



Tivoli software

Extend business reach with a robust security infrastructure.



Contents

- 2 Overview**
- 3 Adapt to today's security landscape**
- 4 Drive value from end-to-end security solutions**
- 5 Assess security requirements**
- 6 Institute effective identity and access control management**
 - 6 Manage user accounts across the enterprise***
 - 6 Validate and exchange user identification with trusted enterprises***
 - 7 Enforce policy-based access control***
 - 8 Synchronize identity data across multiple repositories***
- 8 Help identify attacks, malware, misconfigurations and misuse to mitigate security risks**
- 9 Implement, enforce and report on security compliance policies**
- 10 Leverage IBM leadership in security solutions**
- 11 Summary**
- 11 For more information**
- 12 About Tivoli software from IBM**

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. IBM security management solutions are designed to work across platforms and applications to integrate and support critical business initiatives. Through extensive features and tools, an organization can establish centralized, automated policies and processes to help minimize security risks and address regulatory mandates – freeing IT staff from routine security tasks to focus on integrating existing systems and extending the network.

IBM provides end-to-end service management solutions for successful innovation, including the implementation and management of new-generation architectures. Our proven solutions enable customers to establish an enterprise-wide hardware and software foundation, manage optimal business flexibility and ensure effective service delivery. New technologies can be quickly and cost-effectively assimilated into their environments. Workload balancing, provisioning, availability and security can be more easily and effectively managed across new architectures.

IBM service innovation solutions represent one of a number of modular entry points into IBM Service Management, a comprehensive, fully integrated approach to closing the gap between business and IT innovation. IBM Service Management helps organizations both create and manage value, with products and services that address the complete service management life cycle, from business management to IT development and IT operations, with solutions spanning hardware, software, consulting and financing services.

This white paper discusses the advantages of IBM security management offerings, which are designed to deliver integrated, comprehensive solutions across a heterogeneous environment. Specifically, this white paper discusses how this comprehensive offering of software, services and expertise from IBM helps organizations create an on demand operating environment, where trading partners, suppliers and customers can interact dynamically – and securely.

Adapt to today's security landscape

As more and more business processes depend on IT, an IT department must demonstrate that it has established and is consistently enforcing controls to manage the confidentiality, integrity and availability of business information and processes. In other words, IT security is critical to supporting the business goals of nearly every organization. Examples include:

- Providing anytime, anywhere access to business applications and services from a variety of devices to enhance employee productivity and strengthen consumer relationships.
- Supporting the transition to component-based applications and a service oriented architecture (SOA) to enable the business to adapt quickly and take advantage of opportunities.
- Addressing myriad compliance initiatives, from government and industry bodies as well as from contractual arrangements with business partners.

All of these dynamics and many more add to the complexity and increase the requirements for effective security management. To manage this complexity efficiently and become more effective about managing IT as a whole, enterprises turn toward more formalized governance efforts, often based on frameworks such as IT Infrastructure Library® (ITIL®) and Control Objectives for Information and related Technology (COBIT). To implement security management effectively, organizations should:

- Define security policy that addresses multiple external and internal requirements.
- Consistently enforce that policy across geographic locations, business units and heterogeneous resources.
- Be able to demonstrate the effectiveness of the controls, especially in response to audit requests.

According to IT research and analysis firm Gartner, identity theft generated almost \$15 billion in losses in 2005. “Enterprises bear the brunt of the financial losses” — about \$13 billion of the total, according to Avivah Litan, vice president and research director at Gartner.¹

A comprehensive security management infrastructure can help reduce the burden on people inside and outside the organization, from line-of-business executives to IT managers and beyond to include trading partners and customers. It also helps keep employees available to work on the innovations that can deliver value to the business, rather than stuck responding to, or paralyzed by, the latest audit request or security incident.

