White paper
December 2009

Tivoli® software

IBM Tivoli access management delivers market-leading foundational capabilities for strengthening identity, data, and application security

Contents

Introduction

When it comes to providing access security, today's organizations are facing two major challenges—a wide variety of users who need access to numerous business services, applications, and data, and the dynamic IT infrastructures that are being transformed to facilitate secure collaboration among those users and business services. Organizations have to address the unique access needs of multiple types of users, including employees, contractors, suppliers, customers, citizens, business partners, and privileged users.

After determining which users are valid, the challenge becomes one of managing their access to specific data and applications, ensuring that only the right people have access to the right assets at the right time. Today's emerging dynamic IT infrastructures compound the challenge, transforming the traditional IT landscape through virtualization, service-oriented architecture (SOA), cloud computing, software as a service (SaaS), and other technologies, and opening the IT environment to new vulnerabilities.

Organizations that effectively address these access security challenges can gain a competitive advantage and transform security into a business enabler. These organizations can reduce IT and application development costs while consistently securing their business-to-enterprise (B2E), business-to-business (B2B), and business-to-consumer (B2C) connections, enabling secure access, facilitating collaboration, and driving growth in a rapidly changing business environment. IBM has continued to drive investment and innovation in access security, and for over 30 years has empowered organizations from around the world with market-leading access management solutions.

Highlights

The IBM Tivoli access management family of products provides the foundational, closed-loop controls for enterprise security to protect the most demanding infrastructures.

The IBM Tivoli® access management family of products provides the foundation of user access security to protect the most demanding infrastructures. This flagship portfolio delivers identity, data, and application security capabilities that can help organizations reduce operating costs, manage business and IT risk, and improve service to their constituents.

A holistic approach to enterprise security

Tivoli access management solutions are offered as part of the IBM Security Framework to deliver identity, data, and application security (see Figure 1). This framework was developed to offer enterprise security capabilities in terms of the business resources that need to be protected, dividing IT security needs into five discrete domains. These domains are addressed in a context of security governance, risk management, and compliance, and are supported by a comprehensive IBM portfolio of security hardware, cross-brand software, and services. The IBM Security Framework allows organizations to better understand and prioritize risks and vulnerabilities based on their potential to disrupt critical processes.

Figure 1: The IBM Security Framework enables a holistic approach to enterprise security, defining security capabilities in terms of the business resources that need to be protected.

Highlights

Strong user access security is a must-have in order to reduce costs, improve services, and manage risk across the enterprise IT environment.

IBM understands that, in an uncertain economy, organizations have limited resources with which to address a growing list of security requirements. Strong access security is a must-have in order to reduce costs, improve services, and manage risk at the same time. IBM has continued to demonstrate the technical leadership and depth of expertise to deliver end-to-end access management solutions that can help organizations meet their short-term security goals as well as their long-term strategic objectives. With highly scalable, flexible, and standards-based solutions backed by a world-class support organization, IBM stands at the forefront of access security.

This white paper explores the major access management scenarios facing organizations today:

- *Providing secure access to a wide variety of Web applications and services*
- *Enabling secure collaboration with business partners and across lines of business*
- *Expanding customer reach through secure Web portals*
- *Strengthening end-point and desktop access control*
- *Protecting access to data within applications and services on a need-to-know basis*
- *Controlling privileged user access within the data center*
- *Enabling secure access to mainframe resources*

The Tivoli access management portfolio enables end-to-end identity and access management governance, helping organizations manage risk and demonstrate compliance.

The Tivoli access management portfolio can help organizations effectively address each of these scenarios by applying industry-leading identity, data, and application security capabilities to enable end-to-end identity and access management governance, managing risk and demonstrating compliance across the organization.

Highlights

IBM Tivoli access management solutions provide the capabilities today's organizations need to secure user access to critical Web-based resources and provide Web and federated single sign-on.

Providing secure access to Web applications and services

With the proliferation of Web applications and Web-based services adoption across the organization, traditional IT infrastructures have given way to porous cyber infrastructures that are much more challenging to secure. To enable the business expansion and quality services required to stay competitive, organizations have become de-perimeterized, introducing a new generation of application and data security concerns. As a result, the number of online security incidents resulting in the loss of critical data has grown significantly in recent years.

