastructure management solution that uses robust security to connect employees, business partners and customers.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Printed in the United States of America
04-02

G325-1769-00