Security solutions
Executive brief

Tivoli software

Help improve security and lower costs with repeatable identity management solutions.

September 2003

Contents

2 *Executive summary*
2 *Pressures drive companies to centralize security*
3 *Reusable, identity-driven security infrastructure maximizes investment*
4 *Benefits of identity-driven infrastructure*
5 *Basic security functions*
6 *Five consistent patterns into which business operations fall*
8 *Build specific solutions based on business security patterns*
10 *IBM offers integrated solutions composed of best-of-breed components*
11 *For more information*
11 *Tivoli software from IBM*
11 *IBM software integrated solutions*

Executive summary

Ever-increasing numbers of users are getting "connected." That's good for communication and for commerce. However, the convenience, ease-of-use and sheer numerical acceleration of these connections lead to daily increases in the security, privacy and auditing challenges faced by IT managers.

While providing more robust security, privacy and auditing, IT managers must simultaneously meet directives to reduce costs. Symptoms of this drive to cut costs include consolidation and streamlining of IT, outsourcing efforts, high interest in customer self-service and constant focus on automation.

Faced with these pressures, businesses generally turn to identity management. This business automation practice maximizes security efficiency and quickly returns investments in technology and services.

Companies must be disciplined to make security policies consistent, but discipline can go only so far if security solutions lack a clear methodology. This paper describes the way to develop the most effective and cost-efficient identity management solutions: utilize a reusable solution infrastructure.

Pressures drive companies to centralize security

Increasingly, IT systems must let in more users. They range from unknown users in unsecured locations who access a company's public Web site to corporate partners who use secured conduits to access shared data and applications. With so many users needing different levels of access, any individual user's access requirements can shift frequently (for example, from customer to employee to former employee).

Previously, proprietary administration systems in each individual application kept out unauthorized users. But recently, increasing numbers of users, privacy regulations, audit requirements and cost-control directives have driven companies toward centralized security solutions.

Financial cost of ignoring security risks

What is the financial impact of not adequately addressing security? In 2002, corporations in the United States lost $59 billion in proprietary information and intellectual property.[1] The average single security breach costs $2 million.[2] Recent regulations, such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA) and California Senate Bill 1386, can impose serious fines and can cause immeasurable brand damage to companies that fail to protect information. With security incidents rising drastically over the past decade,[3] it's not surprising that approximately 40 percent of IT managers rate security—more than customer relationship management, Web site management, e-business and integration—as their highest priority.[4]

At this moment, facing potentially disastrous risks (see sidebar) but needing a cost-efficient solution, your company should avoid multiple security infrastructures that duplicate efforts and can actually increase the likelihood of breaches. You need one set of security solutions that can be used for multiple business purposes and can support initiatives into future environments, such as Web services.

Companies without centralized security solutions fail to establish a necessary strategic infrastructure. They remain vulnerable to security breaches. And they suffer from inconsistent access provisioning and access rules that diverge from business goals.

Reusable, identity-driven security infrastructure maximizes investment

Today's security infrastructure is identity driven. User identities are essential for answering the two key questions that secure business applications ask: who are you and what can you access?

Effective and comprehensive identity-driven infrastructures synchronize identity information throughout companies to produce highly accurate stores of identity information. They link user accounts to that identity information. And they administer access by applying rules that accurately reflect business priorities and policies.

Recently, vendors have offered identity-driven, best-of-breed solutions that manage security functions across multiple applications and that integrate with one another. They reduce costs and improve security.

IBM has identified consistent and common business security patterns from its many security engagements with satisfied customers. Proven solutions for these patterns demonstrate how best-of-breed components can be reused across an enterprise to maximize security and minimize costs. Basing your security solution on these patterns reduces unneeded parts, repetitive and unnecessarily expensive integration, support costs, and user education.

When you deploy an identity-driven infrastructure, your organization will benefit in the short term. You will also establish a strategic infrastructure with enterprise-wide applicability and long-term value.

