Manage user identities efficiently to help increase administrator and user productivity, while facilitating compliance initiatives.

Highlights

- Centralize and automate repetitive identity life-cycle management tasks to drive productivity, consistently enforce security policy and simplify audit processes
- Consistently enforce access policies, centrally collect audit data and enable enterprise single sign-on
- Streamline identity management across organizational and corporate boundaries with identity federation products and services

Time-consuming tasks related to identity management constantly pull your IT administrators and employees throughout your enterprise away from high-value initiatives that enable innovation.

For example, service level agreements (SLAs), legal requirements and internal policies can place significant stress on user identity management processes. You must track the life cycle of each user identity: When was the account created? When was the user given access to each service or application throughout your enterprise? Who approved the account creation? How has the account changed? Collecting this and many other types of data manually across the breadth of endpoints that your team manages can require a significant dedication of time and resources. Without some level of automation and repeatability, collecting identity information becomes a new project each time reports are required for internal and external audits.

Think also about the productivity drains associated with password management and account creation. Because a high percentage of help-desk calls are typically to reset passwords, it has been estimated that manually resetting passwords represents up to 40 percent of help-desk costs.* In addition to taking the time of administrators who could otherwise pursue more strategic

activities, users who request password resets temporarily lack access to the resources they need to be productive. When users are waiting for new accounts, getting them provisioned quickly is critical for productivity.

To help optimize security, productivity, and audit and compliance efforts, IBM offers a broad portfolio of identity management solutions — systems, software and services, plus financing — that help organizations stay ahead of threats. Centrally managing and streamlining identity management is one of several components of IBM security solutions, which help customers establish effective risk management strategies to manage and secure business information and technology assets, anticipate vulnerabilities and risk, and maintain timely access to information. IBM security solutions help organizations align technology with business priorities and redirect resources that might otherwise be dedicated to resolving security problems toward initiatives that deliver innovative, strategic and substantial value to the business.

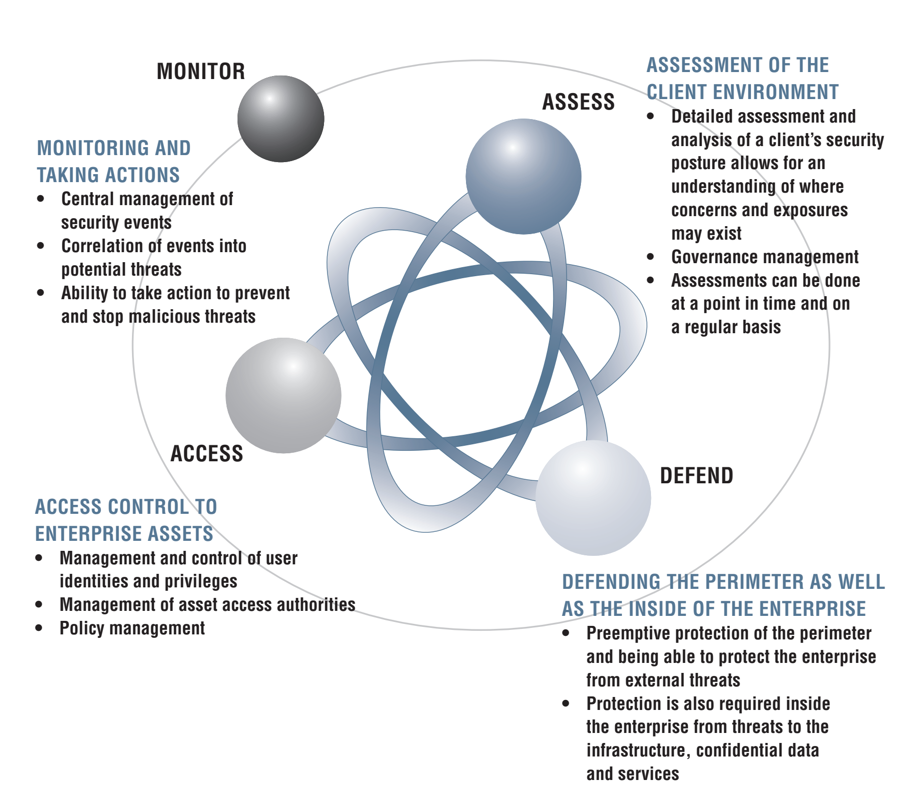
The following sections describe ways that IBM offerings help organizations centrally manage and automate identity life-cycle management, access control and identity federation across the enterprise, from mainframe to workstation.