But organizations are compelled to create increasingly open IT and application environments with shared touch points in order to share data with a wide variety of users and to facilitate valuable partner and customer interactions. Critical applications such as enterprise content management (ECM), business intelligence (BI), customer relationship management (CRM), home-grown Java™, mainframe and Microsoft® applications, and enterprise resource planning (ERP) are among the major applications driving the distribution of processes and sharing of data across and beyond an organization's heterogeneous IT infrastructures.

Addressing access security effectively in this environment calls for centralized, policy-based user authentication and authorization technologies that can provide closed-loop access management—with capabilities that can span IT and application platforms, SaaS, cloud-based services, corporate data centers, service-oriented architectures, and collaborative communities. IBM Tivoli access management solutions provide the flexible user authentication, authorization, session management, and audit capabilities today's organizations need

Highlights

in order to secure access to these critical Web-based resources and enable Web and federated single sign-on (SSO) to address dynamic infrastructure and line-of-business security needs.

Many organizations are also implementing service-oriented architecture (SOA) to transform their application environment and deploy large numbers of Web services to support business-specific needs. Appliances like IBM WebSphere® DataPower® help secure and accelerate XML and Web services deployments. This type of appliance needs to be integrated with the organization's broader user access management infrastructure to support centralized SSO, enable consistent session management and security policy management, and help demonstrate compliance in a dynamic infrastructure. IBM Tivoli access management integrates out-of-the-box with appliances like DataPower to provide centralized SSO and consistent session management and security policy management.

IBM Tivoli access management solutions provide organizations the ability to centrally administer and enforce permissions and data-level access controls within applications and services.

In addition, IBM Tivoli software's fine-grained entitlement management capabilities provide organizations the ability to mitigate risk and strengthen data security by centrally administering and enforcing permissions and data-level access controls within applications and services. These security policy management capabilities can be integrated with existing identity management systems to extend and enforce roles-, rules-, and attributes-based fine-grained access security across the application environment.

Finally, the closed-loop approach to access management enabled by IBM Tivoli solutions not only allows security administrators to manage and enforce user access, but gives them integrated audit and compliance capabilities that help minimize application security risk and ensure compliance throughout the identity and access life cycle.

Enabling secure collaboration with business partners and across lines of business

For organizations in healthcare, finance, and other customer services industries that rely heavily on interaction and data exchange between numbers of partners, enabling secure interorganizational collaboration and shared services is a critical security requirement. For many organizations, this type of collaboration also helps support new business models and enables more efficient business processes.

For example, in healthcare, a community of internal and external users such as physicians, pharmacies, insurance agents, and patients needs to be able to exchange information across a complex interorganizational information system. In insurance, government, and financial organizations, internal applications need to be extended to external users such as field personnel or independent agents in order to enable efficient and expedited sales and services transactions.

Internal and external users in these scenarios may require access to on-premise and off-premise applications, including SaaS deployments and emerging public, private, and hybrid cloud computing environments (See Figure 2).