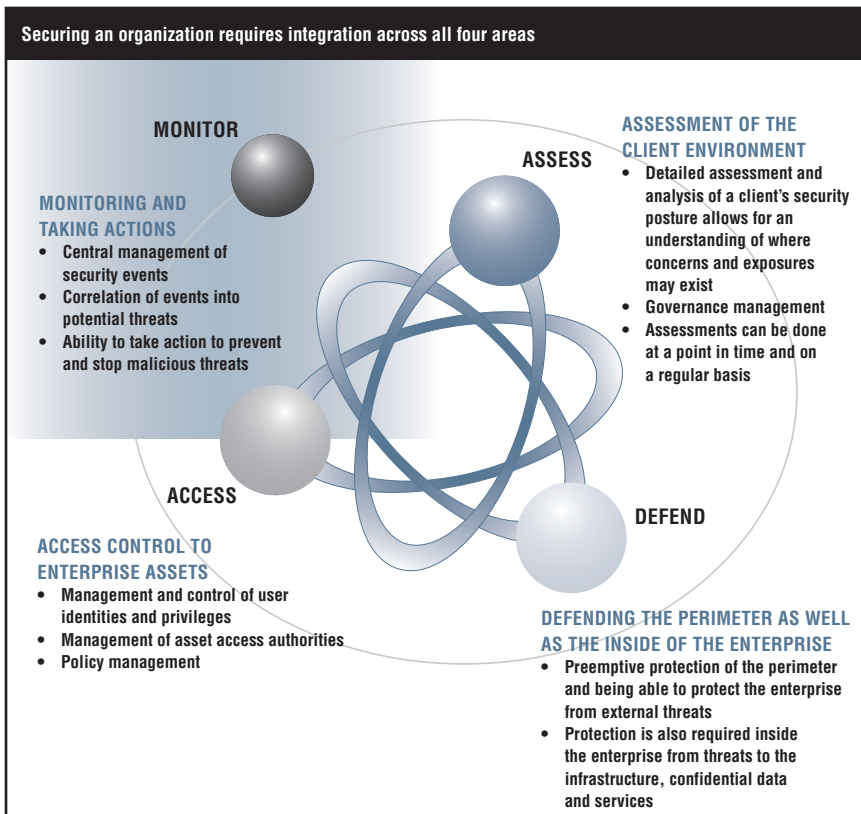
Rather than rely on a variety of point products and impromptu security procedures that are not integrated across the enterprise, an organization should view, analyze and manage enterprise security as a whole, rather than as individual pieces.

Drive value from end-to-end security solutions

Maintaining open, flexible and secure IT systems is a critical ingredient for on demand growth. Open standards enable organizations to manage user access and security within a complex, heterogeneous environment, while ensuring the flexibility to meet evolving business needs. To facilitate integration, IBM security management solutions are based on open standards that work across multiple platforms and seamlessly integrate with other business processes to maintain consistency.

Together with IBM Service Management, IBM security management solutions can help organizations identify and consistently implement best practices for the processes they choose to deploy. IBM security management solutions help:

- *Set IT and business policies*, keeping audit and compliance requirements in mind.
- *Define processes* to implement those policies.
- *Identify workflows* by codifying the specific tasks that will be automated to execute a process.
- *Tune access rules* to meet the real-time conditions dictated in typical on demand environments.
- *Share data* to enable processes to seamlessly interact.
- *Automate execution* of both workflows and data exchange.
- *Audit and monitor* data and systems.



IBM provides a global platform of flexible, standardized security solutions that span assessment and discovery, defense, identity and access management, and monitoring and reporting analytics.

Assess security requirements

IBM solutions provide self-managing capabilities to regulate access, giving users simplified access to critical applications in compliance with security policies.

The solutions are designed to address a closed-loop process – implementing security controls, changing them as needed to meet business and IT service requirements, managing security incidents and demonstrating the effectiveness of the security controls to comply with regulations.

“The initial savings [from managing all customer identities with one centralized platform] are made from automating password resets from users. Up to 40% savings can be made just in help-desk costs. [...] The savings made from not having a disgruntled ex-user compromising a system they still have access to could run into millions.”

**— Maxine Holt
Senior research analyst
Butler Group²**

IBM security management solutions help organizations address three main security challenges:

- *Identity and access management.* Provision and manage user identities, facilitate collaboration outside the organization, define and enforce access controls, and perform the auditing necessary to help demonstrate control over disclosure of information.
- *Threat management.* Identify and address attacks, malware, misconfigurations and misuse by automating security event collection and management, alerting, analysis, reporting, patching and other measures for a variety of IT resources.
- *IT compliance management.* Establish, monitor, enforce and report on corporate IT policies to facilitate compliance with expanding regulations and service level agreements (SLAs).

