White Paper
October 2009

Tivoli® software

Managing data and application security risks cost-effectively

Contents

Executive summary

Protecting the integrity and confidentiality of data and transactions is becoming increasingly critical, as the amount of data grows and the risk of loss or compromise continues. But the need to expand security often conflicts with the need to reduce IT costs. IBM Tivoli® Data and Application Security can help achieve these seemingly divergent goals by providing cost-effective capabilities for securing data and applications. This solution is designed to drive ROI by controlling the IT costs associated with developing and managing application security, and by delivering capabilities that help mitigate data security risks. By addressing the challenges of costs and risk, Tivoli Data And Application Security can help organizations position themselves for competitive advantage, enabling them to respond more quickly to new market opportunities.

Overcoming today's data and application security challenges

Incidents in which sensitive data, such as credit card information or other personal data, is lost or compromised can significantly damage a company in many ways. From imposing actual financial losses to causing less quantifiable but equally serious losses of reputation and goodwill, data security breaches have the potential to dramatically impact a company's operations. Unfortunately, these types of incidents are occurring every day. And as data volumes increase, protecting against such breaches becomes increasingly important and all the more difficult. This has led industry regulators and standards bodies to require more and more stringent security controls for data, both while it is active (used in various business applications and services) and while it is at rest (stored in databases and file systems).

Highlights

Applications constitute a highly vulnerable area for data security breaches, as well as a particularly challenging area in which to deploy security measures that are both effective and cost-effective.

Applications constitute a highly vulnerable area for data security breaches, as well as a particularly challenging area in which to deploy security measures that are both effective and cost-effective. The complexities of today's composite applications, coupled with efforts to make applications more accessible to more people, mean that applications are more vulnerable in more ways to security breaches. Organizations must guard against attacks on many levels, and attacks of various kinds: inadvertent or malicious, internal or external. These threats call for investments in risk reduction; at the same time, however, today's economic environment demands cost reduction.

Protecting applications while responding to cost-reduction pressures requires that organizations actively seek ways to reduce the cost of protection without compromising its effectiveness. Focusing on complete solutions, instead of individual products, can deliver financial benefits, such as by eliminating the need to dedicate resources to maintaining and supporting multiple products. By the same token, using a single source for application security can reduce the costs and inefficiencies associated with managing multiple product vendors.

Data and application security today must provide a strong ROI. An organization's ROI is defined by tangible benefits that can translate directly to monetary gain. ROI can take the form of cost avoidance, such as through productivity improvements that reduce labor costs for managing security or that reduce the time and cost required to develop and release secure applications to market. ROI can also be improved by reducing the risk of a security breach and its attendant impact on the business. Further, a dynamic security solution can drive ROI by enabling companies to leverage existing applications in profitable new ways, providing a distinct competitive advantage.

Highlights

This paper shows how organizations can manage data and application security risks cost-effectively by using IBM Tivoli Data and Application Security to reduce costs and improve ROI. It also provides examples of IBM customers who have realized the benefits of the solution.

Industry-leading data and application security from IBM

Tivoli Data and Application Security is a comprehensive solution that helps organizations protect data both in enterprise storage systems and within critical applications.

IBM Tivoli Data and Application Security is a comprehensive solution that helps organizations protect data and applications by enabling fine-grained control of user privileges; centralizing management of security policy, compliance reporting, and data encryption keys; providing auditable access controls; and making online collaboration more secure. The solution provides end-to-end protection of sensitive data both in enterprise storage systems and within critical applications, helping organizations support regulatory compliance initiatives and improving data and application reliability. Key features of Tivoli Data and Application Security include:

- **Fine-grained data and application entitlements**–*protects access to critical data and processes at the application level.*
- **Centralized security policy management**–*enhances security by enabling fine-grained authorization and data-level access control.*
- **User activity monitoring, auditing and reporting**–*improves compliance with a comprehensive overview and record of user activity.*
- **Federated single sign-on and identity service**–*simplifies application integration and improves collaboration by allowing trusted partners to securely share identity data.*
- **Application-level and privileged user operating system controls**–*enables better oversight of privileged accounts on UNIX® and Linux® operating systems.*

Highlights

- **Centralized encryption key management for tape and disk storage**—*improves security and compliance of data at rest through effective data encryption.*
- **Centralized, automated log management and compliance reporting**—*fosters compliance with a variety of regulations and standards such as PCI DSS, HIPAA, Basel II, NERC-CIP and ISO 17799.*

The key features of Tivoli Data and Application Security can help you manage data and application security risks while reducing costs and improving ROI.

