IBM Software

Thought Leadership White Paper

February 2013

When millions need access: Identity management in an interconnected world

Best-practice security solutions that scale to meet today's huge numbers of users

Contents

Introduction

With millions of transactions occurring online almost every day, business today really occurs without boundaries. Customers, business partners, vendors and other constituents all need to access your network—or your cloud—to make purchases, find information or use applications. While these new categories of users are essential for maintaining a competitive edge, your organization also needs to carefully monitor them and grant appropriate, safe access to protected resources. And there are thousands—in many cases, millions—of them.

Their interest and involvement can be good for business. But how do you manage such a number? Manual procedures for identity management—everything from granting access to assets to managing user accounts—are a classic example of processes that simply don't scale. They can work when the number of users is small. But manual procedures can become a significant burden when numbers reach into the thousands—and impossible when the numbers stretch to millions. Just think about resetting passwords. How could you maintain a help desk big enough for a world full of customers?

As organizations transform business by opening their systems to large numbers of internal and external online users, many of whom are mobile, they are increasingly adopting automated solutions that secure sensitive data, support end-user self service and help resolve problems. For today's instrumented, interconnected and intelligent IT operations, best practices for identity management can help ensure secure, optimized and regulatory-compliant operations.

Effective management based on self service and access control

Today's need for effective identity management is the result of an explosive growth in connectivity. An insurance company, for example, that until recently managed access for a few thousand employees now needs to manage millions of customers and partners conducting online transactions through a sales portal. A government agency previously managing access only for its employees now needs to manage access for millions of citizens and a wide range of other agencies accessing information online. Organizations in areas such as healthcare, finance and other customer services industries rely heavily on interaction and data exchange between large numbers of partners and consumers.

The result has been a sudden and unprecedented increase in the scale and requirements of online business operations—and an increased demand on organizations' identity management systems. Organizations now need systems that can give employees, business partners and external end users the self-service capabilities they need to quickly enroll for new services and resolve individual problems—including the ever-present issue of password resets—without having to contact the help desk. At the same time, organizations need systems that give administrators—whether IT operators, line-of-business managers or human resources professionals—control over permissions and other user-access functions.

IBM offers industry-leading solutions based on the principles of the IBM Security Framework to meet scalable identity and access management needs. These solutions deliver user administration and management, resource protection, and audit-reporting capabilities to help reduce the risks of security breaches and non-compliance.

For example, IBM® Tivoli® Federated Identity Manager provides capabilities such as business-to-consumer self-service enrollment and federated single sign-on (SSO) support that organizations can supply to their external constituents. IBM Security Identity Manager is an automated, policy-based solution that manages the lifecycle of user access across IT environments within the organization. IBM Tivoli Security Policy Manager allows organizations to centralize fine-grained security policy management to enforce access control across applications, databases, portals and business services.

Security and compliance across the full user lifecycle

An effective identity management solution meets a full range of online business needs—from pressures to stay competitive by providing greater access to more information and services, to requirements to demonstrate compliance by controlling and monitoring all user activities and their associated access privileges. The solution should include tools for restricting user access to only those IT resources appropriate to their role and/or job function, centralized user self service, simplified administration and approvals processing, periodic revalidation of user access rights, and documentation of policy controls. Add to all that the need to manage the rising costs of account provisioning and deprovisioning, recertification of access rights, help-desk calls, password resets and other administrative tasks.

As organizations grant access to different types of users, including employees, customers, business partners and suppliers, they need best-practice solutions that can support the full lifecycle of user identity, from the efficient onboarding of new users to their final off-boarding and the elimination of unidentified or "orphan" accounts.

Externally, they need a secure, easy-to-use solution that makes minimal demands on the organization's IT staff to administer.

Internally, they need to create user accounts in ways that allow new hires or employees with new roles to be productive as soon as possible. To avoid potential security exposures, they need to retire accounts and associated access privileges quickly for employees who leave the company. Additionally, internal users need secure access to externally hosted applications, including cloud-based applications and business partner applications.