Institute effective identity and access control management

Identity management and access control solutions combine a range of business processes and strategies, including automation, synchronized identity data, policy-based access control and privacy control.

Manage user accounts across the enterprise

IBM Tivoli[®] Identity Manager provides a single point for creating and managing user accounts across resources. Through a robust workflow engine, Tivoli Identity Manager helps automate the user provisioning process, including approvals and account creation, as well as the user deprovisioning process to mitigate the risk of invalid accounts and privileges. Tivoli Identity Manager provides a flexible, Web-based self-service interface for password resets, password synchronization and user account updates.

Validate and exchange user identification with trusted enterprises

Federated identity management enables an organization to share identity information and privileges in a trusted fashion with other organizations to help relieve the burden of managing users from outside the organization. Leveraging secure, standards-based Web-services protocols, IBM Tivoli Federated Identity Manager extends identity management between partners’

“Tivoli Security solutions are an important component of our overall security strategy. It enables us to increase our level of security and enforce consistent policies across all our systems.”

**— Bill Jenkins
Senior Director, Information Technology
UNICCO**

infrastructures. Trusted partners can now share an open standards-based authentication framework to exchange user identification and attributed information. And IBM Tivoli Federated Identity Manager Business Gateway provides small-to-midsize organizations with an ideal entry point for establishing federated Web single sign-on (SSO) capabilities that bring together customers, partners and suppliers.

Within an SOA and Web services environment, Tivoli Federated Identity Manager also delivers unique trust management capabilities. Organizations can use these capabilities to secure access to distributed and mainframe applications and services.

Enforce policy-based access control

IBM Tivoli Access Manager software lets an organization control IT resource and application access privileges across its enterprise, according to corporate policy and privacy requirements. Using a consolidated, policy-based approach to access control eliminates the need to manually code security into each application, and therefore helps minimize deployment and administration costs. This approach also consolidates the multiple sign-ons required by individual applications and IT infrastructure components. Single sign-on minimizes the various combinations of passwords and user identities that frustrate users – and burden the administrators who manage them manually. Tivoli Access Manager software supports a variety of strong authentication methods and access devices, including desktops, handhelds and other pervasive devices. The dynamic rules of the software enable an organization to key access decisions to real-time decision points that are typical in on demand environments.

“When customers ask about our IT governance policies as a result of SOX and HIPAA, Tivoli Identity Manager Express provides us with a strong story to tell.”

**— Bill Jenkins
Senior Director, Information Technology
UNICCO**

Synchronize identity data across multiple repositories

With accounts spread across heterogeneous business applications and servers, it can be difficult to identify and resolve conflicts among all the sources of identity data. But with IBM Tivoli Directory Integrator, organizations can synchronize information across data stores, registries, directories and more – in real time.

Tivoli Directory Integrator acts as a flexible synchronization layer between an identity structure and the application sources of identity data. The offering can work as an effective metadirectory, and leverage open standards to built-in connectors to act as a directory for multiple sources that lack an overriding, authoritative source. Ultimately, it helps an organization create the trustworthy data that is necessary for both enterprise security and automation.

Help identify attacks, malware, misconfigurations and misuse to mitigate security risks

Both intentional and unintentional threats from outside and within an organization can expose it to potentially significant IT infrastructure damage and loss of productivity. But comprehensive threat management capabilities from IBM help quickly detect and proactively resolve security risks.

IBM Tivoli Security Operations Manager collects and quickly analyzes disparate security data from across the enterprise to streamline and automate incident management – and thereby maximize network availability. As a security information and event management platform, Tivoli Security Operations Manager can help detect attacks, misuse and anomalous activity; prioritize security activities according to business impact; and facilitate the flow of incident management data between security, network and systems management operations teams.