The key features within Tivoli Data and Application Security can help you manage data and application security risks while reducing costs and improving ROI. The following sections describe each feature in detail and explain how they can deliver efficiencies and cost savings in the form of security management labor savings, reduced application security development time and costs, reduced compliance management and reporting costs, and avoidance of security risks that could have serious financial consequences. Several examples from actual deployments demonstrate how benefits are being realized from Tivoli Data and Application Security.

Fine-grained data and application entitlements and centralized security policy management

Fine-grained entitlements are security policies that can control access to key resources based on very specific conditions, attributes, or business rules—in any combination. These entitlements are defined by the business but must be carefully managed and enforced as part of the IT environment. Tivoli Data and Application Security enables fine-grained control of application entitlements, providing consistent, granular security to strengthen access control and help protect critical data and processes—from the application level to the operating system level.

Fine-grained entitlements can be used wherever protection is needed—in Web-based applications such as Microsoft® SharePoint, with in-house, portal-based applications, or with commercial applications like SAP. Centralized entitlement policy management helps reduce the costs associated with siloed controls by centralizing administrative tasks, eliminating redundant security systems and leveraging an integrated platform for streamlined administration and enforcement. Centralization also enables administrators to respond more quickly and efficiently to new or more stringent compliance requirements that need to be addressed by changes in entitlement policy.

Efficiencies and cost savings extend to:

- **Security management cost reduction and labor savings** – *reduces workload for IT staff by streamlining and centralizing security management, so that fewer management tasks need to be performed in fewer places. Typically an organization can expect a 15 to 35 percent productivity improvement by centralizing administrative tasks and eliminating redundant security systems.**
- **Business operating efficiency and strategic advantage** – *reduces application security time to market by reducing the number of application security development tasks required. Typically an organization can expect a 15 to 25 percent improvement in operational efficiencies and strategic advantage.**
- **Security risk avoidance** – *eliminates common data access-related security risks resulting from inadequate control over entitlements at the Web application layer, which reduces the potential for costly breaches. Typically an organization can expect a 10 percent reduction in exposure to costly internal security incidents.**

Highlights

A U.S.-based provider of prescription benefits implemented Tivoli Data and Application Security to provide enforcement of fine-grained authorization at the database level and to monitor that access in near real-time. The company fulfills medication claims for numerous insurance companies and, as a consequence, has access to thousands of patient health records. The privacy of the information in these records is protected by federal law, in the form of provisions in the Health Insurance Portability and Accountability Act (HIPAA).

For this reason, the company decided they needed the fine-grained data entitlements and enforcement capabilities provided by Tivoli software to meet its goal of ensuring that access to health-records information would be granted only on a need-to-know basis. The company is also using the solution's HIPAA compliance management module to provide customized reporting on HIPAA compliance to regulators. They are benefiting from a significantly improved data security posture, the ability to centrally manage and enforce data access, and the ability to respond to audit requests more cost-effectively.

User activity monitoring, auditing and reporting

Tivoli Data and Application Security features comprehensive, automated monitoring, auditing and reporting on user activity for databases, applications, servers and mainframes across the enterprise.

Tivoli Data and Application Security features comprehensive, automated monitoring, auditing and reporting on user activity for databases, applications, servers and mainframes across the enterprise. An easy-to-use compliance dashboard summarizes billions of log files in one overview, providing continuous assurance that data and systems are being managed in compliance with company security and access policies. At the same time, the dashboard provides documentary evidence of compliance by capturing native audit log data into easily understood language and using automated log management to store and retrieve logs as needed. Compliance management modules and an advanced report distribution engine allow you to jumpstart your compliance management initiatives. Flexible report distribution makes it easy to send reports where and when they're needed based on your unique requirements.

Efficiencies and cost savings extend to:

- **Security management cost reduction and labor savings –** *reduces daily workload requirements by automating the monitoring and enforcement of acceptable use and change management policies. Typically an organization can expect a 15 to 25 percent productivity improvement in monitoring of user activity.**
- **Compliance management and reporting cost reduction and labor savings –** *automates activities associated with compliance management and audit preparation and reporting. Typically an organization can expect a 25 to 35 percent productivity improvement in log management, compliance management, and reporting.**
- **Security risk avoidance –** *specifically addresses internal threats of data compromise—whether intentional or through an inadvertent, yet damaging, error—by collecting and allowing you to view audit trail logs as evidence of user activity. Typically organizations can expect a 15 percent reduction in insider risk.**

An energy and public utility company is using Tivoli Data and Application Security to enable its IT infrastructure and business processes to support the automated, secure collection of real-time meter data through an advanced metering system (AMS). The AMS replaces traditional electric meters with smart meters that transmit meter data on energy usage to the utility via Web services and that give consumers the ability to monitor and track their consumption via an online portal. As a result, the company eliminates the cost to send personnel out to manually read meters, while customers gain the advantage of being able to know at any given time just how much energy they are using.