Cloud environments usually support a large and diverse community of users, so managing identities across multiple cloud services is especially critical. Identity federation and capabilities for rapid onboarding must be available to coordinate authentication and authorization with the enterprise's back-end or third-party systems. A standards-based, SSO capability is required to simplify end-user logins for both internally hosted applications and the cloud, allowing end users to easily and quickly leverage cloud services.

When it comes to compliance, organizations need enterprise-wide capabilities to ensure that both internal and external access are governed by effective authentication, to monitor authorization and network traffic, and to support the system with comprehensive audit and reporting capabilities.

Regardless of the type of user, the solution should enhance security by helping to fill gaps in security measures. It should mitigate the risk of issues such as fraud, theft of intellectual property or loss of customer data. It should help reduce costs by streamlining business and IT processes that grant users access to resources.

Paths to success in the identity and access management environment

Each organization has to determine the details of ensuring effective identity management, because each organization has its own needs, goals and set of users. Leading use cases for identity and access management, however, typically fall into three categories:

- Portal-based access for large populations of users
- User access to cloud-based services
- Business partner access and application integration

In each case, organizations are transforming the way they provide user access. To achieve this transformation, they typically provide self-service functions as they help ensure secure operations and support regulatory compliance.

For these scenarios—which are rapidly increasing in number and complexity as banking, retail and public sector organizations increase the value-added services in their online operations—the organization not only must address issues of security, scalability and usability, it must also manage back-end tasks for application integration. Organizations deploying service-oriented architecture (SOA) solutions need an effective policy-based approach that incorporates security management and services that can be integrated with existing SOA components.

Use case 1: Portal-based access for large populations of users

A large state health information exchange portal needs to provide 3 million consumers and several hundred payers and associated providers with access to clinical and administrative data. It also must enable secure collaboration among healthcare organizations, facilities operators and insurance companies. It needs a solution that can centrally manage user authentication to ensure that patient records remain private as it securely expands access to consumers, payers and providers. By ensuring identity management and enforced access control, the solution must support compliance with Health Insurance Portability and Accountability Act (HIPAA) security regulations and updated healthcare information exchange (HIE) requirements.

How Security Identity Manager helps

Through the use of roles, accounts and access permissions, Security Identity Manager helps automate the creation, modification and termination of user privileges throughout the entire user lifecycle. For internal enterprise users and for trusted partners or suppliers who need access to internal company resources, Security Identity Manager enables the organization to grant permission to access information and applications and then to control access as the user's role and responsibilities change. Users are granted self-service capabilities in areas such as password reset, but the detailed workflow and processes for defining access rights based on role/job requirements and for avoiding access conflicts of interest make Security Identity Manager the most appropriate choice for effective internal identity management.

How Tivoli Federated Identity Manager helps

For business-to-business and business-to-consumer scenarios, in which organizations extend access to large numbers of external users, Tivoli Federated Identity Manager provides self-service enrollment capabilities, as well as federated SSO and centralized authentication support to enforce access control. It also validates users and eliminates the need to provide multiple IDs and passwords, reducing the workload for IT administrators. Using federated SSO and user access management techniques to help integrate this information can provide quick benefits and savings.

Tivoli Federated Identity Manager can expand collaboration with business partners who need limited access to internal resources by providing entry-level federation capabilities and by scaling to larger numbers of applications and users when necessary. The result: lower identity management costs, improved compliance and reporting, and simplified integration of services including centralized user access to software as a service.

Use case 2: User access to cloud-based services

A global financial services company with 120,000 employees, 3 million external users and operations in 50 countries implements a cloud computing architecture to standardize its IT infrastructure and services. In the process, the company consolidates several data centers into a few next-generation data centers. The hybrid cloud solution that results provides the company with an automated, virtualized infrastructure on a single platform with different severs, self-service request-driven provisioning from a service catalog, and secure access to services based on roles and business needs.

