IBM access management solutions for portal and Web security

Enabling secure access in complex Web application environments

Highlights

- Centralize user access to IBM WebSphere® Portal systems, Microsoft® SharePoint deployments, and your custom applications built in Java™ and Microsoft .NET development environments
- Reduce application development costs, enable compliance, and extend Web protection to enforce access control for a wide variety of users
- Secure collaboration and data sharing with business partners and across lines of business

With the proliferation of Web portals, applications and Web-based services, traditional IT systems architectures have given way to porous cyber infrastructures. In order to share data with a wide variety of users and to facilitate valuable partner and customer interactions, organizations are creating increasingly collaborative environments with shared touchpoints, such as through IBM WebSphere Portal systems, Microsoft SharePoint deployments, and custom applications built in Java and Microsoft .NET development environments. In addition, information-rich applications such as enterprise content management (ECM), business intelligence (BI), customer relationship management (CRM), and enterprise resource planning (ERP) are among the major systems driving the distribution of processes and data across and beyond an organization's heterogeneous IT infrastructure.

The financial services sector provides a perfect industry example. Most large financial institutions offer their services through online portals that expose a variety of mission-critical applications and services. These services involve the exchange of critical data such as credit card numbers, social security numbers, or other personally identifiable information (PII). As more and more customers take advantage of these online channels, organizations face the challenge of ensuring that user access remains secure. They must also secure access to critical data from

inside the organization. Corporate security policies dictate that this access be managed on a need-to-know basis in order to minimize risk of both intentional and unintentional data loss or breach of data security.

But hard-coding security controls into these applications generates redundant logic, while running the risk of introducing inconsistency among applications. Once in place, such controls are difficult to change, contributing to higher operational costs and heightened security risks for the organization.

For many organizations with increasingly complex IT infrastructures that support multiple Web-based applications and services, externalizing this security function is a more effective and more cost-effective choice. IBM Tivoli® access management solutions enable comprehensive Web and federated access control, and fine-grained entitlement management and enforcement at the services, application, and data layers, integrating into existing IT security infrastructures to provide seamless security coverage. This centralized approach can reduce application development costs, improve IT staff productivity, expedite the secure implementation of new initiatives, and facilitate compliance reporting and audit processes.