Highlights

To help ensure that this information isn't compromised in transmission and is only accessed on a need-to-know basis, the company relies on the capabilities of Tivoli Data and Application Security, along with IBM WebSphere® DataPower® and WebSphere Service Registry and Repository capabilities. The integrated solution enables the company to secure its Web services interface and collect, protect and control access to all the energy usage data and related information that is kept in a common data store. Its automated, centralized log monitoring and reporting capabilities are essential to helping the company cost-effectively address the data privacy compliance requirements that the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation impose on the energy and utility industry.

Federated single sign-on and identity service

Tivoli Data and Application Security provides federated single sign-on, which allows identity data to be shared for authentication purposes.

Collaboration across traditional company boundaries is essential for many organizations today, and federation facilitates collaboration by enabling trusted partners to share applications, software as a service (SaaS), cloud-based services, and information securely. Federated capabilities in Tivoli Data and Application Security include federated single sign-on, which specifically allows sharing of identity data for authentication purposes when people log on to applications, and provides an identity service that simplifies application integration for external collaboration and secure data sharing with trusted partners. The advantage to partners who use federated single sign-on is that they need not expend time and resources recreating user profiles from partner identity stores every time they want to give users access to their applications. The advantage to users is in not having to log in again with a new password every time they move from one application to another within a federated site. Tivoli Data and Application Security federation supports all three standards for sharing identity information (Liberty, SAML and WS-Fed).

Efficiencies and cost savings extend to:

- **Security management cost reduction and labor savings** – *streamlines workloads by providing a common infrastructure for managing user identity information among trusted partners; simplifying user management in federated environments; and consolidating auditing across a number of federation locations to a single point. Typically an organization can expect a 7 to 15 percent productivity improvement in managing user identities and provisioning policies.**
- **Business operating efficiencies and strategic advantages** – *reduces application security time to market by providing discrete federated capabilities rather than duplicating fine-grained authorization in each portal instance. Also allows businesses to safely provide access to entities outside the enterprise, enabling businesses to leverage existing applications in new ways, driving profit and competitive advantage. Organizations typically experience a 15 to 20 percent improvement in operational efficiencies and strategic advantage.**

A payment transaction services company wanted to improve customer service by deploying to a broader array of customers a portal application that offers single sign-on and other conveniences. However, it would be extremely time-consuming and costly to adapt its portal application to include the level of fine-grained authorization needed to protect the abundance of personal data in the financial accounts the company handles. In addition, changing the portal itself in order to allow fine-grained authorization would also mean continually having to further adjust the application implementation whenever a change in federation membership occurred—such as a customer leaving the federation or a new customer needing to be accommodated.

Highlights

By instead using the federated single sign-on and fine-grained authorization capabilities of Tivoli Data and Application Security, the company eliminates the need to alter the portal implementation in any fundamental way. Rather, they merely make edits to the security policy engine to accommodate changes to data-level entitlements. The result is improvement in the company's service to customers, as well as improvements in data security and regulatory compliance.

Application-level and privileged user operating system controls

Many security breaches and audit failures in UNIX and Linux environments are the result of a lack of oversight and control of privileged user accounts, or "root" accounts. Privileged users generally have IT permissions to access highly sensitive data and to make fundamental changes to critical systems and applications. For this reason, they can pose a potentially higher data and application security risk, through actions such as defining new user privileges for themselves, changing other users' capabilities, or modifying audit logs. This is true now more than ever, as the increased use of virtualization can easily extend their access to virtual applications and systems across the enterprise.

Tivoli Data and Application Security provides a policy-based access control system for UNIX and Linux environments that addresses the unique vulnerabilities associated with privileged user access.

Tivoli Data and Application Security protects application and operating system resources by providing a policy-based access control system for UNIX and Linux environments that addresses the unique vulnerabilities associated with privileged user access. The solution audits application and platform activity to defend against inappropriate access by internal users. It also facilitates documentation of compliance with government regulations, corporate policies, and other security mandates.

Efficiencies and cost savings extend to:

- **Security management cost reduction and labor savings** – *simplifies policy management and reduces administration efforts by providing a common infrastructure for defining and enforcing security policy and access rights for UNIX and Linux operating systems. Typically an organization will experience an 7 to 10 percent productivity improvement in policy management, access provisioning, and auditing of privileged user activity.**
- **Security risk avoidance** – *provides tighter enforcement of higher-risk access privileges to reduce exposure to costly internal security incidents, typically by 10 percent.**

A large financial services company needed to meet both their internal access control policies for granular privileged user control and their regulatory compliance and audit requirements. Their production environment consists of over a thousand UNIX servers across multiple data centers and geographies—all requiring granular "root" user access while managing and enforcing privileged user access policies.

