Security management solutions
Buyer's guide: purchasing criteria

IBM

Tivoli software

Address your security priorities by selecting the right identity management solution.

February 2004

Your company needs identity management—now what?

Organizations of all sizes, across all industries, are realizing that the complexity of today's IT security demands a robust solution. A solution that manages the growing variety of users who now require access to your IT resources. One that enables your organization to comply with regulations and audit requirements. One that does more even as it reduces costs.

The solution lies in managing identities. Identity management establishes centralized control to enable consistent execution of your security policies across the breadth of your organization. But it facilitates administration in a decentralized mode, giving the right amount of responsibility to the right individuals and groups—wherever they are.

Choosing to implement identity management is one thing. Figuring out how to get started toward the identity management solution that's right for your organization is another. It can be intimidating to identify what kind of software you initially need to invest in, let alone to choose the best vendor in the area you select—a vendor that can support you throughout the process of implementing your total solution.

Help locating the right first step

If you identify the security concern that most affects your business priorities, then you can focus on the kind of security solution that directly addresses that concern. Later, over time, you can expand into the other security areas that support your business goals.

This document helps you get started. It outlines the most common challenges that lead companies to invest in identity management, then indicates which components directly address each challenge. For each component, the document provides a guide for assessing whether a particular vendor's solutions are sufficiently robust. This buyer's guide also helps you analyze whether the vendor can provide the support you will need when you expand into other areas of identity management.

The overall goal: manage more users and more regulations at a lower cost

Becoming an on demand business requires giving more users more access to your IT systems. Your IT staff must manage the access not only of your employees but also of your customers, your business partners and even of unknown users in unsecured locations who access your company's public Web site. And it's not simply a matter of assigning each user one set of rights. You need the flexibility to shift rights as frequently as an employee's responsibilities change, for example.

Managing that much complexity is a substantial challenge. It's made even more difficult by the increasing numbers of regulations and audit requirements with which you must comply. Furthermore, the situation is complicated by IT-cost-reduction directives that include the consolidation and streamlining of IT, outsourcing efforts, providing more customer self-service, and automating more and more IT tasks.

Meet these challenges by implementing identity management solutions

Companies turn to identity management solutions because they address the full range of today's security challenges. Identity management is a way to address two key questions: who are you and what can you access? It helps you manage the growing number of users that come in contact with your IT systems, and consistently administer access to those users in alignment with your business requirements. Plus, it can do so in a manner that is not just cost-effective but actually provides a substantial return on your investment.

Identity management involves functions in three main areas:

- *Synchronizing identity data across your organization*
- *Linking user accounts to that identity information*
- *Administering access by applying rules that reflect your business priorities and policies–in a way that prevents the unauthorized disclosure of private and sensitive information*

When you establish an authoritative source of identity information, efficiently manage changes to both that information and the accompanying rights, and effectively implement your security policy—then you have a basis for access decisions, self-service, authorization and personalization.

The total identity management cycle encompasses all three of these areas—each reinforces the others. For example, the more authoritative your data stores are, the more confidence you can have that your security policy will be administered correctly. And when you establish user accounts that incorporate privacy preferences, that helps you to properly balance the protection and disclosure of private information in accordance with each user's desires.

Three places to get started with identity management

Each of these three main categories of identity management provides a way to start to implement an identity management solution—to move toward exerting full control over the total identity management cycle. You can begin by:

- *Establishing an authoritative store of identity information;*
- *Controlling information about users and their privileges; or*
- *Enforcing access controls and the release of data.*

To identify the ideal starting point for your organization, it helps to see what each category encompasses. Doing so also gives you a sense of how your initial investment in identity management provides a foundation for implementing a complete identity management solution.

- Fixing identity data—*collect, store and protect user identities by:*
  - *Leveraging a Lightweight Directory Access Protocol (LDAP) directory.*
  - *Synchronizing identity data across multiple data stores, each with some authoritative information.*
  - *Enabling a variety of departments to retain ownership of some user data.*
  - *Delivering high availability and scalability.*
- User management and provisioning—*control both identity changes and resource access rules by providing:*
  - *User enrollment and account provisioning.*
  - *User self-care (including password management and updating personal information).*
  - *User privacy preference management.*
  - *User profile management.*
  - *Credential management.*
  - *Policy management.*
- Access control—*use identities to:*
  - *Control access to applications, Web services and middleware.*
  - *Implement more granular control of access to UNIX® and Linux system resources.*
  - *Manage disclosure of private personal information.*
  - *Monitor and audit user activities.*
  - *Deliver single sign-on.*
  - *Support embedded and decentralized implementations.*

The next section of this buyer's guide can help you identify which of these three starting points—fixing identity data, user management and provisioning, or access control—best meets your business needs.