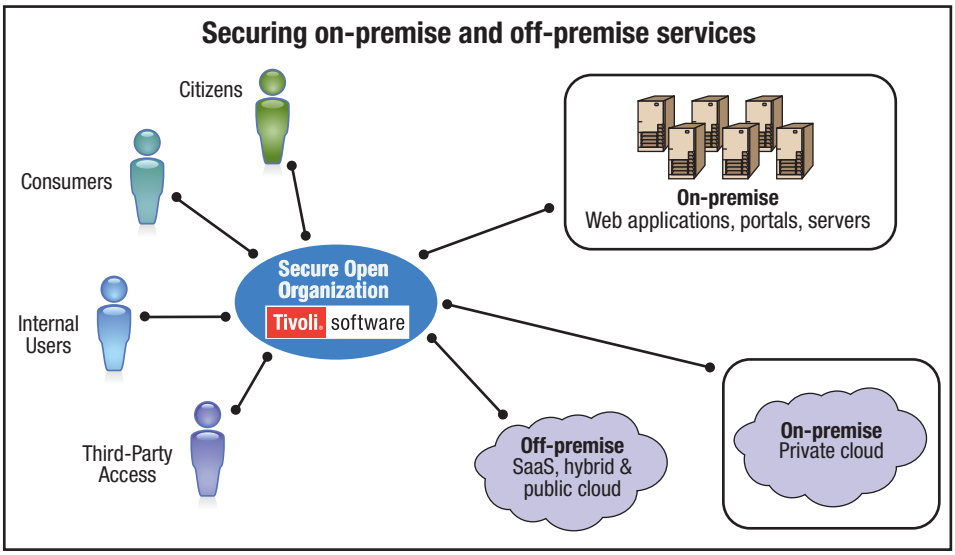

Figure 2: Effective collaboration requires secure and flexible access to both on-premise and off-premise applications by a wide range of internal and external users.

Highlights

IBM Tivoli access management solutions can help organizations across a wide range of industries enable secure collaboration with trusted business partners and across lines of business.

But the user's identity and organizational trust are the enabling factors in achieving secure collaboration in these scenarios. For example, before providing a supplier with forecast information, a manufacturer has to be certain that the requesting party is actually the supplier in question, as opposed to a competitor or corporate spy, and that the "rules of engagement" for data exchange are established and enforced.

IBM Tivoli access management solutions can help organizations across a wide range of industries enable secure collaboration with trusted business partners and across lines of business. These solutions support industry standards such as Liberty Alliance, SAML, WS-Federation, OpenID, RACF PassTicket, and more to allow disparate organizations to use their internal identification data to obtain access to the shared applications and services of all organizations in the group.

The key capabilities offered by the Tivoli portfolio include federated single sign-on, compliance reporting, and integration with existing Web access management systems, helping organizations extend the value of their existing investments.

Expanding customer reach through secure Web portals

Banking, retail, and public sector organizations are increasingly transforming their online portals to offer value-added services and leveraging them as an additional channel for conducting business with their customers. In many cases, these organizations are also exposing the applications and data residing in the mainframe environment. As more and more customers take advantage of these online channels, organizations are facing the challenge of scaling these customer-facing portals in order to handle the increasing traffic while ensuring that user access remains secure.

Highlights

A key security challenge lies in determining the identity of each user when they enroll and access the services, since initial face-to-face identity proofing is generally not practical in these scenarios. The type of identity assurance and the level of authentication strength an organization requires, whether it's a business enterprise or a government agency, are determined by that organization's risk threshold, business requirements, and IT security constraints. For example, knowledge-based authentication (KBA) entails the validation of an individual identity based on knowledge of personal information, which can be substantiated by a real-time interactive question-and-answer process. This approach is an example of low-cost identity verification and provides sufficient security in instances where users are performing low-risk online transactions or accessing nonsensitive information.

For other use cases that require an additional level of identity assurance, such as for online retail transactions, password resets, or financial transactions, a more robust KBA approach is needed, requiring users to answer a series of relevant questions and verifying the answers such as by scanning multiple public record databases. For high-assurance scenarios, identity verification typically involves a multistep process that could include integrity checks using validation of personal identification numbers, voice biometrics, and pattern recognition algorithms, and, in some cases, providing a risk assessment score based on the likelihood of fraudulent identity.

Using the IBM solution approach, organizations can centrally manage and enforce large-scale end-user access to online portal environments.

Tivoli access management solutions provide a flexible B2C enrollment facility to use built-in or integrate with a wide variety of external multifactor and risk-based authentication systems, and also use third-party identity verification and proofing systems to meet the organization's identity assurance needs. Using the IBM solution approach, organizations can centrally manage

Highlights

and enforce large-scale user access to online portal environments while reducing the cost of application development every time the security needs change to address business requirements and ensure continuity of service.

Strengthening end-point and desktop access control

The complexity and number of logons employees must manage on their desktops on a daily basis are increasing, resulting in frustration as well as lost productivity. In most organizations, employees must remember between 5 and 20 unique passwords and are required to change them every 30 days. In many work environments, such as manufacturing, hospitals, and banks, different users need to access common kiosks and terminals using passwords.

To work around this burden, users often select low-quality passwords, write down their passwords in unsecured locations, and share their passwords with co-workers—behaviors which constitute a significant corporate security weakness. In addition, the time employees spend entering, changing, and resetting multiple passwords not only contributes to lost productivity but also represents a measurable drain on IT help desk resources. For organizations with large distributed desktop environments, the help desk costs associated with password maintenance can be significant.

