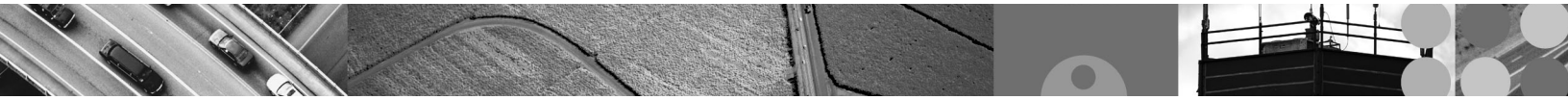
Security management solutions
White paper

Tivoli® software

Enhance enterprise security and compliance for lines of business with flexible solutions from IBM.



September 2007

Contents

Overview

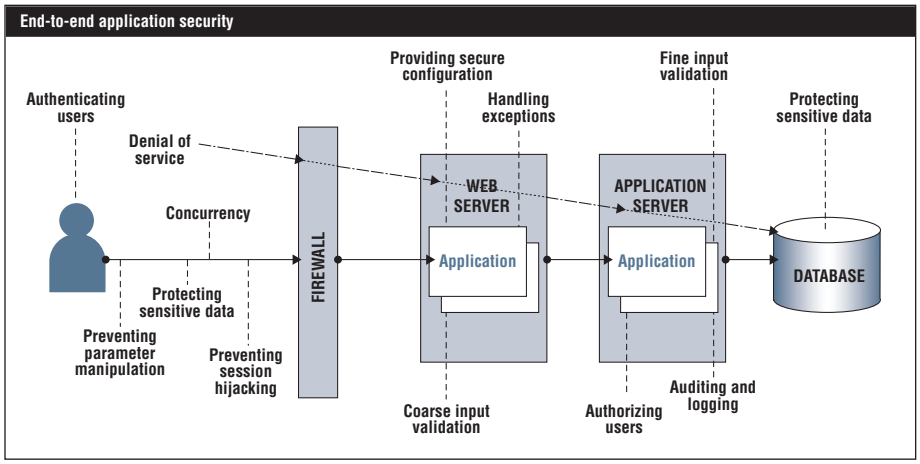
Enterprise applications such as payroll, procurement and inventory management have become essential to the success of today's lines of business. At the same time, companies often are increasing their exposure to threat and fraud as more end consumers are given direct access to corporate services. Consequently, managers face a number of challenges in providing effective, centralized security and compliance for these applications.

A centralized security and compliance solution typically cannot be provided by any single enterprise application, and managers worry that a third-party security solution might prove itself to be rigid or difficult to implement. They also know that enterprise IT infrastructures are large, complex and rapidly evolving, making integration sometimes difficult. According to IBM research, the average corporation supports five major enterprise applications. Finally, managers must meet rigorous compliance requirements even as the portals and access points in their environments and across enterprise applications continue to increase in number.

To help address these challenges and requirements for the enterprise, IBM solutions provide visibility, consistent control and automation across heterogeneous business applications. More specifically, we provide a number of comprehensive solutions for identity management, access management and compliance management. With IBM, lines of business have a trusted, deeply experienced business partner to help them minimize their risks and maximize their investment in their enterprise applications.

Review the security and compliance challenges for enterprise applications

According to an IBM survey, most large corporations support at least five enterprise applications, provided by companies such as SAP, Oracle, PeopleSoft, Microsoft and Siebel. If you are a line-of-business manager, you know that these applications can deliver unique benefits – and present some unique challenges.



In many ways, you "own" these applications and use them to provide more and better services to a growing number of users involved in your business, both internally and externally. At the same time, owning the applications means that you own responsibility for providing effective, manageable security and support for compliance – and this is where the challenges arise.

You realize that you need a centralized security and compliance solution, something that typically cannot be provided by any single enterprise application. You also wonder if a third-party security solution might prove itself to be rigid or difficult to implement.

You also know that enterprise IT infrastructures are large, complex and rapidly evolving. The same technology that helps you grow your business can introduce new issues about security and compliance. Service oriented architecture (SOA), for example, is a highly appropriate architecture for implementing enterprise applications and providing a flexible, service oriented approach to integration across diverse environments. However, the very openness of an SOA environment – integrating what were formerly separate domains of authorization and access control – requires new technology solutions for the secure management and protection of information across networks, applications, platforms and business entities.

Finally, and in some ways most importantly, you understand that your compliance burden will only continue to grow as you provide more Web-based services to a diverse set of users, including employees, customers and business partners. Furthermore, the costs continue to climb for securely managing access for a growing number of users across multiple applications and environments.

These are the issues that keep managers up at night. You want your business to meet user service demands, capture new markets and continue to grow. But you also need to protect the brand and reputation of your business. A security breach or unauthorized use of data can result in serious, long-term damage.

In short, you need a proven, effective solution for your enterprise application that provides:

Authentication: A common identity management solution across the business and beyond should be used to successfully authenticate and manage user identity.

Authorization: An automated system for access and privileges is required that will identify the user once and then automatically map the user's identity across multiple systems, services and infrastructure components. Authorization should also be entitlement-based, limiting access to each individual according to his or her specific roles and functions within the company.

Compliance: Proper compliance involves all the issues raised by authentication and authorization. Security controls as well as reporting and audit capabilities should form an integral part of the application environment.

Highlights

Assess vulnerabilities in application security

As a first step in developing any application security solution, scanning tools should be in place so that Web applications can be assessed for vulnerabilities. Web application vulnerability scanning represents one of the best ways for security auditors to defend against targeted attacks from both within and outside the enterprise.