To achieve security management in its new cloud-based data centers, the organization implements Tivoli Federated Identity Manager, securing collaboration with business partners and providing SSO for external users into the hybrid cloud environment.

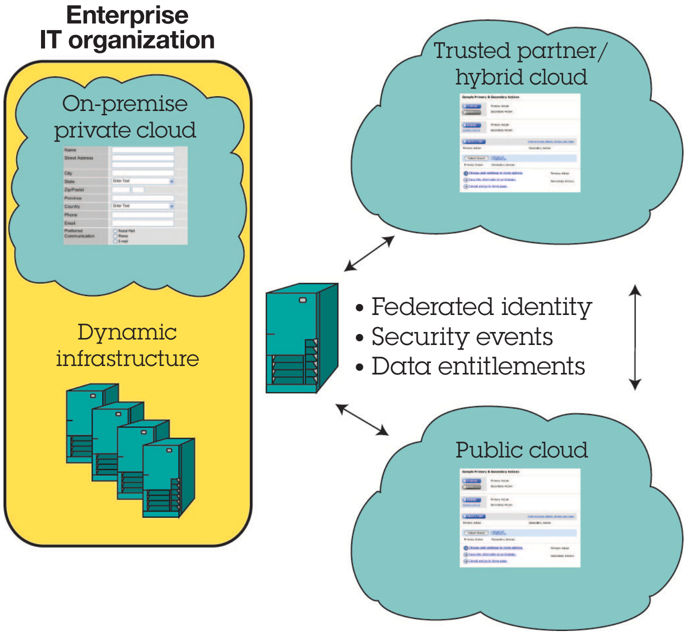
Similarly, an organization with 2,000 software engineers spread across 25 teams implements a developer cloud environment to give teams access to services whenever and wherever they need it. Users log in to request capabilities—including operating systems, memory, disk space, middleware and more—and gain access in minutes.

To achieve secure and dynamic access for users and to eliminate lag times in delivering that access, the organization implements Security Identity Manager. Password resets that used to take hours or days to complete now take only minutes—because users can log into a self-service portal and reset their passwords themselves. As new members join the team, they can gain rapid access to services, and as members depart, IT staff can remove their access rights to all systems with one command, rather than logging into dozens of different systems.

How Security Identity Manager helps

Giving internal users access to a cloud-based application is essentially the same as providing access to other applications. Security Identity Manager provides identity management capabilities that enable the organization to provide internal users, including privileged users, with self service and access rights to cloud-based services.

Securing access to cloud-based applications and services

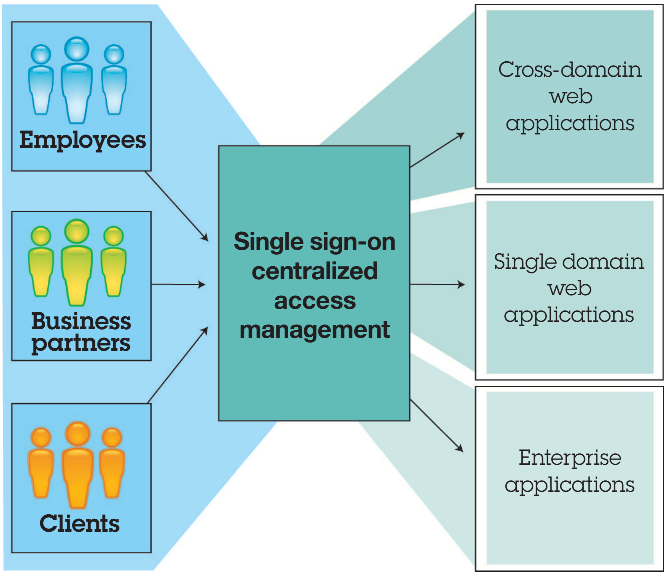


With Tivoli Federated Identity Manager, the organization can centrally control access for large numbers of users to its cloud-based services hosted by external providers such as salesforce.com.

