Identity and access management solutions
Buyer's guide: purchasing criteria

Tivoli® software

Remove barriers to innovation by choosing the right identity and access management solution.

March 2008

Business leaders everywhere are renewing their focus on top-line growth — and they're seeing innovation as the means to achieve it. How does innovation happen? By eliminating the barriers to collaborative work environments and making critical resources readily accessible for effective usage by employees, customers and partners.

Yet the very access that puts innovation within reach can expose organizations to serious risk. On any given day, organizations are exposed to a multitude of internal and external security threats. Beyond these very real threats is an even bigger challenge: the need to protect the use of business systems and disclosure of sensitive business data in compliance with enterprise and governmental mandates. Without tight controls in place, business value can rapidly evaporate from a lack of customer confidence and compliance certifications, an inability to innovate due to business disruptions and the theft of customer or corporate data. To protect business integrity and facilitate compliance, organizations must:

- **Validate the authenticity of all users who access resources.**
- **Monitor that the access follows appropriate use policies and is consistent with regulations.**
- **Take corrective action where violations exist.**

What's needed is a security management solution that helps protect assets from unauthorized access but can do so without diminishing productivity. And that's why companies turn to identity and access management solutions.

Identity and access management is a way to address two key questions: who are you and what can you access? Organizations should be able to efficiently address these two questions across a variety of domains: data, processes, applications, networks and other end points, as well as the physical infrastructure. All too often, however, organizations have time-consuming, inefficient manual processes to define, implement, maintain and audit identity and access policies, such as:

- **Building security into each application and database.**
- **Managing user information in numerous directories, databases and files, in many different formats.**
- **Managing security rules for many of the same people in hundreds of places.**
- **Requiring multiple passwords.**
- **Retrieving and creating critical — yet difficult to interrelate — compliance and audit information manually from spreadsheets and other documents.**

This buyer's guide helps you select the right solution to help manage and control access within and across the enterprise. It outlines the most common identity and access management challenges organizations face from the perspective of CSOs, IT operations staff, line-of-business managers and enterprise architects. It then provides an overview of the components that directly address each challenge to help you assess whether a particular vendor's solutions best address the challenges you've prioritized.

Getting started with identity and access management

When selecting an identity and access management solution, these main categories should be addressed:

1. **Managing users and user information throughout the entire life cycle**
2. **Maximizing user productivity by ensuring efficient access to valid resources**
3. **Managing and enforcing access control policies across every application, data source, operating system and company boundary consistently**
4. **Monitoring and proving who has access to what through identity governance**
5. **Accelerating time to value**
6. **Selecting the right security provider**

For each category, you'll find checklists that you can use when evaluating vendors and their products.

1. Managing users and user information throughout the entire life cycle

IT staff often spend an inordinate amount of time managing user permissions and policies that can exist in hundreds of different places. Adding user rights on a case-by-case basis can take from hours to weeks. Removing user rights can take just as long and brings the additional risk of missing an application that should have access terminated.

To eliminate invalid access paths, teams of IT staff must perpetually audit every production server and application manually. Every time a person changes jobs, roles or employment status, all of their existing user accounts must be appropriately altered or deleted — across every application, operating system and other system.

To find a superior solution, look for one that:	IBM	Other Vendor
Provides a single, secure identity repository.	✔	
Provides an integrated Web-based interface that includes both simple wizards and a rich configuration editor to enable you to easily create, modify and view configuration objects and their relationships.	✔	
Delivers flexible account adoption methods needed to effectively and securely map accounts to their users.	✔	
Supports role-, rule- and request-based provisioning use cases equally well.	✔	
Offers core role management and separation-of-duties capabilities and provides open interfaces for integration with continuous business controls systems.	✔	
Supports tools to build user provisioning workflows using both simple wizard-based navigation and a drag-and-drop GUI for more advanced business processes — all from a common Web interface.	✔	
Synchronizes identity data across disparate data repositories, each receiving different authoritative information according to its needs.	✔	
Replicates identity data modifications, received from authoritative sources, out to other databases and directories that need to utilize it.	✔	
Manages distributed sets of users and includes the ability to assign these users to single or multiple roles.	✔	
Reconciles accounts automatically and in an on demand way to rapidly and reliably discover "orphaned" (invalid) accounts and initiates either automatic or manual remediation processes.	✔	
Automates user enrollment, from onboarding to offboarding.	✔	
Leverages identity integration capabilities to establish rules that identify which groups and individuals have the authority to change which data fields.	✔	
Maintains accurate records of configuration and user access-rights changes for auditing purposes.	✔	
Provides access to operational workflows allowing customization of the provisioning activity.	✔	
Supports provisioning intranet and extranet profiles equally well.	✔	
Supports manual services out-of-the-box so that you can quickly and easily automate business processes and gain governance over targets while still performing the actual provisioning tasks manually.	✔	
Supports manual services out-of-the-box, enabling you to quickly and easily automate business processes around phone orders and other manually administered items.	✔	
Provides a customizable role-based user GUI with views such as Manager, End User, Auditor, Help Desk and more.	✔	