Benefits of identity-driven infrastructure

When you deploy an identity-driven infrastructure, your organization will benefit because you will:

- *Establish a new asset: an authoritative source of information on all users.*
- *Derive a corresponding business value from increased and more accurate knowledge of people.*
- *Reduce administrative costs, because IT administrators are freed from manual security management processes and are therefore available for revenue-enhancing initiatives.*
- *Reduce new application development costs by eliminating reinvention of security implementations—a cost reduction of as much as 20 percent.*
- *Improve audit scores, thanks to more extensive and productive tracking.*
- *Manage access to systems, applications and personally identifiable information according to a clear and complete policy.*
- *Enhance user experiences by speeding access times, delivering single sign-on to Web and other applications, and enabling the use of consistent passwords across applications.*
- *Gain control of the content in, and the relationships between, the multiple identity stores in your IT environment.*
- *Establish prerequisite groundwork for service-oriented architectures such as Web services.*

Basic security functions

The following identity management blueprint identifies the basic security functions within an identity-driven system. This blueprint groups them into three categories: identity life-cycle management, identity-driven control and identity foundation.

Identity management blueprint

Identity life-cycle management: control identity changes and resource access rules

- User enrollment and provisioning
- User self-care (including password management and updating personal information)
- User privacy preference management
- User profile management
- Credential management
- Identity policy management (for example, access rights change processes, user ID formation, password strength)

Identity-driven control: use identities

- Access control to applications, Web services and middleware
- Single point of access control decision — for new and legacy applications
- More granular control of access to UNIX® and Linux system resources
- Access control to private personal information
- Monitoring and auditing of user activities
- Single sign-on and entitlements

Identity foundation: collect, store and protect user identities

- Enterprise-wide reference providing a single authoritative set of identity information
- Standardized store based on Lightweight Directory Access Protocol (LDAP)
- Identity synchronization across multiple directories, each with some authoritative information
- Retained ownership of some user data by a variety of departments
- High availability and scalability

Five consistent patterns into which business operations fall

In early 2003, IBM augmented its own research and experience with interviews of customers from diverse industries (financial services, government, manufacturing, health, transportation, retail and others), company sizes and sectors (public, private, regulated and unregulated). Five consistent business security patterns emerged: Web presence, business-to-consumer, business-to-business, operational security and high assurance.

Leverage these patterns when you develop security solutions. Develop one solution for each business security pattern related to your business. Then apply the solution to all current and future applications within that pattern to achieve repeatable, cost-efficient, highly secure results.

Web presence

These applications provide Internet access to a company's public information. Solutions deploy multilevel security barriers and highly available servers against denial-of-service and site-defacement attacks. The goal is protecting the integrity and availability of the brand and disseminated information.

Business-to-consumer (B2C)

B2C applications include online commerce, financial services, benefits administration and subscription-based services. B2C security solutions combat impersonation, collateral access and misuse of personal data. Tools include anti-virus technology, access and authorization controls, privacy management and encryption. Security must balance enabling transactions with preserving brand and business value.

Business-to-business (B2B)

B2B interactions facilitate efficient and secure commercial transactions that reinforce trust between institutions. In addition to firewalls, access controls and intrusion detection, B2B security includes separation-of-content tools and virtual private networks. These systems prevent access to unauthorized data on other business systems and, ideally, adhere to WS-Security standards.

Operational security

Operational security refers to IT used for day-to-day business, whether in centralized or decentralized infrastructures. Security must meet geographic, regulatory and employee needs, and must supply tiered access to information. Data separation controls, audit capabilities, software provisioning and version management, and recovery from security failures are all added to access controls.

High assurance

Only a small subset of business information systems justifies multiple-method, reinforced security. These systems must properly protect sensitive information; meet service-level guarantees; fulfill missions despite attacks, accidents and failures; and prevent events that result in death, injury, illness or property damage. High assurance solutions establish and, as needed, link tamper-evident and tamper-resistant, non-bypassable trusted computing bases (TCBs).

Build specific solutions based on business security patterns

After identifying the patterns into which your business operations fall, you can begin to envision solutions that fit into your IT structure. For each of the five business security patterns that applies to your organization, you can determine what components you should deploy.