How Tivoli Federated Identity Manager helps

Using cloud-based computing to provide online applications and data to a large group of users—everyone from employees in other parts of the organization to customers and business partners—requires particular attention to security. The larger the group, the more difficult it is to manage user identity. With Tivoli Federated Identity Manager, however, the organization can centrally manage and enforce access policies to on- and off-premises applications and services (including integrating with software-as-a-service and cloud-based solutions) and reduce IT administration costs while helping enterprises strengthen and automate user access rights.

Tivoli Federated Identity Manager's SSO capabilities enable the user to go directly to cloud-based applications and information without having to manage identities within the cloud. The user's identity is federated into the cloud transparently to the user. In a typical scenario, authentication of the user takes place outside the cloud and involves IBM Security Access Manager for Web, included within Tivoli Federated Identity Manager. Security Access Manager for Web, also available as a standalone offering, combines user access and web application protection into a highly scalable user authentication, authorization and web SSO solution. The Tivoli Federated Identity Manager package also includes IBM Tivoli Federated Identity Manager Business Gateway, which provides standalone capabilities to support federated SSO and integration into cloud and software-as-a-service offerings.


Employees
Business partners
Clients
Single sign-on centralized access management
Cross-domain web applications
Single domain web applications
Enterprise applications

Single sign-on can simplify user access to multiple applications and sources of data.

Use case 3: Business partner access and application integration

An insurance company is migrating its legacy, host-based application to a new portal-based solution and needs to provide service providers, mobile agents and clients with information on their policies and contracts. The organization also requires fine-grained, authorized access to insurance policies and contracts based on roles and additional attributes. Concern for compliance and data security issues lead the company to deploy Tivoli Federated Identity Manager and Tivoli Security Policy Manager to enable easy and secure SSO capabilities for both internal and external users, ensure an auditable record across the enterprise, and enforce data-level access control on a need-to-know basis.

How Tivoli Federated Identity Manager helps

Tivoli Federated Identity Manager simplifies application integration for identity management via an identity mediation service. Instead of requiring tiers of access for reaching the application, the solution validates, transforms and authenticates users one time to provide application access, whether it is to legacy mainframe-, Java- or Microsoft .NET-based applications. For enterprise users and business partners who require special access to secure information, this use of identity management provides a record as identities are mapped to access for audit and compliance use.

How Tivoli Security Policy Manager helps

Tivoli Security Policy Manager provides organizations the ability to manage and enforce fine-grained entitlement and data-level access control on a need-to-know basis. In the case of the insurance company, Tivoli Security Policy Manager allows mobile employees access to client contracts based on roles and on additional business attributes and context critical to ensuring privacy and data security.

IBM self-service solutions for internal and external users

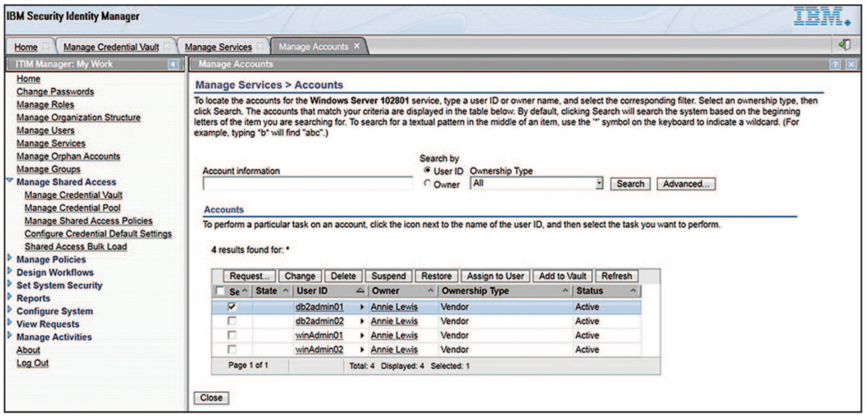
Security Identity Manager and Tivoli Federated Identity Manager provide self-service functions for streamlined management of internal or external user access to business information and applications. The results can be dramatic—up to 80 percent reduction in provisioning time for new employee accounts, up to 40 percent reduction in identity management administrative costs and up to 35 percent reduction in password-related calls to the help desk.[1]