Streamline identity provisioning and enable user self-care

Manual identity administration frequently leads to slow and inconsistent operations. It is easy for an administrator to miss a group assignment, particularly when facing numerous accounts whose privileges change frequently. Many organizations also find that they commonly have too many orphan accounts — a byproduct of manual administration that creates unnecessary risk.

To help you address these challenges, IBM offers identity life-cycle management tools and services that automate repetitive tasks in alignment with your business requirements. The workflow and provisioning engines embedded in IBM Tivoli® Identity Manager help streamline the submission and approval

Securing an organization requires integration across all four areas



MONITORING AND TAKING ACTIONS

- Central management of security events
- Correlation of events into potential threats
- Ability to take action to prevent and stop malicious threats

ASSESSMENT OF THE CLIENT ENVIRONMENT

- Detailed assessment and analysis of a client's security posture allows for an understanding of where concerns and exposures may exist
- Governance management
- Assessments can be done at a point in time and on a regular basis

ACCESS CONTROL TO ENTERPRISE ASSETS

- Management and control of user identities and privileges
- Management of asset access authorities
- Policy management

DEFENDING THE PERIMETER AS WELL AS THE INSIDE OF THE ENTERPRISE

- Preemptive protection of the perimeter and being able to protect the enterprise from external threats
- Protection is also required inside the enterprise from threats to the infrastructure, confidential data and services

of user requests and can consistently enforce your security policies. Working with your existing platforms — across distributed and mainframe environments — Tivoli Identity Manager helps you centralize user definition and user service provisioning to help minimize errors and inconsistencies.

While the software centralizes administration to execute your best practices consistently, it also offers a flexible administration model so you can delegate administrative privileges where appropriate. Managers of groups used for access can control their own groups, and the central Tivoli Identity Manager server synchronizes their changes and checks them for noncompliance.

Furthermore, Tivoli Identity Manager features user self-care capabilities that allow end users to reset and synchronize passwords themselves — in line with your policies. As a result, the product helps you both optimize security and free your IT staff from administrative functions to pursue more strategic activities.

Tivoli Identity Manager also helps you reduce the time spent responding to audit requests and manual policy reviews. Drawing on its centralized audit trails across key information systems, it can quickly create standard, centralized reports on security policy, current access rights and audit events. You can use this information not only to respond to audits but also to take a more proactive approach to compliance.

IBM Identity and Access Management Services provide assistance in implementing, deploying and managing

Draw on identity foundation components to enrich solutions

To help companies with their directory integration and workflow requirements, IBM offers IBM Tivoli Directory Server and IBM Tivoli Directory Integrator. These products are frequently combined with the other identity management solutions described in this document to supply a scalable, standards-based foundation for storing and synchronizing the disparate sources of user identity data throughout your enterprise. Tivoli Directory Server and Tivoli Directory Integrator can help you manage identities consistently and with great flexibility. Additionally, Tivoli Directory Integrator provides data object–level integration beyond user identities. Its open, Java™-based architecture and broad set of technology handlers help you streamline and mitigate the risk associated with custom-scripted data integration.

integrated identity management solutions. Whether you need to identify the deficiencies in your current identity management processes; find a host for provisioning, credentialing and reporting services; or anything in between, IBM Identity and Access Management Services can help you with any phase of identity life-cycle management. Examples include the following:

- Identity assessment and strategy
- Identity proofing
- Identity life-cycle management
- Directory services
- Access management
- Strong authentication solutions

IBM Identity and Access Management Services draw not only on robust IBM offerings but also on leading technologies from IBM Business Partners to deliver the identity management capabilities your particular organization requires.