Then you can select best-of-breed components for each pattern and reuse them for all the applications that fit into that pattern. When possible, you can reuse components across patterns; for example, you should be able to use one access management solution for all your B2C, B2B and operational security requirements.

Because the most cost-effective components will be reusable across the breadth of your IT system, you should select ones that are robust. A lesser access management solution that can handle B2C transactions might seem inexpensive. But if you have to buy another access management solution for your full operational security requirements, your costs rise and inconsistent security can result.

Your security solutions provider should produce components that integrate well with one another. In most cases, best-of-breed products are applied in combinations. Avoiding functional duplication, multiple learning curves and complex integrations can significantly improve your total cost of ownership. You want a partner who makes your transition to a centralized security solution as painless as possible.

Therefore, identify a provider who supplies all of the security components you need, across the identity foundation, identity life-cycle management and identity-driven control functions described on page 5. These components include:

- *Identity stores.*
- *User administration.*
- *Access rights administration.*
- *Privacy administration.*
- *Access control.*
- *Single sign-on.*
- *Identity store synchronization.*
- *Authorization administration.*

Leveraging knowledge of your organization's business security patterns to generate solutions built on reusable, best-of-breed components will minimize your costs and maximize the integrity of your security.

IBM offers integrated solutions composed of best-of-breed components

Tivoli® identity management software from IBM provides powerful, best-of-breed components that integrate seamlessly with one another. Based on open standards, the Tivoli components can work together and with other products. Together, they provide reusable building blocks that you can use to construct a customized security solution rapidly and cost-effectively.

Tivoli identity management software from IBM

Identity life-cycle management solutions from IBM bring users, systems and applications online faster to realize operating efficiencies, cost savings and increased return on investment (ROI).

- IBM Tivoli Identity Manager centrally coordinates the creation of user accounts, the automation of the approval process and the provisioning of resources.

The IBM Tivoli Access Manager software family provides consistent identity-driven control from a single administration console, enabling single-policy access management across a broad range of resources.

- IBM Tivoli Access Manager for e-business provides end-to-end security for e-business, including single sign-on, distributed Web-based administration and policy-driven security.
- IBM Tivoli Access Manager for Operating Systems protects individual application and operating-system resources by establishing rules that fine-tune access for all accounts, including UNIX and Linux super-user and root accounts.
- IBM Tivoli Access Manager for Business Integration provides end-to-end access control, application-level data protection and centralized security policy management for the IBM WebSphere® MQ environment.

IBM Directory solutions provide a reliable, scalable and authoritative identity foundation solution you can use to maximize the value of identity management.

- IBM Directory Server supplies a powerful LDAP infrastructure that enables you to deploy comprehensive identity management applications and advanced software architectures.
- IBM Directory Integrator provides real-time synchronization among identity data sources, allowing you to establish an authoritative, up-to-date identity data infrastructure and maximize the return from your investment in products like Microsoft® Active Directory.

Privacy management solutions from IBM protect consumer trust and brand integrity by implementing and enforcing privacy policies that guard consumers' personally identifiable information.

- IBM Tivoli Privacy Manager for e-business integrates with both Tivoli Identity Manager and Tivoli Access Manager software.

For more information

To learn more about Tivoli identity management solutions and integrated solutions from IBM, contact your IBM sales representative or visit **ibm.com**/tivoli/solutions/security

To find out more about security patterns, visit http://www-3.ibm.com/security/patterns/wh_papers.shtml

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 software integrated solutions

Tivoli identity management solutions support 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®*
  Gives you the most advanced self-managing database in the world
- *Lotus®*
  Offers the instant collaboration and communication capabilities for the on demand world
- *Rational®*
  Provides best practices and tools for developing new software and customizing existing applications
- *Tivoli*
  Helps you manage the complexity of an integrated, on demand operating environment
- *WebSphere*
  Provides the must-have, open-standards architecture for the on demand era

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

09-03

[1] *CSO Security Sensor* magazine, January 2003.

[2] CSI/FBI, April 2002.

[3] www.cert.org.

[4] US IDC IT Manager Survey, December 2002.

e business on demand software