IBM Tivoli access management software can help organizations streamline password management for users and IT administrators while strengthening desktop access security.

IBM Tivoli access management software can help organizations streamline password management for users and IT administrators alike while strengthening desktop access security. Tivoli solutions deliver enterprise single sign-on capabilities for Microsoft Windows®, Web, Java, mainframe, and teletype applications, and makes them available on all major network access points, including Windows desktops, laptops, shared kiosks, Citrix servers, Microsoft Terminal Servers, and Web portals.

Highlights

Tivoli's advanced access management capabilities support a wide range of authentication factors such as USB smart tokens, smart cards, active proximity cards, passive proximity badges, biometrics, and one-time password tokens.

With Tivoli single sign-on solutions, employees authenticate once, and the software then detects and automates all password-related events for that employee, including logon, password selection, password change, password reset, and logoff.

As security needs continue to expand, organizations in some industries are looking beyond passwords to stronger authentication methods. Tivoli's advanced access management capabilities support a wide range of authentication factors such as USB smart tokens, smart cards, active proximity cards, passive proximity badges, biometrics, and one-time password tokens for step-up authentication needs. These solutions also enable existing identification devices, such as building badges, photo badges, and cell phones, to be used for stronger authentication, leveraging existing assets to facilitate adoption and reduce the total cost of ownership.

Protecting access to data within applications and services

From intellectual property and business intelligence to proprietary operational data and customer information, businesses have critical data to protect within their applications and services. And when that critical data includes credit card numbers, social security numbers, or other personally identifiable information (PII), the security stakes are even higher. Access to this data must be managed on a need-to-know basis in order to minimize risk of both intentional and unintentional loss or breach of data security.

Organizations can suffer brand damage when reports of data losses appear in the press, often resulting in a financial impact to a company's net worth. To combat identity theft and fraud, a number of industry regulations including Payment Card Industry Data Security Standard (PCI DSS) and the

Health Insurance Portability and Accountability Act (HIPAA) have been enacted, mandating the protection of sensitive information. In some instances, civil penalties are levied for failure to properly protect sensitive information.

The protection of access to sensitive information, including that used in mission-critical applications, is vital for business success as well as for building trust with consumers and other stakeholders. For many organizations, critical data is stored and accessed within applications and services such as Microsoft SharePoint, portals (e.g. WebSphere), and enterprise content managers (e.g. IBM FileNet®), as well as within in-house developed applications using Java and Microsoft .NET middleware, and popular databases for business functions such as customer call center, billing and payment transactions, and customer relationship management. Critical data is often requested across distributed and mainframe systems throughout the IT infrastructure. With increased adoption of service-oriented architectures, customer and business-critical data are opened to a wide variety of users and Web services.

Organizations have a number of options for managing and securing data access within applications and services. Some organizations choose to build fine-grained security controls into their applications and services with hard-coded logic. But this approach can be time consuming, error prone, and difficult to manage. The application developers and administrators have to duplicate this effort for multiple applications, while running the risk of inconsistency from application to application. Once in place, the controls are difficult and expensive to change, contributing to operational costs and putting the organization at risk. Other organizations choose to assign responsibility to IT operations to interpret, implement, and enforce the data-level security policies within the existing security infrastructure. But this approach can also be error prone, as the intent of security policies are subject to interpretation at the IT operations level, and often seem to be based on the constraints of the existing IT infrastructure.

Highlights

IBM Tivoli access management software delivers standards-based, fine-grained entitlement management and enforcement at the services, application, and data layers, integrating into existing IT security infrastructures.

For all these organizations, particularly ones with complex IT infrastructures that support multiple applications and services, externalizing this data security function from the applications and services is a more effective and more *cost-effective* choice. IBM Tivoli access management solutions deliver standards-based, fine-grained entitlement management and enforcement at the services, application, and data layers, integrating into existing IT security infrastructures to provide seamless coverage. This centralized security policy management approach can reduce application and services development costs, improve IT operational control, and enable organizations to bridge the resulting gap between business and IT to demonstrate compliance.