Security Identity Manager provides complete identity lifecycle management capabilities that support enrollment, permission and access control for the complete period in which a person is employed at a company—with management functions that also work for business partners, suppliers and other external constituents who may need trusted access to internal resources. The solution combines role management and user provisioning to deliver appropriate access rights to users. In addition, a hierarchical role structure streamlines administration and provides visibility into user access to infrastructure resources. Web self service for managing roles, accounts and passwords further simplifies administration and reduces administrative costs by enabling users to perform tasks themselves. Self-service requests can be configured to define which attributes are allowed for self service and which require approval. This is ideal for a high-volume, large-scale web environment where the exact identity of users is not known.

When users must access resources beyond their own organization, Tivoli Federated Identity Manager provides a highly scalable business-to-consumer self-service solution for enrollment, along with strong authentication, in which:

- External users initiate enrollment and select their passwords.
- The organization customizes challenge/response options, authentication methods and access to applications.
- The user deletes the account when it is no longer needed.

Tivoli Federated Identity Manager provides the federated SSO and user access management techniques that are necessary for integration across organizational boundaries.



Manage Services > Accounts

To locate the accounts for the **Windows Server 102801** service, type a user ID or owner name, and select the corresponding filter. Select an ownership type, then click Search. The accounts that match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the "*" symbol on the keyboard to indicate a wildcard. (For example, typing "b" will find "abc".)

Account information

Search by ● User ID ○ Owner

Ownership Type: All

Accounts

To perform a particular task on an account, click the icon next to the name of the user ID, and then select the task you want to perform.

4 results found for: *

□ Se	State	User ID	Owner	Ownership Type	Status
☑		db2admin01	Annie Lewis	Vendor	Active
□		db2admin02	Annie Lewis	Vendor	Active
□		winAdmin01	Annie Lewis	Vendor	Active
□		winAdmin02	Annie Lewis	Vendor	Active

Page 1 of 1 Total: 4 Displayed: 4 Selected: 1

Security Identity Manager is a centralized source for identity management throughout the user lifecycle.

The solution provides an identity trust management framework that enables an organization to know who is connecting to resources and what credentials they are using—without having to manage users individually. This is ideal for protecting assets where users are connected to critical resources from access points over the Internet or other less-secure environments.

The two solutions can be deployed independently or together. While Tivoli Federated Identity Manager manages user authentication and authorization to applications, Security Identity Manager focuses on the management of user identities and passwords in a closed-loop, workflow-based solution. Combining both products can provide access to an expanded set of applications and services. Organizations also can employ a phased implementation to gradually increase the number of users supported. This enables the organization to prove the solution's business value with a smaller initial set of users, and then expand the number of supported users over time.

Security Identity Manager

This automated, centralized, policy-based solution utilizes roles, accounts and access permissions to manage user access throughout the entire user lifecycle. Using user self service, delegated administration, automated approvals processing, periodic revalidation of access rights, and documentation of controls, it can help increase user efficiency, reduce IT administration costs, enforce security and manage compliance. Security Identity Manager is designed to reduce cost and risk by easing the onboarding and off-boarding of users, and by reporting on user activity and ongoing access certification.

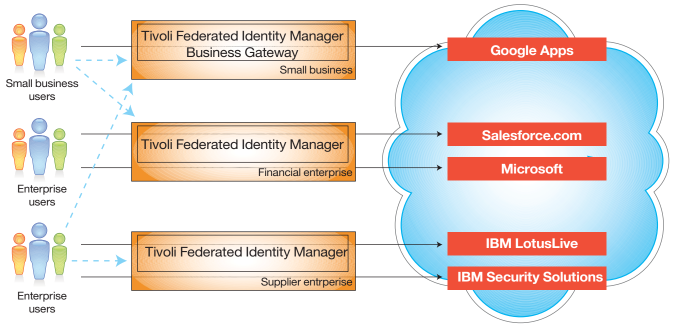
Security Identity Manager helps organizations solve major challenges of identity management: meeting internal and regulatory compliance requirements, maintaining an effective security posture and achieving a measurable return on investment.