Web security across a heterogeneous IT infrastructure: A banking example

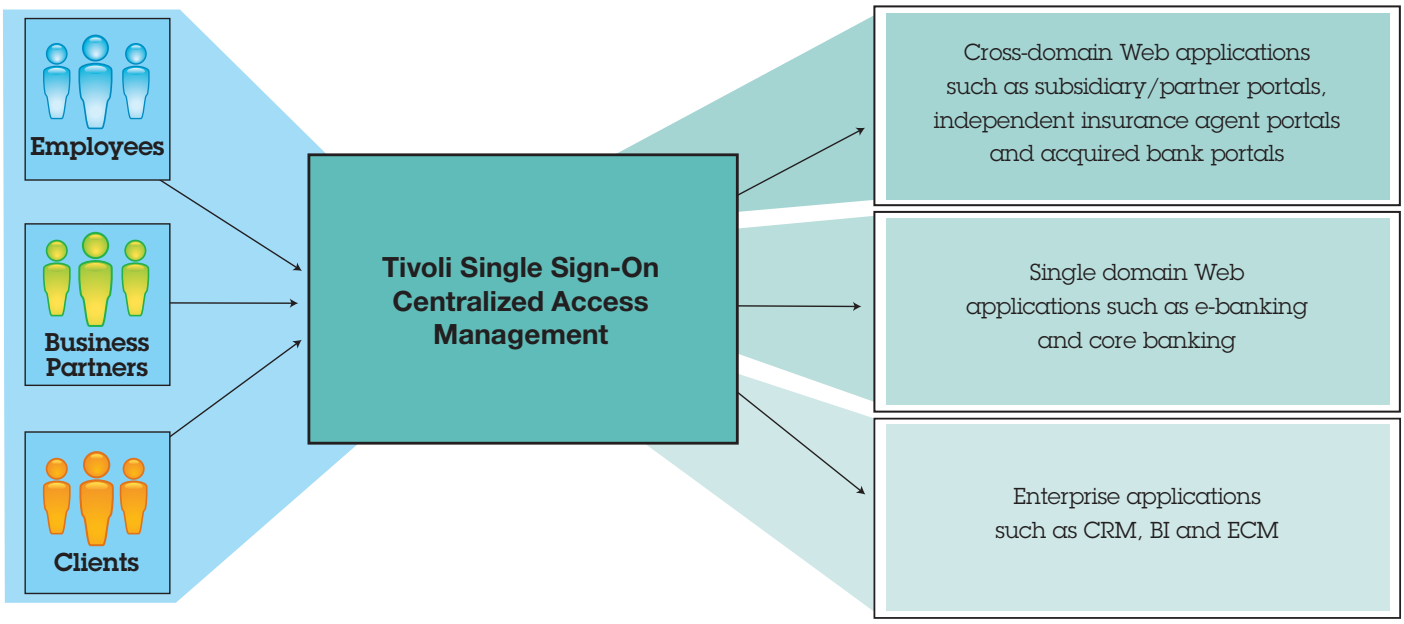
Like many businesses, banking supports multiple heterogeneous applications, including core banking systems, credit card applications, e-banking systems, CRM applications, and other proprietary applications, all of which typically have their own sign-on mechanisms that capture user ID and password information separately. Some of these applications authenticate users based on Microsoft Active Directory, while some use information stored in databases. Still others authenticate users based on other means. The user authentication and password policies for these applications may also vary from one to another.

In these scenarios, it can be very difficult for banks to mandate a common user authentication policy for all of the applications in the organization, since changing the authentication policy may mean changing the authentication mechanisms within each of the applications. These organizations also often face help-desk challenges associated with high volumes of password reset requests. Implementing a single, organization-wide mechanism for policy-based user authentication can help organizations solve multiple security challenges.

IBM Tivoli access management solutions provide scalable single sign-on (SSO) and centralized authentication capabilities, including support for strong authentication, required to manage complex IT application environments. These capabilities give employees, business partners, citizens, customers, and other users secure and seamless access to the Web applications they need, whether from within the corporate intranet or from an extranet.

Federated single sign-on for cross-organization collaboration

In an age where the financial industry is seeing constant mergers and acquisitions, enabling secure inter-organization collaboration and shared services can enable more efficient business processes. It also opens up new business models. For example, in insurance and financial organizations, internal applications need to be extended to external constituencies such as field personnel or independent agents in order to expedite sales transactions. But establishing identity and trust are the critical factors in achieving successful collaboration in these scenarios.



IBM Tivoli access management solutions give employees, business partners, customers, and other users single sign-on and authorized access to the applications they need.

Tivoli access management solutions enable federated SSO in different security domains by interoperating with a wide variety of federation standards such as SAML 1.1.x and 2.0, Information Card Profile, OpenID, Liberty ID-FF, and WS-Federation. It enables users to sign on to the sites of multiple businesses using one set of credentials, while helping to preserve the confidentiality of the user data. The loose coupling between the application layer and federated SSO functionality eliminates the need to use proprietary programming interfaces, enabling users to enroll and gain access to a wide variety of Web applications in the federated environment with little to no change to applications.

Compliance capabilities, granular access control, and extended Web protection

As in other highly regulated industries, the financial services industry is governed by a number of government regulations and standards, including the Payment Card Industry Data Security Standard (PCI DSS), and compliance with them is critical. Tivoli access management solutions provide comprehensive audit logging capabilities, with audit log collection that stores logs in a secure central location. With these closed-loop access control capabilities, organizations can quickly produce user- and data-oriented reports to meet specific audit reporting requirements such as those of PCI DSS.