Centralized, automated solutions enable you to manage tasks for administering user identities, credentials, accounts, access permissions and auditing more efficiently. Automation reduces the cost of having IT staff perform a repetitive task and helps ensure that security is administered in a uniform manner. Freed from building security into every application, IT staff can call on the solution to administer security — and thereby achieve highly effective security at a minimal cost.

2. Maximizing user productivity by ensuring efficient access to valid resources

Giving employees timely, straightforward access to valid information, applications and services can make them more productive. And opening the door to customers and partners carries with it the promise of new value and growth opportunities. But increasing the number of legitimate users creates significant security and usability challenges. Users will not be satisfied or productive if security controls block access to the resources they need or make it excessively cumbersome by requiring multiple logins and authentications.

Entering, changing and resetting passwords add up to a significant consumption of employee and IT administrator time. Single sign-on (SSO) capabilities across local, Web-based and remote systems — as well as identity and access control solutions — can 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**

Federated SSO capabilities enable users to use SSO to navigate seamlessly among Web sites across domain boundaries. Reducing both frustration and user administration costs, federated SSO capabilities promote a seamless collaboration environment with partner organizations.

Self-service capabilities can further enhance the user experience by allowing users to manage their own accounts and reset passwords. With these capabilities, users can get back up and running quickly without the added time and cost of calling the IT help desk.

The solution should increase productivity. Make sure the solution you choose:	IBM	Other Vendor
Offers an intuitive, customizable administration GUI with point-and-click capabilities that enable you to easily create new user GUI views.	✔	
Includes a multitasking feature within the administration GUI that enables you to start a task, open a second task and then toggle back to the original task and complete it.	✔	
Provides a single application architecture with a single GUI through which all administrative functions can be performed.	✔	
Allows you to submit and track status requests and monitor workflow tasks from a single GUI.	✔	
Delivers wizards and templates for fast, easy configuration along with easy GUI access to the generated script for granular customization.	✔	
Provides out-of-the-box authentication integration using a documented integration path for a wide variety of authentication solutions.	✔	
Provides a complete and integrated federation and trust management solution that includes a general-purpose security token service for common standards-based identity propagation within a Web services/SOA environment.	✔	
Offers strong integration with IBM WebSphere® Enterprise Service Bus to facilitate and secure federated access to the ESB.	✔	
Includes robust directory and directory integration and synchronization products at no additional charge.	✔	
Takes automation beyond simple SSO through the ability to automate the logon, password change and logoff processes through workflow extensions.	✔	
Provides fast user switching between users on the same shared workstation so that one can log off and another log on with minimal downtime.	✔	
Offers a wide choice of authentication factors, including user IDs and passwords, USB smart tokens, one-time passwords, active RFID and biometrics.	✔	
Supports designating the authorization level required for access to protected resources and enforcing a step-up policy when users must provide the next level of authentication.	✔	
Offers a completely configurable authentication mechanism, along with an external authentication interface to accommodate Web applications written in any language.	✔	
Provides full end-point coverage for both local and remote; extends SSO with session management, including support for personal, shared (kiosk), private (kiosk with multiple sessions), terminal clients, dial-up session, pervasive devices and roaming desktops.	✔	
Integrates widely with identity servers, applications, middleware, operating systems and platforms.	✔	