To begin with identity management, address your most pressing security challenges

Drawing on its own research and experience working with clients of all sizes and in all industries, IBM has identified eight challenges that frequently drive companies to implement identity management solutions. Each of these eight challenges is addressed by one or more of the three identity management starting points. The challenges are listed on the next page with their corresponding starting points.

Which of these challenges is most relevant to your business priorities? When you identify the challenge (or multiple challenges) that are most important to your company, then you will know where your company should concentrate its initial investment in identity management.

If your company needs to:	Start with:
Reduce security administration and support costs	User management and provisioning
Implement single sign-on and unified user experience	Access control
Reduce the cost of developing adequate security for industry-leading and internally built applications	Access control
Control disclosure of sensitive, private information	Privacy management
Comply with regulations and audit requirements in a heterogeneous environment (including UNIX and Linux)	User management and provisioning, access control with privacy management
Keep track of all the users that access systems	User management and provisioning, access control
Manage identity information that is spread out across multiple stores	Fixing identity data
Shore up security for deploying portals and Web services	Access control, user management and provisioning

Identifying a starting point is important, but as the next section shows, it is also important to keep in mind how you will achieve your overall security goals. That way, you can use the remainder of this buyer's guide to help you select the best solution provider for the starting point you prioritize—and still position your company to succeed when you're ready to address other security challenges.

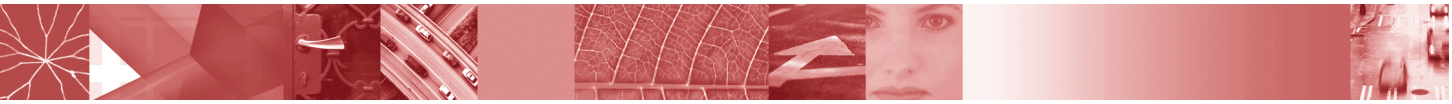
Select a solution—and a solution provider—that is designed to support your long-term security needs

Because today's security challenges are so complex, most companies choose to establish an overall architecture and then deploy it in stages. Each of these companies acts tactically and implements a solution in one area. But if the company loses sight of how that initial solution will help with the full range of the company's security goals, then it risks investing in a solution that becomes merely a short-term step—without a long-term return on investment.

Here's how you can think strategically about your long-term solution even as you begin to implement identity management:

- *You may end up with more than one of the identity management components this document identifies. Select a solution provider that can see you through the entire process.*
- *The most cost-effective solutions deploy components that are reusable across the breadth of your IT system. Choose solutions with end-to-end functionality.*
- *Components should integrate well with one another. Avoid a solution that starts you on a path toward functional duplication, multiple learning curves and complex integrations.*

Regardless of which identity management starting point is best for your organization, it's crucial to select a solution provider that can be a long-term partner with you as you implement identity management solutions.



In the following sections and for each starting point, this buyer's guide provides checklists that you can use when evaluating vendors and their products. As you look for the solution that best addresses the challenge you've prioritized, keep in mind the importance of a provider who will be able to support the full breadth of your identity management solution.

Implement a solution for fixing identity data that turns user information into a powerful business asset

With more and more users requiring access to your systems, information about those users is stored in more and more places. Your human resources department may keep up-to-date information about your employees. Your sales staff may maintain definitive information about prospective clients. Other databases may house current client and business partner information.

To administer security consistently across your organization, you require some way to synchronize user information in a highly efficient fashion. If an employee changes her name, both the human resources database and all the databases that deliver information about your company to your customers should reflect the change. When a prospective client or business partner becomes an active client, changing the status in one information store should initiate the same change in all other stores.

An identity integration solution synchronizes data across your organization. It enables you to maximize the accuracy of the data you maintain and to reduce the costs associated with manually updating that data. With a superior identity integration solution, you establish rules that identify which groups and individuals have the authority to change which data fields. The solution then pushes changes made by those with authority out to all the other databases where the same data is stored and utilized.

