Identity and access management
White paper

Secure and compliant collaboration and access.

March 2008

IBM Service Management
Visibility. Control. Automation.™

Contents

Overview

In today's competitive and global business climate, information flows faster, new products get to market quicker, customers and competition are better informed, and new innovative and competitive business models continually emerge. To respond and adapt to these ever-changing pressures and opportunities, businesses must remain agile and connected. This means giving their people faster access to actionable information, making collaboration easier and enabling individuals and teams to work when, where and how they choose.

This need for more dynamic collaboration and access creates significant security and compliance challenges for organizations – especially in light of the growing mobile workforce – as well as the need to link customers, partners and suppliers into many of an organization's systems and processes. To facilitate compliance and help protect the confidentiality, integrity and availability of its data, applications and systems, organizations must validate the authenticity of all users who access resources, ensure that access controls are in place, consistently enforce them, and monitor and report security events.

Unfortunately, traditional security offerings take a bottom-up approach to addressing these challenges, solving point problems with point products that rely on fragmented policies and processes. This narrow approach to security results in increased complexity, redundant costs, resource inefficiencies, security gaps and data silos that often undermine the ability and productivity of the business and its people.

Organizations need to take a holistic approach to security, aligning security initiatives with the goals of the business. This top-down approach to security enables organizations to leverage security as a way to protect and enhance business processes and collaboration. However, such an approach needs to be modular in design, allowing organizations to focus on those areas of greatest importance first.

Highlights

Drawing on a deep understanding of today's security threats from both within and outside the enterprise, IBM offers an adaptable, business-driven, holistic approach to security that addresses the different risk domains that affect an organization's security posture:

- **People and identity** — Make sure people inside and outside the organization — including its suppliers, partners and customers — have access to the data and tools that they need, when they need it, while blocking those who do not need or should not have access.
- **Data and information** — Support widespread electronic collaboration, while protecting critical data whether in transit or at rest.
- **Applications** — Proactively protect business-critical applications and processes from external and internal threats throughout their entire life cycle — from design to implementation and production.
- **Network, server and end point** — Preemptively and proactively monitor and manage emerging threats and vulnerabilities to an organization's network, server and end points.
- **Physical infrastructure** — Protect IT assets with physical access controls as well as ensure that physical assets are protected from security threats in order to enhance overall security.

As part of its comprehensive security framework, IBM offers a broad, unified array of integrated access authorization and identity management solutions that enable organizations to secure their collaboration and access processes in alignment with their overall business needs.

Leverage a standards-based, business-driven life-cycle approach to identity and access management

Innovation has always been a hallmark of information technology, with new ideas driving better ways to gather, share and leverage the power of information across the enterprise. But with more robust ways to share and use information come more potential vulnerabilities – not only from outside but also from within the enterprise. Employee errors, data stolen by employees or business partners, and insider sabotage are all among the top 10 threats to enterprise security, according to industry analysts.

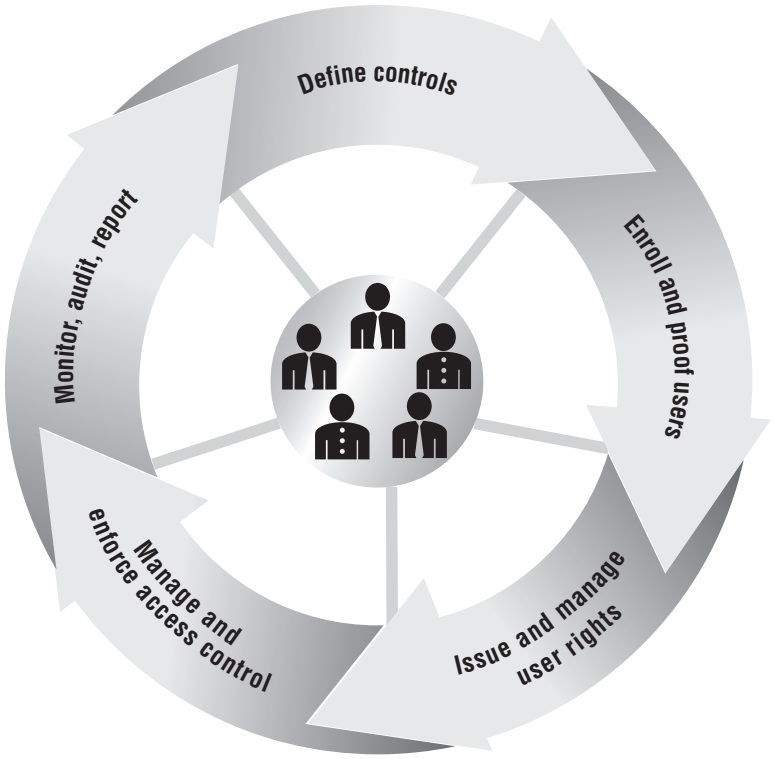
Employee errors, data stolen by employees or business partners, and insider sabotage are all among the top 10 threats to enterprise security, according to industry analysts

To address these critical security and business challenges, IBM takes a standards-based, business-driven life-cycle approach to identity and access management. This life-cycle process integrates access authorization and identity management in a way that enables organizations to cost-effectively protect assets and information, while empowering dynamic collaboration and access that fuels business productivity. As a repeatable process, the life cycle enables organizations to manage these risks across numerous business initiatives, while reducing costs, improving user experiences, increasing efficiencies and supporting compliance efforts. Doing so also enables them to support compliance with regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Basel II, EU Data Protection for personal information and Health Insurance Portability and Accountability Act (HIPAA).