The solution should provide efficient access to valid resources. Make sure the solution you choose:	IBM	Other Vendor
Delivers SSO to users across Web applications and more, including IBM WebSphere, Microsoft®, Oracle and many other portal and application environments.	✔	
Provides direct SSO support for .NET environment applications such as Microsoft SharePoint® and Exchange servers.	✔	
Simplifies Microsoft user logins by honoring password changes for Active Directory® (AD), supporting the use of AD alternate userPrincipalName (UPN) e-mail addresses for authentication and Active Directory Application Mode (ADAM) as a user registry.	✔	
Supports multiple standards for cross-site authentication, including Security Assurance Markup Language (SAML), Liberty Alliance and Web Services Federation Language (WS-Federation) token-passing protocols.	✔	
Supports the Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) protocol to enable users to access multiple Web resources with just one login.	✔	
Builds fault tolerance into the solution, versus relying on optional third-party tools.	✔	
Provides self-service interfaces for password resets, password synchronization and user account updates.	✔	
Provides high availability by replicating policy (versus caching only), so that policy enforcement can take place even if the link to the policy server is down.	✔	
Utilizes a Web authorization approach that offers high performance and scales to user implementations in the tens of millions as well as hundreds of applications.	✔	
Offers a flexible Java™ EE Web-based architecture that can protect resources using either a hardened reverse proxy, or a plug-in module to an existing Web server. (In certain cases, a dedicated proxy can offer a higher level of security.)	✔	
Offers proven reverse proxy technology as demonstrated by over 1,000 customer installations, which is vastly superior from a change and configuration management perspective.	✔	
Includes session management services that can improve performance by limiting the number of sessions created on a per-realm basis, eliminating server restarts and allowing multiple server instances to share user sessions.	✔	
Offers a post-office feature to aggregate like e-mails and to-do work items configurable to a heartbeat of your choice.	✔	
Supports a lightweight federation solution to enable smaller organizations to quickly establish federations with a large enterprise.	✔	
Supports business-to-consumer (B2C) federation with emerging user-centric identities including OpenID and Information Card Profile using identity selectors such as Microsoft CardSpace or Higgins identity framework.	✔	

The solution should provide enterprise single sign-on (ESSO). Make sure the solution you choose:	IBM	Other Vendor
Includes an ESSO solution that is distinguished in the marketplace by its advanced capabilities to work with many different kinds of applications, integration with strong authentication, flexible approach to session management, and ability to log and audit end-user activities.	✔	
Includes a leading ESSO solution that is fully integrated, developed and supported by the same vendor providing the entire identity and access management suite.	✔	
Offers an ESSO solution built on a Java EE architecture that is easily integrated with identity, Web access, federation, strong authentication and other security components.	✔	
Provides an ESSO solution that includes a wide variety of session management capabilities including shared desktops, private desktops and roaming desktops, which facilitate fast user switching and integration of a broad set of third-party strong-authentication form factors.	✔	
Provides an ESSO solution that integrates with Web, desktop, teletype and mainframe applications, as well as many client device platforms such as Microsoft Windows® CE and Windows XPe to accommodate the broadest possible range of applications.	✔	
Provides an ESSO solution that supports desktop password reset functionality.	✔	
Supports ESSO without placing additional load on the directory infrastructure or impacting the directory schema.	✔	

3. Managing and enforcing access control policies across every application, data source, operating system and company boundary consistently

To address regulatory requirements, organizations need to protect data and applications by ensuring access policies and data disclosure rules are implemented and enforced consistently across every application, data source and operating system. Once these capabilities are in place, you should be able to conduct an audit to prove and report on the effectiveness of IT security controls, with ready answers to these questions:

- **Who can come into our applications or databases?**
- **What data resides there and what access controls should we establish as a result?**
- **Who needs access to that data?**
- **Can I easily prove that those users only accessed what they were supposed to access?**
- **Am I effectively auditing the critical data that is being accessed on my servers?**

The right identity and access control solution applies the same business policies to control access throughout your organization, including a sophisticated audit trail for tracking system administrators. It offers a closed-loop view of who has access to what, why they have access to it and what they are doing with that access. This visibility must extend to privileged and trusted users, because super-user accounts are particularly vulnerable to abuse — often there are no controls on the access rights of these accounts, and no way to audit the actions taken by people using them.

Ideally, the identity and access management solution you choose should address the full life cycle of onboarding a new user with correct role-based access permissions, enforcing those access control policies and detecting and correcting any attempts to modify security policies or user permissions.