To ensure the security of financial data and applications, financial organizations need fine-grained access control mechanisms—the ability to control access based on rules and conditions, and based on roles, groups, attributes and contact. For example, security managers need to be able to provide entitlement enforcement for specific fields (such as transaction amount) within a banking application or to restrict access to insurance policies based on an individual insurance agent's current status or scope. Tivoli access management solutions can help organizations manage and enforce fine-grained access to applications, externalize security from the applications, and simplify the management of complex entitlements and data-level access control policies.

Moreover, the network intrusion prevention capabilities offered by IBM security solutions help provide expanded Web protection for external Web content and applications and strengthen Web security by stopping Internet-based threats before they impact business. These solutions help protect networks, servers, desktops, and revenue-generating applications by addressing security vulnerabilities at the network core, along the perimeter, and on remote segments such as those in branch offices and other off-site locations.

Meeting the unique security challenges of portal deployments

Portals, whether provided through WebSphere Portal or Microsoft SharePoint services, play a vital role in an organization's IT infrastructure. As frameworks for integrating applications and processes within and across organizational boundaries, portals have taken on growing importance as well as daunting complexity. Implementing a portal raises difficult issues about security, scalability, and usability, and as applications within the organization grow, the value of a portal deployment comes more from the ability to provide features such as SSO, login consistency, and password and session management. Portal managers also have to be concerned about external threats such as viruses and denial of service attacks, as well as internal threats.

Securing access for WebSphere Portal deployments

Tivoli access management solutions provide a consolidated authentication framework for WebSphere Portal deployments, integrating with WebSphere Portal to provide security capabilities that go beyond the native portal security functionality. The loose coupling with WebSphere Portal and other applications offered by the proxy-based solution provides increased scope and flexibility for secure access control across intra-organization and inter-organization application environments. Support for protocols such as SAML 2.0, OpenID, Liberty 1.2 and Web Services (WS)-Federation enables secure information sharing across portal deployments within the business ecosystem.

Tivoli access management solutions also provide benefits that go beyond just security controls. They enable more rapid development and testing of new portal applications, because of consistent access control enforcement and policies that can be applied across the application framework. These solutions also support a wide variety of strong authentication mechanisms and session management capabilities that can further strengthen access control. They also offer user self-care utilities to automate the enrollment and maintenance of portal user accounts and entitlements. Additional authorization middleware functionality such as fine-grained access control is also available for portal developers.

Securing access for Microsoft SharePoint and Java/.NET deployments

Tivoli access management solutions also provide capabilities that fortify the security of SharePoint portal and Java/.NET-based application deployments. Tivoli solutions enable the use of common security services for authentication, authorization and entitlement management for implementing fine-grained authorization controls based on contextual information such as users, resources, and environment for SharePoint and .NET application environments. These solutions also provide extended (Web and federated) SSO capabilities that simplify the user experience, and they provide reporting options that facilitate an organization's compliance efforts.

Tivoli access management solutions enable policy-driven management of all identities in a SharePoint environment, along with unified management of claims and access policies across a heterogeneous infrastructure.