The five main phases of this identity and access management process life cycle include:

- Defining controls.
- Enrolling and proofing users.
- Issuing and managing user rights.
- Managing and enforcing access control.
- Monitoring, auditing and reporting on user rights and activities.

Identity and access management process life cycle	
1. Defining controls	IBM identity assessment and strategy services IBM Tivoli identity and access management solutions
2. Enrolling and proofing users	IBM Identity Resolution IBM Relationship Resolution
3. Issuing and managing user rights	IBM Tivoli Identity Manager IBM Tivoli Directory Server IBM Tivoli Directory Integrator IBM Tivoli zSecure suite with RACF®
4. Managing and enforcing access control	IBM Tivoli Access Manager IBM Tivoli Federated Identity Manager IBM Tivoli zSecure suite with RACF
5. Monitoring, auditing and reporting on user rights and activities	Tivoli Identity Manager Tivoli Security Information and Event Manager



The following sections of this paper describe the five main phases in greater detail.

Define controls

Effective identity and access management doesn't start with tools and technologies – it starts with the proper definitions of controls and related processes. In this phase of the process, IBM identity and access management

Highlights

By defining appropriate controls and processes at the beginning of the life cycle, organizations can establish effective security policies that focus on the essential security capabilities that meet their business priorities

solutions help organizations define controls and processes based on relevant standards, legal and regulatory requirements, and business needs and objectives. This approach includes assessing the identity requirements of the business environment, as well as identifying what resources need access controls applied to them, what users and types of users should be entitled to resource access and what type of access should be granted. By defining appropriate controls and processes at the beginning of the life cycle, organizations can establish effective security policies that focus on the essential security capabilities that meet their business priorities.

Enroll and proof users

IBM identity and access management solutions help organizations discover and detect identities and relationships of interest at the point of contact before it's too late to stop inappropriate user access. It enables them to identify who is who, and what relationships individuals have with others. It provides entity resolution and analysis methodologies that can identify obvious and nonobvious relationships in real time. It includes the ability to uncover relationships, even if individuals on the network are trying to hide or disguise their identities. In addition, it enables organizations to perform analytics at the time of enrollment on data streams across multiple data sources.

Issue and manage user rights

Beyond providing the capability to issue the proper credentials to users and groups, IBM identity and access management solutions give organizations an effective and efficient means to keep user rights up to date, including adding, updating, reconciling and removing rights as the user's access needs evolve.

These include the ability to help:

- Quickly provision user identities and credentials, and manage them throughout their life cycle.
- Easily identify and eliminate orphan accounts to reduce the risk of former partners and employees accessing information and resources that they should no longer have access to.
- Match accounts with identities, as well as verify access rights via account recertification.
- Provide user self-service, allowing users to reset their own passwords without delay, while reducing help-desk overhead.

Manage and enforce access control

Visibility into user access is critical to an organization's ability to manage and enforce access control. IBM identity and access management solutions provide a centralized access control policy management platform to deliver this needed level of visibility and help facilitate security and compliance efforts. It can also help organizations control user access to the right resources, validate that users are who they say they are and enforce what users can do within various applications or services. To enhance user productivity, it automates user access with single sign-on (SSO) capabilities. Furthermore, as organizations establish service oriented architectures (SOAs), the need to connect multiple user accounts as part of a composite SOA transaction becomes paramount – and a potential management and compliance challenge. The identity and access management capabilities within IBM WebSphere® Enterprise Service Bus enable organizations to map, propagate and validate user identities across different identity systems.

Monitor, audit and report on user rights and activities

To ensure existing controls and policies can protect critical business processes and sensitive information, organizations need the ability to constantly and easily monitor, audit and report on user rights and activities. IBM identity and access management solutions offer critical monitoring, auditing and reporting on user accounts and activity to help organizations ensure they're properly protected, efficiently address audits and compliance reporting, and continually improve their identity controls.

Protect business systems and information with identity and access management

The foundation of any information security strategy is the ability to authenticate and authorize the users in the enterprise. As the definition of a legitimate user expands to cover not only traditional employees but partners and customers, the challenge of identity and access management becomes more complex, and threats to the enterprise infrastructure and valuable corporate information increase.

Highlights

IBM solutions enable monitoring of user activity to enforce compliance with enterprise security management policies

IBM solutions streamline user life-cycle management and facilitate fine-grain control over access to the resources entitled to an organization's users. Furthermore, IBM solutions enable monitoring of user activity to enforce compliance with enterprise security management policies, allowing organizations to more easily document and prove that they have an effective control environment in place. IBM's leadership in this area is demonstrated by its consistent positioning in the leadership category of Gartner's Magic Quadrants for Web Access Management and User Provisioning reports.