Among its key benefits, identity integration:

- *Synchronizes data across multiple stores.*
- *Reduces the number of people trying to maintain the same data.*
- *Enables migration of data to new applications.*

In short, identity integration helps reduce the cost of establishing an authoritative store of information. Your company can use that store to help maximize the usability of your systems for your employees and deliver outstanding service to your customers and partners.

To find a superior identity integration solution, look for one that:

- *Deploys a distributed architecture that allows local groups to manage the data they know best with the tools that make them most productive.*
- *Supplies connectors to the data stores in your organization.*
- *Can respond to predefined events, enabling automated, real-time updates to your identity stores.*
- *Deploys rapidly and extends with minimum dependencies on centralized data stores.*
- *Provides a centralized "metaview" with whatever directory or database best meets your needs—without being locked into a vendor's proprietary data store.*
- *Can be deployed on any OS platform to maximize flexibility.*
- *Leverages reusable connectors and components.*
- *Integrates a wide variety of data types, including passwords.*

Implement high-performance 24x7 directory infrastructure for global enterprise applications

To enable comprehensive identity management solutions, your infrastructure needs to be able to drive identity data to an increasing number of directory-enabled applications. The situation is analogous to critical highway infrastructure. The more comprehensive and reliable the road network, the more value can be derived from all the cars that use it. Similarly, the more comprehensive and reliable your identity data infrastructure, the more value you can derive from all the identity management and enterprise applications that use that data.

What on demand businesses require for their identity data needs is a data engine that is open, reliable and scalable:

- Open—*your data engine should run on all major platforms. To truly be a software platform for your entire enterprise, the directory must offer dynamic, extensible support into the many applications on which your enterprise depends.*
- Reliable—*to support global applications, companies like yours increasingly need to create a 24x7 directory infrastructure. Advanced replication capabilities—including multi-master capability—help ensure high availability and rapid delivery of frequently accessed content to anywhere in the world.*
- Scalable—*because your directories are growing and consolidating, you require a trusted relational database—not merely a proprietary data store. Demand a powerful data engine that can support large groups—up to hundreds of thousands of users—and continue to demonstrate superior performance even as the directory scales.*

To locate a directory infrastructure solution that meets these three standards, seek one that:

- *Is Certified LDAP Version 3 Compliant by the Open Group.*
- *Supports leading platforms, including Microsoft® Windows®, Linux, IBM AIX®, Sun Solaris, HP-UX.*
- *Offers a strong Linux solution, because many enterprises consolidate their directories on this cost-effective, powerful platform.*
- *Enables you to achieve the 24x7 availability required for global enterprise applications through advanced replication and multi-mastering capabilities—including support for dozens of master copies of the directory, and the ability to replicate different directory subtrees against different masters.*
- *Has been widely deployed in a broad range of customer applications around the world.*
- *Relies on a highly trusted relational database—rather than a proprietary data store—for excellent scalability, reliability, and performance.*

Deploy a user management and provisioning solution to cost-effectively establish consistent security

Without a system for managing security across the breadth of your enterprise, your organization can face any number of challenges. Rights may be granted to accounts for people who no longer need access because they left the company or changed roles. Your IT staff may spend an inordinate amount of time granting and limiting user rights on a case-by-case basis—draining resources away from projects that deliver greater business value. Or your company may find it costly and time-consuming to gather the information you require to comply with security audits.

User provisioning and management solutions help your company establish consistent security while reducing the cost of security administration. These solutions automate the provisioning and deprovisioning of user accounts. For example, when a new employee is added or an employee's status changes, the employee's access rights must be properly assigned or reassigned. A user provisioning and management solution applies rules about which groups of users should have which rights to automatically provision access to each employee. Automation reduces the cost of having IT staff perform a repetitive task and helps ensure that security is administered in a uniform manner.

Because user provisioning and management solutions administer access rights in a centralized, organized fashion, these solutions provide visibility across your enterprise into exactly who has what rights. This visibility enables you to track everyone who has access to your systems, and to properly align the degree of access you grant with your business priorities and needs. User provisioning and management solutions also maintain accurate records of access-rights changes for auditing purposes—reducing the cost in terms of staff time and money of complying with audit requirements.

These solutions can also integrate with privacy management solutions to help your company ensure compliance with regulations and secure the private information distributed throughout your organization.