IBM Tivoli Security Compliance Manager scans servers and workstations to verify whether IT security controls are in place and that the systems comply with security policy. Tivoli Security Compliance Manager integrates with system management tools across the enterprise to help centrally manage all aspects of the ongoing process of minimizing security vulnerabilities. Compare current configurations with “baselines” that the organization establishes and automatically identify deviations. Leverage that data to help prioritize the risks the organization wants to mitigate against and shield the infrastructure from high-priority vulnerabilities.

Implement, enforce and report on security compliance policies

Expanding regulations and standards in many industries require compliance with and enforcement of security policies. In an effort to measure and control risk and compliance, organizations look for a structured approach that lets them quantify risk, identify and prioritize internal controls, and establish records to meet a multitude of compliance obligations.

IBM security management solutions enable organizations to define security policies and enforce IT controls – ahead of an audit. As business needs change, policies and IT controls can adapt innovatively.

IBM solutions also facilitate reporting on the effectiveness of compliance efforts – on a continuous basis and in response to audit requests. The IBM offerings described in this white paper collect centralized audit data that can save time when responding to requests. Additionally, IBM Tivoli Compliance Insight Manager helps securely and reliably collect, store, investigate and retrieve native logs from virtually any platform across the enterprise for compliance and forensics use.

Lower the costs of compliance

The ability to analyze, review and determine the appropriate technology infrastructure to address compliance requirements is crucial for companies in financial services, healthcare and manufacturing industries that face new or changing regulations on a constant basis. Public companies that deploy compliance management architectures will typically spend 50% less annually to meet federal requirements than those companies that do not.³

Through its patent-pending W7 methodology, IBM Tivoli Compliance Insight Manager helps translate syslogs and native logs into easily understood language that reports on Who, did What, When, Where, Where from, Where to and on What. An easy-to-use dashboard that summarizes billions of log files on one overview graphic provides an at-a-glance view of your current compliance posture.

Plus, Tivoli Compliance Insight Manager offers more than 100 best-practices audit and compliance-oriented reports to help meet corporate and audit reporting requirements; multiple customizable templates to help jump-start the monitoring and reporting; and the custom report writer, which helps you meet your exact compliance reporting needs.

Leverage IBM leadership in security solutions

IBM has been a world leader in security for the past 40 years, with an ever-expanding range of experience, technical knowledge and expertise. Today, more than 3,500 IBM security and privacy experts worldwide – backed by a network of IBM Business Partners – help organizations respond faster and more appropriately to security violations, threats and regulatory mandates.

The IBM commitment to security innovation is visible in more than 100 patents in identity management products and technologies. But IBM consultants also concentrate on the industry-specific requirements and unique business problems of clients in virtually every industry.

Drawing on IBM resources and expertise, IBM security solutions can help an organization assess its security exposure and needs, defend itself from internal and external threats, implement and manage user identities, provide access control across applications and data sources, and watch for security exposures and intrusion attempts.

Summary

Protecting critical assets requires a comprehensive, automated security management solution and a layered approach to enforcement. An organization needs to verify that access to sensitive information is effectively controlled and managed – and is available to meet audit requirements.

Integrated security management solutions from IBM help enterprises maximize their existing and future technology investments. In addition to integrating with one another to help automate within and across IT processes, IBM security management solutions interoperate with other IBM infrastructure management solutions to support a wealth of other IBM software offerings.

Beyond protecting assets, a robust security management infrastructure from IBM can become a key business enabler, providing the flexibility and integration required to quickly adapt to changing market requirements and secure new, innovative initiatives and services.

For more information

To learn more about IBM security management solutions or to find out how IBM can help you develop a security strategy to meet your unique business requirements, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli/solutions/security



About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards-based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers 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

© Copyright IBM Corporation 2007

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

Produced in the United States of America
7-07
All Rights Reserved

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

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

¹"How to Plug the \$13 Billion Leak," *Business Week*, March 20, 2006 Special Advertising Section. www.businessweek.com/adsections/2006/pdf/0320_theft.pdf

²Quoted in René Millman, "Avoiding an Identity Crisis," *SC Magazine*, April 5, 2006. scmagazine.com/uk/news/article/551843

³Gartner Group. Cited by Brice Dunwoodie. *CMSwire*. "IBM Managing Compliance." October 26, 2004. www.cmswire.com/cms/enterprise-cms/ibm-managing-compliance-000461.php

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 