Controlling privileged user access within the data center

Privileged users have the most powerful administrative control defined within applications and are also able to directly access the servers, operating systems, and databases on which they run. These privileged user accounts provide wide-ranging administrative access to the applications, servers, operating systems and databases. If privileged user accounts are not properly managed and secured, it leaves these critical resources vulnerable to deliberate or inadvertent misuse, breaches, and potential data theft. For this reason, privileged user accounts are under increasing scrutiny by auditors to ensure that the organization has the proper controls in place and are in compliance with requirements like Section 404 of the Sarbanes-Oxley Act and other relevant regulations.

IBM Tivoli access management software can help organizations close the "back door" that privileged user accounts have in the data center.

IBM Tivoli access management solutions can help organizations close this "back door" that privileged user accounts have in the data center, combining unique root login policy enforcement, robust user tracking and auditing controls, and privileged identity management services. These solutions help

Highlights

prevent abuse of root privileges such as unauthorized assumption of application administrative IDs, and tampering with log files, and they provide persistent universal auditing to demonstrate compliance.

Enabling secure access to RACF mainframe system resources

As organizations continue to transform their application and IT environments, a growing number of secure mainframe applications and data are being included in new services accessed by external organizations or even exposed within customer-facing portals. In the mainframe domain, Resource Control Access Facility (RACF®) provides a robust native security capability to identify, classify and protect system resources, along with identifying and verifying users. As these mainframe-based applications are exposed through new services, organizations need the ability to integrate these new mainframe-based services into the centralized access management environment.

IBM Tivoli access management software provides the ability to seamlessly integrate mainframe-based applications and services into a centralized access management environment.

IBM Tivoli access management solutions provide the ability to seamlessly integrate mainframe-based applications and services into a centralized access management environment and support Web-SSO, federated SSO, identity mediation, and closed-loop compliance reporting.

How IBM solutions can address your needs

Whether you are looking for a comprehensive portfolio of identity and access management solutions, or you need specific capabilities to address an immediate concern, IBM can help. IBM gives customers the flexibility to choose the right solution package to meet their individual needs, empowering them to implement solutions in ways that work best for their organization.

IBM Tivoli access management capabilities are available in the IBM Tivoli Identity and Access Assurance solution offering, which provides end-to-end identity management, access management, and user compliance auditing features for IT infrastructure security, and as part of the IBM Tivoli Data and

Highlights

IBM gives customers the flexibility to choose the right solution package or individual access management software to support their specific security objectives.

Application Security solution offering, which helps organizations protect access to data and applications using fine-grained control and centralizing management of data encryption keys.

IBM also offers individual access management products, which can be implemented as standalone solutions or as part of a custom combination of products designed to support specific customer objectives:

- *Tivoli Access Manager for e-business helps organizations centrally manage and enforce user access control and Web SSO to diverse Web applications and services across the organization.*
- *Tivoli Access Manager for Operating Systems can help manage, enforce, and provide individual accountability for privileged user, root user, or super user account access to operating systems and servers.*
- *Tivoli Federated Identity Manager delivers user-centric federated SSO to enable organizations to expand secure collaboration with business partners and across lines of business, including adoption of off-premise applications including SaaS and cloud-based services.*
- *Tivoli Federated Identity Manager Business Gateway provides an entry-level federation solution for small to medium organizations, as well as a low infrastructure option for department and project-focused federation implementations.*
- *Tivoli Security Policy Manager strengthens data access control and helps organizations demonstrate compliance by managing and enforcing fine-grained entitlements and message protection policies across IT and SOA environments.*
- *Tivoli Access Manager for Enterprise Single Sign-On simplifies desktop access to applications by eliminating the need to remember and manage multiple user names and passwords—strengthening password security while reducing password-related help desk costs.*
- *IBM Resource Access Control Facility provides native security capability on z/OS to identify, classify and protect system resources, along with identifying and verifying users. The Tivoli access management solution integrates with RACF to enable organizations to centrally manage identity, data and application security across mainframe and distributed IT environments.*

For more information

To learn more about how IBM Tivoli access management solutions can help you build a foundation for strengthening identity, data, and application security in your organization, contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com**/tivoli/security

IBM Corporation
IBM Systems and Technology Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2009

Recyclable, please recycle

TIW14048-USEN-00