Make sure that the user management and provisioning solution you select:

- *Manages distributed sets of users and includes the ability to assign users to one or more roles.*
- *Enforces security policies proactively—automates based on roles and rules.*
- *Extends security automation to business partners.*
- *Routes access requests through authorization processes and escalates to alternate approvers if prompt action is not taken.*
- *Interfaces with systems across your organization and those you might introduce in the future, and does so in a bidirectional, secure and bandwidth-efficient fashion.*
- *Scales as your organization changes.*
- *Has few installation dependencies.*
- *Mirrors, replicates and partitions data to maximize data integrity and availability.*
- *Includes all necessary software components, including any necessary databases, LDAP servers, and Web and application servers.*

Select an access control solution that minimizes your vulnerability and facilitates ease of use

The reason that so many more users need to access your systems is that you are offering greater numbers of more robust applications to your customers and partners. To maximize the value of these applications, they should be easy to use. To spend more time developing applications that deliver business value, your IT staff should spend less time on administration of your existing applications.

Access control solutions enable you to improve the usability and security of your customer-facing and partner-facing applications. By providing single sign-on not only for your employees but also for your partners and suppliers, access control solutions minimize a number of password-related problems:

- *Multiple-password confusion*
- *Security exposure when people write down passwords*
- *Downtime that end users experience when locked out of accounts*
- *IT staff time spent administering passwords*

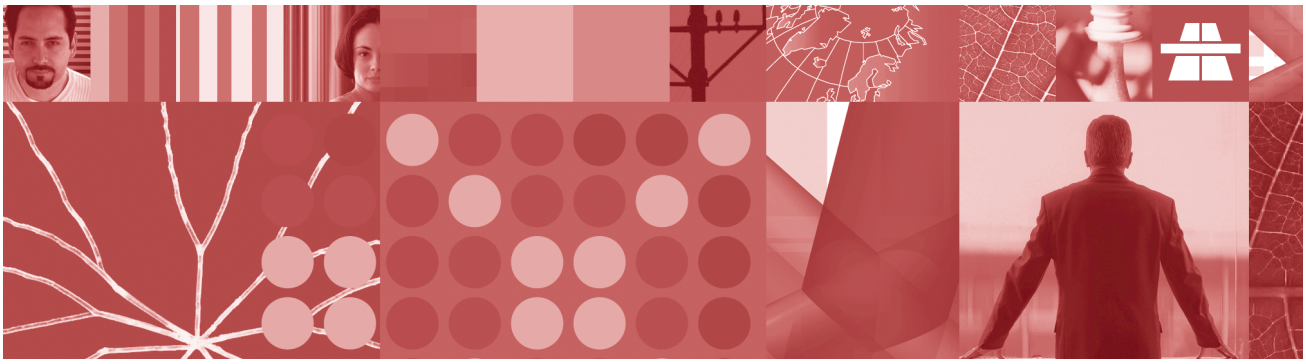
Access control also provides a foundation for personalization of content to enhance the quality and efficiency of the user experience.

By taking security development out of the application development process, access control solutions help your IT staff focus on high-value activities. When developers create security for every application, it increases the cost of development and reduces the consistency of security across your enterprise. With a centralized access control solution, your developers can call on the solution to administer security—and thereby achieve highly effective security at a minimal cost.

Additionally, access control solutions enable you to consolidate multiple access-control and authorization solutions, close security back doors into operating systems, and audit access and privacy requests.

The access control solution you choose should:

- *Support multiple authentication methods and access devices (desktops, PDAs, mobile phones, and more)—work with as many different protocols as your users deploy to access your system.*
- *Integrate widely with identity servers, applications, middleware, operating systems and platforms.*



- *Deploy policy-based security infrastructure to ease administration and align security with your business rules and business goals.*
- *Enable delegated administration, self-care and self-registration to reduce your administration workload.*
- *Rely on open standards, including Web services, to maximize interoperability both now and in the future.*
- *Handle large influx of activity—whether or not it's expected—seamlessly and without diminishing performance or availability.*
- *Use access-request data to anticipate weaknesses and enable proactive security improvements.*
- *Enhance security for all major platforms, including mainframes and applications that run on mainframes.*
- *Maximize interoperability—including single sign-on—with your existing desktop infrastructure, other security environments and leading e-business applications.*

Identify an access control solution for UNIX- and Linux-specific security challenges

Access control for UNIX and Linux environments faces the particular challenge of controlling super-user and root accounts. The top security threat that enterprises face is misbehavior by internal users and employees. Super-user accounts are particularly vulnerable to abuse because traditionally there are no controls on the access rights of these accounts, and no way to audit the actions taken by people using these accounts.