The company implemented Tivoli Data and Application Security, which allows them to subdivide UNIX root access and enforce those access controls granularly. It also provides a tamper-resistant audit trail that associates each specific root action with the user who carried out the command. These audit trails provide detailed information for internal audits and for meeting regulatory compliance requirements. The solution provides the same core access policy management and audit capabilities for virtual environments, including IBM AIX® workload partitions (WPARS) and Solaris Zones. It manages these systems via a centralized console that supports hierarchical access control policies across multiple operating systems—and multiple versions of those operating systems.

Highlights

Centralized encryption key management for tape and disk storage

Effective encryption of data at rest—that is, data stored on tape or disk and not in active use—enhances data security and compliance management. It also provides a cost-effective alternative to data disposal, which would be necessary if data could not be satisfactorily secured through encryption and therefore safely stored long term. Protecting against breaches resulting from physical loss of storage media has resulted in the inclusion of encryption into storage hardware and standards for using self-encrypting storage.

Tivoli Data and Application Security provides simple, secure and cost-effective key storage, key serving, and key lifecycle management for IBM self-encrypting storage devices.

Tivoli Data and Application Security helps organizations better manage the encryption key lifecycle by centralizing and strengthening the processes associated with key management. The solution specifically provides simple, secure and cost-effective key storage, key serving, and key lifecycle management for IBM self-encrypting storage devices. Organizations can use these capabilities to centralize and automate the encryption key management process, reduce the number of keys to be managed, and simplify key management through an intuitive user interface for configuration and management. By building the encryption natively into the storage devices, performance concerns, complexity, and the cost of using server CPU cycles for encryption are mitigated. IBM's approach is to introduce encryption and key management so as to be transparent to operating systems, middleware, and applications.

Efficiencies and cost savings extend to:

- **Security management cost reduction and labor savings** – *automates and centralizes key management and eliminates costly data disposal that would otherwise be required for sensitive data. Typically an organization will experience a 10 to 15 percent productivity improvement in this area.**
- **Security risk avoidance** – *eliminates data security risks associated with theft by rendering stored data unreadable—and therefore unusable—without encryption keys. Typically organizations can expect a 15 percent reduction in data security risks.**

A healthcare organization needed to ensure the security of data on the storage media leaving its data center—and needed to do so in a way that would reduce operating expenses, including data destruction costs. In addition, the company needed a solution that would support both mainframe and distributed platforms. The solution was to encrypt the data on the drives and leverage simple, secure encryption key management to render it unusable in the event of a breach. Encryption key management capabilities within Tivoli Data and Application Security enabled the company to secure critical customer information without increasing overall operational costs—and improved its compliance with industry regulations such as HIPAA.

Highlights

With the Tivoli Data and Application Security solution, IBM has integrated a powerful combination of enterprise security capabilities from the Tivoli software portfolio, addressing a wide range of data and application security requirements.

Conclusion

With the Tivoli Data and Application Security solution, IBM has integrated a powerful combination of enterprise security capabilities from the Tivoli software portfolio, addressing a wide range of data and application security requirements. Tivoli Data and Application Security can help organizations reduce operational costs by enabling centralized security management—simplifying and centralizing administrative tasks, eliminating redundant security systems, and leveraging an integrated platform for streamlined administration and enforcement. At the same time, the solution can help organizations manage risk by preventing unauthorized access to or use of sensitive data that could lead to data breaches or compliance violations. But the solution can also help organizations position themselves for competitive advantage, by reducing the time to market of their applications enabling them to respond more quickly to new market opportunities.

Why IBM

For organizations seeking a cost-effective approach to their critical data and application security challenges, IBM security solutions deliver a broad range of benefits. IBM provides complete solutions, helping organizations reduce the costs and risk associated with disparate point solutions. IBM's integrated offerings help streamline management and support, reducing overhead expenses and enabling operational efficiencies. IBM also offers special bundled pricing that allows organizations to expand their security capabilities without the burden of additive cost. With a comprehensive portfolio of solutions to meet security needs across the enterprise, IBM makes it easy to leverage a single-vendor approach to security, helping organizations extend the value of their IT investments.

For more information

IBM can provide a Business Value Assessment for your organization to rapidly assess the business value of implementing Tivoli Data and Application Security. Through this valuable service, IBM can help you determine the strategy you need to enhance the security of your data and applications and realize a rapid return on your investment. To request a Business Value Assessment, or to learn more about Tivoli Data and Application Security, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/network.

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.

*The savings percentages are created in collaboration with IBM Product Managers and Alinean, Inc. and are based upon product and industry knowledge, information from independent analysts, and anecdotal information from customer implementations of Tivoli solutions.

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

Produced in the United States of America
October 2009
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

Recyclable, please recycle