Using Security Identity Manager, the organization can:

- Simplify and reduce the cost of administration with streamlined group management and bulk user recertification
- Reduce setup time and training with simplified policy, workflow and configuration
- Support enhanced security and reduce help-desk costs with centralized password management
- Correct and/or remove non-compliant access rights automatically or through periodic access recertification workflows
- Enhance security and compliance with separation of duties
- Define processes for workflow and provisioning using predefined templates

Separation-of-duties capabilities can strengthen security and compliance by creating, modifying or deleting policies that exclude users from membership in multiple roles that may present a business conflict. For example, a user in an accounts receivable role cannot also have an accounts payable role. This preventive approach can guard against violations occurring in the first place.

Security Identity Manager supports role-based provisioning, which grants access rights according to corporate policies and individual duties, as well as request-based user provisioning, which automatically routes a user's requests for access to the appropriate manager for approval. The resulting flexibility helps organizations administer quick, secure user access. It enables the provisioning of new users in minutes rather than days so they can be productive as soon as possible.



Tivoli Federated Identity Manager provides users external to the organization with easy-to-use, self-service access to services.

Tivoli Federated Identity Manager

Tivoli Federated Identity Manager facilitates collaboration inside and outside an organization by delivering federated SSO. It provides a central, standards-based web access management system to manage and enforce user authentication, SSO and self service for business-to-business, business-to-employee and business-to-consumer deployments across the enterprise. For scenarios in which the number of consumers connecting and interacting with a company often number in the millions, this user-centric solution relieves the complexity and expense of provisioning and managing user accounts.

Tivoli Federated Identity Manager helps organizations establish a framework for knowing which users are connected to services and what credentials are being used to connect without having to manage individual users.

Using Tivoli Federated Identity Manager, an organization can:

- Provide federated SSO for secure information sharing across private, public and hybrid cloud deployments
- Support user self care for business-to-consumer and mobile user scenarios with initial password selection, password change/reset, and the ability to customize challenge/response options for customer-specific needs
- Manage user authentication and identification information about business partners through multiple open standards-based identity and security tokens
- Reduce administrative costs, establish trust and facilitate compliance by managing, mapping and propagating user identities
- Simplify integration with business partner websites to reduce security vulnerabilities
- Allow users to share private information without needing to share user identities and passwords

Tivoli Federated Identity Manager provides automation for creating accounts, creating or modifying user profiles, and creating and changing passwords or secret questions. It is also an SOA identity service solution that provides end-to-end identity mediation and token validation across diverse applications, services and mash-ups through its Security Token Service (STS).

The IBM Security portfolio of identity and access management solutions

Security Identity Manager and Tivoli Federated Identity Manager are included within the IBM Security identity and access management portfolio, which enables organizations to control, monitor and authenticate user access to protected data and applications. These solutions balance security and usability, while also simplifying management of the complex user profiles and access needs in cloud computing environments. At the same time, they can help organizations cope with the security challenges of mobile workers and trusted insiders, who often pose the biggest threat to an organization's information integrity and data privacy.

IBM: Your trusted partner for leading IT security solutions

The IBM Security Framework, an integrated portfolio of software, hardware and services built to deliver security intelligence, helps organizations address today's complex security environment. The IBM Security Framework delivers a unified approach to enterprise security that manages key functions ranging from threat detection to user access, compliance, cost reduction and configuration management—and much more—all with a foundation in world-renowned research and development to help protect business-critical data, support compliance activities, and reduce the risk of today's advanced threats.

For more information

To learn more about IBM Security solutions, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

[1] Results and savings based on IBM customer experience from installed systems.

Please Recycle