An access control solution for your UNIX and Linux systems enables you to secure the applications, files and data on these operating platforms, as well as the platforms themselves. It applies the same business policies you use to control access throughout your organization, and creates a sophisticated audit trail for tracking your system administrators. For your business-critical applications that reside on UNIX and Linux systems—and especially for companies in security-sensitive and regulated industries—an access control solution targeted at these environments is crucial if you want to implement an end-to-end security policy.

To find a superior access control solution for your UNIX and Linux environments, look for one that:

- *Combines full-fledged intrusion prevention—host-based firewall, application and platform protection, user tracking and controls—with robust auditing and compliance checking.*
- *Includes best-practice, yet customizable, policies that enable enterprises to quickly ramp up to effective security.*
- *Centrally manages access and audits across large numbers of UNIX and Linux servers.*
- *Provides extensive auditing and detailed reports you can give to regulators, external and corporate auditors.*
- *Delivers mainframe-class security and auditing in a lightweight, easy-to-use product.*
- *Integrates its GUI and policy database across security applications for your UNIX and Linux systems, Web applications, and IBM WebSphere® MQ installations.*
- *Imposes negligible overhead (less than 1%), maintains security during system backup and results in a highly scalable system.*

Choose a solution that enhances the security of your IBM WebSphere Business Integration environment

Companies that use WebSphere MQ to process personally identifiable information and other types of sensitive data often seek to extend WebSphere MQ's native security services to protect message data end to end. Additionally, as they use WebSphere MQ to tie together more and more line-of-business applications, these companies look for a way to centrally manage both data protection and access control policies across all the systems in their enterprises.

An enhanced security solution for WebSphere MQ enables these companies to demonstrate the integrity and confidentiality of messages not just while in transit from system to system, but also while under the control of WebSphere MQ itself. Moreover, such an enhanced security solution can apply business policy to provide the desired level of confidentiality and integrity for each transaction.

When analyzing enhanced security solutions for your WebSphere MQ environment, make sure you select a solution that:

- *Helps strengthen security for high-value WebSphere MQ transactions, without the need to modify or recompile WebSphere MQ applications.*
- *Maintains strict data integrity and confidentiality, using message-level audit capabilities to demonstrate compliance with the defined security policy.*
- *Helps reduce administration costs through centralized administration of access-control and data-protection policies across mainframe and distributed servers.*
- *Provides enterprise-wide management of security policies for WebSphere MQ, including message integrity and confidentiality, security audit posture, and queue access-control permissions from a Web-based administration tool.*
- *Is compatible with the other members of IBM WebSphere Business Integration family of products, including IBM WebSphere MQ Workflow, and the IBM WebSphere Business Integration Message and Event Brokers.*

Control disclosure of sensitive information with a privacy management solution

Increasingly, companies seek efficient ways to meet the growing number of regulations and consumer demand for privacy protection. The magnitude of the task can be daunting because without an automated, centralized way to manage private information, privacy policy must be coded into every individual application and implemented manually throughout an organization.

For example, companies that use common identifiers—such as Social security numbers in the United States, or taxpayer ID numbers in other countries—as ways to identify users need to hide those numbers from all employees who are not authorized to see the numbers. But in most cases, it is cost-prohibitive to rewrite applications and databases to eliminate the usage of certain sensitive data. Recoding existing applications has another drawback: this process may have to be repeated if there is a policy change in the future. An infrastructure solution is needed—one that can intelligently manage data according to policy and user preferences, without depending on individual applications for compliance.

An ideal automated, centralized privacy management solution enables you to administer privacy policy in accordance with each individual user's privacy preferences—and does so across all the privacy-sensitive applications and databases within your enterprise. Automation of privacy management helps minimize the cost of implementing your privacy policy and changes to it. And centralization enables your privacy policy to be applied consistently throughout your organization—and facilitates the automatic generation of audit reports.

