

Effectively manage access to systems and information to help optimize integrity and facilitate compliance.



March 2007

Contents	
2	Overview
3	Answer key questions related to identity and access management
3	Understand the unified IBM strategy for security
5	Protect business systems and information with identity and access management
5	<i>Identity management</i>
6	<i>Access authorization</i>
8	Take advantage of the wide range of IBM services
8	Summary
8	For more information
8	About IBM solutions for enabling IT governance and risk management

Overview

In the face of growing numbers of complex regulatory requirements, organizations must find a way to protect their information and systems while giving ever-growing numbers of users access to the systems and applications they need. This is particularly critical when it comes to the continually growing business requirement to increase employee, customer and trading-partner access to valuable data and resources, such as in a service oriented architecture (SOA) environment.

Equally challenging for today's organizations is finding robust security capabilities to address the major aspects of identity and access management: provisioning, productivity, access and audit.

An organization needs a solution that helps manage users and their access to business systems and information. To help protect data integrity and facilitate compliance, the organization must validate the authenticity of all users who access resources, ensure that access controls are in place and consistently enforce them.

Drawing on a deep understanding of today's security threats from both within and outside the enterprise, IBM provides a unified strategy for developing enterprise security solutions, and identity and access management represents a modular entry point into IBM security solutions. A comprehensive, standards-based approach that integrates access authorization and identity management enables organizations to cost-effectively provide authorized users with access to applications and data while protecting these assets from unauthorized access.

Helping to protect assets and information without affecting business productivity, IBM solutions for identity and access management can enable companies to address their enterprise security needs and help reduce costs, improve user experience, increase efficiencies and support compliance.

Highlights

Answer key questions related 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 IDC analysts.*

As part of addressing the critical challenges of security in general, today's organizations need ways to answer a number of questions related to access control:

- **Provisioning** — Is every user account on every resource valid? Is user access configured correctly to every resource? And does it stay that way?
- **Productivity** — Are users efficiently gaining access to valid resources?
- **Access** — Are access policies and data disclosure rules implemented consistently across every application, data source and operating system?
- **Audit** — How can the organization identify inappropriate access by privileged and trusted users? How can it find inappropriate access to database management system (DBMS) resources?

Understand the unified IBM strategy for security

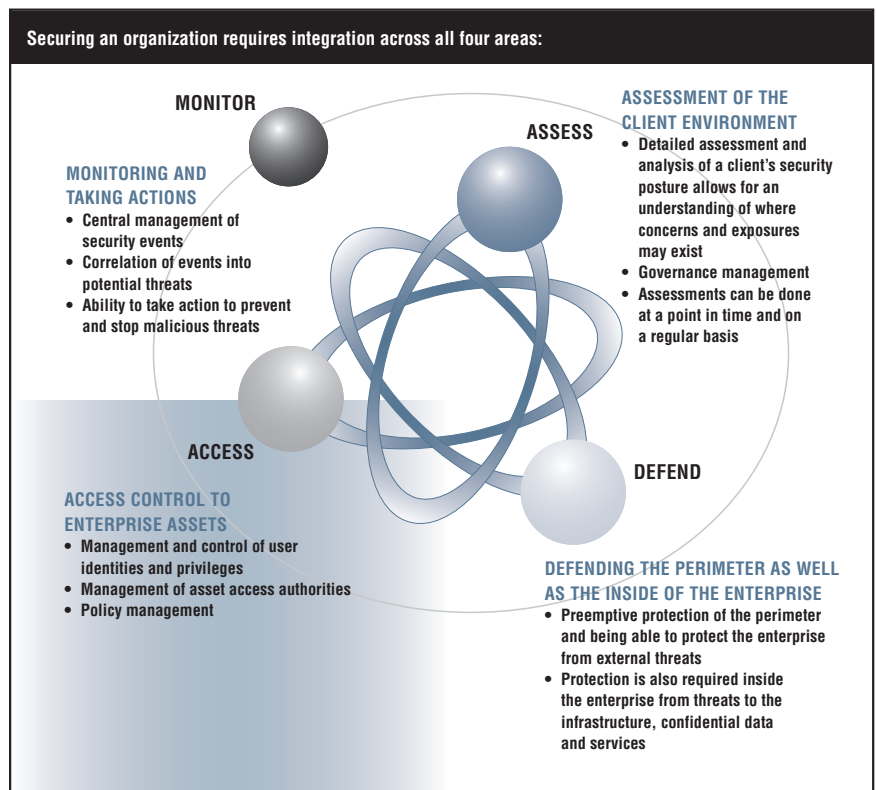
IBM is a leader in developing IT security solutions. Drawing on extensive customer experience, broad technical knowledge and deep understanding of today's security threats, IBM provides a unified strategy for enterprise security that includes four essential functions:

Assess: *to understand an organization's security exposure.* Assessment solutions combine security consulting expertise with product and service offerings to help accurately inventory enterprise assets, apply trusted security policies, and identify and prioritize vulnerabilities.

A leader in developing IT security solutions, IBM provides a unified strategy for enterprise security, including assess, defend, access and monitor solutions

Defend: *to protect the organization from external and/or internal threats.* Solutions for security defense integrate products and services that support effective threat detection and fraud prevention while helping to protect data, Internet-based systems, physical environments and applications.

Access: *to implement and manage user identities and to provide access authority across applications and data sources in a secure environment.* Access solutions enable organizations to define, implement, maintain and audit identity and access policies, as well as the rights of individuals. As such, the



Access control is best enabled by an integrated program of identity management and access authorization.

Highlights

IBM technology and service offerings help organizations stay ahead of security threats and support compliance and business requirements

solutions help protect assets and information from unauthorized access – but can do so without diminishing business productivity.

Monitor: *to monitor and act on security exposures and intrusion attempts.*

Monitor solutions include monitoring and reporting capabilities to help organizations proactively detect, analyze and react to threats.

IBM believes that today’s enterprise security solutions should address all four of these functions but enable customers to implement them at their own pace. Advanced, modular and affordable IBM technology and service offerings help organizations stay ahead of security threats while supporting compliance and business requirements.

Protect business systems and information with identity and access management

Looking at the IBM strategy for identity access and management in greater detail, you will see that IBM offers a number of different identity and access solutions. Depending on the organization, the security management strategy typically supports one or both of the following management 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 single sign-on (SSO) and auditing

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

IBM Identity and Access Management Services helps organizations 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.

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.

Access authorization

Access authorization should provide timely access throughout the user's life cycle – across multiple environments and security domains – while enforcing security and protecting the IT environment from external threats. 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 to help improve user experience and reduce help-desk costs.
- 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 a simple authentication capability across applications. The product helps 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 addressing system vulnerabilities surrounding UNIX[®] and Linux[®] privileged user or 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 an SOA and Web services environment, Tivoli Federated Identity Manager also 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.

IBM Tivoli Federated Identity Manager Business Gateway is the ideal entry point for establishing federated Web SSO capabilities. Built especially for small-to-midsized organizations, this powerful collaboration software uses open standards to bring together customers, partners and suppliers with a single, easy-to-deploy application that provides a smooth migration pathway to an enterprise-level application. For example, a large enterprise can improve its customer experience by providing new and expanded services from its small, value-added service partners using Tivoli Federated Identity Manager Business Gateway.



Take advantage of the wide range of IBM services

IBM Identity and Access Management Services can provide extensive 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.

Summary

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 a unified strategy for developing enterprise security solutions.

For requirements involving secure, controlled access, IBM products and services are designed to protect assets and information from unauthorized access, but without affecting business productivity. IBM solutions for access and identity management help companies address their enterprise security needs while supporting compliance and business requirements.

For more information

To learn more about how IBM security solutions can help you defend against threats both known and unknown – or to find the entry point that is right for your organization – contact your IBM representative or IBM Business Partner, or visit ibm.com/itsolutions/security

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards-based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit ibm.com/itsolutions/governance

© Copyright IBM Corporation 2007

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

Produced in the United States of America
3-07
All Rights Reserved

IBM, the IBM logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks or service marks of others.

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.

*Brian Burke and others, *Worldwide IT Security Software, Hardware, and Services 2006–2010 Forecast: The Big Picture*, IDC study, December 2006.