IBM Rational® AppScan offers a solution for all types of security testing – outsourced, desktop-user and enterprise-wide analysis – and for all types of users, including application developers, quality assurance (QA) teams, penetration testers, security auditors and senior management. The AppScan scan engine continuously audits Web applications, tests for security and compliance issues and provides actionable reports with fix recommendations.

Automate controls with identity management

Managing user identities for access to resources throughout the identity life cycle is the foundation for security

Managing user identities for access to resources throughout the identity life cycle is the foundation for security. A comprehensive, automated identity management solution should enable a line of business to:

- Set up new accounts and passwords quickly for employees and customers.
- Provide granular, selective access through role-based access control (RBAC), management review and periodic recertifications.
- Enable users to reset and synchronize their own passwords, according to access control policies.
- Increase user and IT efficiency by cutting elapsed turn-on time for new accounts.
- Decrease errors by automating user submission and approval requests.
- Help reduce IT administration costs by providing Web self-care interfaces; creating local autonomy; and automatically managing accounts, credentials and access rights throughout the user life cycle.

To address these requirements, IBM Tivoli® Identity Manager is designed to provide a secure, 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. Tivoli Identity Manager also provides closed-loop provisioning to detect, correct and audit access to help ensure that user permissions are compliant with approved policy.

Enforce proper access control

Access authentication should provide timely access throughout the user's life cycle – across multiple environments and security domains – while enforcing security and protecting the line of business from external threats. Accordingly, an access management solution should provide:

- Centralized control to help ensure consistent execution of security policies across applications and users.
- Automation with a policy-based security infrastructure guided by both IT requirements and business goals.
- Single sign-on (SSO) to help improve user experience and reduce help-desk costs.
- Integration of access and identity management within one infrastructure environment.

IBM Tivoli Access Manager can help 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. For example, Tivoli Access Manager supports security for content management applications such as FileNet and IBM Content Manager by providing an integrated way to maintain auditable user access. Tivoli Access Manager can also be used to develop portal solutions through integration with line-of-business applications from Siebel, PeopleSoft and SAP.

IBM Tivoli Access Manager for Operating Systems helps protect individual application and operating system resources by addressing system vulnerabilities surrounding UNIX®/Linux® super-user or root accounts. An example of this capability involves companies that have large numbers of confidential and customer-specific data files on UNIX/Linux machines. Tivoli Access Manager for Operating Systems provides a policy-based access control solution to secure this unstructured data content, including core servers where business data and applications reside. With integrated access control and reporting, Tivoli Access Manager for Operating Systems also enables these companies to address their compliance requirements.

IBM application controls and compliance in action

A leading bank provides a range of services online to its customers. However, this e-commerce activity means that the bank's applications are exposed through its Web portals. The applications must be protected even as a growing number and diversity of users demand fast, convenient access. Furthermore, audit policies must be tightly enforced to support compliance for banking regulations.

The bank implements IBM Tivoli Access Manager for e-business, providing a common platform for authentication, authorization and audit policies. Users have to log on only once — Tivoli Access Manager for e-business provides seamless authorization across applications and security domains. In addition, Tivoli Access Manager for e-business records each access to the Web applications. These records are used to generate reports for verifying compliance with various corporate and regulatory requirements.

The bank also integrates Tivoli Federated Identity Manager with Tivoli Access Manager for e-business to provide security-rich SSO for the bank and various business partners. As with customer transactions, activities between the bank and business partners are digitally stored and maintained for record-keeping purposes.

Strengthen efforts toward compliance

Compliance solutions are based on proper identity and access management, as well as audit and reporting capabilities aligned with regulatory requirements. The right solution should:

- Provide automated user activity monitoring across heterogeneous systems, with dashboard and reporting to help measure your security posture and respond to auditors' requests.
- Automate audit reporting through a compliance dashboard and flexible report distribution.
- Perform effective privileged-user monitoring and audit (PUMA) on databases, applications, servers and mainframes.
- Support auditing needs by translating captured native audit log data into easily understood languages.
- Integrate with other security products to help optimize compliance and incident response.
- Efficiently collect, store, investigate and retrieve logs through automated log management.
- Provide Web site compliance testing to help with regulatory compliance and accessibility.

IBM Tivoli Compliance Insight Manager and IBM Tivoli Security Compliance Manager can be used by businesses to develop a multilayered compliance management and security solution. Tivoli Compliance Insight Manager provides automated user activity monitoring across diverse systems, with dashboard and reporting to help measure your security posture and respond to auditors' requests. Tivoli Security Compliance Manager acts as an early warning system by identifying security vulnerabilities and security policy violations. These policies can be based on both internal security requirements and industry-standard security policies.

IBM Rational Policy Tester is a comprehensive solution for identifying and reporting Web application policy and compliance with corporate standards and industry regulations and best practices. Rational Policy Tester helps reduce business risk by providing visibility to issues that impact Web visitor experience and regulatory compliance requirements.

Summary

With IBM, lines of business have a trusted, deeply experienced partner to help them minimize their risks and maximize their benefits, while developing comprehensive security and compliance solutions for their enterprise applications.

Designed for rapid, flexible integration, IBM solutions can help lines of business:

- Automate and enhance identity management for both internal and external users.
- Provide integrated access control for all users.
- Support regulatory compliance efforts in an efficient, effective manner.
- Leverage their investment in the enterprise application.

For more information

To learn more about how IBM can help today's lines of business support security and compliance for enterprise applications, contact your IBM representative or IBM Business Partner, or visit **ibm.com**

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

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

Produced in the United States of America
9-07

TAKE BACK CONTROL WITH Tivoli®

TIW10448-USEN-00