In today's marketplace, it is hard to find one solution that encompasses a full range of privacy management capabilities—both to meet today's privacy challenges and to flexibly address future privacy requirements. Look for a privacy management solution that:

- *Minimizes the rewriting or redeployment of your existing applications in order to meet data-protection and privacy regulations.*
- *Generates several types of reports that help demonstrate compliance with corporate policies.*
- *Discloses the sensitive and personal data in your organization only to the right people and only for the right business reasons.*
- *Incorporates an individual's privacy preferences and applies them when granting requests for data.*
- *Helps achieve compliance with regulations without negatively impacting productivity, complicating business processes, raising costs or blunting your competitive advantage.*
- *Adheres to the common standards for privacy management, such as support for P3P (Platform for Privacy Preferences).*
- *Provides an easy-to-use administrative console that manages policies in English (or other natural languages) and doesn't require the user to have IT expertise to set and manage policy.*

Superior integration enables IBM security software to support your long-term security strategy

When you begin to evaluate vendors for whichever identity management starting point you prioritize, you'll find that IBM offers not only a best-of-breed solution in that area, but also unsurpassed breadth and integration across its security solutions. What does that mean for you? It means that when you're ready to expand into other areas of identity management, IBM can best support your long-term security goals.

IBM's leadership in integration is manifested not only in the way that its solutions work together seamlessly. Additionally, IBM solutions are built from reusable components. When you deploy a new solution that shares underlying functionality with your already-installed solution, you don't need to run two instances of the same component. IBM helps minimize the software footprint of your integrated solution, and thereby helps maximize efficiency. That is especially important when you want to deliver highly usable applications to your employees and outstanding, speedy service to your customers.

When you select IBM, you can have confidence in your partner's stability and viability. Years from now and decades from now, IBM will be there to deliver leading solutions that simplify the administration of security, no matter how complex it becomes.

Enter into identity management with superior security solutions from IBM

For every phase of the identity management cycle, IBM offers software that meets all of the criteria of a superior solution:

IBM Directory Integrator and IBM Directory Server for fixing identity data:

- *IBM Directory Integrator provides real-time synchronization among heterogeneous identity data sources, allows you to establish an authoritative, up-to-date identity data infrastructure and helps maximize the return from your existing investment in directory products.*
- *IBM Directory Server provides a powerful LDAP identity infrastructure that is the foundation for deploying comprehensive identity management applications and advanced software architectures.*

IBM Tivoli® Identity Manager for user management and provisioning—centrally coordinates the creation of user accounts, the automation of the approval process, the provisioning of resources and the generation of audit trails; Tivoli Identity Manager enables you to bring users, systems and applications online quickly, and thereby helps you realize operating efficiencies, reduce costs and increase return on investment.

IBM Tivoli Access Manager software for access control—provides consistent identity-driven control from a single administration console, enabling single-policy access management across a broad range of resources; Tivoli Access Manager family includes:

- *IBM Tivoli Access Manager for e-business, which provides end-to-end security for e-business, including single sign-on, URL and application-level authorization, distributed Web-based administration, and policy-driven security.*
- *IBM Tivoli Access Manager for Operating Systems, which protects individual application and operating-system resources by establishing rules that fine-tune access for all UNIX and Linux accounts, including super-user and root accounts.*
- *IBM Tivoli Access Manager for Business Integration, which enhances the native security services of WebSphere MQ to provide end-to-end integrity and privacy of message data, and centralized management of both data protection and access control policy.*

IBM Tivoli Privacy Manager for e-business for disclosure control—leverages Tivoli Identity Manager and Tivoli Access Manager software to implement and enforce privacy policies that guard consumers' personally identifiable information, and protect consumer trust and brand integrity.

For more information

To learn more about which identity management solution is the right starting place for your company, and to discuss the benefits of IBM security management software for your organization, contact your IBM marketing representative or IBM Business Partner, or visit:

ibm.com/tivoli/solutions/security

For an overview of how identity management can work as a cost-effective security framework across your enterprise, read the IBM executive brief on identity management:

ftp.software.ibm.com/software/tivoli/whitepapers/wp-idm.pdf

IBM also offers more detailed buyer's guides you can use when considering user provisioning and management, and access control solutions:

ftp.software.ibm.com/software/tivoli/buyers-guides/bg-ident-mgmt.pdf

ftp.software.ibm.com/software/tivoli/buyers-guides/bg-access-mgt.pdf

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.

02-04

e business on demand.™

G507-1051-00