The solution you choose should:	IBM	Other Vendor
Provide flexible, quickly configured and extensible identity feed methods that push identity data from either a single authoritative source or pull and aggregate data from multiple sources.	✔	
Provide business managers and auditors with a business-friendly description of what users can actually do with their access rights for better decision making in new access approval requests, recertification and audit reviews.	✔	
Allow administrators to apply a meaningful description to a fine-grained resource, categorize it for quick reference and search, assign an owner to it, define unique approval and recertification workflows, and provide detailed reports on these resources.	✔	
Have a workflow that seamlessly integrates with SAP and Oracle ERP, and fine-grained separation-of-duties checking with flexible exception-handling methods.	✔	
Provide a centralized management GUI for control and making modifications, to eliminate the need to manually update each individual adapter to reflect changes in authentication and authorization methodology.	✔	
Include a what-if policy change simulation analysis to identify who and what entitlements will be impacted before a change is made.	✔	
Incorporate business rules into access control decisions and evaluate these rules at run time.	✔	
Manage access control business rules outside of the application code to enable you to change policy parameters that affect access without having to rewrite and recompile applications.	✔	
Scan applications for vulnerabilities, such as cross-site scripting, and then help remediate these vulnerabilities once they are detected.	✔	
Keep track of what a user is doing across multiple concurrent sessions so that when a user logs out once, the solution can log them out everywhere to avoid concurrent logons.	✔	
Enforce access policies for inactivity timeouts, three-strikes rules and other options across multiple enforcement points.	✔	
Offer unified policy management to centrally manage and control access from operating system resources to Web-based application SSO.	✔	
Define policy-based rules that allow you to easily set security policies that apply to different systems, users, storage or information.	✔	
Set an access policy that automatically detects and remediates both intentional and inadvertent noncompliance events in real time.	✔	
Have a workflow automatically escalate and redirect workflow processes to alternate participants when prompt action is not taken.	✔	
Scale to tens of millions of users for authentication and authorization, and also scale to meet the needs of intranet, extranet and Internet user populations.	✔	
Provide scalability and availability through support for nonstandard, secure IP load balancers, intelligent load balancing over replicated servers and included clustering support.	✔	
Leverage SSL accelerator card technology by securing hardware key-stores, and providing a failover capability that allows automatic switchover to backup Web servers.	✔	

4. Monitoring and proving who has access to what through identity governance

The most effective identity and access management solutions take a centralized, scalable approach, delivering proven features and robust security across all applications in accordance with SOA design goals. Centralized administration can improve the consistency of security efforts by providing the visibility to track everyone who has access to your systems and to align the degree of access you grant with your business priorities and needs.

To manage user identities across composite business applications and business units, enterprise architects should be able to create a common identity broker service or "trusted identity management as a service." Doing so enables the business flexibility to add new services or connect existing services without having to recode identity processing as business needs change. And it allows line-of-business experts to focus on delivering the business logic that is required within the application — not on the security of the application itself.

Enterprise architects should also be able to expand the capabilities of an enterprise service bus (ESB) through the ability to efficiently and effectively manage and provision user identities across the SOA. This approach creates an "identity-aware" ESB, enabling enterprise architects to ensure users have access to applications, data and information based on their security credentials and access level, regardless of which application they are accessing.

Look for a solution that:	IBM	Other Vendor
Provides true closed-loop policy compliance enforcement that both detects and remediates access entitlements granted outside the provisioning process, instead of a complex, multiple-step serial process which could have multiple points of failure.	✔	
Includes out-of-the-box automated, configurable and sophisticated attestation/recertification processing to help address requirements such as Sarbanes-Oxley (SOX) 404 recertification of access requirements.	✔	
Utilizes a single, secure identity repository from which virtually all identity events are tracked and can be audited.	✔	
Provides a single identity GUI through which all administrative functions are performed and identity events are tracked and can be audited.	✔	
Offers audit logging of all activity — including administrative activities like policy modifications — automatically and provided out of the box.	✔	
Includes workflows as an integral part of the solution so that all life-cycle and provisioning events are managed and monitored by the solution, which can then log all transactional data for forensic audit and reporting purposes.	✔	
Establishes a central framework to govern and protect your SOA environment.	✔	
Enacts and governs proper access controls for each services application.	✔	
Translates and maps a diverse set of user identities across different services.	✔	
Manages application-specific identities across organizational silos and firewalls.	✔	
Establishes an identity trust management framework to ensure transactions are performed securely.	✔	
Propagates the required credentials end to end — from a point of contact such as an XML gateway through ESB to the back end such as an ERP or mainframe application.	✔	
Tracks and collates all login events, allowing you to audit application access.	✔	
Provides extensive auditing and detailed reports you can give to regulators, external and corporate auditors.	✔	
Centrally collects, simplifies and correlates security-related events and alerts across a wide variety of perimeter security devices.	✔	
Provides an audit trail of who has access to what and who approved those access rights.	✔	
Offers privileged user monitoring and reports.	✔	
Offers a common reporting system for scheduling, distributing, viewing and customizing reports across all solution components.	✔	

5. Accelerating time to value

As you're evaluating different identity and access management solutions, it's important to select one that offers rapid time to value. A cost-effective solution includes a number of key features designed to provide easy configuration, integration and maintenance.