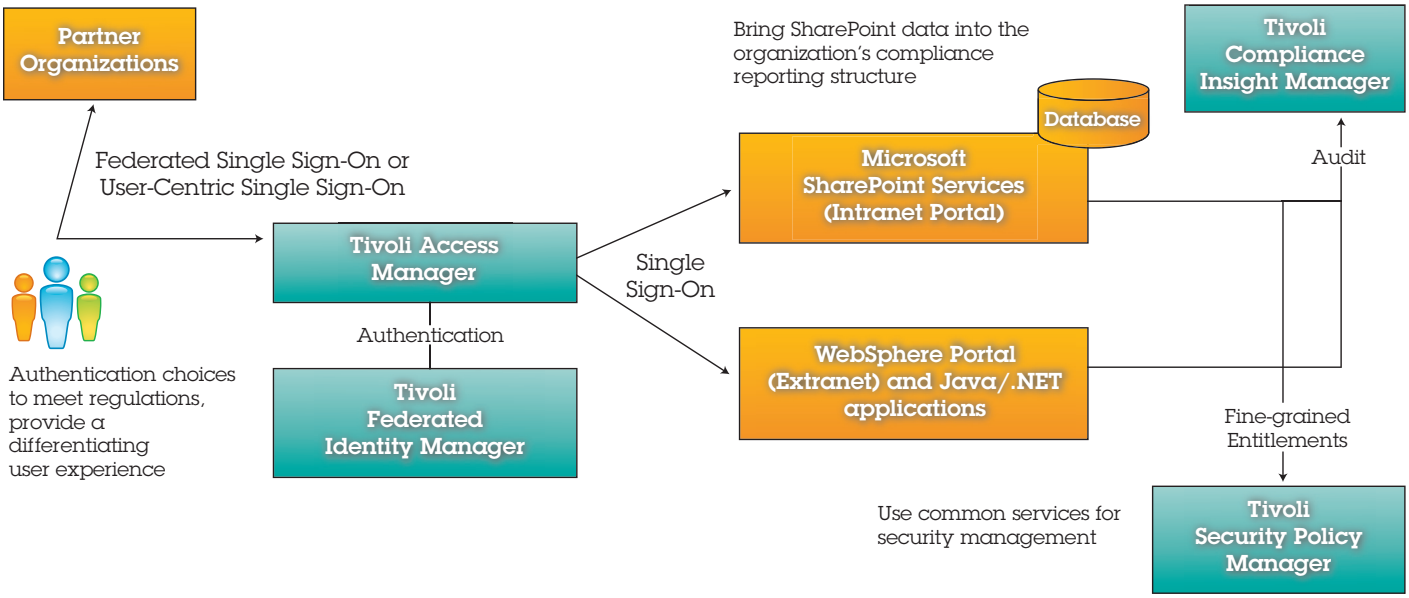
Enabling Web security with IBM security solutions

The IBM security portfolio provides a wide range of solutions to help organizations secure their business-critical portal and Web-based deployments. This comprehensive portfolio includes the following solutions:

IBM Tivoli Federated Identity Manager

Tivoli Federated Identity Manager is a user-centric federated identity management solution that facilitates secure information sharing between trusted users within an organization. It simplifies application integration using many forms of user credentials, enables quick identity service deployments in SOA and Web services environments, provides improved visibility into identities, and facilitates compliance. It also provides full-featured Web access management with the inclusion of Tivoli Access Manager for e-business.

Securing Microsoft SharePoint Portal and Java/.NET application infrastructures



IBM Tivoli access management solutions provide capabilities that fortify the security of SharePoint and Java/.NET-based portal deployments.

IBM Tivoli Identity and Access Assurance

Tivoli Identity and Access Assurance provides comprehensive identity management, access management, and user compliance auditing capabilities in a single solution offering. It centralizes and automates the management of users, then closes the identity and access loop, providing industry-leading capabilities for assigning and enforcing user rights, monitoring user activity, and detecting and correcting situations that are out of compliance with security policy.

IBM Security Network Intrusion Prevention System

The Security Network Intrusion Prevention System from IBM provides intrusion protection at all layers of the network, helping organizations stay ahead of Internet threats. It employs multiple intrusion prevention technologies to monitor, detect, and block a wide range of network threats, including application attacks, scripting attacks, malware, operating system attacks, protocol tunneling, and Web server attacks.

For more information

To learn more about IBM security solutions for portal and Web environments, please contact your IBM sales representative or IBM Business Partner, or visit **ibm.com**/tivoli/security

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 customer may need 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.

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

Produced in the United States of America
March 2010

Tivoli software

TIS14052-USEN-00