Access authorization

Access authorization should provide timely access throughout the user's life cycle – across multiple environments, security risk domains, data processes, applications, networks and other end points, and the physical infrastructure. And, it needs to do this while enforcing security and protecting the IT environment from internal and external threats, as well as supporting compliance efforts. Accordingly, an access management solution should provide:

- Centralized control to help ensure consistent execution of security policies across multiple applications and users.
- Automation with a policy-based security infrastructure guided by both IT requirements and business goals.
- SSO capabilities across local, Web-based and remote systems, as well as identity and access control solutions to minimize a number of password-related problems, including multiple password confusion, security exposure caused by people writing down their passwords, end-user downtime due to account lockout and time spent by IT staff administering passwords.
- Integration of access and identity management within one infrastructure environment.
- Identity federation to share user authentication and attribute information between trusted Web services applications.

IBM solutions in this area include Identity and Access Management Services as well as IBM Tivoli® Access Manager for e-business. Serving as a hub for authentication and authorization for Web and other applications, Tivoli Access Manager for e-business centralizes security management and makes it easier and more cost-effective to deploy secure applications.

IBM Tivoli Access Manager for Enterprise Single Sign-On provides simple authentication capability across Web and non-Web applications to help automate SSO, enhance security with automatic password management, reduce help-desk costs, and extend audit and reporting capabilities.

IBM Tivoli Access Manager for Operating Systems 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 Federated Identity Manager enables customers, suppliers and partners to conduct business across disparate environments and multiple security domains in a protected, flexible and efficient manner. Providing a simple, loosely coupled model for managing identity and access to resources, Tivoli Federated Identity Manager also helps reduce integration, help-desk and security administration costs with an easy-to-use, rapidly deployable SSO solution. In addition, IBM Tivoli Federated Identity Manager Business Gateway facilitates the ability of small-to-midsize organizations to establish federated Web SSO capabilities, allowing them to bring together customers, partners and suppliers with a single, easy-to-deploy application.

In an SOA and Web services environment, Tivoli Federated Identity Manager delivers trust management capabilities to secure access to mainframe and distributed services. For example, it offers robust token mediation and can map identities from multiple sources and security domains.

To give organizations the ability to monitor user behavior across their entire infrastructure, IBM Tivoli Security Information and Event Manager provides an enterprise security compliance dashboard with in-depth privileged user monitoring capabilities, powered by comprehensive log and audit trail collection capabilities.

Identity management

Managing user identities and their rights to access resources throughout the identity life cycle is critical to effective identity and access management. An integrated solution should include the key areas of identity management:

- Identity life-cycle management, including user self-care, enrollment and provisioning
- Identity control, including access and privacy control as well as SSO and auditing

To address these requirements, IBM Tivoli Identity Manager provides a security-rich, automated and policy-based user management solution to help effectively manage user accounts – along with access permissions and passwords – from creation to termination across the IT environment.

For directory, directory integration and workflow requirements, organizations can turn to IBM Tivoli Directory Server and IBM Tivoli Directory Integrator. These identity foundation components supply a scalable, standards-based way to store and synchronize the disparate sources of user identity data throughout an enterprise.

IBM Identity and Access Management Services helps organizations assess, design, implement, deploy and manage integrated identity management solutions that draw on technologies from IBM and IBM Business Partners. IBM Identity and Access Management Services can help with all phases of identity life-cycle management.

Highlights

IBM provides the full breadth and depth of solutions and services that enable organizations to take a business-driven, holistic approach to security

Take advantage of the wide range of IBM services

IBM Identity and Access Management Services can provide a broad array of consultation, support and other services to help customers manage growth and complexity, control escalating management costs and address the difficulties of implementing security policies across a wide range of Web and application resources.

With IBM, you can develop appropriate policies for managing risk and build the capabilities needed to enforce those policies. IBM teams with IBM Business Partners to provide strong multifactor authentication including smart cards, biometrics and role-based access control.

Secure and enhance business collaboration and access

Drawing on a deep understanding of today's security threats – and backed by more than 40 years of leadership in the IT security field – IBM provides the full breadth and depth of solutions and services that enable organizations to take a business-driven, holistic approach to security. With its comprehensive security framework, IBM has the ability to assist organizations to manage and mitigate risks across the entire realm of IT security risks, delivering the technologies and expertise needed to bring the proper focus and emphasis to the vulnerabilities and impacts most relevant to each organization's unique business needs.

The modular and integrated nature of the IBM security framework makes it easy for organizations to focus their efforts on their most urgent challenges first, while extending their focus to other areas as needed. In terms of securing collaboration and access in alignment with business objectives, IBM offers a broad, unified array of access and identity management products and services designed to protect assets and information from unauthorized access while enhancing business productivity and agility.

For more information

To learn more about how IBM security solutions can help you secure your collaboration and access processes in alignment with your overall business needs – or to learn more about how the various comprehensive security framework offerings from IBM can protect and enhance your business operations – contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM Service Management

IBM Service Management helps organizations deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

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

Produced in the United States of America
March 2008

GMW10330-USEN-01