Look for a solution that provides:	IBM	Other Vendor
All necessary infrastructure adapters, leading commercial versions of middleware and software components, including any necessary databases, Lightweight Directory Access Protocol (LDAP) servers, and Web and application servers.	✔	
Full-featured, out-of-the-box capabilities without limited versions of components, such as a workflow that must be upgraded to get the rich full features needed.	✔	
A best-of-breed directory and data integration and synchronization tool bundled with the solution to elegantly solve any integration challenge.	✔	
Mature, proven capabilities tested through hundreds of worldwide customer installations.	✔	
Experienced services teams available to ensure productivity remains high during the implementation.	✔	
Services specifically designed to help accelerate your implementation.	✔	
Education and training courses available to enable your staff to become productive more quickly.	✔	
The ability to address virtually all your heterogeneous target needs.	✔	
Embedded integration with the industry-leading IBM WebSphere Application Server.	✔	
Custom authentication so existing Web-based authentication applications can be swiftly integrated into the authentication process for all users without the use of third-party development.	✔	
Support for installation and easy configuration on a single server, including all underlying middleware.	✔	

Look for a solution that provides:	IBM	Other Vendor
A broad set of up-to-date integration with applications (including PeopleSoft and Siebel), support using multiple directories/user repositories and heterogeneous middleware (including Oracle Application Server).	✔	
Clear and straightforward pricing and licensing, rather than pricing based on type of use and additional premiums charged for selected servers, applications and more.	✔	
Support for local languages and incorporates dynamic language support to display deployment specific content such as password challenge/response questions or e-mail notifications in each user's preferred language.	✔	
Import/export capability of policies, configurations and workflows to accelerate promotion of systems between QA and production, or for version control of policy definitions.	✔	
Breadth of platform support, including Windows, UNIX, Linux on distributed, Linux® on IBM System z™ and IBM z/OS.®	✔	
The ability to customize the branding (look and feel) and layout of the self-service UI, while still protecting your investment by keeping customizations during fixpacks and upgrades.	✔	
Common criteria certification of Evaluation Assurance Level 3 or higher.	✔	
Standard configuration and programming languages, instead of proprietary scripting or workflow definition languages.	✔	
Tools to monitor the health and availability of the identity and access management solution.	✔	
Self-service password reset integration with service desk (help desk) system, including generation and closure of incidents (trouble tickets).	✔	

6. Selecting the right security provider

The provider you choose should be able to support the full breadth of your identity and access management solution. Ideally, you'll also want a provider who can support you throughout the process of implementing your solution. Before you select a provider, make sure to ask these questions:

Does your vendor's security vision align with yours?

Find a vendor who takes security as seriously as you do and understands how the absence of a solid security infrastructure can impact your organization.

Is your vendor focused on true enterprise security needs?

With a vendor who is focused too narrowly on a solution that addresses only a particular environment, you can run into the "islands of security" problem. Choose a vendor who can address the big picture.

Does your vendor support your business goals through their technology?

Look for vendors whose solutions align with your business objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs and speed time to market?

Does your vendor offer part of the total solution or the complete solution?

Solution costs, and the time it takes to manage multiple vendors, can rise dramatically when multiple vendors are involved. Look for a vendor with a complete portfolio for identity and access management, including UNIX® and mainframe access controls, Web services security and federation.

Are your vendor's products tightly integrated for seamless functionality?

The better integrated the solution, the less work you need to do to manually integrate the technology.

How good is your vendor's customer support?

Your vendor should offer quick, highly responsive and highly effective customer support. Be sure to understand their escalation procedures and ability to support you in a way that puts your business first.

What type of global presence does your vendor have?

If your organization has international offices, you should look for a vendor with a global presence and proven international business experience. Make sure the vendor can support your offices abroad with their own local resources.

Is the solution supported by a mature support organization with the expertise and bandwidth that can be relied on when you need them?

Find a vendor who has a proven support organization to help you maximize the value of your software investment.

Are the vendor's solutions consistently rated highly by the analyst community?