Facilitate auditing and offer single sign-on

While identity life-cycle management is important for effective role-based access, IBM also offers leading access control solutions that help you enforce the access rights, password policies and information management policies you establish. These solutions help ease compliance efforts — by maintaining centralized audit trails for access requests — at the same time that they enable your administrators and users to be more productive.

IBM Tivoli Access Manager for e-business provides a single point of authorization for Web applications, helping you overcome the difficulties of implementing security policies across a wide range of Web and application resources. As a result, you can consistently give employees, partners, suppliers and customers role-based access to the information and services they need.

To help streamline efforts to comply with audit requests, Tivoli Access Manager for e-business centralizes collection and reporting of audit, log, statistics and other information across the extended enterprise. Plus, it writes audit records in a standard XML format that can be easily parsed to extract the information you or your auditors require.

Tivoli Access Manager software supports several strong authentication techniques. Together with IBM Tivoli

Federated Identity Manager, Tivoli Access Manager for e-business comes with 30 out-of-the-box reports that cover the issues most commonly of interest to auditors.

From the perspective of your end users, IBM access control software provides a consistent access mechanism that can improve productivity. Tivoli Access Manager for e-business offers end users the ability to use a single identity to gain access to myriad resources through its support for Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO).

IBM Tivoli Access Manager for Enterprise Single Sign-On enables users to log in once to access applications and services across your enterprise. Only needing to keep track of a single identity and password not only simplifies the user experience, it also helps reduce the incidence of lost passwords (and the resulting loss of productivity for users and IT staff) and minimize security vulnerabilities associated with passwords that are written down in unsecured locations.

IBM Identity and Access Management Services can help you design, implement, deploy and manage access control solutions. For example, IBM Identity and Access Management Services can help you determine and address your requirements for single sign-on, authentication (including multifactor authentication), and physical and logical access.

IBM identity management offerings include:

Identity life-cycle management
- Tivoli Identity Manager
- Tivoli Identity Manager Express

Access control
- Tivoli Access Manager for e-business
- Tivoli Access Manager for Operating Systems
- Tivoli Access Manager for Enterprise Single Sign-On

Identity federation
- Tivoli Federated Identity Manager
- Tivoli Federated Identity Manager Business Gateway

IBM Identity and Access Management Services

Share user authentication and attribute information between trusted parties and Web services applications

A growing desire among today's business entities is to share identity information with trusted parties, such as external partners or other internal business units. Organizations that can do so offer their users a significantly improved, seamless experience. This concept, called *identity federation*, also helps optimize security for even the most complex business services, while minimizing the security management burden on your IT organization.

Tivoli Federated Identity Manager allows you to use leading federation standards to grant access to user identities that a trusted organization manages. As a result, you can more easily develop third-party services to offer other organizations and enable your own users to take advantage of third-party services — without forcing them to navigate between federation sites. Within an enterprise, Tivoli Federated Identity Manager helps you secure transactions using SOA and Web services technology across distributed and mainframe environments. For small-to-midsize businesses, IBM Tivoli

Federated Identity Manager Business Gateway is the ideal entry point for establishing a federated single sign-on solution.

With Tivoli Federated Identity Manager software, you can grant role-based access to your users and enable them to spend less time logging into different organizations and environments, so they can be more productive. You can also use IBM Identity and Access Management Services to develop and/or implement the identity federation solution that's right for your organization.

For more information

For more information about how your organization can use IBM security solutions to manage user identities in ways that help increase both security and productivity — or to find the IBM security solutions 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

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

Produced in the United States of America
3-07
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.

*Maxine Holt, senior research analyst, Butler Group, quoted in René Millman, "Avoiding an Identity Crisis," *SC Magazine*, April 5, 2006. scmagazine.com/uk/news/article/551843