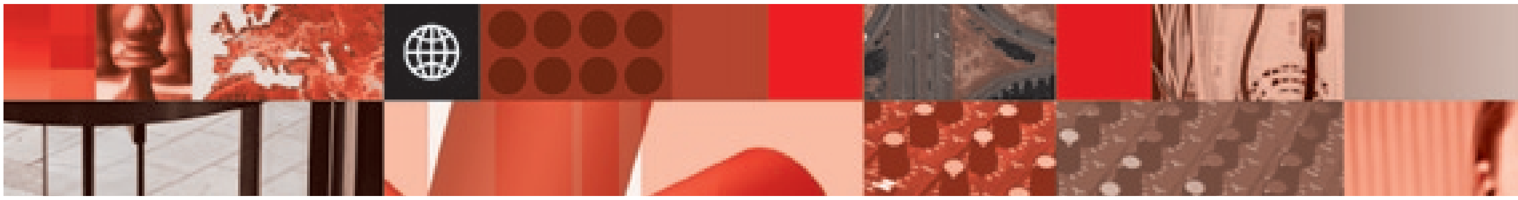
Look for solutions that are recognized through independent analysis and examination across multiple dimensions by leading analysts.

How sure are you of your vendor's stability and staying power in today's tough economy?

A big issue in today's economy is vendor stability and viability. You should consider a vendor who has a long history in the industry, a solid, forward-looking strategy and the resources to overcome adverse economic times.

Can your vendor deliver products that are strategically designed and technically superior?

When comparing various security solutions, look for technical superiority — well-designed functionality, an intelligent architectural design and broad support for industry standards such as Security Assertion Markup Language (SAML), Liberty Alliance, WS-Federation, Service Provisioning Markup Language (SPML) and eXtensible Access Control Markup Language (XACML).



Address your identity and access management needs with IBM

When you begin to evaluate identity and access management vendors, you'll find that IBM offers not only best-of-breed solutions, but also unsurpassed breadth and integration across their security solutions. Only IBM enables you to focus on driving business innovation by reducing the complexity of securing the enterprise through a flexible and adaptable approach across the entire realm of IT security risk. So when you're ready to expand into other areas of security management, IBM is ready to support your long-term security goals.

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

- **IBM Tivoli® Identity Manager software enables you to quickly provision user identities, manage those identities and their access rights throughout their life cycles, and enable user self-service (such as password reset) — all in alignment with your security policy.**
- **IBM Tivoli Access Manager for e-business provides end-to-end application security across the enterprise, including SSO, URL and application-level authorization, distributed Web-based administration and policy-driven security.**
- **IBM Tivoli Access Manager for Operating Systems protects unstructured data files, plus application and operating system resources by establishing rules that fine-tune access for all UNIX and Linux accounts, including privileged user accounts such as super-user and root accounts.**
- **IBM Tivoli Federated Identity Manager delivers cross-domain or federated SSO as well as identity propagation in SOA and Web services environments, enabling partner interactions that are trusted, convenient, auditable and address key compliance concerns related to partner access from other domains.**
- **IBM Tivoli Access Manager for Enterprise Single Sign-On helps simplify, extend and secure ESSO for end users to Web and non-Web applications so that you can optimize productivity, password-related help-desk costs and password management by end users.**
- **IBM Tivoli zSecure Suite joins together administration, audit, alert and monitoring capabilities for IBM z/OS Resource Access Control Facility (RACF®). It is designed to help minimize security exposures and streamline compliance efforts.**

This broad portfolio of identity and access management offerings can help provide the infrastructure necessary to support today's requirements. Beyond managing user identities and access to resources, establishing a centralized and automated identity and access management infrastructure from IBM can ultimately become a business enabler — helping you:

- **Minimize the complexity of responding to multiple internal and external controls and regulations.**
- **Optimize productivity and costs by capturing, creating and automating best practices for repeatable tasks.**
- **Free IT staff to focus on higher-value activities.**
- **Provide the agility needed to stay ahead of new business opportunities by removing the barriers to innovation.**
- **Drive the integrity and confidentiality of business processes.**

For more information

To learn more about which identity and access management solution is right for your company and to discuss the benefits of IBM service management software for your organization, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security

About IBM Tivoli service management software

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation — visibility to see and understand the workings of their business; control to effectively manage their business, minimize risk and protect their brand; and automation to optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

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

Produced in the United States of America
March 2008
All Rights Reserved

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

TAKE BACK CONTROL WITH Tivoli®